TECHNOLOGY BRIEF

Hardware-Based Flow Shunting for Network Security Appliances

SUMMARY

Complete, dynamic control over which traffic flows are forwarded from ANIC adapter to application.

BENEFITS

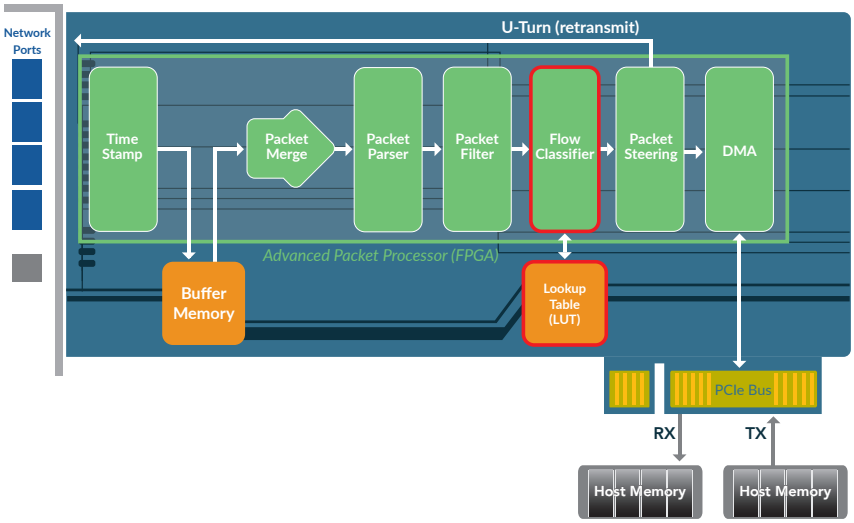
- Eliminate processing (or storage) of unwanted traffic flows.
- Offload host CPU from processing unnecessary traffic, thereby freeing resources to perform more pressing tasks.

Keeping up with the deluge of data is a classic problem for almost every offline security appliance: particularly at 10, 40 and 100G speeds. Security applications such as Suricata and others are all CPU bound and thus their performance is directly related to the number of packets the application has to process. The solution to this problem is obvious: reduce the number of packets the security application has to process. Over the years, there have been many attempts to offload the application using various software and hardware techniques such as packet filtering. These have all been less than ideal, because they are static solutions. In other words, the hardware must be told ahead of time which packets to filter out, with limited or no ability to make adjustments on the fly.

