

Performance Improvement of Suricata IPS in Multicore

Contents

Introduction	2
Performance Objective.....	3
Suricata Overview and Architecture.....	4
Test Environment.....	5
Performance Tuning	7
Conclusion	9
Appendix I - Network Security Capabilities at L&T Infotech	10
Abbreviations and Acronyms	13

Introduction

An Intrusion Prevention System (IPS) monitors network traffic, detects attacks and activates countermeasures to ensure security. According to a pre-programmed set of rules, the IPS either drops the incoming packets if it seems suspicious or sends it to the recipient immediately. It performs Stateful packet inspection to detect protocol anomaly and deep packet inspection (L7 processing and payload content matching) for detecting attacks.

Following are the different types of IPS:

- Network-based Intrusion Prevention (NIPS) - Monitors the entire network for suspicious traffic.
- Host-based Intrusion Prevention (HIPS) - Dedicated to surveying incoming traffic and operations of a single host machine (server, terminal, etc).
- Wireless Intrusion Prevention (WIPS) - Scans wireless networks for suspicious traffic with the help of wireless networking protocols
- Network Behavior Analysis (NBA) - Examines network traffic to identify threats that generate unusual traffic flows, such as Distributed Denial of Service (DDoS) attacks, certain forms of malware and policy violations.

Popular open source IPS softwares are snort and Suricata. Snort was developed in the year 1998, and is the most widely used Intrusion Detection and Prevention System (IDS/IPS). Developed by Source Fire, it is capable of performing real-time traffic analysis and packet logging on IP networks. Suricata is a multi-threaded open source next generation intrusion detection and prevention tool developed by Open Information Security Foundation (OISF).

Performance Objective

In this paper, we have chosen Suricata for measuring performance on Freescale's multi-core platform [P2020 and P4080]. Performance analysis is executed by running Suricata1.0.0 in IPS mode with the Linux kernel stack.

In IPS mode Suricata is made to run simultaneously where it receives packets from Netfilter queues. The following diagram indicates the packet flow both with and without IPS.

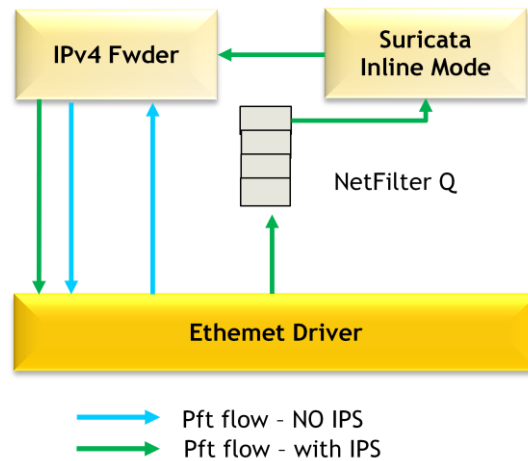


Figure 1: Packet Flow

When a packet comes through the network interface it is first queued up in Netfilter and then pushed to the application layer. Then Suricata processes the packet based on existing rules and later sends it back to the interface with the help of IPv4 forwarder.

Suricata Overview and Architecture

Here in our performance analysis we have Suricata 1.0.0, OISF's first stable version. Since Suricata uses the same rule syntax as snort, Suricata is loaded with snort's rule set. The table below lists out the features of Suricata 1.0.0

Features:

Suricata Features	Description
Multi Threading	Capable of scaling threads to multiple cores
Automatic Protocol Detection	IPS has a set of keywords for IP, TCP, UDP and ICMP. Rules can be written to detect a match in the stream regardless of the port
Standard Input Methods	Support for NFQUEUE, IPFRING and the standard LibPcap to capture packet
IPv6 Support	Supports native IPv6
Postgresql log module	Supports logging in Postgresql database
Unified2 output	Support for output tools and methods

On execution Suricata creates 6 default threads and detect threads based on the detect ratio set. Default threads are Receive NFQ, Decode, Stream, Verdict, Respond and Reject and Output)

Detect Thread Ratio: 1.5 (default); Default Threads: 6;

Detect threads (no. of cores*Detect Thread Ratio) +Default Threads (6) = Packet Processing

As per thread calculation, the diagram below reveals the packet receive functionality and other IPS actions implemented as single thread while the detection functionality remains separated as another thread. Threads are created based on the detect ratio which are then made to run on multiple CPUs using affinity. CPU affinity is used to enhance the performance of detection functionality.

