TEST REPORT

Tolly.

#220132

September 2020

Commissioned by

Xena Networks

Safire Enterprise Firewall Testing

Evaluation of Enterprise-Class Firewalls

Executive Summary

Security is an essential element of every network and the firewall is at network security. Firewall architecture, platform and services configuration can impact both security and performance. Thus, to ensure delivering a superior user experience, it is necessary to benchmark firewalls to establish their performance limits. Xena Networks' Safire Enterprise Firewall Tester has been designed to provide exactly this benchmarking capability.

Xena Networks commissioned Tolly evaluate the capabilities and ease-of-use of the Safire Enterprise Firewall Tester. This was accomplished by running a series of tests on a leading enterprise firewall deployed as a virtual appliance. Additionally, Tolly established the raw throughput limits of the Safire solution.

Tolly tests confirmed the need for benchmarking firewalls as the Safire tests showed dramatically different firewall throughput levels based on the security policy and functions performed by the firewall. Back-to-back tests between ports of the Safire confirmed 10Gbps of throughput. Finally, testers noted the simplicity with which a test could be configured and run with automatic analysis of the raw results. For a summary of example performance results, see Figure 1. (cont.)

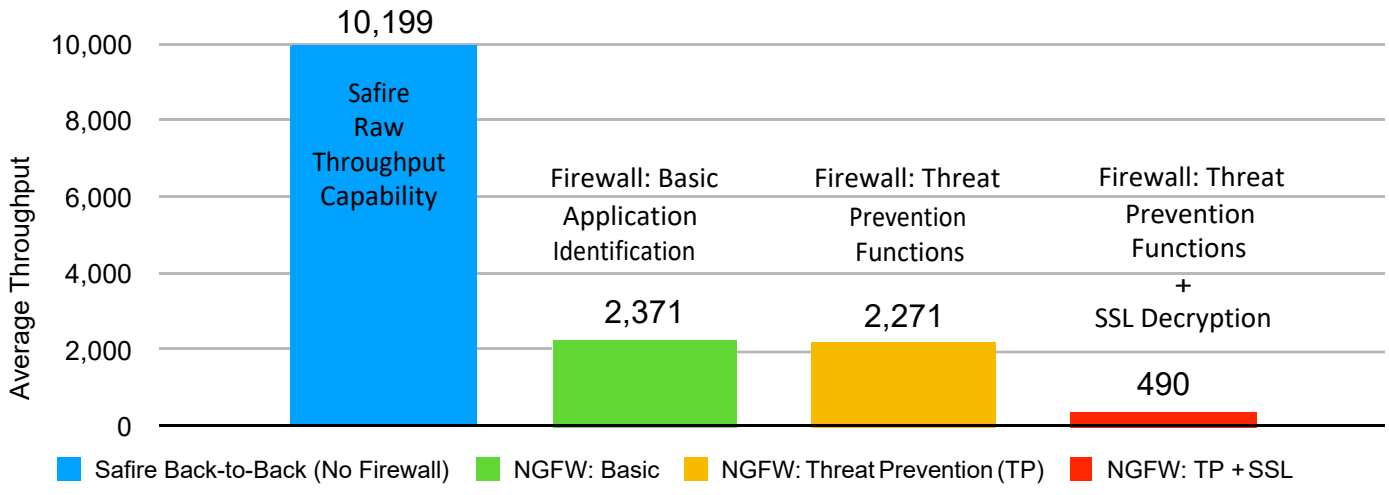
The Bottom Line

Xena Networks Safire Enterprise Firewall Tester provides:

1. 10Gbps bi-directional generation of application streams
2. Compatibility with any physical or virtual traditional or next-generation firewall
3. Range of traffic types including Office 365, Salesforce, Facebook, YouTube, and more
4. Automatic generation of custom traffic profiles from firewall log files.

Firewall Bi-Directional Throughput vs. Firewall Policy Configuration

Virtualized Next-Generation Firewall (NGFW) with 10GbE Interfaces



Notes: Threat Prevention profile includes Application Identification and Control, Anti-Virus, Anti-Spyware, Vulnerability Protection, URL Filtering and Data Leak Prevention. Safire back-to-back is raw throughput where NGFW results are firewall goodput.

