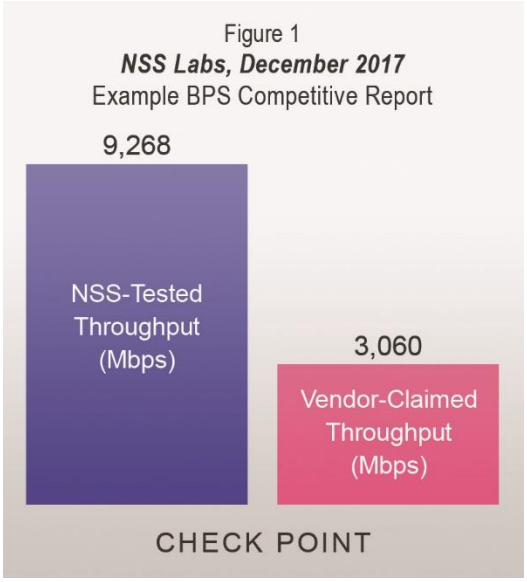
ENTERPRISE SECURITY PERFORMANCE: TESTING AND SIZING

In the past, security appliance selection was based on artificial lab testing conditions when the device is operating at maximum capacity. The appliance was tested in lab conditions with a simple firewall-only security policy with only one allow-all traffic rule. Though the results of these tests yielded a very high throughput number, it did little to forecast the capability to meet customers' security requirements in real world conditions. In essence, it is a measure of a device's maximum forwarding rate and says little of a device's performance when deployed at a customer site.

With increasing security threats and their sophistication in today's world, threat prevention appliances perform advanced security functions under constantly rising traffic volumes. In this new environment, it can be challenging to choose the right appliance to meet your security objectives, performance requirements, and growth expectations. To solve this problem, in 2012 Check Point introduced our Appliance Sizing Tool. The sizing tool was developed from testing security appliances in a typical configuration and using a realistic traffic blend of that time, called "SecurityPower" that was representative of data collected from about 500 production environments at the time.

Figure 1
NSS Labs, December 2017
Example BPS Competitive Report



Fast forward a few years and we now have telemetry data from tens of thousands of reporting devices. Not surprising to most, our analysis reflects what others report that there is a shift towards HTTPS; 69% according to the Google Transparency Report [1] which closely matches the 70% we find in our assessment. There is also an expected increase of media content; up to 82% of all IP traffic for consumer and business will be video[2] by 2021. In addition to traffic we also analyzed how well our security appliances were performing, gathering memory consumption and CPU utilization statistics.

So how well did our early model do in calculating a recommended appliance to match customers' requirements? In short, we found our early model erred on the conservative side. The majority of the installed gateways were over-sized for the customer's needs with about 70% operating at 9% or lower CPU utilization during peak traffic periods. This has also been verified in third party tests like that of NSS Labs where the figure depicts the difference between NSS-Tested throughput and vendor performance claims, as vendor tests are often performed under preferred or unrealistic conditions.[3]

CUTTING CORNERS

Whilst we strive to introduce the real world conditions to performance testing, we know the playing field is not level. The configuration of modern security appliances has a massive impact on performance and throughput capacity. If you remove or disable certain aspects of traffic inspection, an appliance will perform better.