Shunt
/SHənt/ *v.* to move to the side. to turn off to one side

FLOW CLASSIFICATION

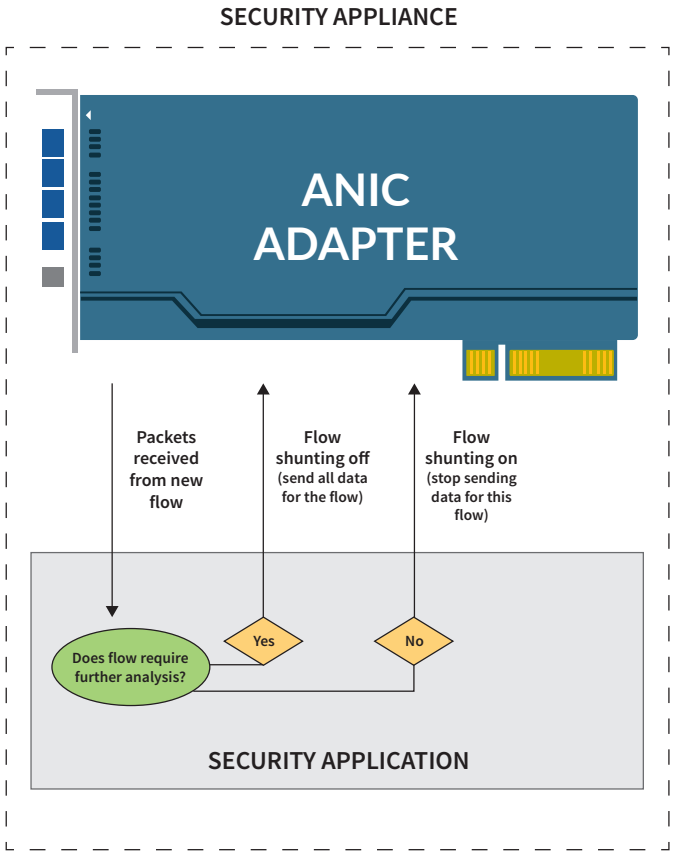
Flow shunting is a technique which relies on the flow classification capability in each ANIC adapter from Accolade Technology. As shown below, each ANIC adapter performs a series of packet processing functions including flow classification. The flow classifier block inspects each packet and determines whether it is part of a new flow or an existing flow. The associated lockup table (LUT)—a physical bank of memory (DRAM)—is updated with the flow classification decision. It is in this LUT or DRAM that flow entries for up to 32 million unique IP flows are stored. For each flow entry, standard packet header information (e.g. source/destination IP, protocol etc.) is recorded, in addition to metadata about the flow such as total packet count, byte count and the last time a packet was seen. Furthermore, information about both directions of a flow are tracked in the same flow entry so a bi-directional context is maintained. With information about each flow in place, the ANIC adapter is now in the unique position of being able to take specific actions on an individual flow such as forward, drop or re-direct the flow. Control over which action to take is completely in the hands of the application that controls the ANIC adapter. This control forms the basis for flow shunting.



Hardware-Based Flow Shunting for Network Security Appliances

FLOW SHUNTING

At a high level, flow shunting allows an application to programmatically turn packet transmission on or off—for a given flow (based on 5-tuple). In other words, the application can decide from which flow(s) it does and does not want to receive data traffic. By intelligently "toggling" the flow shunting switch, an application can greatly reduce the amount of data it has to analyze, thereby freeing up CPU resources for more pressing tasks.



This diagram clearly illustrates the flow shunting process. Inside a security appliance there is an Accolade ANIC adapter (in PCIe slot) and the security application. The security application communicates with the adapter via a well-defined API (natively integrated into Suricata, PF_RING etc.) which it uses to configure and control the adapter. The adapter classifies each flow and subsequently sends the entire packet (header + data payload) to the application. The application in turn examines the packet (or more likely many packets in a row) and decides whether this particular flow requires further analysis or not. If the flow is not of interest then the application tells the adapter to ***turn flow shunting on*** or in other words to stop sending any packets from that flow. If for some reason the situation changes, flow shunting can always be turned off for this flow, in which case packets will resume being forwarded to the application. There may be instances when "toggling" flow shunting on and off is necessary.

There are many reasons why an application may not want to continue receiving traffic for a given flow. For example, if the application cannot process encrypted traffic there is no point in receiving encrypted flows. Or an application may not want to examine video traffic (e.g. NetFlix) because it doesn't pose a threat or wastes too much disk space, so all video traffic could be shunted away. Or perhaps the application has an IP blacklist (or whitelist) on which it operates and therefore any flows which don't match the list should be shunted aside. The value of flow shunting is clearly that it puts control in to the hands of the application, so that dynamic decisions such as which traffic flows should be analyzed can be made based on programming logic.

ACCOLADE TECHNOLOGY PROFILE

Accolade is the technology leader in FPGA-based Host CPU Offload and 100% Packet Capture PCIe Adapter/NIC's and Scalable 1U Platforms. Accolade's line of 1-100GE products enable 100% packet capture, flow classification, deduplication, packet filtering and more. Our customers are global leaders in network monitoring & cybersecurity applications as well as in the network test and measurement, telecom and video stream monitoring markets.

ID:170111

Accolade Technology

Headquarters:
124 Grove Street, Suite 315
Franklin, MA 02038

phone: 877 653 1261
email: inquire@accoladetechnology.com
www.accoladetechnology.com