Source: Tolly, August 2020

Figure 1

The Need for Firewall Benchmarking

Even a quick glance at Figure 1 reveals the most important finding of the study - that firewall throughput can and does vary dramatically based on the services one configures on the firewall. Importantly, without proactively benchmarking this throughput and establishing operational limits, networks cannot be designed properly.

In our example, the firewall is rated at 2Gbps. It delivers that throughput in the basic configuration and when the suite of threat prevention services are enabled. (A firewall with a less efficient architecture that requires multiple scans of packets would likely show a performance drop in the threat prevention scenario.)

However, when SSL cryptography functions are performed by the firewall, throughput drops to less than 25% of its basic and threat prevention throughput. Adding SSL to this firewall could instantly degrade the throughput of hundreds of existing users.

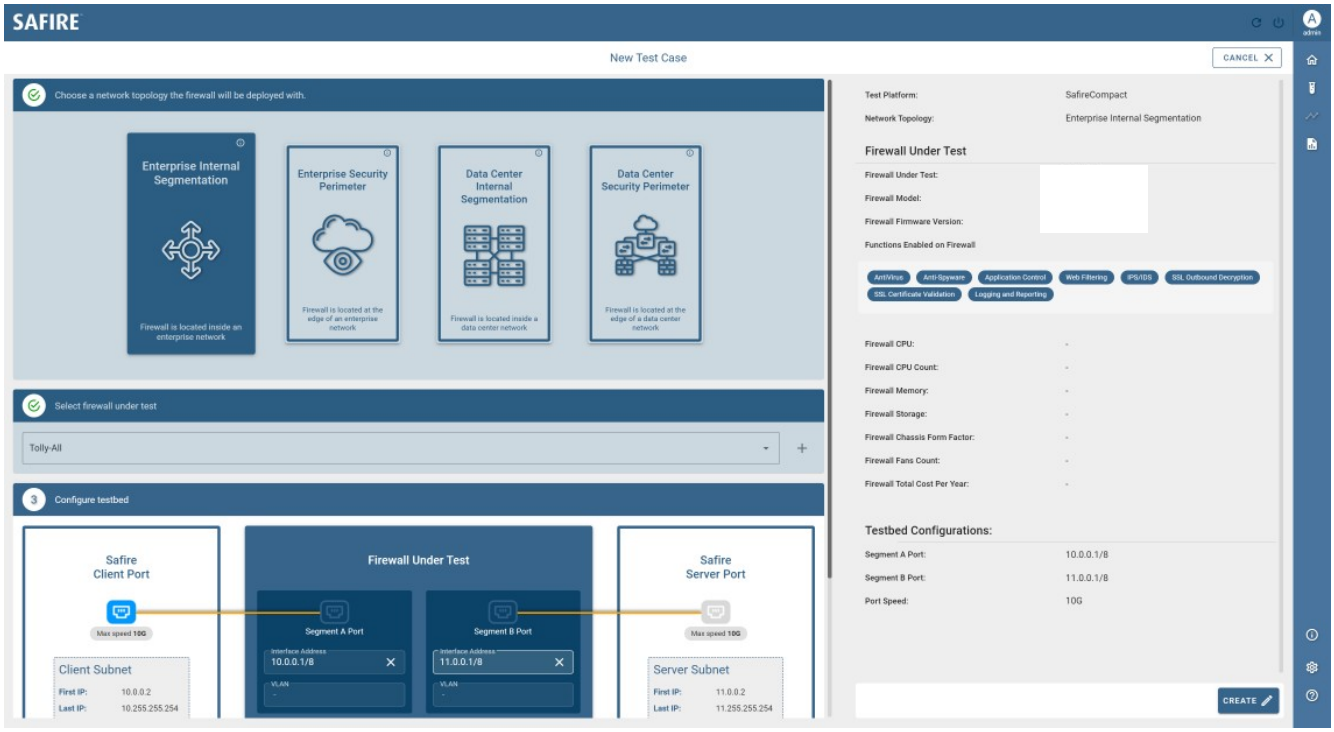
Only by running your own benchmarks can you be confident that your security perimeter can deliver the performance that you need.

