EANTC

EANTC Independent Test Report

Fortinet FortiGate VM on Lenovo NFVi Intel Select Solution Performance Benchmarking

February 2019

intel

Lenovo

FORTINET

Executive Summary

Today, LTE mobile operators typically deploy All-IP and flat network architectures. This elegant and flexible solution requires deployment of an adequate security infrastructure. One of the major security challenges is to protect and secure the connections between the access network (eNodeB) and the evolved packet core (EPC).

The virtualization of telecom networks (NFV) opens the doors for vendors to provide innovative and powerful security solutions decoupled from hardware appliances. They can be deployed in automated, efficient ways. An interesting question is whether such virtualized network functions (VNFs) will perform adequately, compared with physical appliances.

EANTC was commissioned by Lenovo to verify the performance and service scalability of the Fortinet FortiGate as a virtual security gateway (SecGW). 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 their organic Open Cloud automation toolset for rapid deployment of the OpenStack environment.

Test Highlights

- 31,684 active site-to-site IPSec tunnels between eNodeB and SecGW
- Stable/peak setup rate of 1,300 tunnels/sec
- Up to 2.55 Gbit/s unidirectional throughput

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 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.

Communications service providers (CoSPs) are looking to transform their infrastructure to better support 5G and IoT. Data traffic over communications networks is expected to continue growing rapidly over the next decade. As a result CoSPs are evaluating and implementing Network Functions Virtualization (NFV). This enables applications in a performance-optimized, secure and cost-effective manner — spanning from 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 infrastructure. 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][1]

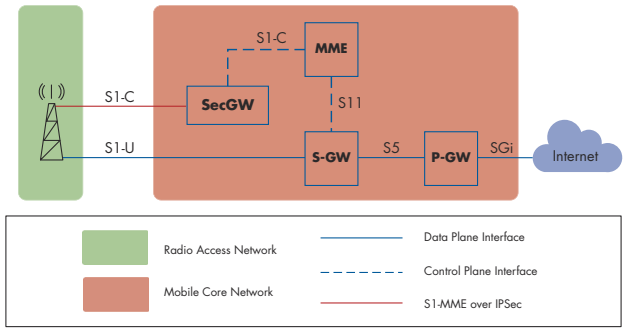


Figure 1: LTE Network

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 Intel® Select Solution for NFVI program.

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

Compute node servers were equipped with two Intel Xeon Platinum 8176 processors and Intel XXV710 NIC cards. Lenovo RackSwitch G8052 and Lenovo ThinkSystem NE2572 RackSwitch were used for management purpose and for data traffic, respectively.

Figure 3: Lenovo ThinkSystem NE2572 RackSwitch

For maximizing the data plane performance, the Lenovo NFVi environment has accelerated NUMA partitioning for the 2 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.

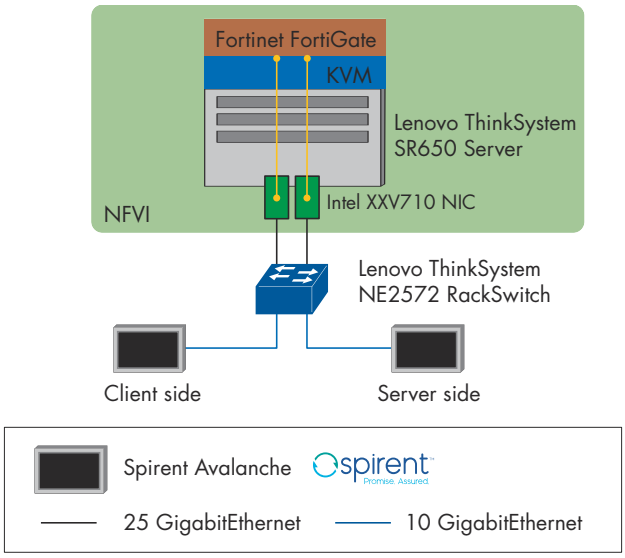


Figure 4: Logical Test Bed Topology

The function under test (FUT) was a virtual SecGW 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,build0817,190128 (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: 2.3.2-k Firmware version: 6.01 0x8000385c 1.1892.0
Lenovo ThinkSystem NE2572 RackSwitch	Software 10.9.1.0 Grub: 10.9.1.0
Spirent Avalanche	4.93

