

## pfSense - Feature #3329

### Allow creating "not" rules for IPsec Phase 2

11/19/2013 09:51 AM - Jim Pingle

<b>Status:</b>	Resolved	<b>Start date:</b>	11/19/2013
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Renato Botelho	<b>% Done:</b>	100%
<b>Category:</b>	IPsec	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	2.5.0		
<b>Release Notes:</b>	Default		

#### Description

We should have the ability in Phase 2 to negate the action ("none" in the SPD) so that specific traffic can be made to not enter an IPsec tunnel.

Somewhat related to [#3328](#) (reordering P2 entries) so these exceptions can be moved above the other entries as needed.

These entries would not need to have any encryption options chosen, only the networks defined.

#### Associated revisions

##### Revision 14b52494 - 03/18/2020 09:29 AM - Viktor Gurov

IPsec PH2 bypass mode. Issue #3329

#### History

##### #1 - 07/22/2014 05:55 AM - Jim Thompson

- Assignee set to Renato Botelho

##### #2 - 09/09/2014 04:45 PM - Ermal Luçi

Now these should be called specific policies.

Since phase2 is totally managed by the ipsec daemon there can be what is called shunt policies. I am not sure where to put these on the GUI at this moment though!

##### #3 - 10/20/2014 07:56 PM - Chris Buechler

- Target version deleted (2.2)

not important for 2.2

##### #4 - 07/28/2017 02:16 PM - Markus Stockhausen

This feature will be really helpful. Lets assume a office firewall connected to a HQ firewall. It serves sub multiple small subnets via different interfaces. Lets assume these are 10.11.12.0/24 (LAN) and 10.20.30.0/24 (OPT1). To build a working routing one would need tens of SAs and build them around the subnets.

A simple implementation could be a single checkbox for each SA. If it is set the local SA part will create a shunt entry in ipsec.conf

##### #5 - 07/28/2017 02:20 PM - Markus Stockhausen

- File shunt.png added

Example implementation

**#6 - 08/08/2018 06:38 AM - NCATS LAB**

Strongly Request feature.

We just lost a lot of time because this isn't implemented on SG-4860s.

On our REMOTE SG-4860, we has set up bridging for OPT1-OPT4 and couldn't figure out why everything worked to the GATEWAY except testing the DEF GW with PING.

System should be flexible enough to allow IPSEC tunnels on any interface without some background rule that only makes exceptions on LAN.

Thank-you

**#7 - 03/12/2020 07:02 AM - Viktor Gurov**

<https://github.com/pfsense/pfsense/pull/4230>

**#8 - 03/12/2020 09:58 AM - Jim Pingle**

- Status changed from New to Pull Request Review

**#9 - 08/27/2020 08:41 AM - Renato Botelho**

- Status changed from Pull Request Review to Feedback

- Target version set to 2.5.0

- % Done changed from 0 to 100

PR has been merged. Thanks!

**#10 - 10/06/2020 12:16 PM - Steve Beaver**

- Status changed from Feedback to Resolved

**Files**

---

shunt.png	21.9 KB	07/28/2017	Markus Stockhausen
-----------	---------	------------	--------------------