In general, firewall vendors publish limited performance information about their firewalls. In most cases what performance information is published is "best case" performance when running only basic services. Such information is of little practical use if you are running more resource-intensive services.

Importantly, many firewalls are now available as virtual appliances. While this may reduce cost and simplify deployment virtual appliances raise new challenges with respect to performance.

Since the performance of virtual appliances depends completely on both the underlying hypervisor and CPU/network interface card

Safire Enterprise Firewall Tester GUI
Firewall Test Definition Main Screen



Source: Tolly, August 2020

Figure 2

hardware, firewall vendors cannot even begin to publish useful performance information as they cannot possibly foresee all of the different hypervisor/hardware configurations that might be in use. Again, without benchmarking the virtual appliance yourself you will have no way of establishing its operational performance capabilities.

With the need for firewall testing firmly established, one more step is needed and that is to "test the tester." The test tool must never be the bottleneck. The test environment must be able to achieve performance levels equal to or greater than the firewalls being tested. To prove this, we ran the firewall tester ports "back-to-back" without a firewall and validated that the tester could generate a full 10Gbps of line rate. See Figure 1.

Ease-of-Use

To maximize value, a test tool must be easy to use and this was the other focus area of this evaluation. In this report, we will look at three aspects of ease-of-use: 1) Test Setup, 2) Results Analysis, 3) Custom Traffic Profiles

Test Setup

Safire is completely GUI-driven. No "terminal" or command line interaction is required at any point. Firewall testing can be set up with a few clicks on a few screens. The main setup screen can be seen in Figure 2.

Traffic profiles are key. To evaluate performance correctly one must test using application traffic profiles that map as nearly as possible to the traffic mix of the production network where the firewall will be deployed. Depending upon the firewall deployment option, Safire will suggest appropriate traffic profiles.

Safire can be configured to generate traffic that simulates dozens of specific applications. These include Microsoft Office 365, Salesforce, Dropbox, Facebook and many others.

Xena Networks

Safire Enterprise Firewall Tester

Performance and Feature Evaluation *Tested August 2020*

Tolly. Certified

Safire Enterprise Firewall Tester GUI
Define/Select Test Traffic Profiles

Source: Tolly, August 2020

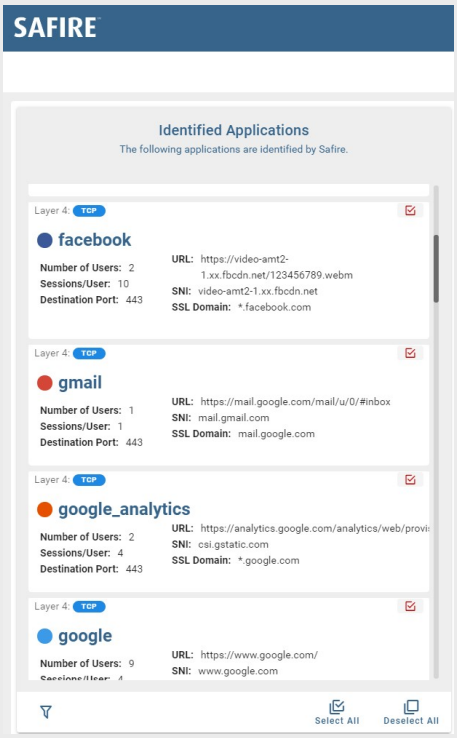
Figure 3

Additionally, Safire comes with predefined traffic profiles that can be used for tests or can be used as a starting point for customization. Traffic types can be easily enabled or disabled using sliders. An example traffic profile screen can be seen in Figure 3.

Results Analysis: Automatic Comparisons

It is important not only to understand the absolute performance of a firewall but also the performance between different implementations, vendors or feature sets. Making manual comparisons can become tedious work. Safire can automatically generate comparison charts for any of the firewall tests that have been run on the unit. See Figure 4 for an example comparison chart.

Safire Custom Traffic Profile Generation



When test traffic closely matches your current or planned network environment, the test results will always be more meaningful.

