strongSwan - Issue #2898

VPN Client (including strongSwan client) hangs if upstream router IP changes (behind NAT)

27.01.2019 20:04 - James Dogopoulos

Status:	Closed		
Priority:	Normal		
Assignee:	Tobias Brunner		
Category:	configuration		
Affected version:	5.7.2	**Resolution:**	No change required

Description

Just brain storming here. Currently if I do something on the client end like restart a cable modem (which in turn grabs a new public IP to use for NAT), connected VPN sessions appear to just hang indefinitely(? where is the timeout?) and you need to manually disconnect and reconnect to the VPN. The internal private IP assigned by the router has not changed, just the public IP used for NAT on the router. Could there be a way to somewhat gracefully handle this event?

History

#1 - 28.01.2019 09:07 - Tobias Brunner

- Status changed from New to Feedback

> Just brain storming here.

Not sure if this is the right place for it.

> Could there be a way to somewhat gracefully handle this event?

Yes, MOBIKE (requires DPDs on the client to recognize changed NAT endpoints, or some other event to trigger a MOBIKE update).

#2 - 28.01.2019 09:50 - James Dogopoulos

Well by brain storming what I really mean is, reporting things that could be a bug.

In this case the router is Linux kernel based so this will be common bug for people using VPN clients unless this vendor (Mikrotik) is doing something different that breaks MOBIKE (possible). I can re-create this any time I want, pull the plug on the cable modem and let the router get a new public IP. The strongSwan client and others also hang when a new IP is pushed to clients by the ISP for whatever number of reasons, i've had it hang my clients a few times but obviously most ISPs are stable and don't need to change assigned IPs much. This differs from when you move from a wifi router to a mobile network etc. strongSwan handles that pretty well from what I can tell so far. I'm not sure what is different in these scenarios at this point that causes it to not work. OpenVPN connections die out eventually when this happens and disconnect. It seems like strongSwan is trying to keep things going but for some reason isn't fully rebuilding a workable connection and isn't realizing it. I was thinking maybe this has something to do with sessions being held open in the router that shouldn't be too. I will check for that in case and I will test with another router here soon.

#3 - 28.01.2019 10:09 - Tobias Brunner

> In this case the router is Linux kernel based so this will be common bug for people using VPN clients

It's not at all specific to IKE/IPsec/strongSwan or Linux. It's an inherent "bug" of bidirectional packet-based communication over NATs.

> I can re-create this any time I want, pull the plug on the cable modem and let the router get a new public IP.

So? What exactly did you expect to happen after you did that? Unless the host *behind* the NAT sends some traffic (IKE, i.e. DPD to trigger a MOBIKE update, or ESP, which might trigger a kernel event on the remote peer if it supports it) the host *outside* the NAT will **never** be able to communicate again with that client. It can't learn the new IP address in any way (unless there is some dynamic DNS involved, which gets updated after the IP change, and the host outside can initiate a new connection after e.g. DPD - depends on the authentication method and other config parameters if that's even possible, for common roadwarrior scenarios it's not).

> The strongSwan client and others also hang when a new IP is pushed to clients by the ISP for whatever number of reasons, this isn't a common thing but iv'e had it hang my clients a few times.

Same thing as above. Unless the IP of the actual client changes, there won't be a roam/MOBIKE event (unless you can trigger this manually via an event from the router e.g. UPnP).

> This differs from when you move from a wifi router to a mobile network etc.

Obviously, because then the client's IP/routing changes, which triggers roam/MOBIKE events.

> OpenVPN connections die out eventually when this happens and disconnect.

And how exactly is that different?

> it seems like strongSwan is trying to keep things going but for some reason isn't fully rebuilding a workable connection and not realizing it.

Read the log for what's actually going on.

#4 - 28.01.2019 10:20 - James Dogopoulos

> So? What exactly did you expect to happen after you did that?

That is why I asked if it could be handled more gracefully. You said MOBIKE, which I thought the strongSwan client was using.

> Same thing as above. Unless the IP of the actual client changes, there won't be a roam/MOBIKE event (unless you can trigger this manually via an event from the router e.g. UPnP).

This is a good thought for possible workarounds the end users can implement if that's the only way possible.

> And how exactly is that different?

Well it's different because the client machine knows for a fact the VPN is dead and disconnected where with the strongSwan connections, client machines think it's still a usable connection and continually try to send traffic over it. This is probably best for security reasons though. Rather have traffic try to go out and fail over a hung connection than go out over an insecure connection.

#5 - 28.02.2019 15:59 - Tobias Brunner

> You said MOBIKE, which I thought the strongSwan client was using.

Depends on the configuration (it's enabled by default, though), however, such changes would only be detected if DPD is used too. Otherwise, the client won't be able to learn about the changed NAT mapping and then force a MOBIKE update.

> > And how exactly is that different?
>
> Well it's different because the client machine knows for a fact the VPN is dead and disconnected where with the strongSwan connections, client machines think it's still a usable connection and continually try to send traffic over it.

The connection might not actually be dead. While the server won't be able to reach the client anymore, if the client sends DPDs or ESP packets (which, as mentioned above, might trigger a kernel event on the server if the NAT mapping has changed) the connection might recover automatically.

#6 - 21.05.2019 14:38 - Tobias Brunner

- Category set to configuration

- Status changed from Feedback to Closed

- Assignee set to Tobias Brunner

- Resolution set to No change required