Introduction

3GPP TS 33.210 V15.2.0 defines the security architecture for mobile networks, defining how to protect IP-based control plane signaling for the Evolved Packet Core (EPC). The Security Gateway (SecGW) is described as a security node that terminates all IPSec tunnels between the eNodeB and the EPC. The SecGW is considered a mandatory element in the LTE architecture when deployed with an untrusted backhaul network. Please refer to Figure 1. The majority of SecGW deployments are used to protect the S1-MME interface. In this case, the SecGW functions include authenticating network elements, encrypting traffic and rejecting any non-authorized access by rogue eNodeBs.

In parallel, Mobile Network Operators (MNOs) are re-architecting their networks towards Network Function Virtualization (NFV) to enable dynamic and rapid provisioning of new services. Commonly, MNOs virtualize the EPC as one of the earlier components to start the network transformation journey towards a Telco Cloud architecture.

The virtual Security Gateway (vSecGW) is considered as one of the complementary elements of the vEPC, so it needs to be virtualized alongside the vEPC. In this test report, EANTC sheds light on many performance and security aspects for the vSecGW to secure the S1-MME interface.

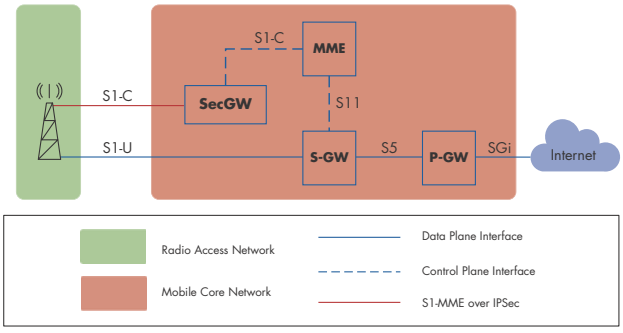

Figure 1: LTE Network

Communications Service Providers (CoSPs) are looking to transform their infrastructure to better support 5G and Internet of Things (IoT). Data traffic over communications networks is expected to continue growing rapidly over the next decade. As a result, CoSPs are evaluating and implementing NFV. This enables applications in a performance-optimized, secure and cost-effective manner — spanning from the data center to central office and network edge. Cloud-scale agility, scalability and rapid deployment of network services are critical considerations guiding CoSPs as they deploy this next-generation infra-structure.

Test Highlights

- 73% throughput enhancement using Intel QAT accelerator[a]
- Up to 4.59 Gbit/s unidirectional throughput

a. Based on IMIX distribution of packet sizes

Lenovo and Intel are collaborating on solutions to simplify the selection and deployment of hardware and software needed for today's network workloads and accelerate the migration of CoSPs to NFV.[1]

To achieve the goal of accelerating NFV deployments, Lenovo has launched validated configurations of Lenovo ThinkSystem SR650 and SR630 Servers and Lenovo Ethernet switches as part of the Intel® Select Solution for NFVI program.

Executive Summary

Continuation to the previous report that was published on February 2019, EANTC was commissioned by Lenovo to verify the performance gain that can be achieved by Intel QuickAssist Technology (QAT) using Fortinet FortiGate as a vSecGW. The VNF was deployed on Lenovo ThinkSystem SR650 compute nodes conforming to the Intel® Select Solution for NFVI program. The project was supported by Red Hat; Red Hat OSP 13 was used as the Virtual Infrastructure Manager (VIM). During the tests, Lenovo leveraged its organic Open Cloud automation toolset for rapid deployment of the OpenStack environment.

The test was executed in two rounds. In the first round, we verified the maximum throughput performance for IPSec traffic processed by the FortiGate VNF without Intel QAT adaptor. The results showed a maximum throughput performance of 2.655 Gbps with IMIX distribution.

In the second round, we verified the maximum throughput performance for IPSec traffic processed by the FortiGate VNF with Intel QAT adaptor. The results showed a significant improvement with maximum throughput performance of 4.594 Gbps.

1. https://en.resources.lenovo.com/solution-brief-documents/lenovo-intel-select-solution-for-network-functions-virtualization-infrastructure

Test Bed Description

NFV products have to be tested as a "Full-stack" solution starting from the infrastructure level to virtualized network function and certainly the management layer. As shown in Figure 2, Network Function Virtualization Infrastructure (NFVI) layer includes compute nodes and controller nodes provided by Lenovo ThinkSystem SR650 Server and Lenovo ThinkSystem SR630 Server respectively.

Figure 2: Lenovo ThinkSystem SR650 Server

Figure 3: Lenovo ThinkSystem NE2572 RackSwitch

Compute node servers were equipped with two Intel Xeon Platinum 8176 processors (@ 2.1 GHz, 28 cores) with Intel Turbo Boost Technology was enabled. Intel XXV710 Network Interface Card (NIC) was selected in this test bed. Lenovo RackSwitch G8052 and Lenovo ThinkSystem NE2572 RackSwitch were used for management purpose and for data traffic, respectively.

