6WIND Proves the 5G Virtual Security Gateway Performance

White Paper

6WIND
Virtualized Networking Software

www.6wind.com

Table of Content

Notices & Disclaimers: Performance benchmarks vary by configuration and other factors. Performance results are based on the testing environment described in the testbed description section.

1. Introduction

Security Gateways play a pivotal role in securing fixed and mobile communication networks, safeguarding the confidentiality of end-user payload through data encryption, while contributing to overall network integrity through the authentication of network elements.

Virtualized Security Gateways should benefit Communication Service Providers (CSPs) by lowering their total cost of ownership (TCO), enhancing deployment scalability, flexibility and agility while at the same time delivering a performance level and resiliency that is fit for mission-critical Tier-1 CSP deployments.

2. Virtualizing the 4G/5G Security Gateway

6WIND recently completed a demonstration of its vSecGW Virtual Security Gateway, in close collaboration with two of the largest global Tier-1 European Mobile Network Operators (MNOs). This white paper illustrates the demonstration and its key results.

The purpose of the demonstration is to prove that the 6WIND Virtual Security Gateway, running on a COTS server without leveraging any specific hardware acceleration, **provides scalable IPsec performance of at least 200Gbps aggregate (upstream + downstream) in a realistic 4G/5G set up environment**.

The first part of the demonstration establishes the performance scalability of the 6WIND vSecGW with 8, 16 and 32 CPU cores and different packet profiles (64B, IMIX and 1500B). The second part uses a realistic traffic profile to demonstrate the 200G IPsec throughput.

3. The Test Set-up

The testbed is illustrated in Figure 1 below. It includes a traffic generator that emulates an asymmetrical 4G/5G mobile typical traffic with 90% downstream and 10% upstream profile. The setup also includes a RAN simulation node that emulates a thousand e/gNodeB elements to establish the security tunnels with the Virtual Security Gateway.

The DUT (Device Under Test) is built with an Intel x86 COTS Server running the 6WIND vSecGW as a Virtual Network Function (VNF).

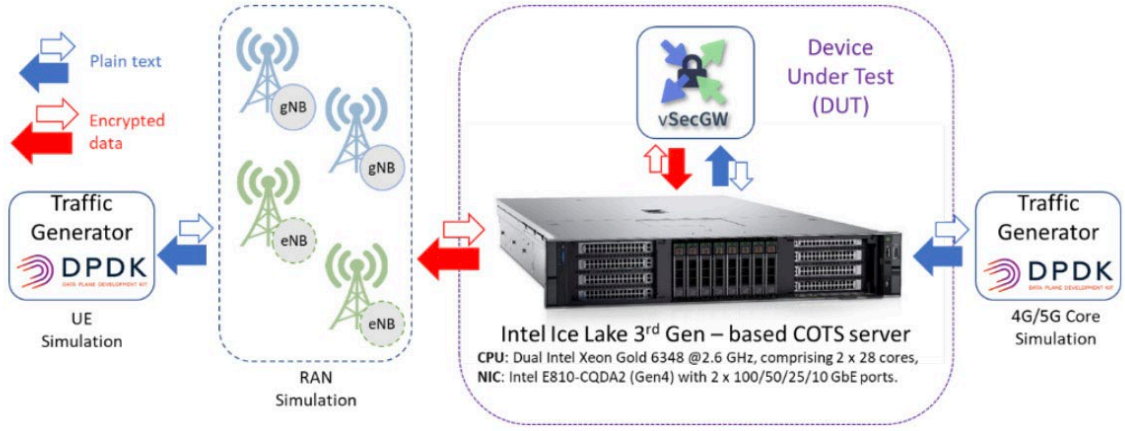

Figure 1: Illustration of the demonstration set-up.

Configuration of the different elements used in the testbed are outlined below.

3.1. The DUT

The DUT (Device Under Test) consists of a 6WIND vSecGW running as a Virtual Network Function (VNF) on an Intel x86 COTS server.

Server description:

- Dual Intel Xeon Gold 6348 @2.6 GHz, comprising 2 x 28 cores
- Intel E810-CQDA2 (Gen4) with 2 x 100GbE ports.

Note: No HW acceleration card used.

Hypervisor description:

- KVM/Qemu version 4.2.1 (Debian 1:4.2-3ubuntu6.21) (on Host)
- Linux Ubuntu 20.04.4 LTS (Kernel 5.4.0-107-generic)

Virtual Machine:

- 6WIND vSecGW v3.4

Note: 6WIND vSecGW software can be downloaded through the 6WIND evaluation portal. Evaluation Self-registration is available through: https://portal.6wind.com/register.php

3.2. The Traffic Generator

The Traffic Generator is used to generate clear, unencrypted, traffic with a pre-determined yet programmable packet-size distribution up to the line rate of the DUT (200 Gbps aggregate). On one side, it is used to emulate the User Equipment (mobile devices, smartphones, etc.) and on the other side, the application traffic generated at the Edge/Core 4G/5G network.

