strongSwan - Issue #3563

Route-based VPN - remote TS 0.0.0.0/0.0.0.0

15.09.2020 12:09 - Jiri Zendulka

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	network / firewall		
Affected version:	5.8.4	**Resolution:**	No change required

Description

There is a mention in documantation about route-based ipsec that it is possible to use 0.0.0.0/0.0.0.0 as local/remote TS. I try use it as remote TS but without success. SA is installed but packets are not routed via ipsecX interface. I guess that it is needed to add a route but I dont know where. If a remote TS is such as 172.16.0.0/16 then it is possible to add route by cmd "ip route add 172.16.0.0/16 dev ipsecX" and everything works. But how to do it if a remote TS is set to 0.0.0.0/0.0.0.0?

```
Daemon Information:

strongSwan swanctl 5.8.4
uptime: 11 seconds, since Sep 15 11:43:41 2020
worker threads: 16 total, 11 idle, working: 4/0/1/0
job queues: 0/0/0/0
jobs scheduled: 3
IKE_SAs: 1 total, 0 half-open
mallinfo: sbrk 532480, mmap 0, used 195576, free 336904
loaded plugins: charon nonce pubkey pem openssl kernel-netlink socket-default forecast farp vici u
pdown xauth-generic dhcp

Connections:

ipsec3: IKEv2, no reauthentication, rekeying every 3060s
  local:  0.0.0.0
  remote: 192.168.7.232
  local pre-shared key authentication:
    id: ipsec3
  remote pre-shared key authentication:
    id: 192.168.7.232
  ipsec3: TUNNEL, rekeying every 3060s
    local:  172.22.169.252/30
    remote: 0.0.0.0/0

Security Associations:

ipsec3: #1, ESTABLISHED, IKEv2, dd47bed01361eaac_i* 0c41c39647b6a4a7_r
  local  'ipsec3' @ 192.168.7.100[4500]
  remote '192.168.7.232' @ 192.168.7.232[4500]
  AES_GCM_16-256/PRF_HMAC_SHA2_256/MODP_1024
  established 9s ago, rekeying in 2543s, reauth in 2303s
  ipsec3: #1, reqid 1, INSTALLED, TUNNEL, ESP:AES_GCM_16-256
    installed 9s ago, rekeying in 2618s, expires in 3591s
    in  ce7bc4b1 (-|0x00000003),      0 bytes,     0 packets
    out c18aee89 (-|0x00000003),      0 bytes,     0 packets
    local  172.22.169.252/30
    remote 0.0.0.0/0
```

Many Thanks.

History

#1 - 15.09.2020 12:16 - Tobias Brunner

- Status changed from New to Feedback

> But how to do it if a remote TS is set to 0.0.0.0/0.0.0.0?

What do you mean?

#2 - 15.09.2020 12:29 - Jiri Zendulka

It cannot be added route 0.0.0.0/0.0.0.0 to ipsecX...

```
# ip route add 0.0.0.0/0.0.0.0 dev ipsec3
RTNETLINK answers: File exists

# ip route show
default via 192.168.7.1 dev eth2
172.22.169.252/30 dev eth0 proto kernel scope link src 172.22.169.253 linkdown
192.168.7.0/24 dev eth2 proto kernel scope link src 192.168.7.100
192.168.7.1 dev eth2 scope link
```

#3 - 15.09.2020 12:31 - Tobias Brunner

> It cannot be added route 0.0.0.0/0.0.0.0 to ipsecX...

Seems you have no idea what you are doing or why.

#4 - 15.09.2020 12:43 - Jiri Zendulka

So it is not possible to use remote TS 0.0.0.0/0.0.0.0 in route-based IPsec? It works in policy-based IPsec. In that mode it is not needed to add any route...so I am wondering how to do it in route-based IPsec.

#5 - 15.09.2020 13:37 - Jiri Zendulka

I added route to the remote side address and then it is possible to change default gw to ipsec3.

```
# ip route
*default dev ipsec3 scope link*
172.22.169.252/30 dev eth0 proto kernel scope link src 172.22.169.253 linkdown
192.168.7.0/24 dev eth2 proto kernel scope link src 192.168.7.100
192.168.7.1 dev eth2 scope link
*192.168.7.232 dev eth2 scope link*
```

#6 - 15.09.2020 13:38 - Tobias Brunner

> So it is not possible to use remote TS 0.0.0.0/0.0.0.0 in route-based IPsec?

Sure it is. But if you use route-base VPNs you have to know how to work with routes or even what your goal is. I really think you are confused.

#7 - 15.09.2020 13:47 - Jiri Zendulka

You can close the issue.

#8 - 15.09.2020 13:48 - Tobias Brunner

- Category set to network / firewall

- Status changed from Feedback to Closed

- Resolution set to No change required