pfSense - Bug #4129

IPsec connections with multiple P2s use only first SA

12/19/2014 12:41 AM - Chris Buechler

Status:	Resolved	**Start date:**	12/19/2014
Priority:	Very High	**Due date:**	
Assignee:	Ermal Luçi	**% Done:**	0%
Category:	IPsec	**Estimated time:**	0.00 hour
Target version:	2.2		
Affected Version:	2.2	**Affected Architecture:**	

Description

Where you have multiple P2s on a P1, only the first is actually used. The SPD and SAD are correct in setkey's output, but all outbound traffic on a given P1 ends up on the first SA. This breaks all the P2s other than the first. Can confirm via byte counters on SAs, and when testing with certain devices you'll get logs such as "the peer is sending other traffic through this security association" (from an ASA).

History

#1 - 12/19/2014 12:50 AM - Chris Buechler

probably the best next step, after discussion with Jim T earlier, is to try ipsec-tools on 2.2 and see if the issue persists. A test setup is in place, but not entirely functional. Setup is on 172.27.44.26. racoon.conf, psk.txt, and spd.conf in /root/ there. racoon is via 'pkg install'. It seems to work fine when the other end initiates, but no traffic ever traverses the connection. I didn't change setkey, and I'm guessing that's where the issue is. I'm running short on time for today though. Ermal, please pick up on that. Unless you already know where the issue is and that won't help, then don't bother.

My suspicion is this seems like it's not a problem with strongswan at all, and this would help determine whether that's the case.

#2 - 12/19/2014 05:52 PM - Pi Ba

To add a little info/reference here from report: #4112, with StrongSwan i was able to make it work in my situation by putting separate 'conn' sections in the config one for each P2. So it might not be required to add ipsec-tools to 2.2. If you guys think thats the better option that is ok for me. However it might be 'better' to use 1 piece of software if it supports everything required, and is only a 'configuration issue' which can be easily solved by writing a different config.

#3 - 12/20/2014 05:16 PM - Pi Ba

- File StrongSwan ipsec logs2.txt added

I've been checking this a bit more, and did see that with the current way it does work properly for a tunnel that uses 'Cisco Unity'.. For the other P1 is only negotiated once, but does require multiple conn sections. Some 'anonymized' logging attached, with and without separate conn sections, with and without CISCO UNITY from the remote device.

#4 - 12/20/2014 05:53 PM - Pi Ba

In my test above i created complete separate conn sections in the config file, it seems possible to not repeat all info by using 'also' like described here: [https://lists.strongswan.org/pipermail/users/2012-March/002746.html].

#5 - 12/22/2014 10:52 AM - Ermal Luçi

- Status changed from Confirmed to Feedback

Changes have been committed to generate single connections for each phase2 and confirmed by https://forum.pfsense.org/index.php?topic=85429.0

#6 - 12/25/2014 04:34 PM - Pi Ba

Tested, works ok for my tunnels. Thanks.

#7 - 12/30/2014 07:04 PM - Chris Buechler

- Status changed from Feedback to Resolved

this works. the only issue introduced by this that I've found is the status widget issue in #4164

Files

StrongSwan ipsec logs2.txt	19.9 KB	12/20/2014	Pi Ba