EANTC Independent Test Report

Palo Alto Networks VM-700 on HPE ProLiant Servers Performance Benchmarking

July 2019

Introduction

The industry-wide network transformation from physical to virtualized deployments and the increased market share of cloud-based workloads make cloud network security solutions inevitable. Virtualized next-generation firewalls (NG-FW) are considered a vital component of any cloud-based security architecture. Deployments of virtualized NG-FWs are quite different from physical NG-FWs as follows:

- They can be applied at any location in the network, even locally inserted into the traffic flow between virtual machines (VMs) hosted on the same compute node.
- East-West traffic is minimized by placing the virtualized firewall function appropriately. This avoids routing traffic out to pass through a physical firewalls as illustrated in Figure 1.

EANTC was commissioned by Intel to verify the performance and service scalability of the Palo Alto Networks VM-700 solution. This was a joint effort between EANTC, Intel and Palo Alto Networks. EANTC's tests were aligned with the use case of small datacenter NG-FW deployments. In these environments, HTTP/HTTPS traffic throughput and concurrent sessions are the significant parameters to evaluate the performance and the scalability of a NG-FW solution. Additionally, advanced security features like antivirus, anti-spyware or vulnerability detection were enabled; which provide content security check and malicious traffic pattern recognition.

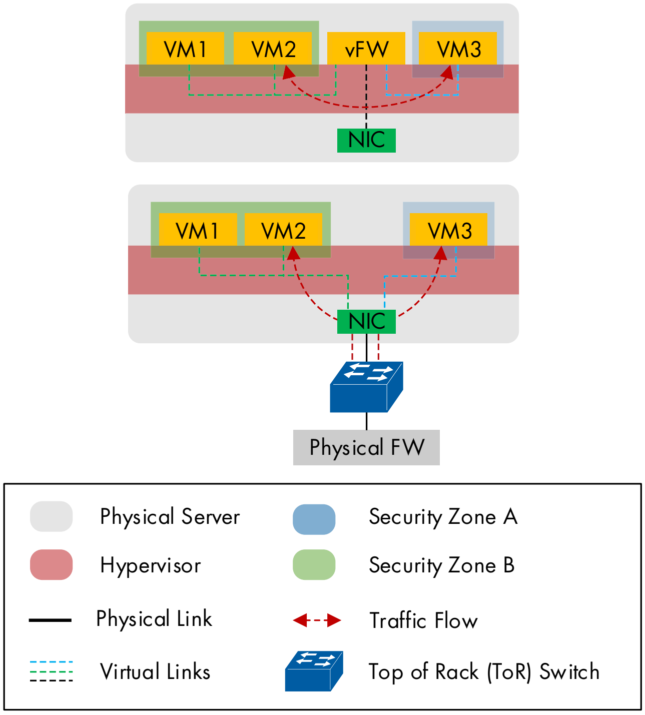

Figure 1: Local Traffic Flow for the Virtual NG-FW and the Physical NG-FW

Test Highlights

→ Up to 9.998 million HTTP concurrent sessions

→ Up to 100,000 HTTPS concurrent sessions

→ Up to 13.5 Gbit/s HTTP throughput with anti-virus, anti-spyware and vulnerability detection enabled and a NetSecOpen Mix object size

→ Up to 2.5 Gbit/s HTTPS throughput with anti-virus, anti-spyware, vulnerability and SSL inspection enabled and a NetSecOpen Mix object size

Executive Summary

Intel commissioned EANTC to verify the performance capabilities of the Palo Alto Networks virtual NG-FW VM-700. The VM was instantiated on a Hewlett Packard Enterprise HPE DL360 Gen10 8SFF CTO Server powered by dual-socket Intel® Xeon® Gold 6152 processors.

The results showed a maximum throughput performance of 13.5 Gbps for an HTTP-only scenario. Likewise, the VM-700 achieved up to 2.5 Gbps throughput in an HTTPS-scenario. In both cases, antivirus and anti-spyware security features were enabled. The session capacity reached up to 9.998 million HTTP and (in a separate test run) up to 100,000 HTTPS concurrent sessions.

The Palo Alto Networks VM-700 demonstrated consistent performance and deterministic behavior during our test session.

NetSecOpen[1] test methodologies and procedures were followed in this test to enable reproducible scenarios and to allow fair comparison between firewalls from different vendors.

