



## **Factors Affecting Network IPS Throughput**

by

**Jack Walsh**

**Intrusion Detection and Prevention Program Manager  
ICSA Labs, an independent division of Verizon Business**

and

**David Koconis, Ph.D.**

**Technical Lead Network Intrusion and Prevention  
ICSA Labs, an independent division of Verizon Business**

**July 15, 2008**

---

---

## Introduction

Following the successful completion of network IPS testing, ICSA Labs publishes the throughput that a device was able to sustain. When reflecting upon these reported throughput numbers, end users may question any differences between what ICSA Labs reports and what the vendor claims in its datasheet for the same product. Because there is likely to be a disparity between published throughputs for the same device, end users might be interested to learn what factors can affect the throughput achieved by a network IPS.

This white paper begins by isolating many of the factors that impact throughput. Additionally the paper explains what some vendors do to attempt to increase the throughput of their network IPS devices. The white paper concludes by explaining why there are differences between the throughput reported following ICSA Labs network IPS testing and the throughput published in vendor datasheets and what comparisons, if any, can be made between the two sources of throughput data.

## The Applied Policy

Imagine a testing lab with two network IPS devices. Both devices are made by the same network IPS vendor. In fact both are the same model. One is configured to pass all traffic without any inspection. The other enables all possible server-side, client-side, evasion, DoS, and any other kind of vulnerability coverage protections. You can probably guess that the first device, which is simply configured to behave like a switch, is most likely to perform better. Even if the first device had half of all protection mechanisms enabled, it is still more likely to perform better.

The thought experiment above reveals that, for most network IPS devices, the policy being enforced – or the collective set of enabled protection mechanisms including any logging and alerting – impacts the maximum throughput the device can achieve. It's also important to note that each individual vulnerability coverage protection mechanism is likely to require differing amounts of processing. For example, suppose the devices mentioned above have two completely different sets of 50 unique vulnerability coverage protections enabled. Chances are that the throughput for each device will differ even with the same mix of traffic.

Because the threat landscape is changing and new vulnerabilities are being discovered all the time, the set of vulnerabilities for which coverage protection must be provided in ICSA Labs network IPS testing changes over time to remain current and relevant. Given that the policy enforced by the device during each testing iteration is almost surely different due to differences in the vulnerability set, and given that policy changes usually impact throughput, then it is not surprising that the achieved throughput may go up *or go down* – when compared to previous testing iterations for the same network IPS device.

## Protocol Inspection Costs

The amount of system resources required to inspect network traffic can depend on the protocols found in the traffic. While analyzing their device, a network IPS vendor may determine that some subset of protocols requires less or delayed inspection. The vendor may then optimize their device to account for this. As a result any processing of traffic primarily composed of those protocols may have less of an impact on throughput than processing traffic containing all other protocols. Similarly, the developer may have determined that having to more carefully inspect network traffic composed of certain protocols more negatively impacts throughput. As an example, it may require more effort to analyze an HTTP session versus an SMB one. Or perhaps it is easier for a network IPS device to process TCP compared to UDP.

---

---

During the vendor's own product analysis, they may determine that almost no inspection can be done. For example, they may conclude that when traffic is encrypted very little if any processing needs to or can be done. Network IPS developers that come to this conclusion may design their device so that few resources are spent inspecting HTTPS, SSL, IPsec, and other encrypted traffic.

Conversely, a network IPS vendor may conduct a study to see which layer 3 protocol is most often impacted by remotely-exploitable, high severity vulnerabilities in enterprise-class software. In ICSA Labs' network IPS testing over the preceding four years, vulnerabilities involving TCP traffic account for almost 95% of the total. If a network IPS developer found similar results they may conclude that inspecting UDP traffic is less of a priority than inspecting TCP traffic.

Clearly then, if the profile of the network traffic that the product encounters during deployment in an enterprise organization matches what the network IPS developer expected, this could have a favorable impact on the throughput. On the contrary, if the network traffic profile in the enterprise where the device is deployed is vastly different than what the developers expected, the throughput may be adversely affected.

### **That Which Impacts Accounting**

A network IPS is typically stateful in that the device keeps track of and accounts for various things associated with the network traffic passing in-and-out. Therefore anything that the network IPS has to keep tabs on is going to impact its throughput.

Being a stateful device, a rise in the average number of new connections, concurrent connections, fragmented sessions, and/or unique hosts adversely impacts throughput. Also the average size of a frame impacts throughput. Often the throughput decreases as the average frame size decreases. This results in part from the device having to process and account for many more sets of headers than it would if the frames were larger.