Table 1: Hardware and Software Versions

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

Test Results

EANTC and Fortinet selected the following test cases to verify the most important aspects of vSecGW performance:

1. Maximum number of active IPSec tunnels
2. Maximum IPSec tunnel setup rate
3. Maximum throughput

Maximum number of Active IPSec tunnels

The first performance test was to measure the maximum number of IPSec tunnels that can be handled by the FortiGate VNF. The traffic generator was configured to instantiate site-to-site IPSec tunnels with pre-defined IP gateway that is set on FortiGate, based on the parameters in Table 2. On the other hand, FortiGate was configured to handle the IPSec tunnels based on the dial-up VPN mode. During the test execution, IPSec tunnels were established between client gateway and FortiGate VNF with a low throughput per connection to reach the maximum IPSec tunnels. The logical topology used for determining the maximum number of tunnels in the performance test is shown in Figure 6.

During the test, up to 31,684 IPSec tunnels were established successfully as shown in Figure 5.

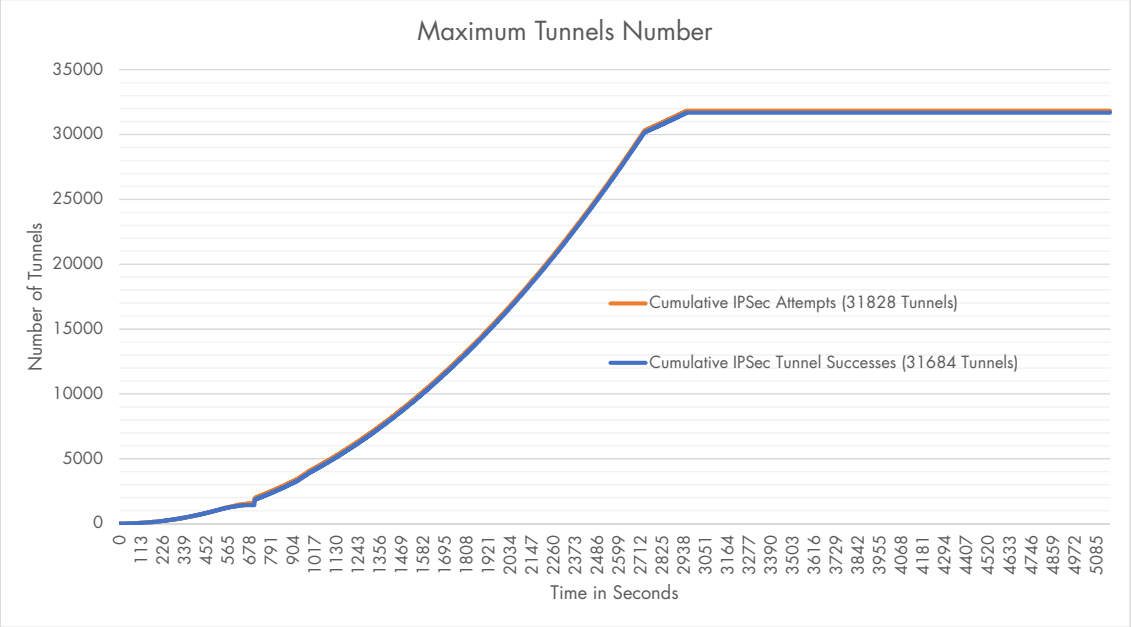


Figure 5: Maximum Number of Tunnels

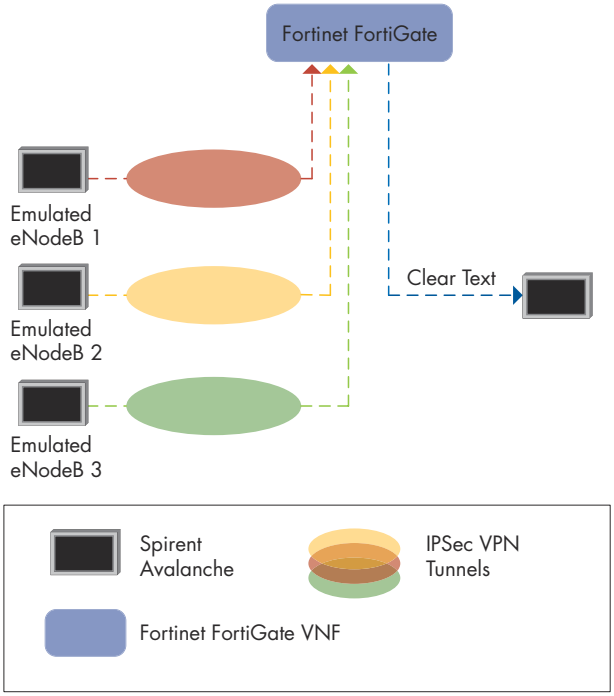


Figure 6: IPSec Test Case Logical Topology

Maximum IPSec Setup Rate

Another important performance test case is to verify the limit of the IPSec tunnels setup rate. This parameter is crucial in stateless high availability scenarios once multiple nodes are implemented as a pool of SecGWs in case there is no control plane synchronization between the nodes.

Spirent Avalanche was configured to create tunnels at a high rate; each of them was torn down after five seconds to avoid exceeding the maximum number of tunnels supported by the security gateway in the course of this test case. The test was continuously run for 300 seconds to measure a stable setup rate. We observed a maximum rate of 1300 tunnel setups per second without any failed tunnel setup attempts as shown in Figure 7.

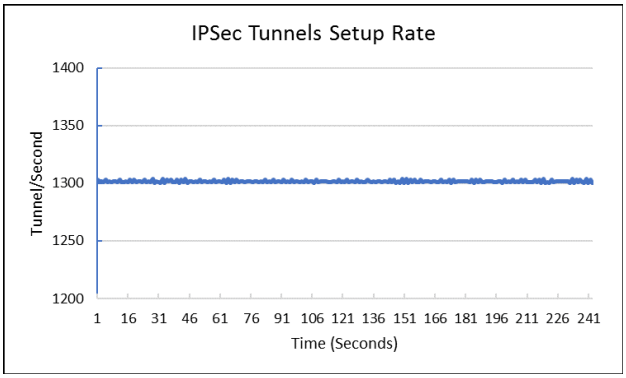


Figure 7: Tunnel Setup Rate

Maximum Throughput

The third performance index tested was the traffic throughput that can be handled by Fortinet FortiGate VM with four CPU cores assigned to handle data plane traffic from SR-IOV enabled NICs. The test was performed with packet sizes that comply with the IMIX distribution shown in Table 3.

The client side of the tester was configured to build the 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 throughput at the Fortinet FortiGate VNF and until the four CPU cores reach the maximum utilization. The generated encrypted traffic has a larger packet size due to the ESP encapsulation overhead. We observed 2.65 Gbps throughput at client side and 2.54 Gbps at server side due to added encapsulation overhead at the client side as shown in Table 4.

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

Table 3: IMIX Distribution

	Frame Size (Bytes)	Throughput (Gbit/s)
Client	IMIX	2.655864352
Server	IMIX	2.546013036

Table 4: Maximum Throughput Results

Conclusion

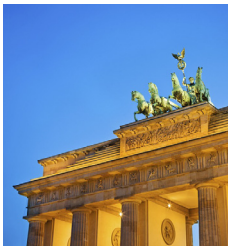
The test results confirm Fortinet's claims regarding the performance of the data plane (packet throughput) and control plane (tunnel setup rate and maximum number of IPSec tunnels supported).

The EANTC spot checks did not reveal any hurdles against the use of the Fortinet FortiGate as a security gateway to protect the EPC from the access network. Certainly, a more extensive test of realistic configurations — such as the NetSecOpen methods — would be useful to assess the performance of a security gateway under versatile, realistic conditions.

Outlook

Boosting the network security solutions to the next level of performance could be achieved by integrating the generic compute nodes with a hardware-based acceleration technology. Intel® QuickAssist Technology (QAT) might provide promising performance improvements in the virtualized environment by off-loading the compute-intensive encryption/decryption security operations to QAT adapters. For future tests, the security solutions that have QAT enabled capability could be targeted to verify incremental performance enhancements.

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.

EANTC AG
Salzufer 14, 10587 Berlin, Germany
info@eantc.com, http://www.eantc.com/
[v1 20190227]