As the traffic generator is required to handle 200G (asymmetric) of raw clear traffic, a DPDK based traffic generator is used.

SW:

- 6WIND-TGen (6WIND proprietary Traffic Generator)

HW:

- Dual Intel Xeon Gold 6348 @2.6 GHz, comprising 2 x 28 cores.
- Intel E810-CQDA2 (Gen4) with 2 x 100GbE ports.

The traffic generator in Figure 1 generates bi-directional traffic that is injected into the DUT. The test traffic packet size distribution, depending on the test, is defined as follows:

- 64B (100%)
- IMIX (average: 350B): 64B (58.3%), 590B (33.3%), 1514B (8.3%)
- $IMIX_2$ (average 700B): 64B (8%), 127B (36%), 255B (11%), 511B (4%), 1024B (2%), 1539 (39%)
- 1500B (100%)

Note: $IMIX_2$ denotes a telecom operator-specific typical 5G traffic mix.
The traffic generator could be replaced by an IXIA, Spirent or Trex (https://trex-tgn.cisco.com).

3.3. The RAN Simulator

The RAN simulator is used to establish the IPsec VPN tunnels with the DUT. In this demonstration, 1000 IPsec tunnels are used to handle the traffic between the RAN simulator and the vSecGW.

3.4. The IPsec Algorithm

This demonstration uses the AES-256-GCM algorithm. The reason for this choice is that of all available AES algorithms, it provides the optimal performance and delivers a high security level.

4. Test Results

In this section we have outlined the test results that prove the 6WIND vSecGW provides scalable IPsec performance of at least 200Gbps aggregate (upstream + downstream) in a realistic 4G/5G set up environment running on a COTS server without leveraging any specific hardware acceleration.

4.1. Performance as Function of Traffic Profile

As outlined above, the first phase of the demonstration focuses on showcasing the 6WIND vSecGW performance scalability. The different measures were performed with a vSecGW using different number of CPUs (8c, 16c, 32c) and different packet sizes. In this first phase you can see that the traffic generator is injecting symmetrical traffic of 100Gbps in each direction.

The following array, summarizes the different results:

	64B	IMIX	$IMIX_2$	1500B
8c	25 Gbps	70 Gbps	111 Gbps	190 Gbps
24c	65 Gbps	182 Gbps	200 Gbps	200 Gbps
32c	104 Gbps	200 Gbps	200 Gbps	200 Gbps

Table1: IPsec throughput (zero-loss) results

The Figure 2 is used to graph the test results. The testbed being capped to 200Gbps, a line is drawn to highlight this line-rate limit.

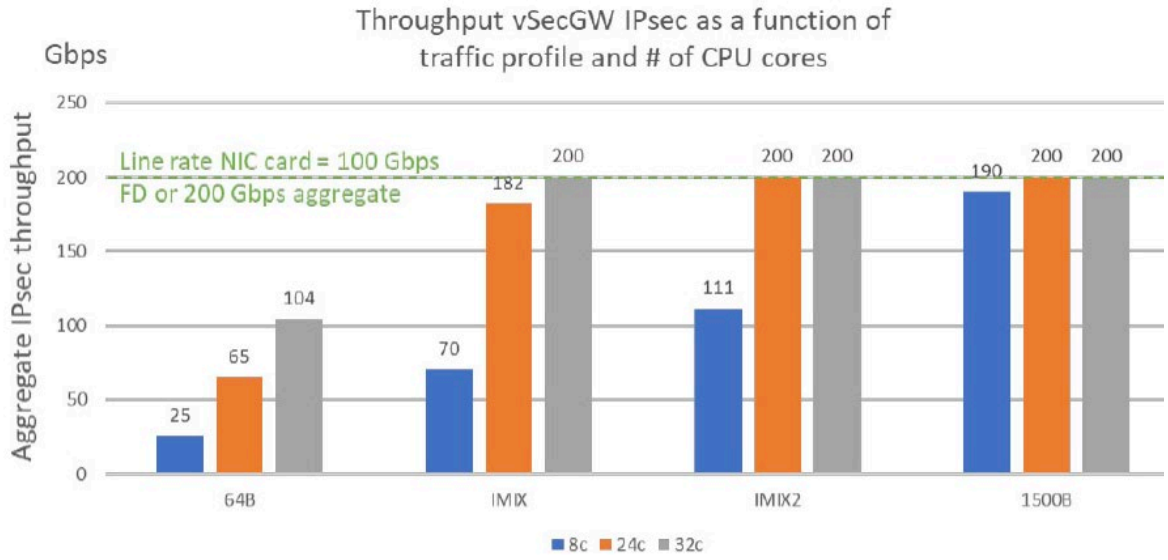

Figure 2: vSecGW IPsec performance scalability

This first test shows that the 6WIND vSecGW performance scales with the number of cores allocated to the virtual machine running the vSecGW.