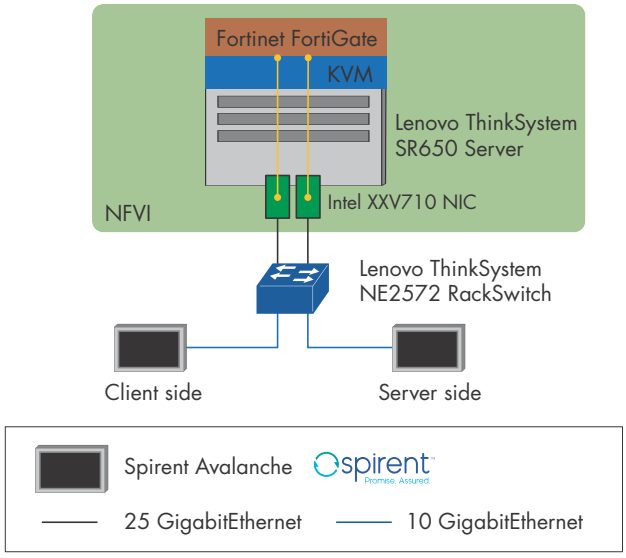

Figure 4: Logical Test Bed Topology

For maximizing the data plane performance, the Lenovo NFVi environment has accelerated NUMA partitioning for the two socket server configuration, and huge pages enabled. Additional configuration and optimization information for Lenovo's NFVi environment can be found at https://lenovopress.com/lp0913.pdf.

The Function Under Test (FUT) was a vSecGW provided by Fortinet, which is a virtualized version of FortiGate. Red Hat OpenStack Platform 13 (Red Hat OSP 13) managed the NFVI on the Lenovo servers as shown in Figure 4.

The FortiGate VNF was configured with:

- 2 SR-IOV capable network ports. Single-Root input/output virtualization (SR-IOV) allows multiple VNFs to share access to a single PCI Express card — in this case the Ethernet NIC
- 16 virtual CPU Cores
- 24 Gigabyte RAM

Hardware Type	Software Version
FortiGate	FortiGate-VM64-KVM v6.2.0,build0965,190724 (Interim)
Lenovo ThinkSystem SR650 Servers and SR630 Servers	BMC Version: V2.12 (Build ID: CDI328N) UEFI Version: V1.41 (Build ID: IVE126O) LXPM Version: V1.30 (Build ID: PDL114N)
Host OS	RHEL 7.6 (Maipo)
Intel NIC XXV710	Driver: i40e Version: 2.7.7.1 Firmware version: 6.80 0x80003da1 1.1937.0
QAT Adapter	Module: Intel QuickAssist Adapter 8950 Driver: v 4.4.0
Lenovo ThinkSystem NE2572 RackSwitch	Software 10.9.1.0 Grub: 10.9.1.0
Spirent Avalanche	4.98

Table 1: Hardware and Software Versions

About Intel QuickAssist Technology[2]

The Intel QAT is a hardware-based acceleration technology for virtual workloads that require encryption and compression. This makes it easier for developers to integrate built-in cryptographic accelerators into network and security applications.

Figure 5: Intel QuickAssist Adapter 8950

The following cryptography and compression algorithms are supported:

- Symmetric cryptography functions include: Cipher operations (AES, DES, 3DES, ARC4); Wireless (Kasumi, Snow, 3G); Hash/Authenticate operations (SHA-1, MD5, SHA-2 [SHA-224, SHA-256, SHA-384, SHA-512]); Authentication (HMAC, AES-XCBC, AES-CCM); Random number generation.
- Public Key Functions include: RSA operation; Diffie-Hellman operation; Digital signature standard operation; Key derivation operation; Elliptic curve cryptography (ECDSA and ECDH) Random number generation and price number testing.
- Compression/Decompression include: DEFLATE (Lempel-Ziv 77)

Intel QAT Adapters are available as PCI Express* Gen 3-compliant cards that support functionality such as the following:

- 4G LTE and 5G encryption algorithm off-load
- IPSec & SSL VPN traffic acceleration
- Compression/decompression
- I/O virtualization using PCI-SIG SR-IOV

Test Equipment

Tests were conducted using Spirent Communications C100-S3 high-performance appliance hardware with Avalanche software. Avalanche provides an assessment framework to test and stress next-generation firewalls and other networking solutions with stateful application and encrypted traffic on interfaces from 1Gbps to 100Gbps. Test results with Avalanche determine real-world maximum bandwidth, connectivity capacities, new session setup rates, IPsec tunnel performance and security policy accuracy. The C100-S3 also supports Spirent's CyberFlood assessment solution for advanced mixed traffic, attack, malware and NetSecOpen methodologies.

The test tool was configured with two 10 Gigabit Ethernet client ports and one 10 Gigabit Ethernet server port.

