



## APU3D4: AES-NI compatible - user configuration necessary on OPNsense?

peanuts 🕒 Apr 28th 2022



peanuts

[Beginner]

Posts:

1

Apr 28th 2022

Hi all,

Can anyone point me to whether I need to select one of the cryptography modules\* in OPNsense to get the best performance out of my Board? I was looking for info in the documentation in regards to AES-NI, but didn't find any.

- Hifn 7751/7951/7811/7955/7956 Crypto Accelerator (hifn)
- Crypto and RNG in VIA C3, C7 and Eden Processors (padlock)
- Intel QuickAssist Technology (qat)
- SafeNet Crypto Accelerator (safe)

My expectation would be that it's baked in the kernel and SoC, and no separate module should be necessary, but I'd like to get that confirmed to be sure.  
I expect those to be more or less external accelerators, but OPNsense sends conflicting info, bc/ for external accelerators, actually none should be selected.

Best regards and thanks in advance;  
Kay



mkopec

[Administrator]

Likes Received:

7

Posts:

24

Apr 28th 2022

Hi @peanuts ,

AES-NI is supported natively by the APU3's SoC, and it should just work without extra configuration or modules. As for QAT, SafeXcel and CESA, none of these are available in the APU3.

So no, you don't need to select any modules in OPNSense to get best crypto performance out of your APU3 😊

You could check out <https://teklager.se/en/knowled...performance-optimization/>  
(<https://teklager.se/en/knowledge-base/opnsense-performance-optimization/>) for other performance tweaks for OPNSense on APU.

Regards