The Figure 2 shows that the 200Gbps IPsec target, depending on the traffic profile (IMIX and $IMIX_2$), is reachable with a number of CPU cores between 24 and 32. Furthermore, the test shows that a single CPU core can deliver with IMIX between 7.6 Gbps and 8.75Gbps of IPsec throughput.

Using data presented in Figure 2, we can plot Figure 3. From available data points, we can devise a formula for approximating the IPsec throughput for the DUT and 64-Byte packets as a function of the allocated number of CPU cores. We can see that the IPsec throughput of the 6WIND vSecGW is nearly linear function of the number of allocated CPU cores, with R squared (coefficient of determination) = 0.9931.

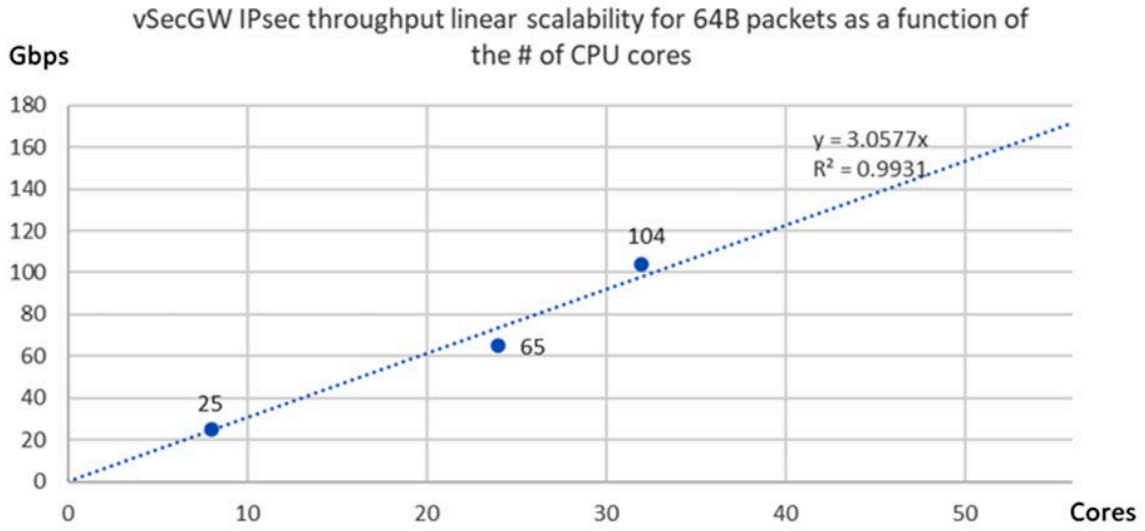

Figure 3: linearity of the IPsec throughput (64-byte packets).

It is important to highlight that the performance linearity applies regardless of packet size. This can be seen thanks to the identical ratio that applies for the throughput values with 8c at 64B and IMIX (25Gbps vs 70Gbps ~ 2.8 times) and with 24c at 64B and IMIX (65Gbps vs 182Gbps ~ 2.8 times).

Note: Because of the testbed throughput limit (line rate @200G), the linearity cannot be shown with mid and big packet sizes (IMIX, $IMIX_2$ and 1500B).

The second phase of the test relies on the different results produced in the first phase and extends the test environment to use an asymmetric traffic aligned with a realistic 4G/5G mobile operator traffic.

4.2. vSecGW Performance in 5G RAN Context

The test set-up depicted in Figure 4 explains how the asymmetric traffic is handled between the traffic generator and the different network elements involved in the demonstration setup.

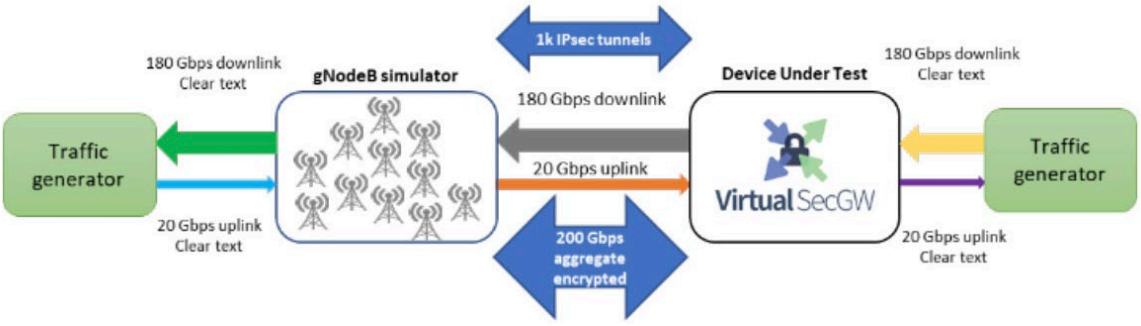

Figure 4: Asymmetric traffic loading

Note: The throughput numbers listed in the figure above are approximates. Unencrypted throughput should be lower than the encrypted one to account for IPsec headers.