[1] https://www.netsecopen.org/

Test Setup

The test setup is shown in Figure 2. One HPE ProLiant DL360 Gen 10 8SFF CTO Server was equipped with two Intel® Xeon® Gold 6152 processors. Each of the CPUs has 22 physical cores. Ubuntu 16.04.6 LTS was installed on the compute node as the host Operating System (OS). Kernel based Virtual Machine (KVM) was installed as the hypervisor. There was no OpenStack or other cloud platform involved in this test.

The Palo Alto Networks Next Generation Firewall VM-700 was instantiated on the KVM hypervisor directly, using 16 CPU cores and 56 Gigabyte of RAM. Hyperthreading was disabled and Intel® Turbo Boost Technology 2.0 was enabled in the compute node. The CPU cores from 1 to 16 on Non Uniform Memory Access (NUMA) node 0 were pinned for the VM-700. The remaining 6 cores on node 0 and all cores on node 1 remained idle. Palo Alto Networks achieves its maximum scale with 16 dedicated cores. To fully utilize HPE server configuration with a total of 44 cores, multiple VM-700 would need to be deployed. Since there was no virtualized load balancer available distributing the workload, tests were conducted with just one VM-700.

Three SR-IOV virtual functions (VF) were created for each physical port of the HPE 40GbE dual-port NIC; in total, 6 VFs were bound to Palo Alto Networks VM-700 as shown in Figure 3. The compute node and the traffic generator were connected through an HPE 5900 Series JC772A switch.

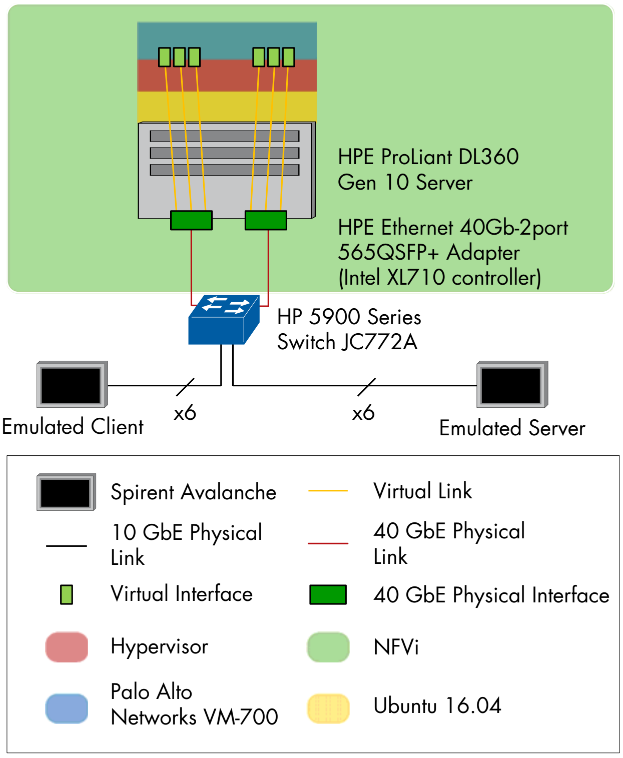

Figure 2: Test Setup

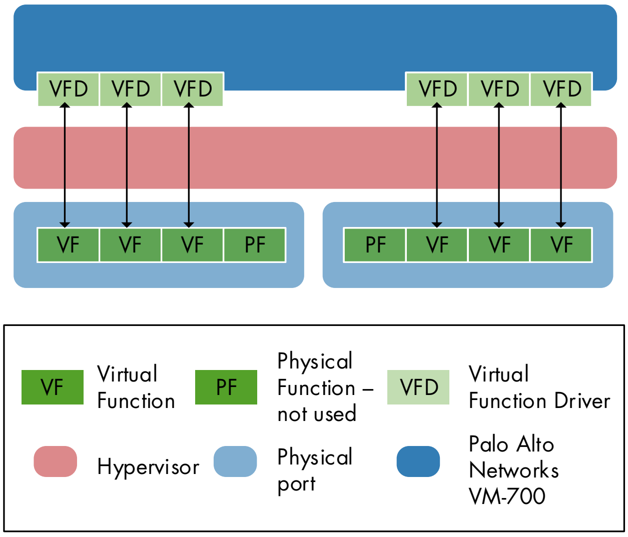

Figure 3: SR-IOV Setup

Test Equipment

The test cases were executed using Spirent Communications C100-S3 high-performance appliance hardware with Avalanche software. The C100-S3 also supports Spirent's CyberFlood assessment solution for advanced mixed traffic, attack, malware and NetSecOpen methodology. EANTC used the C100-S3 to generate traffic and collect statistics. The traffic profile configured on the test tool included HTTP and HTTPS (TLS1.2) flows with a range of object sizes and application behavior settings.