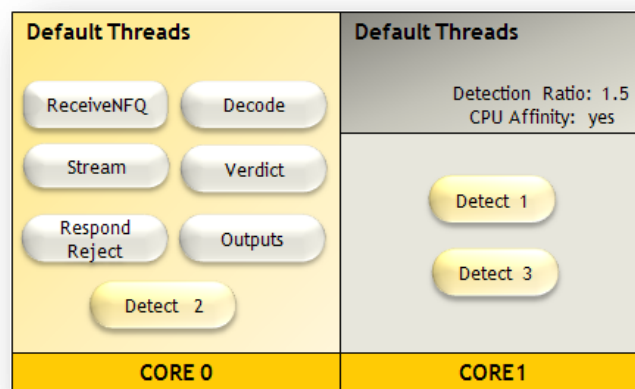


Figure 2: Multi-Threaded Architecture

Test Environment

Suricata was ported on Freescale's P2020 multicore processor by cross compiling Suricata and its dependency packages with Linux target image builder (ltib) of P2020. P2020 communication processor belongs to the Freescale's QorIQ P2 Platform series. It has dual e500 cores built on Power Architecture technology and delivers up to 1.2GHz frequency.

Spirent's Smart Bits 600 is a network performance analysis system which is ideal for 10/1000Mbps and 1Gbps Ethernet connection. The diagram below indicates our experimental setup where we have connected smart bits with port density of 1 gigabit to the P2020 board. We then pump in IP packets through one interface (eth1), which is then forwarded through the other interface (eth0) and the measured throughput is viewed with the help of smart apps (frontend).

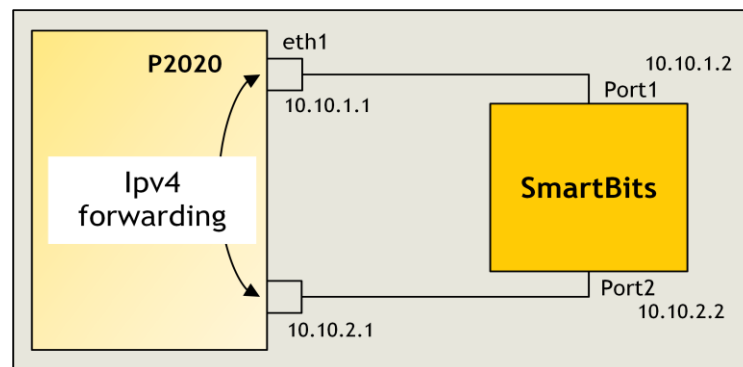


Figure 3: Performance Setup

Traffic Type: UDP

- Total number of SMB flows: 2
- Test duration: 30 seconds
- Initial Rate: 100%
- Acceptable loss: 0.0%
- Direction: bidirectional
- Mac Address resolution: disabled

Frame Size (bytes)	Passed Rate (%)	Throughput (Mbps)
64	10.10	147
128	17.45	288
256	32.55	576
512	61.57	1130
1024	100	1871
1280	100	1878
1518	100	1883

Table 1: Throughput Measurement of P2020 without Suricata

Table 1 represents the throughput measurement of P2020RDB with only IP forwarding, no IPS and no kernel optimization.

Frame Size (bytes)	Passed Rate (%)	Throughput (Mbps)
64	5.48	80
128	10.45	172
256	17.38	307
512	35.66	655
1024	66.08	1236
1280	81.25	1526
1518	100	1883

Table 2: Throughput Measurement of Suricata on P2020

Table 2 represents the throughput measurement of P2020RDB with IP forwarding, Suricata [NIPS] and no kernel optimization.

