CHECK POINT REAL WORLD PERFORMANCE TESTING

NEXT GENERATION THREAT PREVENTION DEMANDS REAL WORLD METRICS

In the past, appliance selection was based on one criterion – firewall throughput. The security 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 equated to measuring the power of a car only by its maximum speed, driving downwind and downhill.

With increasing security threats and their sophistication in today's world, threat prevention appliances must 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. CPU core counts, quantity of RAM, and Network Interface Card (NIC) speed alone are not enough to determine how a given hardware appliance will perform in the real world. We need a new metric that takes into account how underlying components combine to deliver a realistic threat prevention work load.

SecurityPower is that new metric.

SECURITYPOWER IS A REAL WORLD PERFORMANCE METRIC

SecurityPower

The new way to measure the **real power** of security appliances

Old Way Firewall Throughput			New Way SecurityPower		
Based on lab conditions	Only Firewall Security	Single firewall rule	Based on real-world customer traffic	Advanced security functions	Typical security policy

RFC BASED TESTING METRICS LEAD TO NUMEROUS ERRORS IN APPLIANCE SIZING

May 31, 2016

REAL WORLD PERFORMANCE CAPABILITY AND CAPACITY OF SECURITY APPLIANCES

WHAT IS SECURITYPOWER?

SecurityPower is a new measure of the real power of security appliances. A benchmark measuring the capability and capacity of an appliance, SecurityPower tests multiple advanced security functions (Software Blades) such as IPS, Application Control, Antivirus, URL Filtering, and DLP, using real world traffic conditions and a typical security policy. SecurityPower provides an effective metric in evaluating an appliance, predicting its current and future behavior under security attacks and day-to-day operation. SecurityPower capacity can be measured by third parties, both for Check Point appliances as well as security appliances of other vendors.

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 ideal testing conditions”? Sizing and capacity decisions based on such figures cannot be trusted. In “Ideal 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. The Check Point SecurityPower benchmark differs distinctly from “Ideal testing conditions” benchmarks.

	Real World	Ideal Testing Conditions
Signatures	Latest, up to date IPS recommended signatures	Out of the box signatures
Security Policy	Realistic security policy with 100 rules matching test profile traffic	Any-Any-Any-Accept
Traffic Blend	A real life mix of HTTP, SMTP, HTTPS, DNS, FTP and other protocols derived from research conducted over hundreds of customer environments	Simple large, HTTP transactions
Traffic Content	Real world content as seen in customer environments, e.g. HTTP traffic from popular web pages; Google, Amazon, Facebook, etc.	Simple repetitive content
Features	Logging and NAT enabled	Logging and NAT disabled

Production Environment Performance[1]	
SecurityPower™ Units (SPU)	6,200 SPU
Firewall throughput	43 Gbps
IPS throughput	12 Gbps
NGFW throughput (Firewall, Application Control, IPS)	7.2 Gbps
Threat prevention throughput[2]	3.6 Gbps
Ideal Testing Conditions Performance (RFC 3511, 2544, 2647, 1242)	
Firewall throughput, 1518 byte UDP	128 Gbps
Connections per second	200,000
Concurrent connections	12.8 to 28[3] million
VPN throughput, AES-128	26 Gbps
IPS throughput	30 Gbps
NGFW throughput (Firewall, Application Control, IPS)	27 Gbps

Appliance Performance

Recommended Signatures

The Check Point Security Research Group is responsible for our “Recommended IPS Profile”. Emerging IPS signatures detect the most important and current attacks whilst maintaining a predictable performance impact. The Check Point SecurityPower benchmark includes the latest available and recommended signatures. This is used in the performance testing of our security appliances and available in our published datasheets.

PRACTICAL APPLICATION OF SECURITY POWER UNITS

HOW TO USE SECURITYPOWER UNITS (SPU)?

Security requirements can be converted into a SecurityPower value. Each Check Point appliance has a SecurityPower capacity as measured by our performance labs. We compare your needs against the real-world capabilities of our appliances allowing you to determine which appliances meet your needs today and in the future.

