strongSwan - Issue #2275

Why auto=route cannot work with right=%any in tunnel mode

08.03.2017 15:03 - c c

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	configuration		
Affected version:	5.5.0	**Resolution:**	No feedback

Description

It complains "installing trap failed, remote address unknown" with below config when adding policy:
right=%any
type=tunnel
auto=route

If type=transport, adding policy is OK.
What is the rationale for the design?
Thanks.

History

#1 - 08.03.2017 15:10 - Tobias Brunner

- Status changed from New to Feedback

Once a tunnel mode SA is established based on the installed trap policy no further acquires will be triggered by the kernel for other hosts (this is probably mainly because we don't install selectors on IPsec SAs for tunnel mode). Since the main (only?) use case for such wildcard traps are host-host connections transport mode makes way more sense anyway.

I guess you don't really understand what you are doing. Are you?

#2 - 08.03.2017 15:27 - c c

"Once a tunnel mode SA is established based on the installed trap policy no further acquires will be triggered by the kernel for other hosts"
This is not true, after SA is established and if new traffic does not match the existing SA, new SA will be established.

The use case is multi-hosts-net, so want to configure right=%any at net side.
Also there is NAT, so prefer tunnel mode.

#3 - 08.03.2017 15:32 - Tobias Brunner

> "Once a tunnel mode SA is established based on the installed trap policy no further acquires will be triggered by the kernel for other hosts"
> This is not true, after SA is established and if new traffic does not match the existing SA, new SA will be established.

Yes, with transport mode that's how it works. It doesn't with tunnel mode.

> The use case is multi-hosts-net

What does that mean? How do your traffic selectors look like?

#4 - 08.03.2017 15:48 - c c

This is not consistent with what I see.
Please check the config below:

One side A, there is one conn

```
conn rule03
        keyexchange=ikev2
        left=49.102.19.100
        right=44.64.21.100
        leftsubnet=99.99.99.2/32
        rightsubnet=88.88.88.0/24
        authby=secret
        leftid=49.102.19.100
        rightid=%any
        ike=aes128-md5-modp2048!
        esp=3des-md5-noesn!
        type=tunnel
        auto=route
        replay_window=256
        reauth=no
```

One side B, there are three conns

```
conn rule01
        keyexchange=ikev2
        right=49.102.19.100
        left=44.64.21.100
        rightsubnet=99.99.99.2/32
        leftsubnet=88.88.88.1/32
        authby=secret
        leftid=44.64.21.100
        rightid=%any
        ike=aes128-md5-modp2048!
        esp=3des-md5-noesn!
        type=tunnel
        auto=route
        replay_window=256
        reauth=no

conn rule02
        keyexchange=ikev2
        right=49.102.19.100
        left=44.64.21.100
        rightsubnet=99.99.99.2/32
        leftsubnet=88.88.88.2/32
        authby=secret
        leftid=44.64.21.100
        rightid=%any
        ike=aes128-md5-modp2048!
        esp=3des-md5-noesn!
        type=tunnel
        auto=route
        replay_window=256
        reauth=no

conn rule03
        keyexchange=ikev2
        right=49.102.19.100
        left=44.64.21.100
        rightsubnet=99.99.99.2/32
        leftsubnet=88.88.88.0/28
        authby=secret
        leftid=44.64.21.100
        rightid=%any
        ike=aes128-md5-modp2048!
        esp=3des-md5-noesn!
        type=tunnel
        auto=route
        replay_window=256
        reauth=no
```

