pfSense Plus - Bug #16219

pfSense IPsec VTI Mode Incompatible with Juniper Traffic Selector Requirements

05/30/2025 06:25 PM - Henry Zhou

Status:	Incomplete	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:			
Release Notes:	Default	**Affected Architecture:**	All
Affected Plus Version:	24.11		

Description

When configuring an IPsec VPN in VTI (route-based) mode between pfSense (using strongSwan) and Juniper firewalls (e.g., SRX), the tunnel negotiation fails or traffic does not flow due to incompatible traffic selector requirements.

Expected Behavior:
pfSense should successfully negotiate IPsec VTI tunnels with devices that require specific (narrow) traffic selectors, such as Juniper firewalls, ideally allowing for interoperability and full tunnel functionality.

Actual Behavior:

```
pfSense (strongSwan) attempts to negotiate the tunnel using the traffic selector 0.0.0.0/0<->0.0.0.0/0 as required for VTI mode.

Juniper firewalls require specific subnets for traffic selectors and do not accept the universal 0.0.0.0/0 value, resulting in a negotiation failure or a tunnel where no traffic flows.

Error logs indicate mismatched traffic selectors or negotiation failure.
```

Steps to Reproduce:

```
Configure IPsec VTI (route-based VPN) on pfSense with a Juniper firewall peer.

Set Phase 2 on pfSense to use 0.0.0.0/0 (the only available option for VTI mode).

Attempt to configure matching traffic selectors on Juniper (which requires specific subnets).

Attempt to establish the tunnel.
```

History

#1 - 06/01/2025 01:43 AM - Kris Phillips

- Status changed from New to Incomplete

If you're using traffic selectors, you want Policy-mode in pfSense Plus. VTIs don't use traffic selectors, so I'm confused how this is a bug, exactly.

Please advise.

Marking as Incomplete temporarily.

#2 - 06/01/2025 05:31 AM - Henry Zhou

Thanks for taking care of the ticket.

Let me clarify. I don't intend to use traffic selector under VTI mode.

The issue is the VTI mode of pfsense by default sends 0.0.0.0/0 as traffic selector to the other side. While Juniper doesn't allow that, the IKE phase1 connection would not be established.
There's no way for me to override that in pfsense.