

Re: Duplicate SAD entries lead to ESP tunnel malfunction

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2006-01/msg00205.html>

- *From:* Oleg Tarasov <subscriber@xxxxxxxxxx>
 - *Date:* Fri, 27 Jan 2006 11:36:46 +0200
-

Hello,

VANHULLEBUS Yvan <vanhu_bsd@xxxxxxxxxx> wrote:

> net.key.prefered_oldsa, or net.key.preferred_oldsa (changed since
> 4.X).

> It is 1 by default, and it should be set to 0 to help better
> interoperability with lots of peers.....

This seems quite like correct solution. I analyzed behavior of the interface and saw upcoming ping requests (obviously) AND outgoing ping echoes, but remote host didn't get them. Obviously incoming packets were decrypted using one of SAs (the new one) but outgoing packets were encrypted using old SA which is not present on remote host due to some problems (like forced reboot, connection problems etc).

Normally in this case remote host must report of unknown spi, but rather it lacks this function or it just ignores these packets. As it is a hardware router I am unaware of its behavior.

I will test this solution for some time but I am sure this will help.

Thanx for really great help – all these troubles are on my production box and every minute of malfunction returns to me with #not good# words of my boss :/

Best regards,

Oleg Tarasov <mailto:subscriber@xxxxxxxxxx>

freebsd-net@xxxxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-net>

To unsubscribe, send any mail to "freebsd-net-unsubscribe@xxxxxxxxxxxxx"

Re: Duplicate SAD entries lead to ESP tunnel malfunction

- **Follow-Ups:**
 - ◆ **Re: Duplicate SAD entries lead to ESP tunnel malfunction**
 - ◇ From: Julian Elischer

- **References:**
 - ◆ **Duplicate SAD entries lead to ESP tunnel malfunction**
 - ◇ From: Oleg Tarasov
 - ◆ **Re: Duplicate SAD entries lead to ESP tunnel malfunction**
 - ◇ From: Julian Elischer
 - ◆ **Re: Duplicate SAD entries lead to ESP tunnel malfunction**
 - ◇ From: VANHULLEBUS Yvan

- Prev by Date: **Re: Duplicate SAD entries lead to ESP tunnel malfunction**
- Next by Date: **Re: VPN when host is not gateway**
- Previous by thread: **Re: Duplicate SAD entries lead to ESP tunnel malfunction**
- Next by thread: **Re: Duplicate SAD entries lead to ESP tunnel malfunction**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**