Background On Test Methodology

NetSecOpen is a non-profit open working group with an agenda to evolve network security function benchmarking methodology. NetSecOpen collaborates with the industry, labs, security solution vendors and ISPs to create a well-defined and transparent standard that fulfills real-world network security benchmarking requirements. EANTC has contributed the majority of content to the test methodology, and is one of the accredited test labs to conduct certification.

For the Intel/Palo Alto Networks engagement, we followed the latest NetSecOpen methodology draft[2] submitted to the Internet Engineering Task Force (IETF). Based on available resources and preferences of the vendor under test, a limited amount of test cases and different configurations have been chosen. Hence, this test does not meet NetSecOpen certification requirements.

[2] https://tools.ietf.org/html/draft-ietf-bmwg-ngfw-performance-00

Hardware and Software

Component	Description
HPE ProLiant DL360 Gen10 (Intel designed configuration)	2 x Sockets Intel® Xeon® Gold 6152 CPU@ 2.10GHz (microcode: 0x200005e) 12 x 32GB (384GB) DDR4 RAM 1 x HPE Ethernet 40Gb-dualport 565QSFP+ Adapter (Intel XL710 controller) 1 x HPE Ethernet 10Gb-2port 562 SFP+ Adapter 2 x HPE 480GB SATA 6G RI SFF/ LFF SC DS SSD 2 x HPE 1.92TB NVMe x4 RI SFF SCN DS SSD Server Platform Services (SPS) Firmware: 4.0.4.393 System ROM: U32 v1.42 Innovation Engine (IE) Firmware: 0.1.6.1
Host OS	Ubuntu 16.04.6 LTS
Hypervisor	QEMU emulator v2.5.0
HPE Ethernet 40Gb-2port 565QSFP+ Adapter (Intel XL710 controller)	Driver: i40e v2.7.29 Firmware: 6.80
Palo Alto Networks VM-700	PAN-OS 9.0.1
Plugin VM-series	vm-series-1.0.2
Spirent Avalanche Commander C100-S3	Chassis OS v4.96.0172
Spirent Avalanche	v4.96 build 1306 32bit

Table 1: Hardware and Software Details

Test Results

The scope of this testing report was to verify the performance and the capacity of the Palo Alto Networks firewall (VM-700) in terms of maximum HTTP/HTTPS traffic throughput, number of the concurrent sessions and maximum Connection Per Second (CPS) that could be handled by the Palo Alto Networks VM-700. The test procedures and parameters were followed as defined in the IETF draft.

During the test execution, there were three different phases: ramp up, steady and ramp down. In the ramp up phase, the traffic ramps up slowly to reach the target KPI. The traffic was continuously and consistently flowing during the steady phase. Within the ramp down, all the TCP connections were closed and the traffic slowly ramp down to zero. All the KPIs are measured during the steady phase and used as the main source of the results. For the throughput and CPS tests, ramp up time was 180 seconds, steady state time was 600 seconds, and ramp down time was 180 seconds. It is shown in Figure 4.

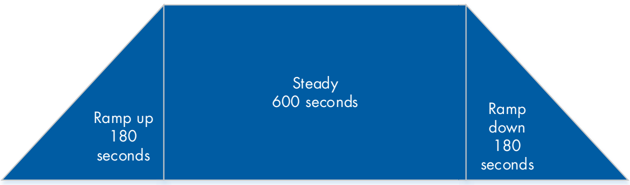

Figure 4: Test Execution Phases

The Transport Layer Security (TLS) version was 1.2. The cipher suite was ECDHE-RSA-AES128-GCM-SHA256. The key size was RSA 2048bit. The TLS and cipher suite were kept the same for all the HTTPS tests.

Palo Alto Networks VM-700 had enabled the anti-virus, anti-spyware, vulnerability detection and traffic log function. SSL inspection had also been enabled which means that the Palo Alto Networks VM-700 decrypted the traffic, detected the content and sent the traffic out after encryption. This configuration remained the same for all the tests.