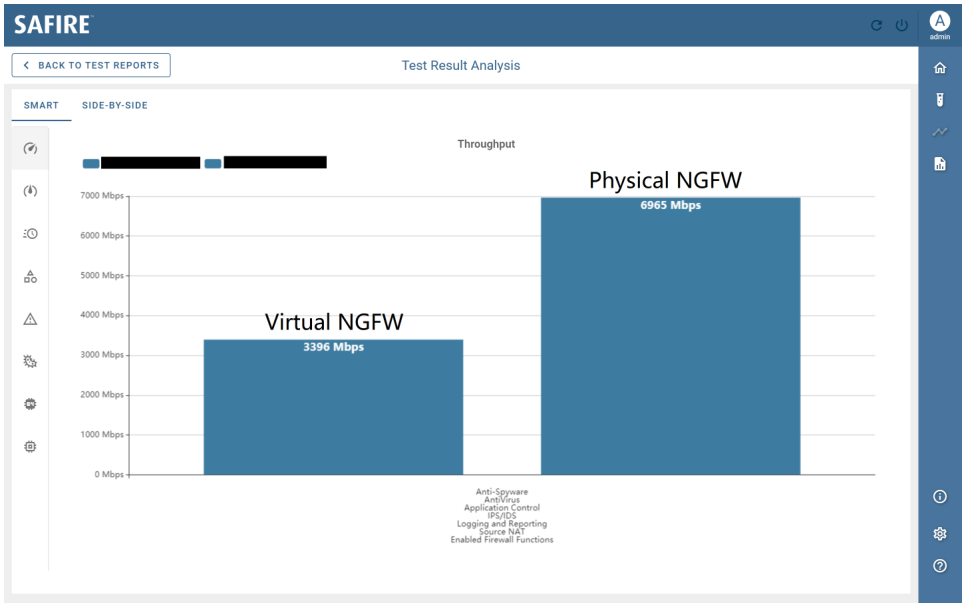
Safire has the capability of importing log data from firewalls, analyzing the data and generating a proposed traffic profile based on the log.

The screen to the left shows a partial view of application identification.

Traffic can then be further customized by the user for various mixes and rates to help benchmark for future network traffic conditions.

Source: Tolly, August 2020

Safire Enterprise Firewall Tester GUI
Automatic Comparison Generation



Source: Tolly, August 2020

Figure 4

Test Setup & Methodology

Testing was focused on illustrating the use of the Safire Enterprise Firewall Tester on a representative next-generation firewall (NGFW) implemented as a virtual appliance. As the point of the test was confirm that changes in services and policy configuration do impact performance, the specifics of the firewall and its environment are not relevant. Xena Networks Safire C-SAFER-24PE-10G versions 2.2.3 and 2.3.1 (generate traffic profiles from logs) were used for the testing. The unit is a 1u appliance with two 10GbE ports.

Test Scenarios

Engineers ran four test scenarios using Safire. In all cases, traffic flowed between two 10GbE networking ports of Safire.

