

Product Brief

Introduction

Network intrusion detection system (NIDS) is an integrated tool capable of detecting intrusions or malicious traffic. NIDS can analyse packets that travel over the actual network and examine packets to verify their purpose (malicious or benign). Typical NIDS is realized as a software application analyzing packets captured by NIC. A popular software-based NIDS is Snort.

Snort is an open source network intrusion detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods. The Snort database contains thousands of rules which describe most of the known viruses and attacks. In Snort, more than 80% of the CPU time is consumed by the string matching task. As network traffic speeds increase faster than PC performance, software-based solutions can not continue to process all traffic. This issue can be solved by moving Snort time-critical paths from software to hardware.

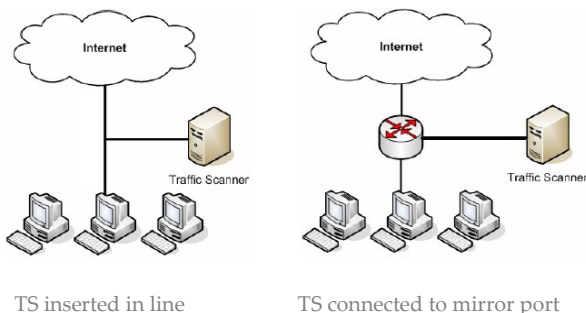
Traffic Scanner

The Traffic Scanner (TS) is a network intrusion detection system composed of hardware acceleration card based on NetCOPE platform and Snort running on host PC. The card is equipped with FPGA chip running a reloadable firmware which performs incoming packets analysis. Only malicious packets are forwarded to Snort for further analysis.



Typical Application

The Traffic Scanner is typically deployed on the LAN side of the WAN router and is totally invisible on the network. TS can be connected to your network in two modes. Firstly, TS can be inserted in a line to make all incoming and outgoing traffic pass through. Secondly, TS can be connected to the mirror port of WAN router or T-splitter is used.



Features

- Passive monitoring of multiple Gigabit interfaces
- System throughput up to 6 Gbps
- Capable to cover the whole Snort database
- Exporting suspicious packets via PCI-Express bus
- Substantially accelerated Snort
- Act as ordinary NIC – transparent for software NIDS
- Prepared filtration rule sets

Capabilities

- Detecting unauthorized access to computer systems
- Detecting viruses and worms
- Detecting and preventing piracy
- Detecting leaks of confidential data

Firmware

The firmware is composed of several units which are chained into processing pipeline. From each valid packet, the TS extracts IPv4 header fields like source and destination address, ports, TCP Flags and other fields. Then TS compares extracted header fields to stored IDS rules. According to this comparison, particular patterns are searched in the packet payload. The pattern matching method is based on the NFA hardware generation. This approach offers high throughput with possibility of searching both strings and regular expressions. High throughput compared to software solutions is achieved thanks to simultaneous search of all strings in contents.

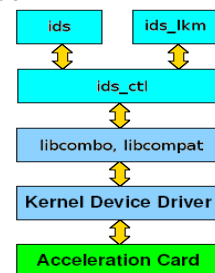


Software

The TS software consists of several parts:

- Linux drivers
- User space libraries (libcompat, libcombo)
- TS control scripts and GUI
- Web configuration application

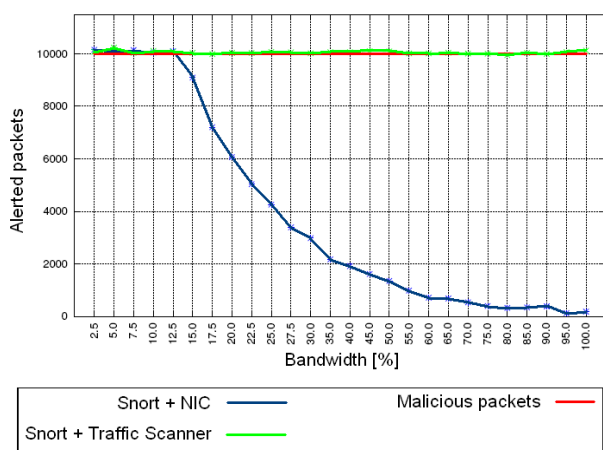
The start-up programs load the firmware into acceleration card and initialize the Traffic Scanner. TS can be user-controlled by special scripts (ids and ids_lkm) and user friendly GUI. The drivers present the TS hardware card as an ordinary NIC, so it is transparent to software applications.



Acceleration Performance

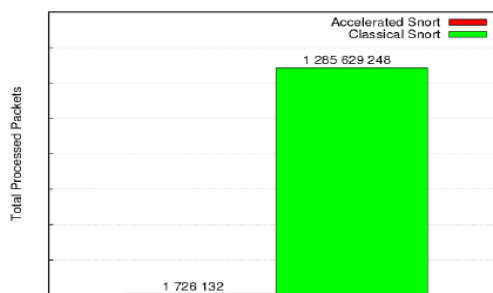
We have performed throughput tests of hardware accelerated and non-accelerated Snort NIDS probes. The accelerated probe was realized by the Traffic Scanner. The non-accelerated probe was realized by common solution of standalone Snort and NIC. The results are shown in the following graph. As you can see, the non-accelerated solution is able to detect malicious packets on the link with maximum bandwidth up to 100Mbps while the accelerated solution is suitable for 1Gbps link analysis.

The maximal throughput is limited by the number of filtration rules. While increasing throughput, the number of supported rules decrease and vice versa. The Traffic Scanner is capable to analyze 3,2 Gbps traffic with the rule set covering the whole Snort database.



Accelerated and non-accelerated Snort performance

Next test was focused on the number of packets filtered by acceleration card. This number affects the Snort performance – the more packets is filtered in hardware, the less have to be processed by software. In this test, both probes were configured for detecting the same virus and worms threads and was monitoring the same 1 Gbps network traffic for 24 hours. The same alerts were generated for both solutions, however the accelerated Snort had to process only 0.02 percent of network traffic. The remaining packets were filtered by hardware card. The results show that Snort performance was significantly increased and can be used in gigabit networks. Following graph shows the number of packets processed by Snort on both probes.



Comparing Traffic Scanner accelerated Snort with non-accelerated solution

How to get Traffic Scanner

The Traffic Scanner can be purchased as an appliance or rented as a managed service. Please contact INVEA-TECH for pricing and additional information about this product.