pfSense - Todo #5526

OpenVPN server should default to topology subnet, not net30

11/24/2015 06:03 AM - Kill Bill

Status:	Resolved	**Start date:**	11/24/2015
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	0%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.3		
Plus Target Version:		**Release Notes:**	Default

Description

Why? Because it's recommended by upstream in the first place. https://community.openvpn.net/openvpn/wiki/Topology

Not to mention the endless forum threads with users complaining about thing not working as expected due to the darned net30 thing.

Associated revisions

Revision 154b0f80 - 11/30/2015 03:50 PM - Jim Pingle

Backend changes to OpenVPN CSC handling to allow per-server configuration. Ticket #5526
Still needs GUI work and other items mentioned on https://redmine.pfsense.org/issues/5526

Revision 3044a0c2 - 11/30/2015 03:50 PM - Jim Pingle

GUI changes to OpenVPN CSC handling to allow per-server configuration. Ticket #5526

History

#1 - 11/24/2015 07:11 AM - Jim Pingle

First: I generally agree "topology subnet" is better. Though I don't have a problem with net30, it's mostly because I'm used to it. Lots of people are confused by it, especially when working with overrides for static addresses.

That said: While OpenVPN recommends the use of "topology subnet" for what they call "modern" servers, they still haven't changed their own default out of fear of breaking older clients. I'm not sure how many older clients (< OpenVPN 2.0.9) are still out there, but that was released nearly 10 years ago so hopefully not many.

If we treat it as we usually do, and not change existing things but start doing this for newly created tunnels, it should be OK. Not sure if 2.3 would be the right time to do that, or the next major version.

Biggest concerns will be:

- Documentation updates that would be required to explain the new behavior and how it works, which currently assume net30 and do not explain "topology subnet" as deeply.
- Changes would be needed in overrides since they assume net30 in their logic. Either an option to switch the topology behavior or a way to make overrides specific to one or more servers. This is still a problem currently but if we change the default it will be more widespread.
- The code to obtain IP addresses from RADIUS also assumes net30, and would need a similar option on the server.
- Client testing on various obscure platforms to form recommendations for cases to keep using net30 (such as SNOM/Yealink handsets)

Might be something I missed, it would need some evaluation/investigation.

#2 - 11/24/2015 07:40 AM - Kill Bill

All I'm after here is a oneliner change to make the checkbox ticked when you create a new OpenVPN server, that's all. As in - the defaults should really cover the needs of vast majority of use cases, not obscure things or clients not updated for ~10 years. If someone doesn't like it or has some whacky/obscure/broken/rare/... stuff out there having issues with subnet topology, they can simply untick it again. This backwards "compatibility" default makes more harm than good (as you noted, tons of people are just badly confused by the whole thing.)

Jim P wrote:

> - Documentation updates that would be required to explain the new behavior and how it works, which currently assume net30 and do not explain "topology subnet" as deeply.

I think you'd actually have less need for documentation; unlike the net30 thing, the subnet topology is something most people are familar with :)

> way to make overrides specific to one or more servers.

^^^ This. The current design it something that's just, hmmm... yuck. (Multi)select with configured OVPN servers is something that people would generally have no trouble understanding.

#3 - 11/24/2015 07:57 AM - Jim Pingle

Kill Bill wrote:

> All I'm after here is a oneliner change to make the checkbox ticked when you create a new OpenVPN server, that's all. As in - the defaults should really cover the needs of vast majority of use cases, not obscure things or clients not updated for ~10 years. If someone doesn't like it or has some whacky/obscure/broken/rare/... stuff out there having issues with subnet topology, they can simply untick it again. This backwards "compatibility" default makes more harm than good (as you noted, tons of people are just badly confused by the whole thing.)

While the code to make the change is a one-liner, the implications are a bit more complex.

> Jim P wrote:
>
> > - Documentation updates that would be required to explain the new behavior and how it works, which currently assume net30 and do not explain "topology subnet" as deeply.
>
> I think you'd actually have less need for documentation; unlike the net30 thing, the subnet topology is something most people are familar with :)

We still need to document net30 since it's still an option, but we'd have to update everything that assumes net30 as the default (wiki, book, export package, GUI text, anything else we can find)

way to make overrides specific to one or more servers.

^^^ This. The current design it something that's just, hmmm... yuck. (Multi)select with configured OVPN servers is something that people would generally have no trouble understanding.

The current method is definitely not ideal, it's amazing it hasn't bitten us sooner. I'd almost prefer the overrides be a sub-function of each server rather than a separate tab with its own server choice. But either way it gets changed will require some non-trivial code.

#4 - 11/25/2015 12:59 PM - Jim Pingle

- Assignee set to Jim Pingle

To me for analysis

#5 - 11/30/2015 12:30 PM - Jim Pingle

Seems doable with some minor effort though it will take several steps to accommodate properly:

- OpenVPN Server Configuration GUI/Backend Code:
  - Topology needs changed to a drop-down. Choose from: "subnet, net30" (default: subnet)
    - Move under the Tunnel Network option
    - In the config, comes through as "topology blah"
  - Fix description text
    - Will automatically push to clients
- Upgrade code to change option format from old checkbox to new drop-down. Unset net30, set subnet
- Client-Specific Overrides GUI/Backend code:
  - Behavior of static IP address allocation via overrides needs to be addressed
    - Best choice:
      - Stop using the same overrides for all. Make override set for each server.
      - Allow server selection on override via multi-select
      - When writing out a server's overrides, check topology setting on server, adjust ifconfig accordingly
  - Means to accommodate existing behavior on upgrade in overrides
    - Grows naturally from the above -- no servers selected == applies to all servers
- RADIUS IP address allocation:
  - The code to obtain IP addresses from RADIUS already accounts for this, when the Framed-Mask reply attribute is sent back it uses "topology subnet" already.
- OpenVPN Wizard
  - Add topology drop-down to wizard during the config step (see above for placement)
- Book:
  - openvpn-configuration-options.rst ("IPv4/IPv6 Tunnel Network" and "Topology Subnet")
  - site-to-site-example-configuration-ssl-tls.rst (One mention of /30)
  - troubleshooting-openvpn.rst (several places)
- Wiki:
  - Fixed: https://doc.pfsense.org/index.php/Why_can't_I_ping_some_OpenVPN_adapter_addresses
  - Fixed: https://doc.pfsense.org/index.php/OpenVPN_Site-to-Site_PKI_%28SSL%29
  - https://doc.pfsense.org/index.php/OpenVPN_Remote_Access_Server (Follows the wizard -- wizard needs fixed first)
- Export package: -- No changes needed, seems to be OK

It could be done without the change to a drop-down but IMO it's better that way -- it avoids the ambiguity of the option being present/not present in config.xml. I had originally put the "p2p" choice in the topology drop-down but it should probably be omitted for now. Seems like a decent time to add it but may add too much complexity.

#6 - 12/01/2015 09:41 AM - Jim Pingle

- Status changed from New to Feedback

Code and doc changes are all complete. I tested it several ways here and it works fine in my setup, but it could always use more testing and feedback. I'll post a message on the forum also.

#7 - 12/28/2015 05:02 PM - Chris Buechler

- Status changed from Feedback to Resolved

this is complete, works, and issues introduced look to all be fixed.

#8 - 03/31/2016 05:03 PM - Chris Buechler

- Tracker changed from Bug to Todo