The test cases we choose from the IETF draft are listed below:

- 7.2 TCP/HTTP Connection Per second (1 KByte and 64 KBytes)
- 7.3 TCP/HTTP Throughput (1 KByte and Mix)
- 7.5 Concurrent TCP/HTTP Connection Capacity
- 7.6 TCP/HTTPS Connections per second (1 KByte and 64 KBytes)
- 7.7 HTTPS Throughput (1 KByte and Mix)
- 7.9 Concurrent TCP/HTTPS Connection Capacity

HTTP and HTTPS Throughput

HTTP and HTTPS are two of the most common traffic profiles which are checked by data center FWs. More and more websites are using HTTPS to secure the data and user privacy. Therefore, the HTTPS traffic profile was also involved in the test. The purpose of this test case was to measure the maximum throughput performance for both the traffic profiles. The selected object sizes were: 1 KByte and a MIX object size. The MIX object size used for the test is derived from the IETF and listed in Table 2. Each TCP connection had 10 HTTP/HTTPS transactions. The TCP connection closed with FIN immediately after 10 transactions.

Number of Requests/Weight	Object Size (KByte)
1	0.2, 6, 8, 9, 10, 25, 26, 35, 59, 347

Table 2: Object Size Distribution

Table 3 shows the achieved HTTP and HTTPS throughput results and other KPIs during the steady phase with 1 KByte object size. Table 4 shows the respective HTTP and HTTPS throughput for mixed object sizes. As we can see in the table, the HTTPS traffic only utilized 56% of the CPU, the reason is that if we keep increasing the traffic, the TCP and HTTP related delay increased to a very high number and the traffic was also not stable. Therefore, the number we presented here is a fine tuned stable number that we have observed.

KPI		Min.	Average	Max.
Throughput (Mbit/s)	HTTP	1,236	1,252	1,259
	HTTPS	123	126	129
HTTP transactions per second	HTTP	107,618	109,015	109,626
	HTTPS	8,796	9,045	9,276
Concurrent Connections	HTTP	143	171	201
	HTTPS	113	138	163
TCP Connections per second	HTTP	10,764	10,900	10,959
	HTTPS	893	904	914
CPU utilization	HTTP	86%	89%	91%
	HTTPS	52%	56%	63%

Table 3: KPI values for HTTP and HTTPS Throughput test; 1 KByte Object Size

KPI		Min.	Average	Max.
Throughput (Mbit/s)	HTTP	13,451	13,552	13,622
	HTTPS	2,388	2,472	2,539
HTTP transactions per second	HTTP	29,825	30,051	30,132
	HTTPS	5,353	5,440	5,545
Concurrent Connections	HTTP	91	109	127
	HTTPS	80	100	124
TCP Connections per second	HTTP	2,984	3,004	3,009
	HTTPS	538	544	549
CPU utilization	HTTP	86%	90%	94%
	HTTPS	57%	69%	76%

Table 4: KPI values for HTTP and HTTPS Throughput test; MIX Object Size

TCP Connections Per Second (CPS) for HTTP and HTTPS Traffic

In this test case, we measured the maximum connection setup per second performance of the Palo Alto Networks VM-700. Each TCP connection had only one transaction and the connection closed immediately after this single transaction. This test was executed in two iterations, first with 1 KByte object size and second with 64 KByte object size.

Table 5 represents the results of the TCP Connections Per Second and other KPIs for HTTP and HTTPS traffic during the stable phase with 1 KByte object size; Table 6 shows the results of TCP Connections Per Second and other KPIs for HTTP and HTTPS traffic during the stable phase with 64 KByte object size. See explanation from last section for the HTTPS performance.

KPI		Min.	Average	Max.
TCP Connections per second	HTTP	58,070	58,936	59,780
	HTTPS	890	904	914
Throughput (Mbit/s)	HTTP	823.8	836.2	848.2
	HTTPS	31.23	31.64	32.23
Concurrent Connections	HTTP	72	87	106
	HTTPS	36	47	62
TCP Time to First Byte (msec)	HTTP	0.39	42.02	329.43
	HTTPS	0.19	0.79	2,061.66
VM-700 CPU Utilization	HTTP	76%	85%	89%
	HTTPS	42%	48%	55%

Table 5: KPI Values for TCP Connections Per Second Test; 1 KByte Object Size

KPI		Min.	Average	Max.
TCP Connections per second	HTTP	20,627	20,649	20,670
	HTTPS	985	994	1,006
Throughput (Mbit/s)	HTTP	11,380	11,394	11,405
	HTTPS	557.06	571.20	586.74
Concurrent Connections	HTTP	93	106	122
	HTTPS	76	93	124
TCP Time to First Byte (msec)	HTTP	0.40	3.06	58.51
	HTTPS	7.79	36.22	164.43
VM-700 CPU Utilization	HTTP	84%	86%	88%
	HTTPS	51%	59%	68%