### **What's a Network IPS Developer To Do?**

Network IPS developers recognize that the factors above conspire to slow down their devices. Is there anything that can be done to reduce the performance impact without adversely affecting what should be the product's bread-n-butter – providing security coverage protection for remotely-exploitable vulnerabilities? In fact, there are some things that network IPS developers can and will do to ensure the highest possible throughput while providing expected coverage protection from network-borne attacks.

One thing developers can do is enhance their existing hardware. Employing faster network processors, parallel processing, using customized ASICs, adding more memory, and utilizing NICs capable of more speedily handling and processing all received network traffic are just some of the changes that network IPS developers can make to ensure the highest possible throughput and lowest possible latency. Of course more and better hardware usually comes with an increased price tag.

While considering the factors above that impact performance, and as alluded to earlier, developers may re-architect how they handle network traffic. Because so much of the attack traffic is TCP based, a product may be designed to initially perform less analysis on UDP traffic and other non-TCP traffic. And since a network IPS may contain algorithms capable of recognizing normal network traffic, it may be able to give higher priority to familiar applications. In these and other ways developers can seemingly improve throughput on as much of the "good" network traffic as possible.

---

---

Though network IPS developers can make these improvements, it's not clear that they can do so without sacrificing security effectiveness. In fact, in ICSA Labs network IPS certification testing, analysts have observed products with intermittent coverage protection for one or more vulnerabilities (i.e., sometimes it blocks an attack while sometimes it doesn't) that may have been due to architectural compromises.<sup>1</sup>

## Whose Throughput Numbers Are Correct?

So far we have discussed a number of factors that influence throughput and the various ways that vendors improve the performance of their network IPS devices. With these things in mind, it may be easier to understand how throughput numbers measured in ICSA Labs network IPS testing could differ – in some cases dramatically – from throughput numbers posted in vendor datasheets.

This stems from the fact that there is no standard set of network traffic to use when determining throughput and no standard method to create it. As a result network IPS vendors (and testing organizations) tend to test differently.

Some network IPS developers use a commercial tool to generate background network traffic. Though there may be a relatively limited selection of traffic types available, the developer tests while the tool is configured to have a traffic mix that they believe is sufficiently representative of what a network IPS might encounter in the real world. Other network IPS developers may use the same commercial traffic generation tool but instead only use HTTP traffic, believing that HTTP is one of the most taxing as well as one of the most common protocols in use today. Still others may use a commercial traffic generation tool from another tool vendor, with a mix of traffic believed to be representative by that network IPS developer. Still other vendors use home-grown tools to generate network traffic rather than be beholden to costly traffic generation tool vendors. And there are developers bit-blasting only UDP traffic with various average frame sizes. In addition to using home-grown and commercial traffic generation tools<sup>2</sup>, ICSA Labs and some vendors replay packet captures that were once live on real enterprise networks.

Still other factors contribute to differences in published throughput measurements. First, the policy enforced by each vendor's device may have been dramatically different when throughput determinations were made. Second, to realistically exercise their device some but not all network IPS developers may have woven attacks into the mix of background network traffic that was used when measuring throughput. Third, if attacks were in the mix, the attacks used by each vendor may have been different, targeting different vulnerabilities. Finally, there is no standard average frame size, number of new connections per second, number of concurrent connections, etc. that should be used when testing throughput.

Ultimately, vendors and testing organizations are free to test throughput however they choose. And because of the lack of uniformity the means and results can vary greatly when it comes to testing and measuring throughput.

Because there are so many differences in how throughput is determined from one vendor to the next, end users should be aware that there are limits on what can be gained when comparing the published throughput of devices made by different vendors. After all, throughput determinations are likely to have been measured differently, involved different traffic mixes, resulted from different traffic

---

<sup>1</sup> We are not talking about intermittent misses related to cases where the device is at or near its throughput limit which have been observed as well.

<sup>2</sup> ICSA Labs uses a traffic generation tool made by BreakingPoint Systems. For more information refer to <http://www.breakingpointsystems.com/>.

---

---

generation tools (not to mention different versions and configurations on the “same” brand of tool), used different average frame sizes, incorporated attacks in some but not all cases, and measured the throughput with varying policies applied. For all of these same reasons, ICSA Labs recommends that end users refrain from drawing conclusions about any differences in the published throughput for a vendor’s network IPS device and the throughput achieved during ICSA Labs network IPS testing of the same device.

