pfSense - Feature #16234

Feature Request: Support for tls-cert-bundle in pfSense WebGUI

06/05/2025 08:03 PM - Robert S

Status:	Not a Bug	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	DNS Resolver	**Estimated time:**	0.00 hour
Target version:			
Plus Target Version:		**Release Notes:**	Default

Description

Dear pfSense Support Team,

I am a pfSense user and have successfully configured DNS over TLS (DoT) using Unbound with forwarding mode. However, I encountered an issue when attempting to enable TLS certificate validation by adding the following line to the "Custom options" in the DNS Resolver settings:
tls-cert-bundle: "/etc/unbound/cert.pem"

This configuration results in a syntax error:
The generated config file cannot be parsed by unbound. Please correct the following errors:
/var/unbound/test/unbound.conf:116: error: syntax error

Upon investigation, I understand that tls-cert-bundle is a global Unbound option and cannot be set within the forward-zone context, which is where the "Custom options" are applied in the pfSense WebGUI.

I would like to request the addition of support for setting global Unbound options, such as tls-cert-bundle, through the pfSense WebGUI. This feature would enhance security by allowing users to enable TLS certificate validation for DoT, ensuring that DNS queries are not only encrypted but also authenticated.

Implementing this feature would be beneficial for users seeking to maximize the security of their DNS configurations without resorting to manual configuration file edits, which can be overwritten by system updates.
Thank you for considering this feature request. I appreciate your continued efforts in developing and maintaining pfSense.
Best regards,
Robert

History

#1 - 06/05/2025 08:15 PM - Jim Pingle

- Status changed from New to Not a Bug

You likely need to add server: to the start of your custom options, as is mentioned in the documentation:

https://docs.netgate.com/pfsense/en/latest/services/dns/resolver-config.html