BREACH DETECTION SYSTEMS COMPARATIVE REPORT

Performance

OCTOBER 19, 2017

Author – Thomas Skybakmoen

Tested Products

Check Point Software Technologies 15600 Next Generation Threat Prevention & SandBlast™ (NGTX) Appliance R77.30

Cisco FirePower 8120 v.6 & Cisco AMP v.5.1.9.10430

FireEye Network Security NX 10450 v7.9.2 & EX 8400 v7.9.0

FireEye Network Security 6500NXES-VA v7.9.2

Fortinet FortiSandbox-2000E v.FSA 2.4.1 & FortiClient (APT Agent) v.5.6.0.1075

Lastline Enterprise v7.25

Trend Micro Deep Discovery Inspector Model 4000 v3.8 SP5 & OfficeScan (OSCE) v.12.0.1807

Environment

Breach Detection Systems Test Methodology v4.0

Overview

Implementation of breach detection system (BDS) can be complex, with multiple factors affecting the overall performance of a solution.

The following factors should be considered over the course of the useful life of the product:

- Where will it be deployed?
- What is the predominant traffic mix?
- What security configuration/policy is applied?

There is frequently a trade-off between security effectiveness and performance. Because of this trade-off, it is important to judge a product's security effectiveness within the context of its performance and vice versa. This ensures that new security protections do not adversely impact performance and that security shortcuts are not taken to maintain or improve performance.

Sizing considerations are critical, as vendor performance claims (where protection typically is not enabled) can vary significantly from actual performance (where protection is enabled). Figure 1 depicts network-based vendors and their bandwidth performance. NSS Labs rates throughput based on the average results of the Enterprise Perimeter and Financial "real-world" protocol mixes, and on 21 KB HTTP response-based capacity tests.

Note that all performance tests are repeated at 25%, 50%, 75%, and 100%[1] of the maximum rated connections of the BDS (see the Breach Detection Systems Test Methodology, available at www.nsslabs.com). At each stage, multiple malware files are passed through the network, and the number detected is logged. The first stage at which one or more attacks are not detected is recorded as the maximum performance. The maximum values shown are the first stage at which one or more attacks are not detected.

[1] The 100% load will actually be less than 100% to allow headroom for malicious traffic.

Table of Contents

Table of Figures

Analysis

As part of the initial BDS test setup, products are tuned as deemed necessary by the vendor. Every effort is made to deploy policies that ensure the optimal combination of security effectiveness and performance, as would be the aim of a typical customer deploying the device in a live network environment. This provides readers with the most useful information on key BDS security effectiveness and performance capabilities based on their expected usage.

Figure 1[2] depicts the difference between the NSS performance rating and the vendor performance claims, as vendor tests are often performed under ideal or unrealistic conditions. Where vendor marketing materials list throughput claims for both TCP (protection-enabled numbers) and UDP (large packet sizes), NSS selects the TCP claims, which are more realistic. Therefore, *NSS-Tested Throughput* typically is lower than the throughput claimed by vendors, and often significantly so, since it is more representative of how devices will perform in real-world deployments.

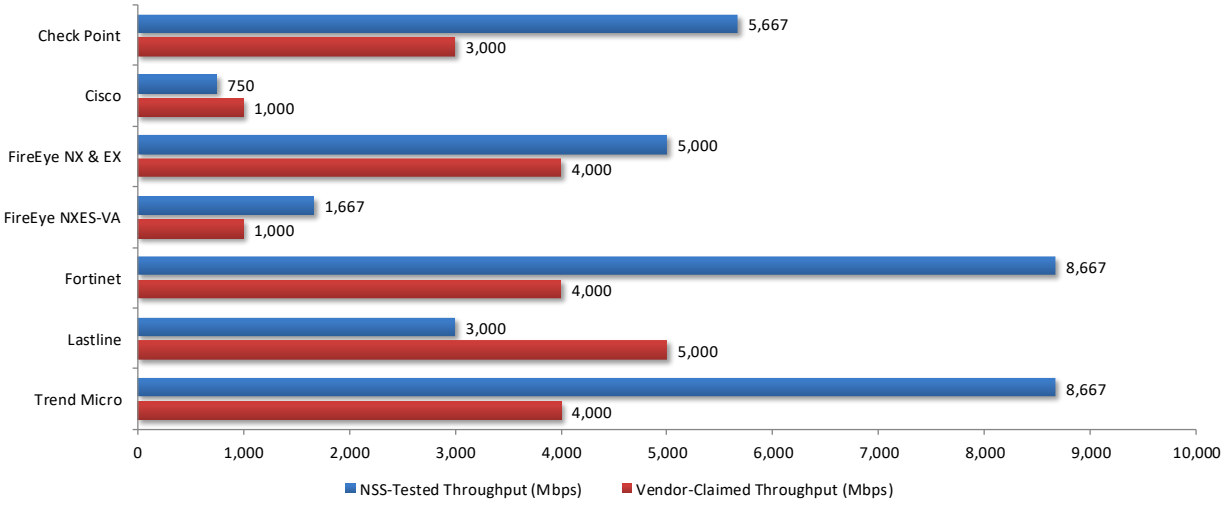

Figure 1 – Vendor-Claimed vs. NSS-Tested Throughput (Mbps)