All the three ping from side B to side A are OK, and 3 SA are established after ping.

```
ping 99.99.99.2 -I 88.88.88.2
ping 99.99.99.2 -I 88.88.88.1
ping 99.99.99.2 -I 88.88.88.3
```

ipsec statusall

```
Status of IKE charon daemon (strongSwan 5.5.0, Linux 4.8.0, x86_64):
  uptime: 10 minutes, since Dec 08 19:01:12 2016
  malloc: sbrk 397312, mmap 0, used 250480, free 146832
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 6
  loaded plugins: charon aes des rc2 sha2 sha1 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7
```

```
 pkcs8 pkcs12 pgp dnskey sshkey pem fips-prf gmp xcbc cmac hmac gcm attr kernel-netlink resolve socket-default
 stroke vici updown eap-radius xauth-generic
Listening IP addresses:
  10.69.97.227
  44.64.11.3
  44.64.21.3
  88.88.88.1
  44.64.21.100
  44.64.21.200
  88.88.88.2
  88.88.88.3
Connections:
rule01:  44.64.21.100...49.102.19.100  IKEv2
rule01:   local:  [44.64.21.100] uses pre-shared key authentication
rule01:   remote: uses pre-shared key authentication
rule01:   child:  88.88.88.1/32 === 99.99.99.2/32 TUNNEL
rule02:   child:  88.88.88.2/32 === 99.99.99.2/32 TUNNEL
rule03:   child:  88.88.88.0/28 === 99.99.99.2/32 TUNNEL
Routed Connections:
rule03{5}:  ROUTED, TUNNEL, reqid 5
rule03{5}:   88.88.88.0/28 === 99.99.99.2/32
rule02{4}:  ROUTED, TUNNEL, reqid 4
rule02{4}:   88.88.88.2/32 === 99.99.99.2/32
rule01{3}:  ROUTED, TUNNEL, reqid 3
rule01{3}:   88.88.88.1/32 === 99.99.99.2/32
Security Associations (3 up, 0 connecting):
rule01[3]: ESTABLISHED 6 minutes ago, 44.64.21.100[44.64.21.100]...49.102.19.100[49.102.19.100]
rule01[3]: IKEv2 SPIs: 6ebfddac0a22f95a_i* 4d4f1207a53f3e9a_r, rekeying in 8 days
rule01[3]: IKE proposal: AES_CBC_128/HMAC_MD5_96/PRF_HMAC_MD5/MODP_2048
rule03{8}:  INSTALLED, TUNNEL, reqid 5, ESP SPIs: c3265baf_i c7fb07d7_o
rule03{8}:  3DES_CBC/HMAC_MD5_96, 504 bytes_i (6 pkts, 400s ago), 504 bytes_o (6 pkts, 400s ago), rekeying in
8 days
rule03{8}:   88.88.88.0/28 === 99.99.99.2/32
rule01[2]: ESTABLISHED 7 minutes ago, 44.64.21.100[44.64.21.100]...49.102.19.100[49.102.19.100]
rule01[2]: IKEv2 SPIs: 8803ca5e8c5a9728_i* 6a4c959e9fc0f8cf_r, rekeying in 8 days
rule01[2]: IKE proposal: AES_CBC_128/HMAC_MD5_96/PRF_HMAC_MD5/MODP_2048
rule01{7}:  INSTALLED, TUNNEL, reqid 3, ESP SPIs: c629d81f_i ce6dbacb_o
rule01{7}:  3DES_CBC/HMAC_MD5_96, 420 bytes_i (5 pkts, 421s ago), 420 bytes_o (5 pkts, 421s ago), rekeying in
8 days
rule01{7}:   88.88.88.1/32 === 99.99.99.2/32
rule01[1]: ESTABLISHED 7 minutes ago, 44.64.21.100[44.64.21.100]...49.102.19.100[49.102.19.100]
rule01[1]: IKEv2 SPIs: 626d5e6a7f7d93ce_i* 946962d9b1cca4b9_r, rekeying in 8 days
rule01[1]: IKE proposal: AES_CBC_128/HMAC_MD5_96/PRF_HMAC_MD5/MODP_2048
rule02{6}:  INSTALLED, TUNNEL, reqid 4, ESP SPIs: c24df0ad_i c56f3eb7_o
rule02{6}:  3DES_CBC/HMAC_MD5_96, 756 bytes_i (9 pkts, 430s ago), 756 bytes_o (9 pkts, 430s ago), rekeying in
8 days
rule02{6}:   88.88.88.2/32 === 99.99.99.2/32
```

#5 - 08.03.2017 15:59 - Tobias Brunner

> This is not consistent with what I see.