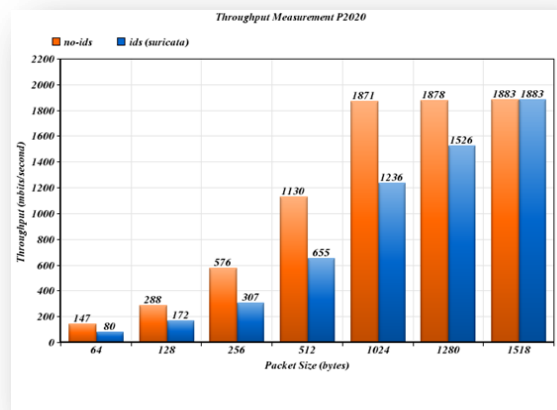


Figure 4: Throughput Comparison without Optimization

From Table 1 and Table 2 we find that the number of packets processed for lower frame size has decreased and the throughput has almost reduced by **50%** when the IPS was running and for higher frame size only a max of **81%** of total traffic was passed.

Performance Tuning

In order to improve the performance of Suricata, the following techniques were used

- Kernel optimization technique [skbuff and TXNAPI]
- Increasing the number of intrusion detection threads per core.

Both the above methods are described in detail below:

Kernel Optimization techniques

- **Skbuff Recycle**
 - SKB Recycle handles network packets and helps in recycling socket and data buffer
 - Reduces unnecessary allocation and de-allocation of memory
 - Improves IP forwarding throughput
- **TXNAPI**
 - Interrupt mitigation technique
 - Reduces packet overheads
 - Reduces latency and improves performance
 - Packet throttling

Application -level optimization techniques

- **Detect thread Ratio**
 - Increases the number of detect threads per core
 - Increases the number of packets processed

Example: Thread Calculation For a Detect Ratio of 3

Detect Thread Ratio: 3 (default); Default Threads: 6; Cores: 2

Detect threads (2*3=6) +Default Threads (6) = 12 Packet Processing Threads

Cores	C0	C1
Detect Thread	Default threads,D2,D4,D6	D1,D3,D5

The following tables represent the throughput measured with kernel optimization and increased detect ratio:

Test Duration(sec): 30 Initial Rate(%):100 Minimum Frame Size(byte): 64 Acceptable Loss(%): 0 Maximum Frame Size(byte): 1518 Mode: bidirectional				
Frame Size (bytes)	without kernel optimization	Skbuff Enabled	Skbuff and TXNAPI enabled	Detect Ratio 3
64	80	106	188	192
128	172	213	381	372
256	307	421	778	763
512	655	845	1516	1462
1024	1236	1570	1678	1871
1280	1526	1827	1878	1878
1518	1883	1883	1883	1883

Table 3: Throughput Measurement of Suricata on P2020 after Tuning Performance

Table 3 represents the throughput achieved by applying kernel optimization techniques on P2020 board with IPv4 forwarder application while Suricata was running. The last column represents the throughput achieved when Suricata’s detect threads were increased to 3 threads per core.

Below are the graphical representations of the throughput achieved for various packet sizes with and without IPS on P2020RDB after tuning the performance

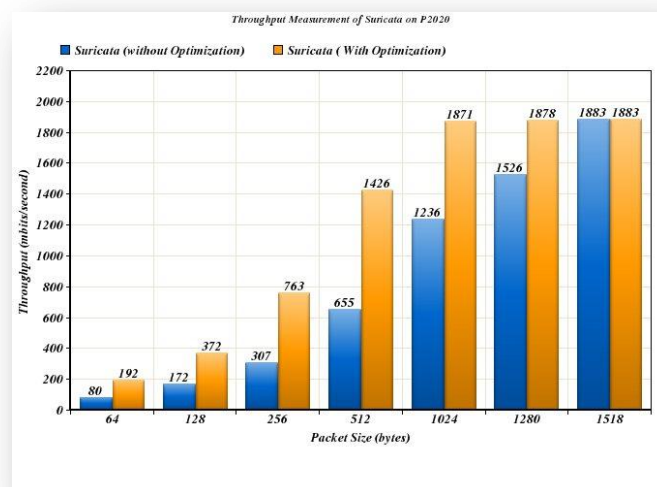


Figure 5: Throughput Comparison of Suricata with & without Kernel Optimization

For lower size packets [64 bytes] we find that, as compared to Suricata without kernel optimization, there is an increase of about **32 %** with Skbuff enabled and about **135 %** increase with both Skbuff and TXNAPI enabled. With application level optimization there is **140 %** increase for lower size packets when compared to the throughput without kernel optimization.

