

Sonda pro zákonné odposlechy na úrovni aplikačních protokolů

Vytvořený funkční vzorek umožňuje filtrovat komunikaci na síti s kapacitou linek 1 Gbps a následně vybrané pakety exportovat na vzdálené úložiště. Filtraci komunikace a určování, které pakety mají být exportovány na ukládací zařízení je možné specifikovat na základě IP adres (IPv4, IPv6), L7 identifikátorů (např. emailová adresa) nebo na základě jejich kombinací.

Sonda je cílena na nasazení do koncových sítí, ale lze ji použít i v datových centrech nebo u poskytovatelů internetového připojení s kapacitou linek 1 Gb/s.

Pro usnadnění nasazení v neznámých sítích sonda umožňuje aktivovat alternativní režim, který zpřístupní statistické informace o provozu na připojené lince. Mimo jiné tento režim uživatele informuje, zda síťové toky na připojené lince jsou kompletní a při aktivaci vybraného záchytu paketů nehrozí ztráta dat z důvodů nekvalitního připojení.

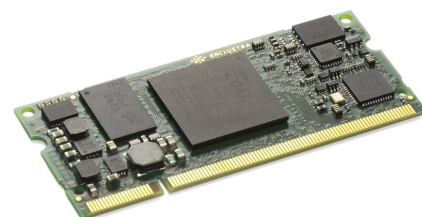
Způsob nasazení sondy, její konfigurace, kompletní specifikace podporovaných identifikátorů a použitý protokol pro export zachycených dat je popsán v uživatelské dokumentaci.

Základní parametry

- Čtyři monitorovací 1GbE rozhraní, jedno management rozhraní
- Využití FPGA SoC Xilinx Zynq pro zpracování paketů na plné rychlosti linky
- Hledání ID uživatelů a rozpoznání aplikačních protokolů přímo v hardware
- Správa cache potenciálně zajímavých síťových toků na úrovni hardware
- Vyrovnávací paměť na pakety potenciálně zajímavých síťových toků
- Hlubková analýza paketů až do úrovně aplikačních protokolů (SMTP, POP3, IMAP, FTP, SIP), využití ARM procesorů v FPGA SoC



Výkonná vestavěná sonda pro síť s kapacitou linek 1 Gb/s síť



**Výpočetní s modul
S FPGA SoC Xilinx Zynq**



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY