# strongSwan - Feature #2162

## Support for trap policies (auto=route) with virtual IPs

31.10.2016 03:18 - Alex Hill

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Tobias Brunner | **Estimated time:** | 0.00 hour |
| **Category:** | kernel-interface | | |
| **Target version:** | 5.6.3 | | |
| **Resolution:** | Fixed | | |

**Description**

Hi,

I'm opening a ticket on the advice of Noel Kuntze on the mailing list. My client and server ipsec.confs are included at the end of the ticket.

I'm having what seems to be a similar problem as that described in ticket #85, but the IPsec connection is established fine - I just have routing problems.

I'm having trouble using auto=route with virtual IPs. My goal is to assign virtual IPs to many roadwarrior clients, which I want to connect to the VPN as soon as possible and remain connected as reliably as possible. I thought auto=route was the best way to achieve that.

When I use auto=add (or auto=start) I can get an IPsec connection, and traffic flows. After doing so, ip route list table 220 looks like this:

172.16.0.0/16 via 192.168.1.254 dev enxxx proto static src 172.16.0.3

However if I use auto=route (or run ipsec route and then ipsec up) I can't send traffic over the tunnel, and my table 220 looks like this:

172.16.0.0/16 via 192.168.1.254 dev eth0 proto static

So presumably traffic is being sent with the src set to my interface's real IP instead of the virtual one. If I remove the leftsubnet directive from the client config, I get a route with src explicitly set to my interface's real IP. I understand that when the route is initially created, there isn't enough information to create the correct route. But shouldn't the route be replaced by the correct one when the tunnel is established?

Thanks,
Alex

```
# Gateway ipsec.conf

config setup
        uniqueids=never
        charondebug="cfg 4, dmn 4, ike 4, net 4"

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        keyexchange=ikev2

conn my-conn
        left=%any
        leftcert=my-server-cert.pem
        leftid=my-server-fqdn.com
        leftsubnet=172.16.0.0/16
        leftauth=pubkey
        leftfirewall=yes
        right=%any
        rightsourceip=172.16.0.0/16
```

```
        auto=add

# Clients ipsec.conf

config setup

conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev2

conn my-conn
        left=%any
        leftsourceip=%config
        leftcert=my-client-cert.pem
        leftid=my-client-fqdn.com
        leftsubnet=0.0.0.0/0 # Removing this gives a more explicitly incorrect route
    leftfirewall=yes
        right=my-server-fqdn.com
        rightid=my-server-fqdn.com
        rightsubnet=172.16.0.0/16
        auto=add
```

**Related issues:**

| | | |
|---|---|---|
| Related to Bug #85: ip pool + auto=root fails | **Closed** | **11.08.2009** |
| Has duplicate Issue #2259: routed connections not working when virtual IPs ar... | **Closed** | |
| Has duplicate Issue #2541: Virtual IPs are not compatible with start_action=trap | **Closed** | |
| Is duplicate of Issue #248: Interface for ipsec tunnel route does not match i... | **Closed** | |
| Has duplicate Issue #3174: route=auto with roadwarrior? | **Closed** | |

## Associated revisions

**Revision 10b8acb5 - 22.05.2018 10:04 - Tobias Brunner**

kernel-netlink: Change how routes are un-/installed

We now check if there are other routes tracked for the same destination
and replace the installed route instead of just removing it. Same during
installation, where we previously didn't replace existing routes due to
NLM_F_EXCL. Routes with virtual IPs as source address are preferred over
routes without.

This should allow using trap policies with virtual IPs on Linux.

Fixes #85, #2162.

## History

**#1 - 31.10.2016 12:16 - Tobias Brunner**

*- Related to Bug #85: ip pool + auto=root fails added*

**#2 - 02.11.2016 10:10 - Tobias Brunner**

*- Description updated*

*- Category set to kernel-interface*

*- Status changed from New to Feedback*

*auto=route* with virtual IPs is currently not supported. #85 was mistakenly closed by Andreas, it was never resolved.

> But shouldn't the route be replaced by the correct one when the tunnel is established?

See #85-5.

I guess for roadwarrior clients you can also use *auto=start*, *keyingtries=%forever* and *dpdaction=restart* and even *closeaction=restart* since you use *uniqueids=never* on the server.

#### #3 - 02.11.2016 10:36 - Alex Hill

> *auto=route* with virtual IPs is currently not supported. #85 was mistakenly closed by Andreas, it was never resolved.

Ah OK, thanks for clearing that up.

> I guess for roadwarrior clients you can also use *auto=start*, *keyingtries=%forever* and *dpdaction=restart* and even *closeaction=restart* since you use *uniqueids=never* on the server.

That's exactly what I ended up doing, and it seems solid so far. Thanks for your assistance and great work with strongswan.

#### #4 - 28.02.2017 09:17 - Tobias Brunner

*- Has duplicate Issue #2259: routed connections not working when virtual IPs are assigned added*

#### #5 - 28.07.2017 15:05 - Oleksandr Kazymyrov

*- File _updown.patch added*

I have made a patch for my particular case that solve this issue. Perhaps it would be useful for someone.

#### #6 - 13.02.2018 11:04 - Tobias Brunner

*- Has duplicate Issue #2541: Virtual IPs are not compatible with start_action=trap added*

#### #7 - 20.04.2018 13:17 - Tobias Brunner

*- Tracker changed from Issue to Feature*

*- Subject changed from auto=route with virtual IPs to Support for trap policies (auto=route) with virtual IPs*

*- Assignee set to Tobias Brunner*

*- Target version set to 5.6.3*

*- Affected version deleted (5.5.1)*

I've pushed a potential fix for this to the *2162-85-track-routes* branch. Would be great if somebody could test it.

#### #8 - 20.04.2018 13:24 - Tobias Brunner

*- Is duplicate of Issue #248: Interface for ipsec tunnel route does not match interface defined by charon.install_virtual_ip_on added*

#### #9 - 16.05.2018 11:30 - Noel Kuntze

Patch passes a simple test using auto=route and then triggering the connection via sending traffic to it. Didn't test roaming yet.

#### #10 - 22.05.2018 10:05 - Tobias Brunner

> Patch passes a simple test using auto=route and then triggering the connection via sending traffic to it. Didn't test roaming yet.

OK, thanks for testing. I'll merge the change to master for the next release.

#### #11 - 24.05.2018 09:45 - Tobias Brunner

*- Status changed from Feedback to Closed*

*- Resolution set to Fixed*

#### #12 - 13.09.2019 12:10 - Tobias Brunner

*- Has duplicate Issue #3174: route=auto with roadwarrior? added*

### Files

| | | | |
|---|---|---|---|
| _updown.patch | 601 Bytes | 28.07.2017 | Oleksandr Kazymyrov |