The throughput portion of ICSA Labs network IPS testing<sup>3</sup> was designed to give end users insight into how the same device might perform in their environment when the device is configured to enforce a similar policy and when the device encounters a similar mix of traffic. Further, the throughput achieved during testing allows for an apples-to-apples comparison from one product tested by ICSA Labs to the next as our testing methodology is consistent across products.

## Summary

There are a number of factors that affect the throughput achieved while testing a stateful network IPS device. Among them are the policy being enforced and the properties of the background network traffic used in testing, such as the mix of protocols, the average frame size, and the number of new sessions being started per second. Network IPS developers often consider these factors and may implement hardware and other architectural changes to optimize the processing of network traffic. By making these changes, network IPS developers hope to improve throughput, without sacrificing security coverage protection.

Because throughput tests are likely to be performed under different circumstances, end users need to exercise caution when drawing conclusions about the differences between published throughput values. This is true for both any vendor-to-vendor throughput comparisons and any ICSA Labs-to-vendor throughput comparisons.

ICSA Labs publishes the throughput achieved during network IPS testing to give end users an idea of how the tested device might perform in a typical enterprise network, while enforcing a policy that provides sensible protection for the end user. Since they are consistent from device to device, ICSA Labs network IPS throughput tests provide end users with a useful metric for making throughput comparisons.

---

<sup>3</sup> In order to learn more about how ICSA Labs performs its network IPS testing, please refer to the initial sections of any ICSA Labs network IPS certification testing report and to the white papers written in 2006, all of which are still relevant: [https://www.icsalabs.com/icsa/topic.php?tid=6807\\$064ec1ee-3a54c0ac\\$dc20-41d3f014](https://www.icsalabs.com/icsa/topic.php?tid=6807$064ec1ee-3a54c0ac$dc20-41d3f014)

---

---

## Biography

### Jack Walsh, Intrusion Detection & Prevention/Anti-Spam Program Manager

Before coming to ICSA Labs, Jack Walsh worked at the National Security Agency (NSA) for 8 years primarily as an evaluator in the Trusted Product Evaluation Program. While at NSA, he helped author the first-ever US Government Firewall Protection Profile. Since then he has worked nearly 10 years at ICSA Labs. He was the Technical Lead in the Firewall Lab for over 4 years before being named Program Manager for the Network IPS Certification Testing Program. He is also the Program Manager for the ICSA Labs Anti-Spam Certification Testing Program. Jack earned his B.S. in Electrical Engineering from The Pennsylvania State University and his M.S. in Computer Science from Johns Hopkins University.

### David Koconis, Ph.D., Technical Lead Network Intrusion and Prevention

David Koconis joined ICSA Labs in July 2005. Prior to joining ICSA, he worked at the Institute for Security Technology Studies at Dartmouth College where he managed and was the lead developer of the Security Cybersleuth, a web-based service that collects and indexes computer security related information from open sources on the Internet. He is also a co-author of "Securing Linux-A Survival Guide for Linux Security" (ISBN: 0974372773). David earned his B.S. degree in Aerospace and Ocean Engineering from Virginia Tech and his M.S. and Ph.D. in Aeronautics and Astronautics Engineering from Stanford University.

## Who To Contact At ICSA Labs

For questions or comments about this paper contact Jack Walsh at [jwalsh@icsalabs.com](mailto:jwalsh@icsalabs.com) or David Koconis at [david.koconis@icsalabs.com](mailto:david.koconis@icsalabs.com). For more information regarding the ICSA Labs Network IPS Certification Testing Program or Network IPS Product Developers (NIPD) Consortium, visit <http://www.icsalabs.com/nips>.

## About ICSA Labs

ICSA Labs, an independent division of Verizon Business, offers vendor-neutral testing and certification of security products. Many of the world's top security vendors submit their products for testing and certification at ICSA Labs. Businesses rely on ICSA Labs to authoritatively set and apply objective testing and certification criteria for measuring product compliance and reliability. For more information about ICSA Labs, please visit: <http://www.icsalabs.com>.

## About Verizon Business

Verizon Business, a unit of Verizon Communications (NYSE: VZ), operates the world's most connected public IP network and uses its industry-leading global-network capabilities to offer large-business and government customers an unmatched combination of security, reliability and speed. The company integrates advanced IP communications and information technology (IT) products and services to deliver leading enterprise solutions including managed services, security, mobility, collaboration and professional services. These solutions power innovation and enable the company's customers to do business better. For more information, visit <http://www.verizonbusiness.com>.