

pfSense - Bug #11051

Unbound: custom TLS listen port ignored

11/10/2020 09:31 AM - Brad Edmondson

Status:	Resolved	Start date:	11/10/2020
Priority:	Low	Due date:	
Assignee:	Viktor Gurov	% Done:	0%
Category:	DNS Resolver	Estimated time:	0.00 hour
Target version:	2.5.0	Affected Version:	2.4.5-p1
Plus Target Version:		Affected Architecture:	
Release Notes:	Default		

Description

Using latest stable pfSense: 2.4.5-RELEASE-p1 (amd64)

Attempting to configure two-tier DNS cache, using either BIND or DNS Forwarder (dnsmasq) for first-level cache and for local DHCP names (due to [#5413](#)), and using DNS Resolver (unbound) at the second level to take advantage of DNSBL. I set BIND/dnsmasq to port 53 and 853 for TLS (BIND only), and intend to run DNS Forwarder (Unbound) on loopback address ports 5053 and 5853, respectively. Although I can set both of these in the Unbound GUI (services_unbound.php), the second setting, for TLS port, is not applied to the config file, so when the Unbound service restarts it listens on 5053 for unencrypted and 853 for encrypted. I've tried a few different port numbers for both, and the unencrypted port configuration is always applied while the encrypted port is never applied (always stays 853).

I think this is a problem with the GUI/pfSense, because when I ssh in and review the unbound config file at /var/unbound/unbound.conf, I can see the port: setting get updated while the tls-port: setting remains 853. I even manually set tls-port: 5853 in unbound.conf and it was changed back to 853 the next time I saved changes in the GUI.

Associated revisions

Revision 298df54d - 11/12/2020 07:17 AM - Viktor Gurov

Unbound custom TLS port fix. Issue #11051

History

#1 - 11/10/2020 09:33 AM - Brad Edmondson

More context: running on bare metal Celeron 3160 with 8gb RAM. Landing page reports:

```
2.4.5-RELEASE-p1 (amd64)
built on Tue Jun 02 17:51:17 EDT 2020
FreeBSD 11.3-STABLE
```

#2 - 11/11/2020 10:34 AM - Viktor Gurov

Fix:
https://gitlab.netgate.com/pfSense/pfSense/-/merge_requests/42

#3 - 11/11/2020 12:03 PM - Jim Pingle

- Status changed from New to Pull Request Review
- Target version set to 2.5.0

#4 - 11/12/2020 07:17 AM - Renato Botelho

- Status changed from *Pull Request Review* to *Feedback*
- Assignee set to *Viktor Gurov*

PR has been merged. Thanks!

#5 - 11/14/2020 04:56 AM - Danilo Zrenjanin

- Status changed from *Feedback* to *Resolved*

Tested on:

```
2.5.0-DEVELOPMENT (amd64)
built on Fri Nov 13 19:02:04 EST 2020
FreeBSD 12.2-STABLE
```

The GUI applies the changes successfully to the unbound.conf file.

```
# TLS Configuration
tls-cert-bundle: "/etc/ssl/cert.pem"
tls-port: 8853
```

Ticket resolved.