Conclusion

Snort had been the de-facto IPS solution in the industry for more than 12 years and is slowly being replaced by Suricata, a next generation IPS. Suricata 1.1 beta 1, the latest release provides a new pattern matcher, improved parsers and greatly improved performance and accuracy. There is heated competition between Snort and Suricata for effectiveness and performance.

From our experiment and hands-on experience with Suricata, we acknowledge that Suricata's multithreaded architecture, flexibility to tune architecture for different multi-core platforms and scalability of detection engines are key features which makes it easily adaptable to different security market segments.

Suricata also supports IP reputation, automatic protocol detection (IP, TCP, UDP, ICMP, HTTP, TLS, FTP and SMB,) gzip decompression, fast IP matching and hardware acceleration. In the recent RSA 2011, Suricata was also commercially released by nPulse Technologies Inc on Napatech's hardware platform to support multi gigabit performance.

With Suricata's recent beta release focusing on improving core feature performance and with the flexible multi threaded architecture, we are confident it would gear up faster to protect against the next generation of threats.

Appendix I - Network Security Capabilities at L&T Infotech

Network Intrusion Prevention System

Expertise

- Strong knowledge on open source NIPS - Snort and Suricata
- Vulnerability Assessment
- Security Information and Event Management(SIEM) tools
- Signature offloading to Hardware
- CEH certified resources

Focus Area

- Software migration to multicore processors
- Software design enhancements
- Performance improvement using Kernel optimizations technique & hardware acceleration
- Testcase development & Automation
- Penetration Testing
- Signature development & Attack generation

Projects handled

- Snort signature offload to Pattern matching engine of Freescale P4080 processor
- Penetration testing of enterprise UTM - Testing Evasions, DoS/DDoS, Attempted Reconnaissance etc

Network Security Capability Overview

- Well-versed in firewall, IPS, VPN, antivirus, DPI and IPv6
- Crypto and signature offload to hardware accelerators to improve performance
- Expertise in industry-leading processors (ARM, Cavium, Wintegra, TI, Intel, Freescale) and multi-core programming
- Services and IP based offerings targeted at reducing time-to-market
- Security testing - protocol fuzzing, vulnerability assessment and penetration testing.
- Security product feature testing - FW,NAT,IPS,VPN
- Test cases development and automation

Network Security Expertise	Firewall	IPS	VPN	Anti-X	UTM	SIEM Tools	Signature Development
Cryptogra-phy Expertise	AES	T-DES	MDS	SHA 1/2	HDCP	BISS-E	PKCS#11
Security Protocol Expertise	IPSec	IKEv1/v2	SSL/TLS	SSH	Radius/Diameter		
Opensource Security s/w Expertise	Strongswan [IPSec-VPN]	Snort [NIPS]	Suricata [NIPS]	ClamAV [Anti-x]			
Security Accelerators	DPI Engines	Pattern Matching Engines		Crypto Accelerators			
Multicore Processors	Freescale	Cavium	Wingegra	RMI	TI		
Security Testing Expertise	Product Feature Validation	Vulnerability Assessment	Penetration Testing	FIPS Certification	IPv6 Ready Logo		
Test Tool Expertise	Ixia - IxDefend	OpenVAS	Nmap	Metasploit	Backtrack Linux		

Figure 6: Security Capabilities at a glance

Our services primary focus is on

- Security product feature enhancements/optimizations
- Security feature integration services
- Product validation
- Hardware acceleration
- Porting to a multi-core environment
- Product management interface
- Test automation and testing for Certifications - FIPS, IPv6 Ready Logo, etc.