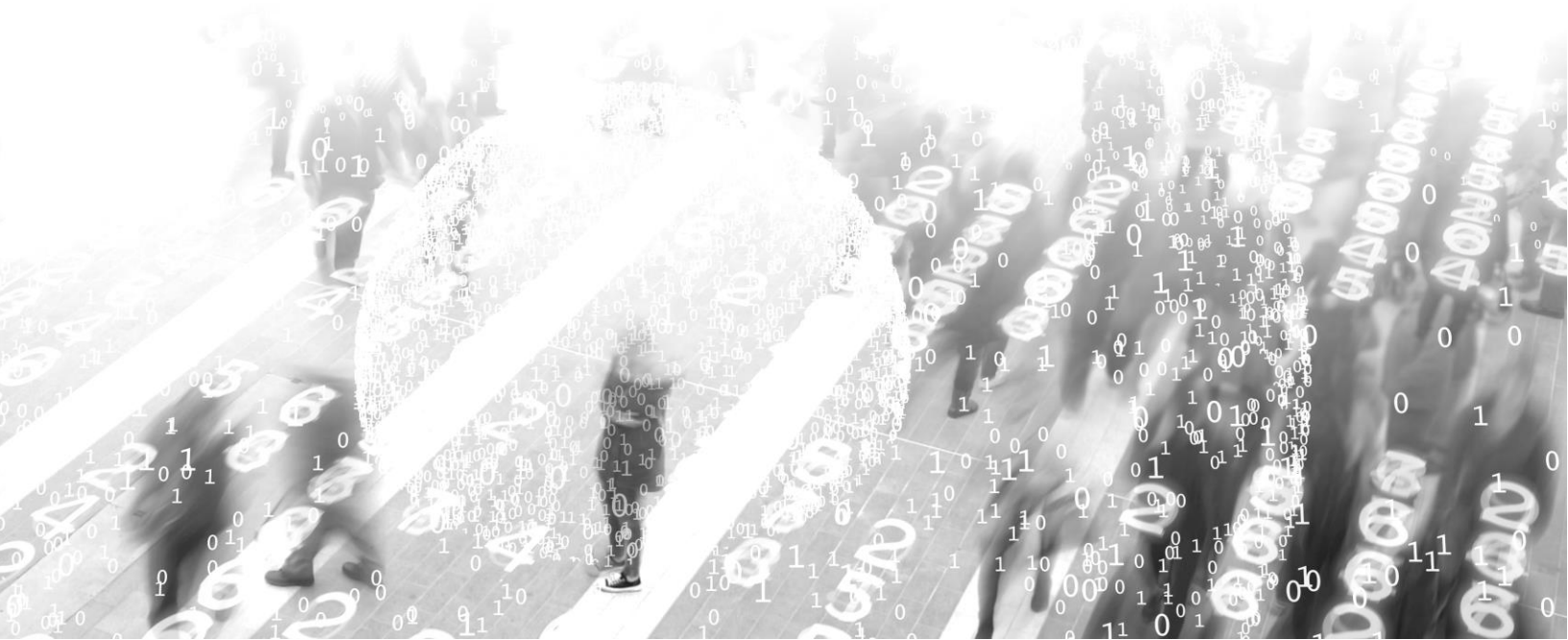
> "…the tyranny of the default is sort of the expression I like to use for that most users don't go in and change things. They just assume that someone smarter than them chose the settings that are best for them…So what that means is that, if it's enabled by default, it'll tend to stay on." Steve Gibson on Security Now Podcast[4]

Members of the security community likely know that defaults such as default passwords need to be changed, but can they also be expected to know of other defaults that change the security effectiveness of their new security appliance? Defaults that bypass inspection such as scanning traffic in one direction and scanning only the beginning of the packet can improve performance, but if you don't know about them they can also expose your organization to threats from hackers who have done their research.

> "…When you cut corners, you're not finding simpler ways to accomplish important tasks. Instead, you're eliminating important tasks…and therefore, compromising the quality of the results." Take Shortcuts or Cut Corners?[5]

This is a problem that can be addressed in Proof of Concept (PoC) exercises. If you are doing a PoC test, configure the box according to the vendor's recommended security configuration. This means inspection is not bypassed, threat prevention signatures are up to date and the settings provide a similar level of security effectiveness.

The traffic load used for testing must include a variety of threat vectors e.g. transport over HTTP, Email, and SMB etc. whilst also employing evasion techniques. Results must measure both the throughput achieved and the number of threats detected for an accurate reflection of the relative capabilities.



