pfSense - Feature #3329

Allow creating "not" rules for IPsec Phase 2

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

Status:	New	**Start date:**	11/19/2013
Priority:	Normal	**Due date:**	
Assignee:	Renato Botelho	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:			

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.

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 specifc 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 wil be really helpful. Lets assume a office firewall connected to a HQ firewall. It serves sub multiple small subnets via different interfaces. Lets assumes 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

Files

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