

## Re: IPsec AH tunneling packet mis-handling?

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/net/2008-03/msg00348.html>

---

- *From:* "Bjoern A. Zeeb" <[bzeeb-lists@xxxxxxxxxxxxxxxxxxxxxx](mailto:bzeeb-lists@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 24 Mar 2008 12:41:09 +0000 (UTC)
- 

On Wed, 1 Aug 2007, blue wrote:

Hi,

Dear all:

I do not know the purpose of the following codes in the very beginning in ip6\_input():

```
#ifdef IPSEC
/*
 * should the inner packet be considered authentic?
 * see comment in ah4_input().
 */
if (m) {
m->m_flags &= ~M_AUTHIPHDR;
m->m_flags &= ~M_AUTHIPDGM;
}
#endif
```

Consider the case: a packet is encrypted as AH tunneled, and FreeBSD is the end point of the tunnel. After it tore off the outer IPv6 header, the mbuf will be inserted to NETISR again. Then ip6\_forward() will be called again to process the packet. However, in ipsec6\_in\_reject(), the packet's source and destination will match the SP entry. Since ip6\_input() has turned off the flag M\_AUTHIPHDR and M\_AUTHIPDGM, the packet will be dropped.

I don't think with the codes AH tunnel could work properly.

I was pointed at this.

I am a bit unsure about your setup as you are talking about "AH tunneled" and "encrypted" while at the end it's "AH tunnel" only. So, are you using IPsec tunnel mode with ESP and AH or just AH, or ...?

Can you describe the setup this would be a problem in detail and maybe file a PR so this won't be lost again.

Re: IPsec AH tunneling pakcet mis-handling?

We've got other ESP+AH+IPv6 problems pending like PR kern/121373 and I could look into both at the same time I guess.

PS: I am assuming this was with (Fast) IPsec, not KAME IPsec implementation? The date was too close to the change, so I thought it might be better asking;-)

Thanks  
/bz

---

Bjoern A. Zeeb bzeeb at Zabbadoz dot NeT  
Software is harder than hardware so better get it right the first time.

---

freebsd-net@xxxxxxxxxxxxx mailing list

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

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