MEASURING PERFORMANCE

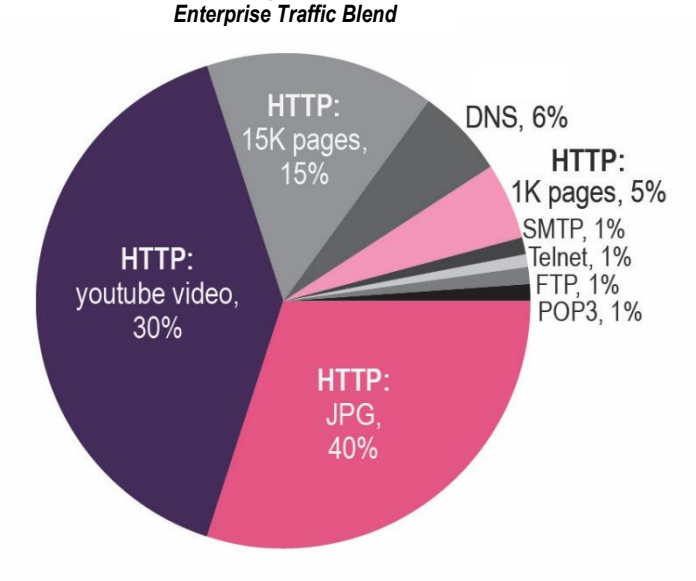
When you examine the detail of performance testing figures on vendor datasheets how often do you see the caveat "Performance and capacities are measured under our preferred testing conditions"? Or there is little to no explanation of the traffic blend or the configuration of the device in the test. Sizing and capacity decisions based on such figures cannot be trusted. In "Preferred testing conditions", the very security that you need to mitigate threats to your organization may be disabled.

You need a meaningful benchmark to make an informed decision when purchasing your new security appliance. Ideally, every vendor would test against the same realistic configuration and traffic blend and make this available in their public collateral. Alas, this has proven to be an unrealistic expectation. At Check Point, our goal is to provide you with the latest, most realistic expectations of how our appliances perform in real-world conditions. Towards this end we've updated our Appliance Sizing Tool to provide you with a more realistic recommendation based upon our 5+ years of analysis. We've updated our traffic blend and the test conditions. Here is how the new Enterprise benchmark differs distinctly from "Preferred testing conditions" benchmarks.

Figure 2
Enterprise Test vs. Preferred Test

	Enterprise Test	Preferred Testing Conditions
Protocols	Typical blend of HTTP, SMTP, HTTPS, DNS, FTP and other protocols derived from research conducted over hundreds of customer environments	HTTP only
Content Types	Realistic blend	Page loads only
Transaction Size	Variety of sizes	Simple, large HTTP transactions
Security Configuration	Full security	Default inspection settings designed for performance over security

Figure 3
Enterprise Traffic Blend



TEST METHODOLOGY

When assessing the capacity required from an appliance, there are three key factors that must be consistent:

- Configuration of the Device Under Test (DUT)
- The load testing apparatus
- The traffic profile

The configuration of the device and the load testing apparatus is consistent for all Check Point security appliances.