HTTP Connections per Second and Capacity

BDS exhibit an inverse correlation between security effectiveness and performance. The more network background traffic there is, the higher the chance that the traffic will not be inspected and that malicious traffic will go undetected. Furthermore, it is important to consider the real-world mix of traffic that a device will encounter.

NSS tests aim to stress the HTTP detection engine to determine how the network sensor copes with detecting and blocking exploits under network loads of varying average packet size and varying connections per second. By creating genuine session-based traffic with varying session lengths, the sensor is forced to track valid TCP sessions, thus ensuring a higher workload than for simple, packet-based background traffic.

[2] Figure 1 depicts vendors that offer a network-based BDS.

Each transaction consists of a single HTTP GET request, and there are no transaction delays; that is, the web server responds immediately to all requests. All packets contain valid payload (a mix of binary and ASCII objects) and address data. This test provides an excellent representation of a live network (albeit one biased toward HTTP traffic) at various network loads.

HTTP Connections per Second and Maximum Capacity (Throughput)

Figure 2 through Figure 6 depict the maximum throughput achieved across a range of HTTP response sizes that may be encountered in a typical corporate network.

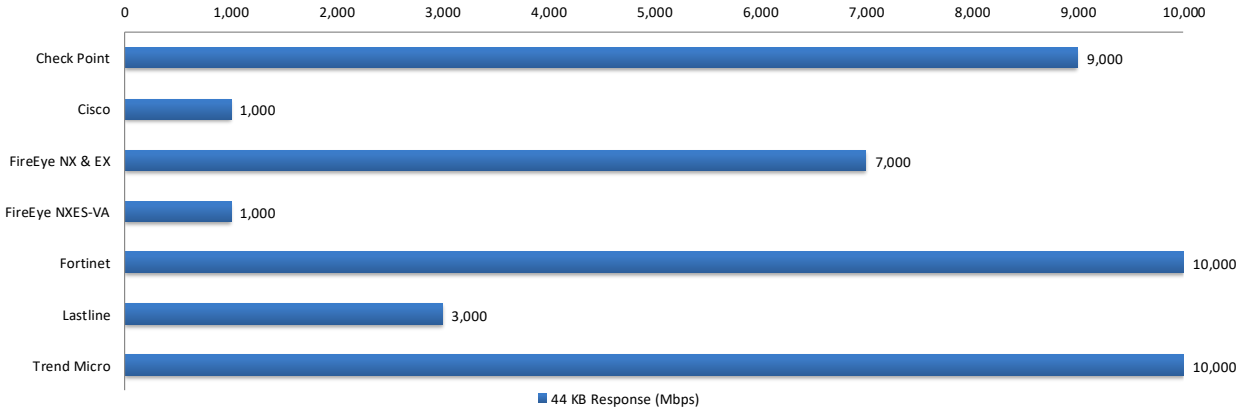

Figure 2 – Maximum Throughput per Device with 44 KB Response

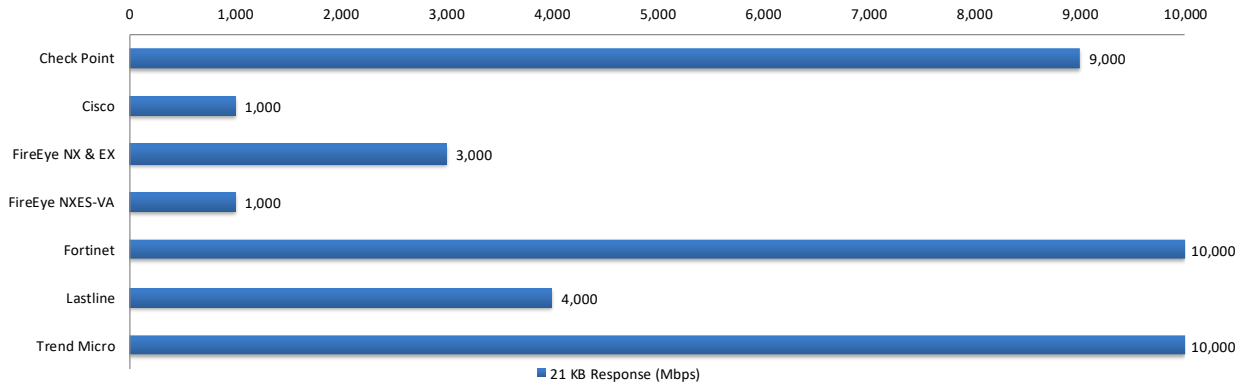

Figure 3 – Maximum Throughput per Device with 21 KB Response

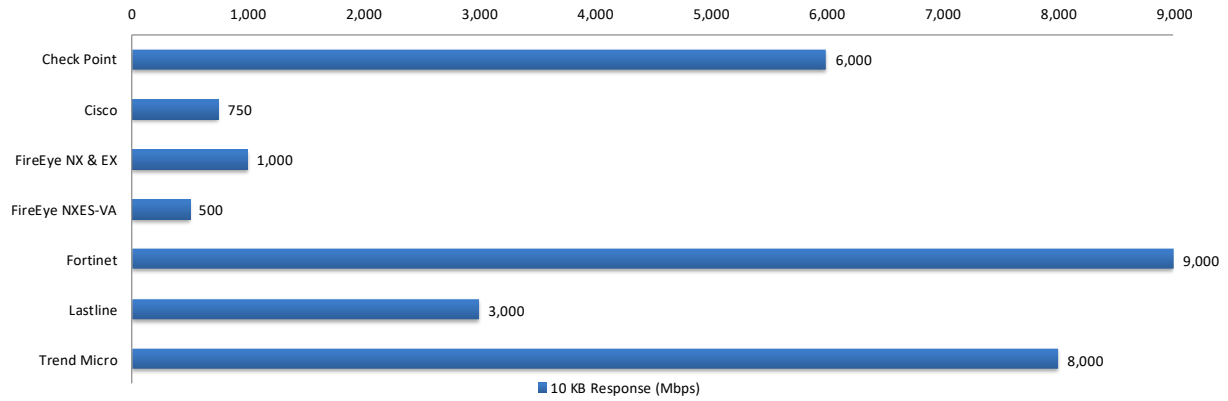

Figure 4 – Maximum Throughput per Device with 10 KB Response

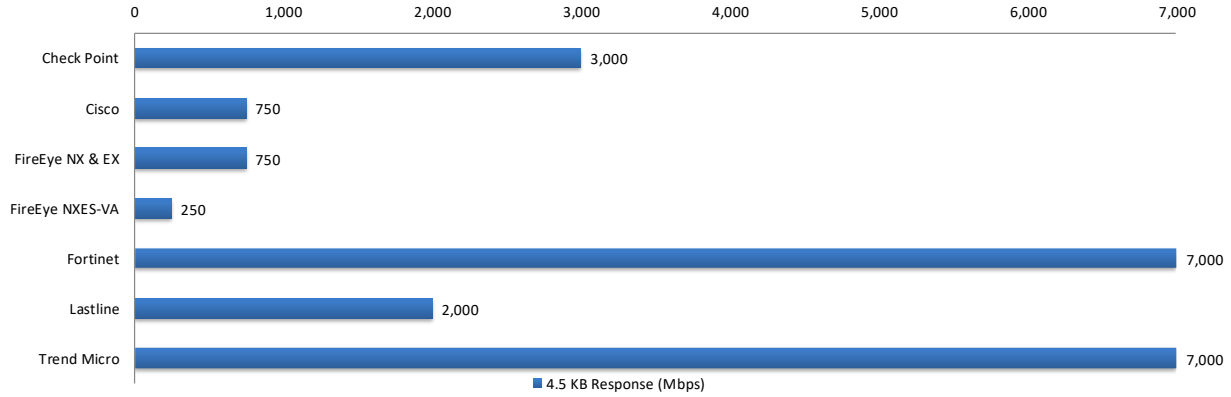

Figure 5 – Maximum Throughput per Device with 4.5 KB Response

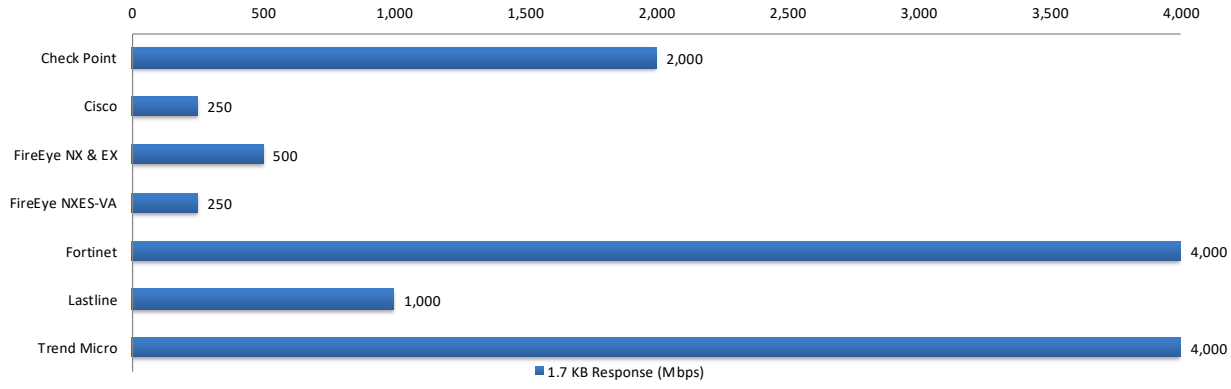

Figure 6 – Maximum Throughput per Device with 1.7 KB Response