LEVERAGE APPLIANCE SIZING TOOL TO CONVERT CUSTOMER NEEDS TO REQUIRED SPUs

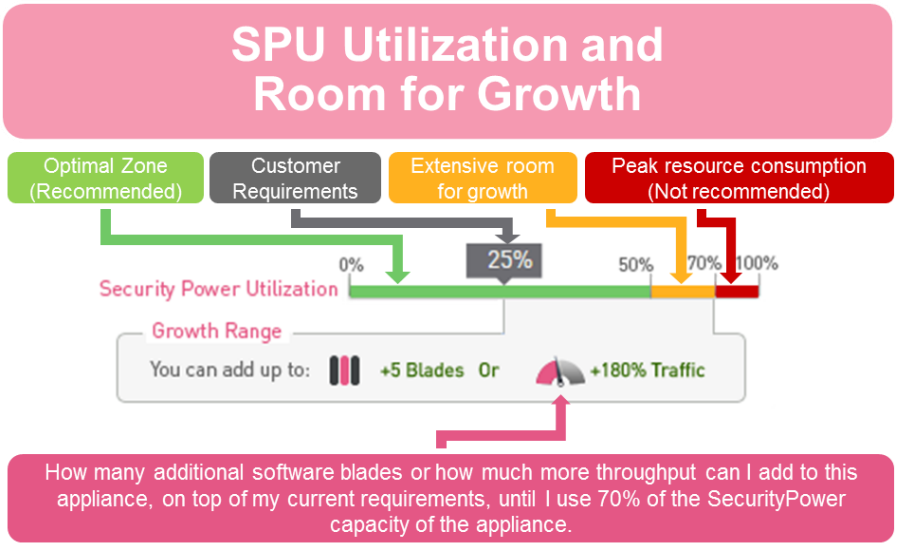
APPLIANCE SIZING TOOL

Traditional stateful inspection requires relatively little processing power compared to advanced security functions such as Application Control, Antivirus, or IPS which requires much deeper analysis and consumes more system resources. 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 correct appliance:

- Throughput
- Required security functions

We translate your environment and security requirements into a required SecurityPower value. This value is then checked against the SecurityPower Capacity offered by Check Point appliances. The end result of the comparison is a small set of recommended appliances appropriate for you.

APPLIANCE SIZING TOOL PROVIDES ROOM TO GROW



SECURITY**POWER TEST METHODOLOGY**

When assessing the capacity required from an appliance three key factors 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 appliances. See our General Assumptions and Testing Methodology.

To reflect different deployment scenarios, we define two different traffic profiles: the Data Center and Internet blends. These traffic blends are the result of in-depth customer analysis.

INTERNET TRAFFIC BLEND REFLECTS TYPICAL MIX OF TRAFFIC SEEN THROUGH AN INTERNET GATEWAY WITH PREDOMINANTLY WEB BROWSING TRAFFIC

Internet Traffic Blend

- Represents the type of Internet traffic, security appliances handle on a day-to-day basis.
- Consists of the following Streams/Protocols: HTTP; HTTPS; SMTP; DNS; POP3; FTP; Telnet.
- The majority of the traffic is Internet Access (HTTP).

GROWING TREND IN HTTPS TRAFFIC

The growing trend in Internet traffic blend towards HTTPS encryption is built into the Appliance Sizing Tool and we are able to factor a specific proportion of customer traffic from the basic mix above (10% HTTPS) all the way up to 100% HTTPS.

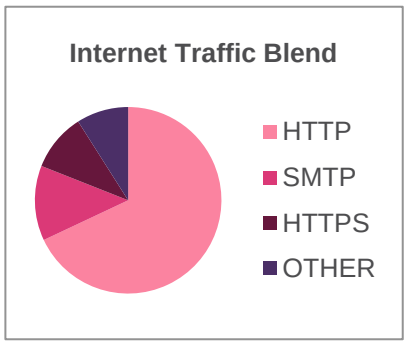
DATA CENTER TRAFFIC BLENDS TYPICALLY CONSUME 20% MORE SPU

Data Center Traffic Blend

The Data Center blend reflects the predominance of the following traffic characteristics:

- Web Services, File Stores, Authentication Services, Line-of-Business Applications, Custom Applications and Data Intensive Applications.
- Consists of the following Stream/Protocols: HTTP, HTTPS, SMTP, SMB_CIFS, SQL, NFS, SMB_DCERPC, Oracle, DNS, LDAP, SSH, FTP.

The Data Center traffic blend consumes approximately 20% more SPU than the Internet traffic blend.



Internet Traffic Blend

Protocol	Content	Action	Per Cent
HTTP	Amazon Home Page	HTTP GET -> 676K	16%
	Yahoo Home Page	HTTP GET -> 292K	16%
	Facebook Home Page	HTTP GET -> 271K	16%
	Google Home Page	HTTP GET -> 41K	17%
	Google Mail	HTTP GET of Gmail index.html file, 21K	2%
	HTTP Post	100K PDF File	1%
SMTP	SMTP 17K	MIME Message with PDF attachment	7%
	SMTP 100K	MIME Message with Word attachment	6%
HTTPS	HTTPS 10K	HTTPS GET of 10K file	5%
	HTTPS 100K	HTTPS GET of 100K file	5%
Other	DNS	DNS Query	6%
	POP3	Message size: 256-512 bytes	1%
	Telnet	Login; cd /disk/images; ls	1%
	FTP	FTP GET, 1MB file	1%

SECURITY SHORTCUTS

Whilst we strive to introduce the real world 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.

This is a problem in Proof of Concept (PoC) exercises. If you're 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. Further information regarding PoC Best Practice and security shortcuts can be found here: http://tiny.cc/poc-shortcuts.

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 assess your security and traffic throughput requirements, translating those into a solution to meet your needs today and in the future.

ENSURE POC EXERCISES COMPARE APPLES WITH APPLES

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim 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: 650-654-4233 | www.checkpoint.com