What are you talking about? In your scenario the outer tunnel addresses are always the same (49.102.19.100 and 44.64.21.100). And the traffic selectors (*left|rightsubnet*) of different conns obviously match the different packets from 88.88.88.x to 99.99.99.2 without problems (with narrowing of the local TS, 88.88.88.0/24, on host A). But this does not relate to using wildcard traps with *right=%any*, where the inner and outer addresses are the same, at all (*right* can only be determined if that's the case).

#6 - 09.03.2017 12:38 - c c

With the configuration above, I wanted to show that with tunnel mode,
After SA is established and if new traffic does not match the existing SA, new SA will be established.
Which you indicated "with transport mode that's how it works."

Maybe you mean that if new traffic is originated from a new host, SA negotiation won't triggered for tunnel mode.
I think this can be improved, anyway I will firstly verify.

PS, regarding "using wildcard traps with right=%any, where the inner and outer addresses are the same"
Can you help explain why with right=%any, inner and outer must be the same?
Thanks.

#7 - 09.03.2017 15:09 - Tobias Brunner

> With the configuration above, I wanted to show that with tunnel mode,
> After SA is established and if new traffic does not match the existing SA, new SA will be established.
> Which you indicated "with transport mode that's how it works."

Again, that's all expected and describes a completely different scenario than using *right=%any* with trap policies.

> PS, regarding "using wildcard traps with right=%any, where the inner and outer addresses are the same"
> Can you help explain why with right=%any, inner and outer must be the same?

left|right define the outer addresses of a tunnel (i.e. the addresses of the IPsec SAs), *left|rightsubnet* the traffic selectors for the tunneled traffic (i.e. the IPsec policies). If *right* is not specified and trap policies are installed, how would you suggest could the remote address for the tunnel be determined, once a the kernel triggers an acquire, if the remote address of the matched traffic won't equal the outer address of the eventual tunnel? So if the outer addresses of the tunnel are different than the inner this only works if *right* is explicitly set to the outer remote address.

What exactly did you originally want to achieve by setting *right=%any*?

#8 - 20.03.2017 12:45 - c c

This is ipsec.conf file at server side for strongSwan 4.3.6, and it works.
I am trying to do the similar thing(road warrior) in strongswan 5.5.0

And the road warrior has auto=add, so it is not triggered by traffic.
The server side has trapped policies so that no unencrypted traffic comes in.

```
config setup
    charonstart=yes
    plutostart=no
    uniqueids=no
    charondebug="knl 0,enc 0,net 0,cfg 2,chd 2" 

conn %default
    auto=route
    keyexchange=ikev2
    reauth=no

ca ZONEVPN
    cacert="/etc/ipsec/certs/defaultCaCertificate.pem" 

conn ZONEVPN
    rekeymargin=8640
    rekeyfuzz=100%
    left=192.168.77.1
    right=%any
    leftsubnet=0.0.0.0/0
    rightsourceip=%ZONEVPN_201737641572
    authby=rsasig
    leftcert="/etc/ipsec/certs/defaultCertificate.pem" 
    leftid=%fromcert
    rightid=%any
    ike=aes128-sha1-modp1024!
    esp=aes128-sha1!
    type=tunnel
    ikelifetime=86400s
    keylife=86400s
    dpdaction=clear
    dpddelay=120
    mobike=no
    auto=route
    reauth=no
    encapdscp=yes
    vrfid=0
```

#9 - 20.03.2017 12:57 - Tobias Brunner

> The server side has trapped policies so that no unencrypted traffic comes in.

Use drop policies for that or firewall rules. That's not what trap policies are for.

#10 - 18.04.2018 14:26 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Resolution set to No feedback

Closing old issues. If this is still a problem, please reopen.