

## pfSense - Bug #10493

### filter\_get\_vpns\_list() issues

04/23/2020 08:47 AM - Viktor Gurov

<b>Status:</b>	New	<b>Start date:</b>	04/23/2020
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>		<b>% Done:</b>	0%
<b>Category:</b>	IPsec	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>		<b>Affected Architecture:</b>	
<b>Affected Version:</b>	2.4.5		

#### Description

1) filter\_get\_vpns\_list() returns only:  
IPsec Mobile IPv4 subnet  
IPsec site-to-site networks  
OpenVPN client/server Tunnel Network / Remote Network IPv4  
PPPoE server networks

but not:  
IPsec Mobile IPv6 subnet  
OpenVPN client/server Tunnel Network / Remote Network IPv6  
L2TP VPN network

This is why the Snort/Suricata *vpnaddresses* option doesn't return a complete list of VPN networks  
see <https://redmine.pfsense.org/issues/8688>

2) Because of filter\_get\_vpns\_list() returns not only IPsec networks, IPsec MSS clamping option will affect unnecessary VPN types.

#### History

##### #1 - 04/23/2020 09:02 AM - Jim Pingle

2) Because of filter\_get\_vpns\_list() returns not only IPsec networks, IPsec MSS clamping option will affect unnecessary VPN types.

There are some people who rely on that behavior, so if it is altered, a means must be added to cover the other cases separately or to preserve the current behavior.

It is probably better to have a different setting for each type of VPN since they may have a different desired MSS value due to differences in overhead for each protocol. If we go that route, however, there should be a master setting to cover all VPNs with the current value.

##### #2 - 05/02/2020 07:58 AM - Viktor Gurov

This fix allows you to select for which VPN types / IP proto do MSS clamping:  
<https://github.com/pfsense/pfsense/pull/4299>

it also allow to resolve <https://redmine.pfsense.org/issues/8013>

**#3 - 05/02/2020 11:29 AM - Viktor Gurov**

+ I think it would be better to split "Advanced Firewall" to "Advanced Firewall" and "Packet Processing" sections:

**Advanced Firewall:**

- Disable Firewall
- Static route filtering
- Disable Auto-added VPN rules
- Disable reply-to
- Disable Negate rules
- Allow APIPA
- Aliases Hostnames Resolve Interval
- Check certificate of aliases URLs

**Packet Processing:**

- IP Do-Not-Fragment compatibility
- IP Random id generation
- Firewall Optimization Options
- VPN MSS Clamping
- Disable Firewall Scrub
- Firewall Adaptive Timeouts
- Firewall Maximum States
- Firewall Maximum Table Entries
- Firewall Maximum Fragment Entries

**#4 - 05/06/2020 01:07 AM - Viktor Gurov**

it can also reduce the scope of [#7815](#)