Picomass uses Netcope Session Filter in IPS200

"The failure to understand and address risks related to technology, primarily the systemic cascading effects of cyber risks or the breakdown of critical information infrastructure, could have far-reaching consequences for national economies, economic sectors and global enterprises." The Global Risks Report, World Economic Forum

Network Security in the 100 GbE Era

The message World Economic Forum is sending about cybersecurity is clear: adapt or perish. There is no doubt that a secure network is an indispensable asset for every large telco, datacentre, and ISP. And a network security solution capable of real-time action and monitoring is a must. It is no wonder that an increasing number of security solution vendors is racing to grab their share of this dynamically developing market. Among them towers Picomass with their highly versatile high-performance network monitoring solution called IPS200.

IPS200 stands out among other solutions for several reasons. It is capable of handling the traffic on simplex and full-duplex 100 GbE links with 100% packet capture rate. It acts as a front-end to extend the life of existing 10G and 1G appliances by shaping and balancing the traffic into lower bandwidths. It can host numerous DPI applications and it can effectively manage IP sessions. This could not be achieved without **Netcope FPGA network adapters**.

Cutting-edge Hardware Accelerators

It is highly impractical to use a standard network adapter for effective DPI at 100 Gbps. Standard network adapters transfer the traffic to software. This means loading the CPU, PCI-E, memory and cache with a deluge of data. The processing power required for a successful software-based DPI of 100 Gbps would have to be enormous, rendering this option unfeasible.

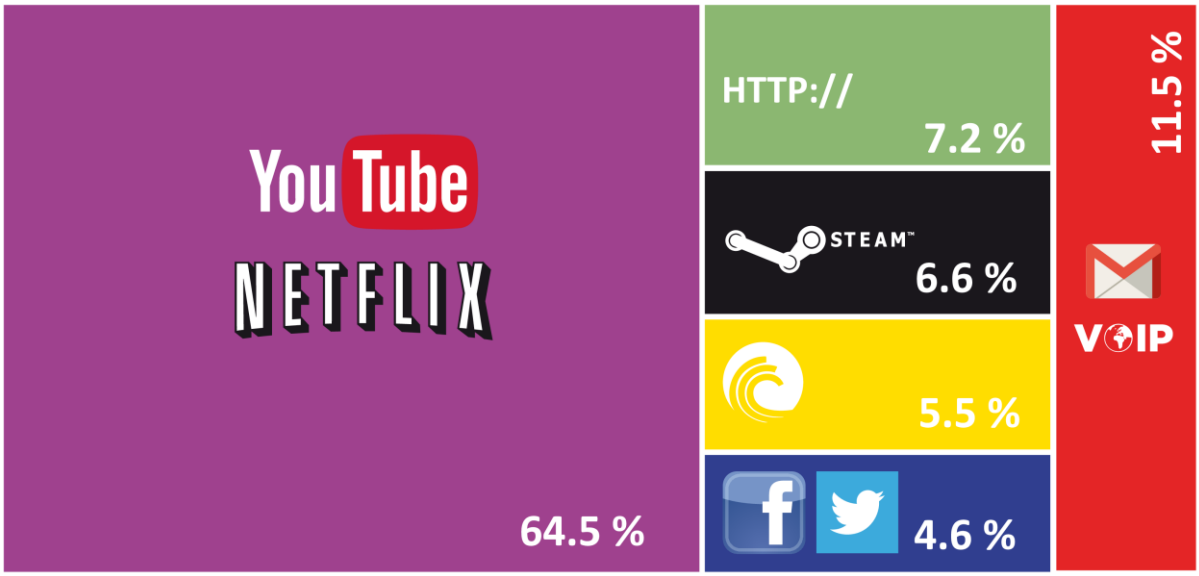
Luckily there is an alternative to standard network adapters: **FPGA based network accelerators**. Netcope Technologies offers a wide range of these network accelerators, while the most powerful is the **NFB-100G2**. This dual port 100 Gbps capable network accelerator offers number of unique features. It can be fitted in a standard commodity server via PCIE-Express bus. It comes with a passive cooling, in a fanless design that reduces the risk of mechanical failure, prolonging the lifespan of the whole server. Two accelerators can be comfortably connected with a network cable, which means that it is not necessary to open two servers in order to connect them.

However, to process the 100 Gbps data deluge, an accelerator suited for an intrusion prevention system like IPS200 needs to be more than just a cutting edge piece of hardware. The hardware needs to be outfitted with a firmware capable of instructing the hardware on how to handle the traffic and a software API and a controller capable of instructing the firmware. **Netcope Session Filter** (NSF) has been chosen for this job, the main reason being that NSF can perform **session-based traffic filtering**.

NETCOPE TECHNOLOGIES a.s., U Vodarny 2965/2, Brno, 616 00, CZ
www.netcope.com / info@netcope.com / +420 511 205 264

Filtering the Monitored Traffic

Although thousands of apps are used on the Internet every second, we can predict which are the most popular. According to the 2015 Sandvine report for North America and Latin America, the aggregated peak period traffic looks like this:

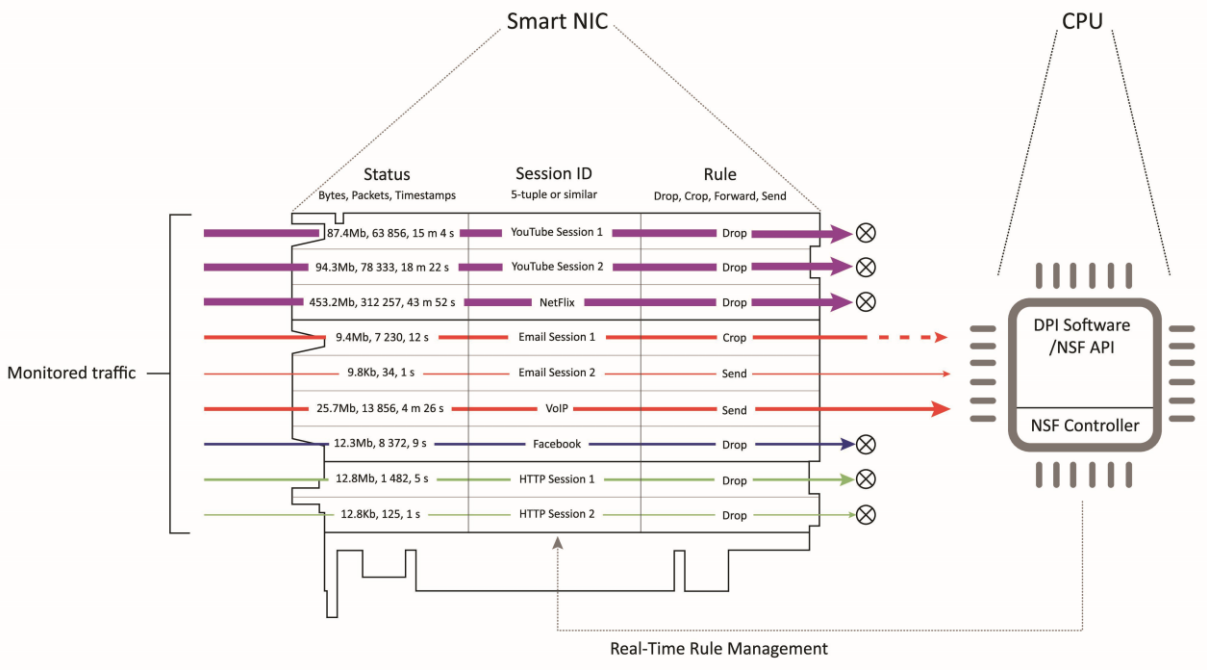


- Real-Time Entertainment 64,54%
- HTTP 7,21%
- Marketplace 6,57%
- File sharing 5,54%
- Social Networking 4,63%
- Other 11,5%

In this figure, we see that real-time entertainment consumes the greatest amount of bandwidth. However entertaining might this activity be for the internet users, it presents no security risk. Loading the DPI software with this type of traffic would be a huge waste of processing power. Although precise numbers vary from network to network, the main problem remains: how to deal with the real-time entertainment data deluge?

This is where NSF shines. It can identify each **session** in the network traffic and **filter** it. A **session** is perceived as a sequence of packets with the same source and destination IPv4/6 address, L4 protocol, TCP/UDP ports, and optionally other fields (input network interface, type & code for ICMP packets). **Filtering** is the process of sorting of the traffic according to commands obtained via NSF API.

NSF is not just an FPGA-based network interface card or a simple piece of hardware. It is a bundle comprised of several components, the most important being the card, the firmware and the software. These components work together and filter the monitored traffic. Initial frames of each session are transferred to the DPI software. Based on this initial inspection and commands received via NSF API, NSF controller instructs the firmware and the firmware instructs the hardware to either keep forwarding the session to the DPI software, crop the session, record metadata (bytes, packets, first frame timestamp, last frame timestamp), or drop the session entirely.



A practical example of this process: a few frames of the 1st **session** are transferred to the DPI software. The DPI software determines that this session is a stream of a YouTube video and therefore it is of no interest to the DPI software. The NSF controller sends instructions to drop the session. The session is offloaded in hardware. Valuable processing power of the server CPU is saved.

The same goes for the 2nd and 3rd session. These sessions are streams of a YouTube and Netflix videos and therefore of no interest to the DPI software. The 4th session is an email session, therefore it is a session worthy of DPI. Based on the first few frames the DPI software determines that it wants to inspect the session. NSF controller sends instructions to keep forwarding the session to software. The same goes for the 5th session (VoIP), the 6th session (HTTP) and so on.

A Unique Piece of Network Technology

The ability of NSF to filter the traffic on per-session basis helps IPS200 to accelerate the DPI software by offloading traffic on hardware has multiple possible use cases. Apart from DPI acceleration, IDS and IPS, NSF has numerous other applications. For instance, two interconnected cards can be used for load balancing on the application level. It can also be deployed in a stateful firewall solution.

Martin Hayes, a CTO of Picomass comments on the cooperation: “10G traffic and current Xeon technology is a suitable processing power ‘demand and supply’ pairing where DPI software has the power to completely analyse each and every packet that arrives into the host. There has been a seismic shift in this balance with the move to 100G which effectively started in 2014 and has been increasing pace. Netcope’s NSF allows for the early classification and hardware offload of sessions that are not relevant to Intrusion Protection using all remaining power to analyse the remaining traffic for Intrusion candidates. Netcope’s Hardware Session-based Offloading coupled with inter-adapter load-balancing of full-duplex links, means that we can deliver 200 Gbps of DPI analyses using standard server configurations.”

Petr Kaštovský, a CEO of Netcope says: “We have always been closely listening to our customers and following trends in network security. DPI for security purposes has been a topic for last few years and its importance is steadily growing. Therefore, we focus on building a solution to accelerate DPI-based network applications to the speed of a backbone network. The cooperation with Picomass was very valuable in terms of testing our product on the market and getting that valuable feedback.”