strongSwan - Feature #3104

EAP-RADIUS: binding address feature for routers with multiple interfaces connected to LAN.

30.06.2019 00:32 - EasyNet .dev

Status:	Feedback	**Start date:**	30.06.2019
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour
Category:	libcharon		
Target version:			
Resolution:			

Description

Hello,

I'm using the Strongswan software on my Linux boxes for long time. My routers are using FRRouting software suite and of course I have multiple interfaces towards my network. Because of this setup I'm facing a problem: RADIUS packets are going out on the fastest/shortest link as source IP. If that link for some reasons is changed, RADIUS packets are going out with another sources IP. PPP software has also a RADIS-ul plugin and I've did a patch for it to use the bind address configuration directive and I'm using one of the loopback interface IP of my router as source IP. In this way the loopback address is distributed in the network and reachable from anywhere in the network.
With this feature the RADIUS plugin will bind on a specific address and it will send the RADIUS packets only from that source IP regarding the uplink and it will not be necessary to add in RADIUS server all the router interface, which is an ugly workaround.

Kind regards,
Adrian

History

#1 - 01.07.2019 10:56 - Tobias Brunner

- Status changed from New to Feedback

> Because of this setup I'm facing a problem: RADIUS packets are going out on the fastest/shortest link as source IP. If that link for some reasons is changed, RADIUS packets are going out with another sources IP.

Why is that a problem? Fix your routing if you want a different behavior.

Also, couldn't you just NAT RADIUS packets to whatever source IP address you want to use?

> to use the bind address configuration directive and I'm using one of the loopback interface IP of my router as source IP. In this way the loopback address is distributed in the network and reachable from anywhere in the network.

Not sure I fully get what you are saying, but it sounds horrible.

#2 - 01.07.2019 11:43 - EasyNet .dev

Hi Tobias,

> Why is that a problem? Fix your routing if you want a different behavior.

How I suppose to "fix" my routing if everything is dynamic? OSPF, BGP etc?
Each router has more than 3 interfaces connected. In your opinion fixing the routing is to use static routes towards the RADIUS server? Sorry, but I didn't get your idea.

> Also, couldn't you just NAT RADIUS packets to whatever source IP address you want to use?

Don't like using NAT for such setups. NAT is using too much resources.

> > to use the bind address configuration directive and I'm using one of the loopback interface IP of my router as source IP. In this way the loopback address is distributed in the network and reachable from anywhere in the network.

Example:

lo1 is a dummy interface renamed to lo1 with IP 10.190.0.1/32.
Interface eth0 has IP 10.190.0.33/30 towards to another switch which is a L3 switch and is connected to LAN.
Interface eth1 has IP 10.190.0.37/30 to the second switch connected to LAN.
Switches are running VRRP.

Everything is running OSPF.

Let's say that the primary link on eth0 is used. Then all radius packets going out from router are using IP 10.190.0.33, right?

If link on ETH0 is going down, OSPF will use eth1 as main link towards radius. Then all packets are going out with IP 10.190.0.37, not with 10.190.0.33.

With bind address on 10.190.0.1, all packets will go out, regarding the uplink, with same 10.190.0.1.
Because all the routes are redistributed in the network with OSPF, RADIUS server will reply back to 10.190.0.1.

Hope now is much clear. Is just an option if you want to use as default behavior address 0.0.0.0 can be used, otherwise you can specify a strict binding address.

This example is prety, think to much complex routers with much more interfaces.

Kind regards,
Adrian

#3 - 01.07.2019 13:42 - Tobias Brunner

> Let's say that the primary link on eth0 is used. Then all radius packets going out from router are using IP 10.190.0.33, right?
>
> If link on ETH0 is going down, OSPF will use eth1 as main link towards radius. Then all packets are going out with IP 10.190.0.37, not with 10.190.0.33.

So? What's the problem with that?

> With bind address on 10.190.0.1, all packets will go out, regarding the uplink, with same 10.190.0.1.

You can add a static route (even multipath) with whatever source IP you like to be used to reach the RADIUS server if you prefer that (or maybe use the same IP as source for the other two routes - no idea what options your routing daemon provides).

#4 - 01.07.2019 14:48 - EasyNet .dev

Tobias Brunner wrote:

> > Let's say that the primary link on eth0 is used. Then all radius packets going out from router are using IP 10.190.0.33, right?
> >
> > If link on ETH0 is going down, OSPF will use eth1 as main link towards radius. Then all packets are going out with IP 10.190.0.37, not with 10.190.0.33.
>
> So? What's the problem with that?

RADIUS server should be reconfigured each time when you do changes in the network. That means even the restart of the daemon. Each interface of the router should be declared in RADIUS server. That is an ugly configuration and workaround.

> > With bind address on 10.190.0.1, all packets will go out, regarding the uplink, with same 10.190.0.1.
>
> You can add a static route (even multipath) with whatever source IP you like to be used to reach the RADIUS server if you prefer that (or maybe use the same IP as source for the other two routes - no idea what options your routing daemon provides).

Using static routes with Multipath: when if the L1 link is not going down the static routes will remain up, then packets are dropped. Not a solution. Dynamic routing is avoiding this.
BFD for static routes in FRR are not implemented. Using static routes with source is not working in routing daemons. In the OS you ca do it, but as I've mentioned earlier will face a drop packets because one of the links are not good.

I did a suggestion which a lot of daemons are using, is a simple feature which can simplify a lot the RADIUS setup and routers strongswan configuration and minimise the issues.

#5 - 01.07.2019 16:18 - Tobias Brunner

- Category changed from configuration to libcharon

> RADIUS server should be reconfigured each time when you do changes in the network. That means even the restart of the daemon. Each interface of the router should be declared in RADIUS server. That is an ugly configuration and workaround.

What are you talking about? What has this to do with what the source IP address in RADIUS packets is? Why would the RADIUS server care?

> Using static routes with Multipath: when if the L1 link is not going down the static routes will remain up, then packets are dropped. Not a solution.

Hm, OK, seems that feature is intended for load-balancing and not for redundancy.

> BFD for static routes in FRR are not implemented. Using static routes with source is not working in routing daemons. In the OS you ca do it, but as I've mentioned earlier will face a drop packets because one of the links are not good.

According to the documentation it should be possible to set a preferred source IP for the installed routes (see http://docs.frrouting.org/en/latest/zebra.html#clicmd-setsrcADDRESS).

> I did a suggestion which a lot of daemons are using, is a simple feature which can simplify a lot the RADIUS setup and routers strongswan configuration and minimise the issues.

We don't bind to addresses in general as it usually complicates stuff a lot. And I've currently no plans to implement it in the radius plugin/libradius.

#6 - 01.07.2019 19:04 - EasyNet .dev

Tobias Brunner wrote:

> > RADIUS server should be reconfigured each time when you do changes in the network. That means even the restart of the daemon. Each interface of the router should be declared in RADIUS server. That is an ugly configuration and workaround.
>
> What are you talking about? What has this to do with what the source IP address in RADIUS packets is? Why would the RADIUS server care?

You really don't know that RADIUS needs some configuration for the devices (like PPPoE AC, strongswan RADIUS client) to be configured and to permit access to query the database? You don't know that you can create multiple client access (ACs) to different setups of RADIUS based on the sourece IP of the AC?
I'm a bit amazed..

https://linux.die.net/man/5/clients.conf

Is about who has permission to access the RADIUS, as a device AC, not a subscriber.

If the RADIUS is configured to permit the packets only from 10.190.0.33 then when the link has a problem and the OSPF is rerouting the traffic towards 10.190.0.37 link, and you don't set the correct configuration to RADIUS server, the RADIUS will drop the requests.
Multiply this with 5-8 times if you have multiple link and then you have to define in RADIUS all interfaces. If you miss one, then problems occurs.

> > Using static routes with Multipath: when if the L1 link is not going down the static routes will remain up, then packets are dropped. Not a solution.
>
> Hm, OK, seems that feature is intended for load-balancing and not for redundancy.
>
> > BFD for static routes in FRR are not implemented. Using static routes with source is not working in routing daemons. In the OS you ca do it, but as I've mentioned earlier will face a drop packets because one of the links are not good.
>
> According to the documentation it should be possible to set a preferred source IP for the installed routes (see http://docs.frrouting.org/en/latest/zebra.html#clicmd-setsrcADDRESS).

This is not dynamic routing anymore, is just static with multiple paths. In case of link issue you'll get one path as blackhole.

> > I did a suggestion which a lot of daemons are using, is a simple feature which can simplify a lot the RADIUS setup and routers strongswan configuration and minimise the issues.
>
> We don't bind to addresses in general as it usually complicates stuff a lot. And I've currently no plans to implement it in the radius

> plugin/libradius.

OK.

#7 - 01.07.2019 20:14 - Noel Kuntze

I am not sure if you are aware that the remaining solution is the usage of iptables/nftables rules to SNAT the RADIUS packets to the required source IP. Just to make sure this is explicitly mentioned as the remaining workable solution.

#8 - 02.07.2019 09:44 - Tobias Brunner

> If the RADIUS is configured to permit the packets only from 10.190.0.33 then when the link has a problem and the OSPF is rerouting the traffic towards 10.190.0.37 link, and you don't set the correct configuration to RADIUS server, the RADIUS will drop the requests.

Again, that's a problem you create yourself if you have multiple paths to your RADIUS server you obviously have to either make the server expect traffic from all of them or you make the client use a static IP address. If the daemon on the client doesn't support the use of a specific IP address use whatever means the OS provides to do it (NAT, source IP in routes, static routes).