Spirent Avalanche set up IPsec tunnels. With reference to 3GPP TS 33.210 V15.2.0 and IETF RFCs 4303 and 7321, the following IPSec profile was selected:

Parameter	Value
Authentication	Preshared Key
Encryption Algorithm	AES-CBC-256
HASH	SHA-1
IKE Mode	Aggressive Mode
IKE version	v2
IP version	IPv4
IPSec Mode	Tunnel

Table 2: IPSec Parameters

2. https://www.intel.com/content/www/us/en/ethernet-products/gigabit-server-adapters/quickassist-adapter-8950-brief.html

Test Results

According to Fortinet, using QAT hardware accelerator does not bring difference to the maximum set up rate and maximum number of active IPSec tunnels. So, the scope of this test round was to measure the maximum throughput which the VNF can handle.

Maximum Throughput

The test was performed with packet sizes that comply with the IMIX distribution shown in Table 3. The average packet size is 645 Byte, and the distribution of the packet sizes reflects the typical packet sizes of control plane and user plane traffic.

Packet Size (Byte)	Weight
64	3
100	26
373	6
570	5
1300	6
1518	16

Table 3: IMIX Distribution

The achieved throughput improvement by using the QAT hardware accelerator is impacted by the packet size of the offered traffic. In general, it's proportional relationship between the packet size and the achieved performance.

The client was configured to build 2500 IPSec tunnels for measuring the maximum IMIX throughput. The test was performed by increasing the traffic load on 2500 tunnels to reach the maximum capacity at the Device Under Test (DUT). UDP based unidirectional payload was sent from client to server. We sent traffic through the IPSec tunnel from the client-side and clear text in the server-side The result is shown as in Table 4.

	Frame Size (Bytes)	Throughput (Mbit/s)	
		QAT enabled	QAT disabled
Client	IMIX	4,594	2,655
Server	IMIX	4,346	2,546

Table 4: Maximum Throughput Results

We used the same flavour in RedHat OpenStack, which means that there are always 16 vCPUs and 24 Gigabytes memory assigned to the FortiGate VNF.

SR-IOV was used as a network acceleration technique for this test setup. Each physical port (total 2x25GbE) was enabled by 4 Virtual Functions (VF).

Intel QAT 8950 adapter supports up to 16 VF by default. However, only 4 out of these 16 virtual functions were used by FortiOS. During the test, we have observed that the average utilization of these 4 vCPUs was 97%.

The deterministic behavior of network functions is a mandatory requirement to deliver reliable and real-time Telecom services. However, in the virtualized environment, the contention on the CPU resources between the applications and the system interrupts could impact the overall performance of the virtualized network function. CPU Allocation (aka. CPU Pinning) is a technique used to isolate the system interrupts from the normal application's tasks.

Regarding the vCPU allocation, 8 vCPUs out of 16 were allocated to handle NIC interrupts. The other 8 vCPUs were free for other system tasks or security functions in FortiOS. For QAT enabled setup, 4 dedicated vCPUs assigned just for handling the QAT interrupts as shown in Figure 6.

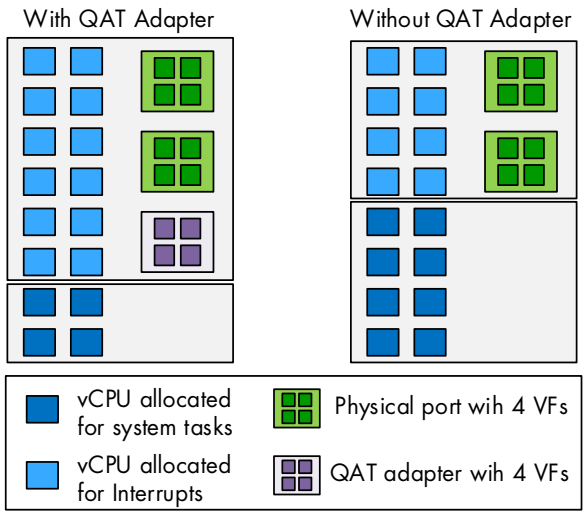

Figure 6: vCPU Allocation

In terms of the whole system throughput improvement, FortiGate VNF achieved 1.73 times more throughput without adding new vCPUs or NIC virtual functions, which means that the network topology can be kept the same without any change.

Conclusion

Integrating the generic compute nodes with a hardware-based acceleration technology is one way to boost the performance of network security solutions to the next level. Our test of the Fortinet FortiGate showed that the Intel® QuickAssist Technology provides performance improvements in the virtualized environment by off-loading the compute-intensive encryption/decryption security operations to QAT adapters.

To calculate the Return of Investment (ROI) of Intel QAT 8950 adapters versus standard, non-accelerated environments, vCPUs allocated to handle QAT interrupts have to be considered as well. QAT adapters will likely reduce the total cost of ownership (TCO) specifically for high-throughput security applications with large packet sizes.

We verified in this test a 73% throughput improvement on Fortinet FortiGate VNF by offloading the IPSec traffic to Intel QAT 8950 adapter and without increasing the number of allocated vCPUs to the VNF.

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.