pfSense - Bug #5764

OpenVPN 'topology subnet' change breaks many upgraded client configs

01/12/2016 06:26 PM - Landon Timothy

Status:	Resolved	**Start date:**	01/12/2016
Priority:	Normal	**Due date:**	
Assignee:	Chris Buechler	**% Done:**	0%
Category:	OpenVPN	**Estimated time:**	0.00 hour
Target version:	2.3		
Affected Version:	2.3	**Affected Architecture:**	

Description

Using OpenVPN client mode, it throw errors when adding routes.
This worked in 2.3 snapshots until sometime last week.
Same config works in 2.2.6

The log shows:
Jan 13 00:26:20 openvpn 8674 OpenVPN ROUTE: OpenVPN needs a gateway parameter for a --route option and no default was specified by either --route-gateway or --ifconfig options
Jan 13 00:26:20 openvpn 8674 OpenVPN ROUTE: failed to parse/resolve route for host/network: 192.168.1.0
Jan 13 00:26:20 openvpn 8674 OpenVPN ROUTE: OpenVPN needs a gateway parameter for a --route option and no default was specified by either --route-gateway or --ifconfig options
Jan 13 00:26:20 openvpn 8674 ROUTE_GATEWAY 192.168.0.1
Jan 13 00:26:20 openvpn 8674 OPTIONS IMPORT: route options modified
Jan 13 00:26:20 openvpn 8674 PUSH: Received control message: 'PUSH_REPLY,route 192.168.1.0 255.255.255.0,route 10.1.151.0 255.255.255.0,route 10.9.0.0 255.255.255.0'

Associated revisions

Revision c4db25a5 - 01/28/2016 10:52 PM - Chris Buechler

Add topology selection to OpenVPN client page. Ticket #5764

Revision 1c1ca39b - 01/29/2016 12:04 AM - Chris Buechler

retain OpenVPN's net30 default topology for upgraded configs so they still work. Ticket #5764

Revision 68e82ecb - 01/29/2016 05:59 PM - Chris Buechler

OpenVPN server config upgrade already handled in 129_to_130. Ticket #5764

History

#1 - 01/12/2016 07:35 PM - Chris Buechler

- Category set to OpenVPN

- Status changed from New to Feedback

- Target version set to 2.3

Is that using tun or tap?

The OpenVPN config generation source hasn't changed at all in a month, and some time longer than that for anything that'd be relevant here. Did something in the GUI maybe muck up the config? Check Diag>Backup/restore, Config History tab.

#2 - 01/12/2016 08:35 PM - Landon Timothy

Sorry, it's tun.

I don't see anything in the diffs but I've played with most of the gui options to see if anything would start working.

This is basically just a vpn client so I restored the 2.3 config to a new 2.2.6 install and the routes work.

Here's the openvpn config section:

```
    <openvpn>
        <openvpn-client>
            <auth_user></auth_user>
            <auth_pass></auth_pass>
            <vpnid>2</vpnid>
            <protocol>UDP</protocol>
            <dev_mode>tun</dev_mode>
            <ipaddr></ipaddr>
            <interface>wan</interface>
            <local_port/>
            <server_addr>server</server_addr>
            <server_port>1195</server_port>
            <resolve_retry></resolve_retry>
            <proxy_addr/>
            <proxy_port></proxy_port>
            <proxy_authtype>none</proxy_authtype>
            <proxy_user/>
            <proxy_passwd/>
            <description/>
            <mode>p2p_tls</mode>
            <custom_options/>
            <caref>549c71ff5bafd</caref>
            <certref>56737445d74df</certref>
            <tls>adsfasdf</tls>
            <crypto>AES-128-CBC</crypto>
            <digest>SHA256</digest>
            <engine>none</engine>
            <tunnel_network>10.8.0.0/30</tunnel_network>
            <tunnel_networkv6/>
            <remote_network>192.168.1.0/24,192.168.2.0/24,10.1.151.0/24</remote_network>
            <remote_networkv6/>
            <use_shaper/>
            <compression/>
            <passtos></passtos>
            <no_tun_ipv6>yes</no_tun_ipv6>
            <route_no_pull></route_no_pull>
            <route_no_exec></route_no_exec>
            <verbosity_level>6</verbosity_level>
        </openvpn-client>
    </openvpn>
```

#3 - 01/13/2016 06:42 AM - Jim Thompson

- Assignee set to Chris Buechler

assigned for eval

#4 - 01/22/2016 11:39 PM - Chris Buechler

There was an issue with SSL/TLS with /30 tunnel networks fixed earlier this week. I suspect this was fixed at that point.

Landon: you still seeing this on the most recent 2.3?

#5 - 01/23/2016 01:16 PM - Landon Timothy

I do still see the same behavior.
On the client side, after updating, I reset to factory defaults and restored the working 2.2.6 config.

Both sides now running:
2.3-BETA (amd64)
built on Sat Jan 23 11:51:09 CST 2016

Changing between TLS and Shared Key in the client settings, the Shared Key field stays when TLS is selected.

Routes are added correctly if I use Shared Key with no other changes.
Using TLS with or without TLS auth, the routes still fail to add.

#6 - 01/28/2016 04:13 AM - Renato Botelho

- Status changed from Feedback to Assigned

Not fixed yet

#7 - 01/28/2016 10:41 PM - Chris Buechler

- Subject changed from OpenVPN client mode no longer adds routes to OpenVPN 'topology subnet' change breaks many upgraded configs

topology subnet requires specifying the gateway, so "OpenVPN needs a gateway parameter" is the expected result for many existing configs. The OpenVPN client page needs a configurable option for topology, and config upgrade code so existing configurations retain their prior net30, otherwise a lot of them are going to break post-upgrade.

#8 - 01/29/2016 02:06 AM - Chris Buechler

- Status changed from Assigned to Feedback

I think that should take care of all the problem scenarios.

Landon: your situation should definitely be good now. Post-upgrade (in a few hours once those changes hit a snapshot), it should work. If you edit your OpenVPN client you'll see the Topology option which should be set to net30, which retain's 2.2.6's behavior.

#9 - 01/29/2016 07:20 AM - Jim Pingle

The server topology was already being preserved as net30 back in upgrade_129_to_130(), so upgrade_140_to_141() should probably only adjust clients.

Also the client case for the option should probably have an additional choice to omit the directive since it can be pushed from the server in cases when it can be used (SSL/TLS, subnet size larger than /30)

#10 - 01/29/2016 09:22 AM - Landon Timothy

Thanks Chris.
Routes get created in TLS mode now.
There is still a cosmetic issue with the shared key field showing when switching from shared key to TLS mode.

#11 - 01/29/2016 08:57 PM - Chris Buechler

- Subject changed from OpenVPN 'topology subnet' change breaks many upgraded configs to OpenVPN 'topology subnet' change breaks many upgraded client configs

Thanks JimP, changed 141 to only do the clients, I missed that in 129-130.

It probably should have a "default" or similar option to just omit topology. Though if the server pushes a topology, it overrides anything defined on the client, so it's not strictly necessary.

Landon: thanks for the feedback. Not seeing anywhere where the shared key field stays where it shouldn't. Please start a new ticket with specifics and screenshots.

#12 - 02/04/2016 09:26 PM - Chris Buechler

- Status changed from Feedback to Resolved

all the issues here are fixed. If the client's configured with a topology and the server pushes one, it prefers the pushed topology, so an option to accommodate that circumstance isn't necessary.