> Multiply this with 5-8 times if you have multiple link and then you have to define in RADIUS all interfaces. If you miss one, then problems occurs.

Automate it.

> This is not dynamic routing anymore, is just static with multiple paths. In case of link issue you'll get one path as blackhole.

Doesn't this just set the preferred source IP to a specific address in the installed routes (at least the option is translated to RTA_PREFSRC). That's what you want, no?

> I am not sure if you are aware that the remaining solution is the usage of iptables/nftables rules to SNAT the RADIUS packets to the required source IP. Just to make sure this is explicitly mentioned as the remaining workable solution.

Thanks Noel, I mentioned that in my very first comment.

#9 - 16.10.2019 10:58 - Karel Hendrych

Another good trick on Linux to source traffic from specific source-address is using iproute2

ip route add [destination-address] via [gw] src [source-address]

if the destination is within interface prefix then:

ip route add [destination-address] dev [eth-dev] src [source-address]

Not sure if dynamic routing software can insert such routes though. For this kind of deployments IMHO binding RADIUS client to loopback is most appropriate.

#10 - 17.06.2021 02:26 - EasyNet .dev

Karel Hendrych wrote:

> Another good trick on Linux to source traffic from specific source-address is using iproute2
>
> ip route add [destination-address] via [gw] src [source-address]
>
> if the destination is within interface prefix then:
>
> ip route add [destination-address] dev [eth-dev] src [source-address]
>
> Not sure if dynamic routing software can insert such routes though. For this kind of deployments IMHO binding RADIUS client to loopback is most appropriate.

Hi Karel,

Thanks. Seems that you understood the situation.
To answer to your comment, unfortunately no. Most of the routing software doesn't allow you to insert such routes. Idea of a routing software is to keep tracking of the destinations.
Your idea is semi-good because you still have static route to the destination because you have to specify the gw or the interface.
I will check the latest version of FRROUTING if I can do some RPB and forcing for a destination to select a source.

At the moment when I created the TT it wasn't possible.

I was very bad surprised by Tobias that came with some hacks doing NAT and other tricks to force the traffic from a specific ip. Noel suggested the same the NAT solution which is ugly hack for a software and router.

Yes, you have right with the loopback address to bind the software to this IP, because, like the BGP, loopback is the most stable interface in the system. If the IP address of the loopback is correctly redistribute in the network, RADIUS knows how to reach this. Exactly like BGP with loopback interfaces redistribute over OSPF.

But I gave it up with the explanation to Tobias because I got the feeling that he is more software developer and not network engineer.

It was just a simple suggestion and an improving for the software.
His answer left me thinking they don't understand that a VPN server can have multiple uplinks with dynamic protocols (yes, for redundancy Tobias!).

To Tobias:
This answer for me is blowing my mind:

> Again, that's a problem you create yourself if you have multiple paths to your RADIUS server you obviously have to either make the server expect traffic from all of them or you make the client use a static IP address.

Sarcastic answer:
Moving the VPN server to a static IP when the router itself is the VPN access point. Right. Let me route everything static with my 3 providers (yes, I'm using 2 routers and 3 ISP with BGP) and VRRP towards Radius.
I will create a BGP protocol to announce me via email when a route is changed and I will do it manual in the router. That's how you left me the impression that you gave me the resolution for this proposal.

More explanations:
In case the direct link towards radius is damaged in R01, VRRP is moved to R02 and R01 is able to access radius via another path. This path can be 1,2 or more paths.
I wish you to do this automatization as you suggested.

More explanations in terms of software development:
PPP daemon, for example, is reading a radius client file and it gets the configuration for radius server from there. Also it has a bindaddr directive which you can specify the source IP address from where to generate the UDP packets for RADIUS client. Simple as that. The communication is done between bindaddr and RADIUS IP and vice-versa which doesn't care the routing paths as long RADIUS servers knows how to reach back to this "bindaddr". No NAT, no static routes, no hacks. Just pure IP routing.
BTW this was an implementation done by me and accepted by PPP team and I'm not a software developer.

And yes Tobias, you can add a "dummy" interface, rename it as lo1 and add a /32 IP. Redistribute in the network and you can access the router over this IP! Is not rocket science!
Binding a software over this IP it will guarantee a stable interface and a fix source IP in case of multiple paths towards a destination, in this case RADIUS server!
SSH is another example to have a FIX ip over a loopback and not looking into the whole list of the IPs of the router to be able to connect to it in case one link is down.

RTA_PREFSRC it could be a solution, but is based in the routing side. For me sounds like patch something at outside which is broken inside. I'm not a software developer, but I couldn't see anything related to IPv4, only for IPv6.

But is useless to talk about this anymore because you already denied an implementation for a such feature.