

[ipsec] KEY_FREESAV() in FreeBSD-Release7.0

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2008-04/msg00066.html>

- *From:* blue <susan.lan@xxxxxxxxxxxxx>
 - *Date:* Tue, 08 Apr 2008 11:56:21 +0800
-

Dear all:

About the KEY_FREESAV() in key_checkrequest() in key.c:

```
line 806:
if (isr->sav != NULL) {
KEY_FREESAV(&isr->sav);
isr->sav = NULL;
}
```

The codes are only going to free the sav used LAST TIME. For outgoing SA entries, the reference count will be always 2, instead of 1 like incoming SA. I thought the proper place to call KEY_FREESAV() should be ipsec6_output_trans() and ipsec6_output_tunnel() after invoking each transform's output function. Then the SA will be freed after its usage rather than being freed if there's next IPsec packet.

If the above condition is accepted, then key_delsp() in key.c should not call KEY_FREESAV() in case SA reference count underflow!

BR,
blue

freebsd-net@xxxxxxxxxxxxx mailing list
<http://lists.freebsd.org/mailman/listinfo/freebsd-net>
To unsubscribe, send any mail to "freebsd-net-unsubscribe@xxxxxxxxxxxxx"