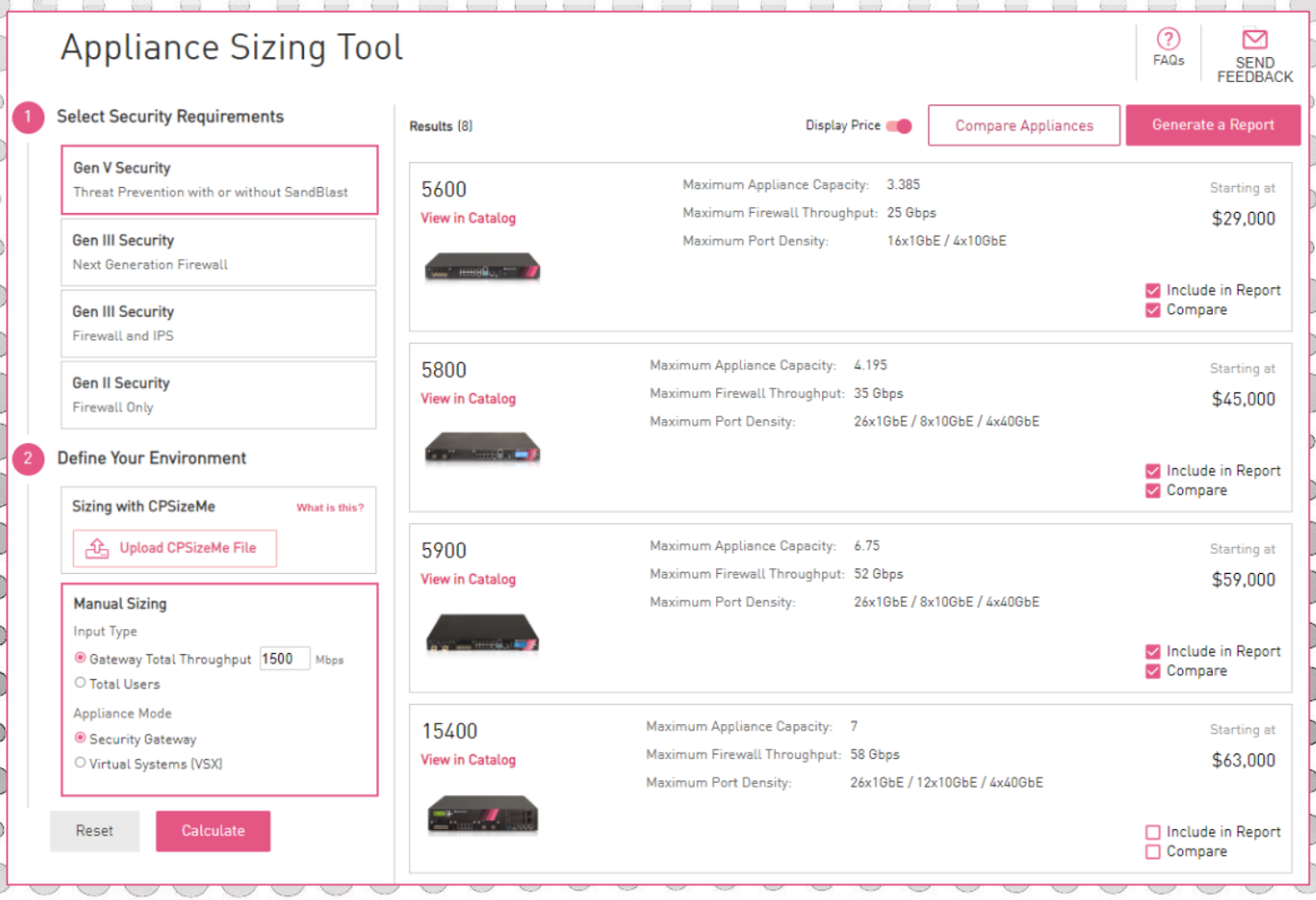
APPLIANCE SIZING TOOLS

Traditional stateful inspection requires relatively little processing power compared to advanced security functions such as application control, antivirus, or IPS, which requires inspecting traffic payloads at different layers, and consumes far more system resources. In addition, Zero-day Protection requires extracting and sending files for analysis of malicious behaviors in a virtual sandbox in the cloud. Check Point provides sizing tools for our customers and partners alike such as the "Appliance Sizing Tool" and "Check Point Size Me" to assist in choosing the appropriate appliance. These tools measure the specifications of an environment and provide the recommended solution sized to the company needs. With Check Point you can consolidate these security functions into a single platform, reducing costs and improving your security posture. Our appliance sizing tool combines two key metrics to help you select the appropriate appliance:

- Throughput
- Required security functions

With the Appliance Sizing Tool for example, you set the total expected gateway throughput or the number of users and which security functions you want to enable. We then provide a set of recommended appliances that is best suited for you.

Figure 4
Recommended Appliances Allowing Room for Growth



SUMMARY

Performance testing is a complex business; the permutations of configuration are so vast that exact answers are impossible. Check Point provides a practical means to measure your security and traffic throughput requirements, translating those into a solution to meet your needs today and in the future.

REFERENCES

1. Google Transparency Report
https://transparencyreport.google.com/https/overview?hl=en
2. Cisco, The Zettabyte Era: Trends and Analysis
https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html
3. NSS Labs, Example Breach Prevention Systems Test Report, December 2017
https://pages.checkpoint.com/nsslabs-bps-sandblast-1.html
4. Security Now Episode 364, Mat Honan's Very Bad Weekend, August 2012
https://www.grc.com/sn/sn-364.htm
5. How-to build a brand, Take Shortcuts or Cut Corners?, May 2017
https://howtobuildabrand.org/branding/take-shortcuts-or-cut-corners/

CONTACT US
Worldwide Headquarters | 5 Shlomo Kaplan Street ,Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | www.checkpoint.com