Real-World Traffic Mixes

These tests aim to measure the performance of the system under test in a "real-world" environment by introducing additional protocols and real content, while still maintaining a precisely repeatable and consistent background traffic load. In order to simulate real use cases, different protocol mixes are utilized to model placement of the system within various locations on a corporate network.

For details about "real-world" traffic protocol types and percentages, see the Breach Detection Systems Test Methodology.

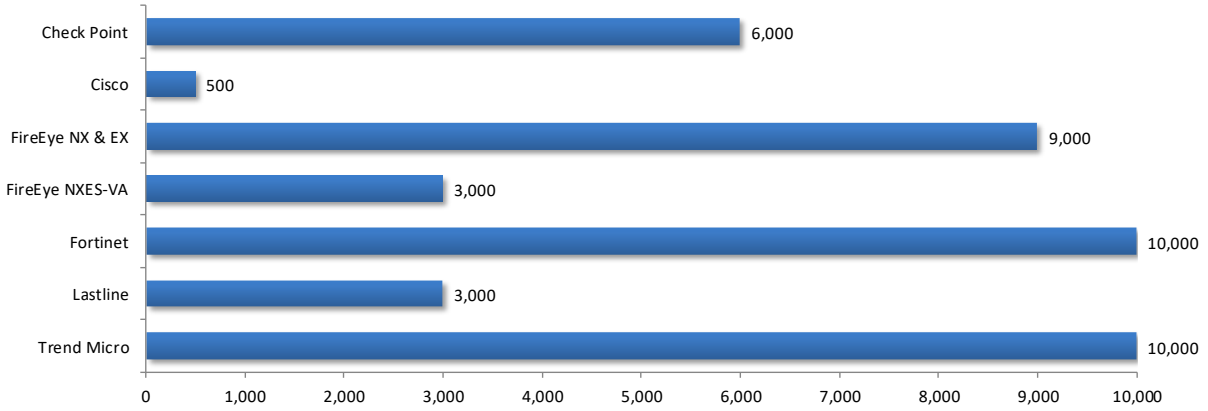

Figure 7 – "Real-World" Protocol Mix (Enterprise Perimeter)

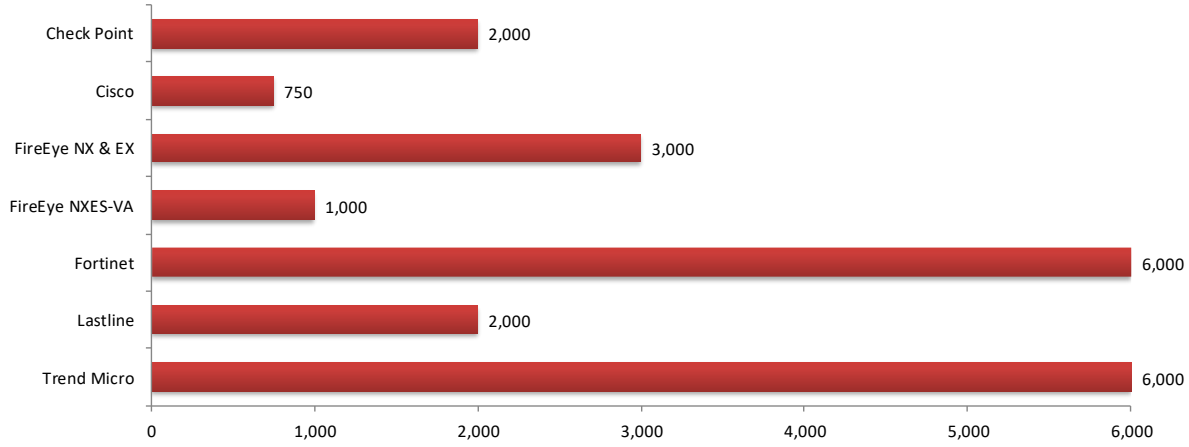

Figure 8 – "Real-World" Protocol Mix (Financial)

Test Methodology

Breach Detection Systems (BDS) Test Methodology v4.0

A copy of the test methodology is available at www.nsslabs.com.

Contact Information

NSS Labs, Inc.
3711 South MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com