

pfSense - Feature #8236

Ability to configure "forward-first" and "forward-host" options for more robust domain overrides in DNS Resolver

12/25/2017 11:43 PM - Alfred Barnat

Status:	New	Start date:	12/25/2017
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:	DNS Resolver	Estimated time:	0.00 hour
Target version:			
Description			
<p>It would be great to have the option to configure both forward-first (a simple checkbox) and forward-host (perhaps an extension of the "IP Address" field currently provided) directives for domain overrides, as the current option to configure only an explicit IP address via forward-addr is limiting and can lead to fragile configurations.</p> <p>My specific use case is a split DNS configuration where the internal DNS server lies on the other side of a site-to-site VPN tunnel. If the tunnel goes down, without a "forward-first yes" on the zone, all DNS resolution under my hostname will fail rather than simply falling back to the publicly routable IPs everyone outside my network sees. This also makes handling of the VPN server's FQDN itself difficult, as I must either define it explicitly as a host override or place it under a different domain which is not forwarded. Again, the forward-first directive should handle this automatically.</p> <p>It would also be very useful to have the option to specify a FQDN for a domain override. There are any number of reasons a privately operated DNS server might need to change IPs, but ensuring the server is resolvable via public DNS record would mitigate this.</p>			

History

#1 - 12/26/2017 01:26 AM - Alfred Barnat

Possibly scratch the request for "forward-first" unless the implementer is very familiar with its behavior. In testing with custom configuration files, I wasn't able to figure out how to have it reliably forward requests in a timely manner.

Still, adding support for "forward-host" instead of "forward-addr" by specifying a FQDN for the target DNS server instead of an IP address would be very useful.