Table 6: KPI Values for TCP Connections Per Second Test; 64 KByte Object Size

TCP Concurrent Connection (CC) Capacity

In this test case, we verified the maximum number of concurrent connections that was supported by the Palo Alto Networks VM-700. The maximum sustained Concurrent Connections gives a better understanding about the limitation of Palo Alto Networks VM-700 based on the assigned computer resources.

Each TCP connection had 10 transactions. The object size was 1 KByte. We added "think time" between each transaction to keep all the TCP connections open during the steady phase. For the CC measurements, we established only the TCP sessions during the ramp up phase. The average CPS rate was around 29,951 connections/second and 556 connections/second with respect to HTTP and HTTPS. All the sessions remained open during the whole steady phase. No session was opened or closed during the steady phase. The traffic was continually flowing and stable during the steady phase.

Table 7 shows the maximum concurrent connection capacity and other KPIs during the stable phase for HTTP and HTTPS traffic respectively. As defined by the draft, there was no new session open and close in the steady phase, and the transaction and the throughput were also very low. We observed only 3% of CPU utilization during the HTTPS concurrent connection test case execution.

KPI		Min.	Average	Max.
Throughput (Mbit/s)	HTTP	699.17	700.45	701.63
	HTTPS	20.06	20.26	20.48
Concurrent TCP Connections	HTTP	9,998,978	9,998,978	9,998,978
	HTTPS	100,000	100,000	100,000
Application transaction latency (msec)	HTTP	<0.001	1.2	73
	HTTPS	<0.001	5.7	25
Application transactions per second	HTTP	59,790	59,907	60,009
	HTTPS	1,649	1,666	1,686
VM-700 CPU Utilization	HTTP	51%	52%	54%
	HTTPS	3%	3%	5%

Table 7: KPI Values for TCP Concurrent Connections Test

Conclusion

The Palo Alto Networks VM-700 provides the functionality required for a cloud-based next-generation firewall. A major benefit of virtualization is that more placement options exist compared with physical next-gen firewalls.

In our test, the solution provided reproducible, high performance in unencrypted HTTP environments. Since the ratio of encrypted HTTPS traffic is continuously growing in the Internet, HTTPS benchmarks will become more important in the future. The VM-700 showed lower HTTPS performance than with HTTP. Additionally, the VM supports at maximum 16 physical cores. With second generation Intel Xeon Scalable processors, the VM performance could be improved by utilizing all available cores.

About EANTC

EANTC (European Advanced Networking Test Center) is internationally recognized as one of the world's leading independent test centers for telecommunication technologies.

Based in Berlin, the company offers vendor-neutral consultancy and realistic, reproducible high-quality testing services since 1991. Customers include leading network equipment manufacturers, tier 1 service providers, large enterprises and governments worldwide. EANTC's Proof of Concept, acceptance tests and network audits cover established and next-generation fixed and mobile network technologies.

Tests were conducted by European Advanced Networking Test Center (EANTC). Hardware configurations: one server with dual Intel Xeon Gold 6152 processors running at 2.1 GHz with 22 cores, 384 Gigabits of RAM, and 40 GbE connections provided by one HPE® Ethernet 40Gb-2port 565QSFP+ Adapter and by one HPE® Ethernet 1Gb 4-port 331i Adapter. Software configurations: Palo Alto Networks PAN-OS 9.0.1, Ubuntu 16.04.6 LTS.* Simulation of application protocol conducted using 1x Spirent Avalanche® C100-S3 appliances using 4x Dual-port 10 Gbps adapters.

Intel, the Intel logo, and Xeon are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit www.intel.com/benchmarks.

Performance results are based on testing as of May 2019 and may not reflect all publicly available security updates. See configuration disclosure for details. No product or component can be absolutely secure.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

While every reasonable effort has been made to ensure accuracy and completeness of this publication, the authors assume no responsibility for the use of any information contained herein. All brand names and logos mentioned here are registered trademarks of their respective companies in the United States and other countries.

EANTC AG
Salzufer 14, 10587 Berlin, Germany
info@eantc.com, http://www.eantc.com/
[v1.0 20190730]