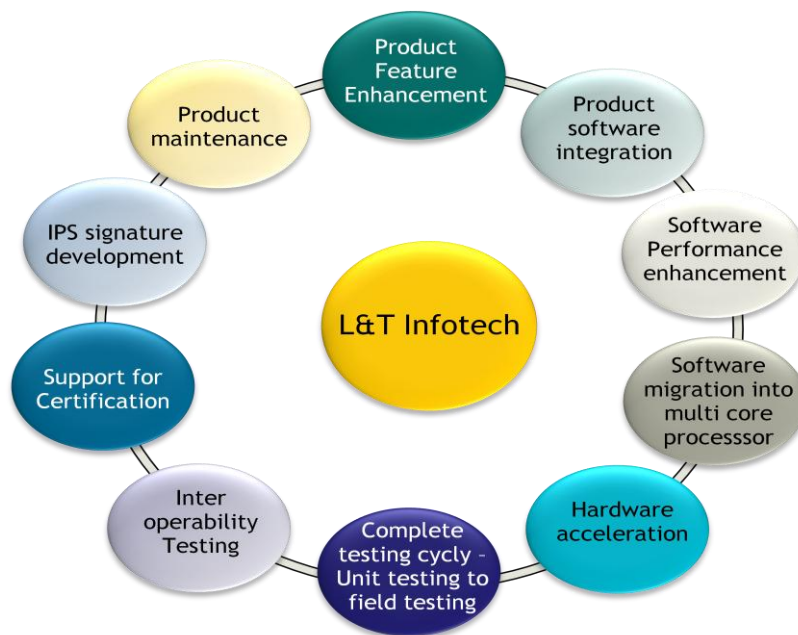


Figure 7: Service Offerings

Abbreviations and Acronyms

BASE	Basic Analysis and Security Engine
DDoS	Distributed Denial of Service
DPAA	Data Path Acceleration Architecture
Gbps	Gigabits Per Second
HIPS	Host Intrusion Prevention System
ICMP	Internet Control Message protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet protocol Version 4
IPv6	Internet control Version 6
Ltib	Linux Target Image Builder
Mbps	Megabits per Second
NBA	Network Behavior Analysis
NIPS	Network Intrusion Prevention System
OISF	Open Information Security Foundation
SMB	SmartBits
TCP	Transmission Control Protocol
UDP	User Datagram protocol
WIPS	Wireless Intrusion Prevention System

References

Open Information Security Foundation site	http://www.openinfosecfoundation.org
Snort website	http://www.snort.org
Snort and Suricata articles	http://www.networkworld.com/community/blog/snort-and-suricata-creators-exchange-heated-w
Commercial release of Suricata	http://www.catapulta.org/index.php/News/1/77-threatmeter

About the Author



Harini Gopalakrishnan started her career with L&T Infotech and has been associated with the security practice for more than a year now. She has good amount of experience in the field of Network security. Her Key expertise and special focus lies in the area of IPSec and Network Intrusion Detection system (NIDS).

About L&T Infotech

Larsen & Toubro Infotech (L&T Infotech), one of the fastest growing IT Services companies, is ranked 5th globally among the Best IT Services Providers by Global Media Services in 2009, ranked 1th by NASSCOM among the top software and services exporters from India and also ranked among the 'Leaders' category in the prestigious Global 100 list released by the International Association of Outsourcing Professionals (IAOP). A wholly-owned subsidiary of USD 9.8 billion Larsen & Toubro, India's largest technology-driven engineering organization, L&T Infotech is differentiated by the unique Business-to-IT Connect, which is a result of our rich corporate heritage.

We offer comprehensive, end-to-end software solutions and services in the following industry verticals: Banking & Financial Services; Insurance; Energy & Petrochemicals; Manufacturing (Consumer Packaged Goods, High-tech, Industrial Products, Automotive, Chemicals & Process, Media & Entertainment, Pharma, Retail and Logistics); and Product Engineering Services (Telecom).

We also deliver business solutions to our clients in the following Service Lines: SAP, Oracle, Infrastructure Management Services, Testing and Consulting. Our other Service offerings are: Business Analytics, Legacy Modernization, Applications Outsourcing, Architecture Consulting, PLM, Service Oriented Architecture, end-to-end integrated engineering services and embedded system solutions.

For more information, visit us at www.Lntinfotech.com or email us at info@Lntinfotech.com