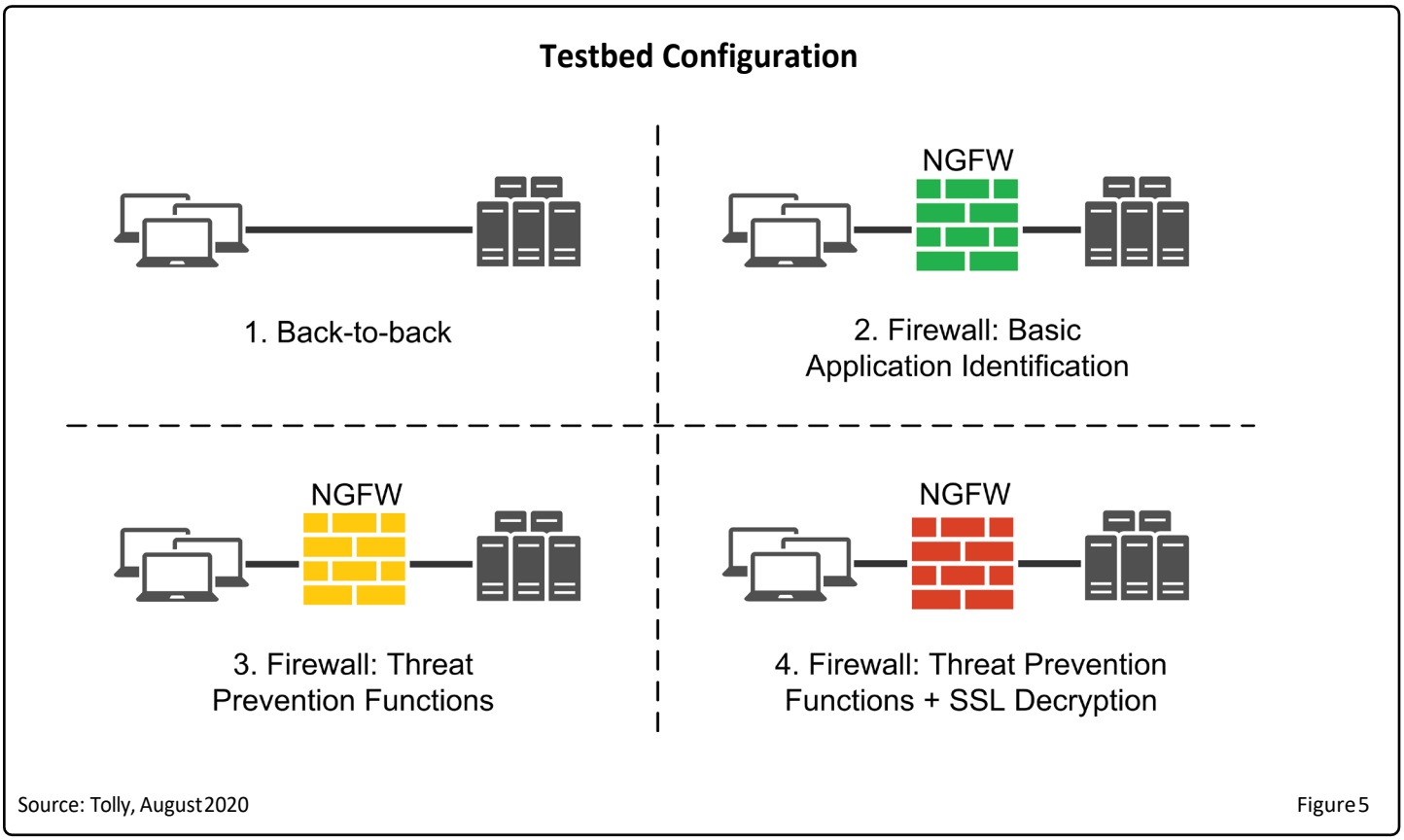
In the first scenario, no firewall was used. Rather, the two ports of the Safire were connected to each other in a "back-to-back" configuration. This scenario was used to establish the maximum throughput between the two Safire ports when no device under test was present.

In the remaining three scenarios, the firewall under test was connected to the two Safire ports. The configuration of the firewall, and thus its workload, was different for each scenario.

Initially, the firewall was tested with basic Application Identification Control enabled. This would generally deliver the best throughput.

For the next test, the Threat Prevention profile was enabled. For this firewall, that profile included the following functions: Application Identification and Control, Anti-Virus, Anti-Spyware, Vulnerability Protection, URL Filtering and Data Leak Prevention. These functions, or a subset thereof, would be typical features to be enabled. This profile would illustrate the performance of the firewall with significant packet inspection functions enabled and would generally be lower than the prior scenario.

Finally, SSL decryption was enabled for the firewall. This is the most resource intensive function as the decryption function is processor intensive. This would generally show lower throughput because of the higher processing burden. For a summary of the testbed configuration, See Figure 5.



Source: Tolly, August 2020

Figure 5

About Tolly

The Tolly Group companies have been delivering world-class information technology services for over 30 years. Tolly is a leading global provider of third-party validation services for vendors of information technology products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

About Safire & Xena Networks

See https://xenanetworks.com/safire

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

220132 yf-1 wt-2020-09-23—VerF