

# Re: enc0 patch for ipsec

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/arch/2006-06/msg00064.html>

---

- *From:* Gordon Tetlow <[gordon@xxxxxxxxxxx](mailto:gordon@xxxxxxxxxxx)>
  - *Date:* Fri, 16 Jun 2006 10:22:22 -0700
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Max Laier wrote:

On Friday 16 June 2006 17:41, Scott Ullrich wrote:

On 6/16/06, Max Laier <[max@xxxxxxxxxxxxxxxx](mailto:max@xxxxxxxxxxxxxxxx)> wrote:

I think it should get a "device enc" on its own. Some people might consider enc(4) to be a security problem so getting it with FAST\_IPSEC automatically isn't preferable.

You have to specifically create the enc0 interface (ifconfig enc0 create) before it becomes active. Otherwise it will not hit the enc code path unless the device is created.

The issue is, if an attacker manages to get root on your box they are automatically able to read your IPSEC traffic ending at that box. If you don't have enc(4) compiled in, that would be more difficult to do. Same reason you don't want SADB\_FLUSH on by default.

Max is absolutely right here. The snooping interface should be a separate option altogether (a la bpf).

--gordon

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.3 (MingW32)

Comment: Using GnuPG with Mozilla - <http://enigmail.mozdev.org>

iD8DBQFEktfGRu2t9DV9ZfsRAvyzAJ9jnUigVW7t2SGV89vXStXAZ30b7QCeJ4tZ  
tBeTqHk9LofxCRf40uFvpZE=  
=RGmG

-----END PGP SIGNATURE-----

---

Re: enc0 patch for ipsec

freebsd-arch@xxxxxxxxxxx mailing list

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

To unsubscribe, send any mail to "freebsd-arch-unsubscribe@xxxxxxxxxxx"