The packet size distribution used by the traffic generator in this second phase of the demonstration setup is the standard IMIX.

As the downstream payload of 180 Gbps exceeds the 100Gbps that a single NIC port supports, port bounding (LAG) is needed to handle the full load. A specific VLAN setup is also needed to segment traffic crossing the LAG in each direction.

The following config extract describes the VLAN and LAG configuration:

```
interface
    vlan vlan30
        ipv4
            address 10.30.0.2/24
            ..
        vlan-id 30
        link-interface bond0
        ..
    vlan vlan11
        ipv4
            address 10.11.0.2/24
            neighbor 10.11.0.3 link-layer-address 10:70:fd:02:e1:5c
            ..
        vlan-id 11
        link-interface bond0
        ..
    vlan vlan21
        ipv4
            address 10.21.0.2/24
            neighbor 10.21.0.3 link-layer-address 10:70:fd:02:e1:5d
            ..
        vlan-id 21
        link-interface bond0
        ..
    lag bond0
        mtu 5000
        ethernet
            mac-address b4:96:91:ae:5d:c0
            ..
        mode lacp
        xmit-hash-policy layer3+4
        lacp-rate fast
        link-interface ntfp1
        link-interface ntfp2
        ..
```

The Figure 5, here below, depicts this VLAN, LAG specific configuration.

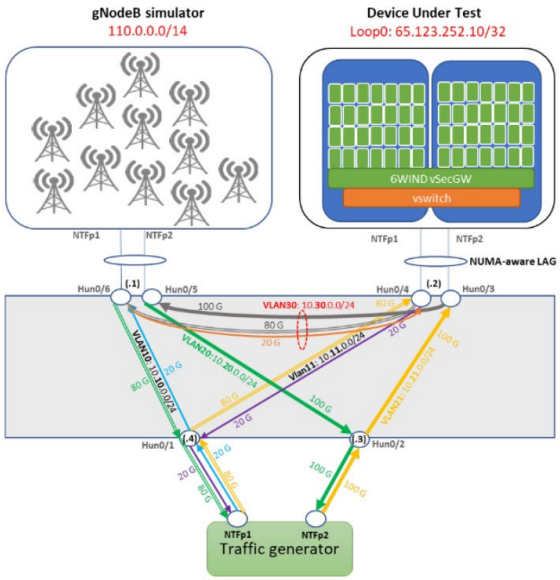

Figure 5: detailed set-up of the configuration depicted in Figure 4

Note: The color coding of the different data streams in Figure 4 is reflected in this figure.

On the DUT and the RAN simulator, the application of Link Aggregation (LAG) allows both ciphered and clear traffic to be spread across all the ports of the LAG group. LAG optimises the utilisation of the network interfaces, especially when the traffic is asymmetric.

In addition, LAG can be configured in a NUMA-aware mode to ensure that any traffic received on a specific NUMA will be sent over a port on the same NUMA node, avoiding inter-NUMA communication. Here, as there is a single 100Gbps port per NUMA node in the LAG group, traffic is sent using the same physical port on which it is received.

The IPsec configuration used for this test setup relies on templates for defining the IKE and IPsec policies. The following extracts describe these templates:

- IKE policy template:

```
ike-policy-template demo-ike-policy
    ike-proposal 1
        aead-alg aes256-gcm-128
        prf-alg hmac-sha384
        dh-group ecp384
        ..
    rekey-time 0
    ..
```

- IPsec policy template:

```
ipsec-policy-template initiator-ipsec-policy
    esp-proposal 1
        aead-alg aes256-gcm-128
        dh-group ecp384
        esn true
        ..
    start-action none
    close-action none
    dpd-action clear
    replay-window 4096
    rekey-time 8h
    ..
```

Note: The IPsec policy is defined with no start-action as the IPsec VPN is initiated by the eNodeB/gNodeB nodes.

In order to simplify the testbed, the DUT and the RAN simulator use pre-shared keys. The following extract provides the full IPsec/IKE configuration:

```
ike
    pool VIP-Pool
        address 192.168.0.0/14
        ..

    pre-shared-key key_wan1
        id 6wind.virtz.net
        id *-wan1
        secret s3cr3t4W@n1
        ..

    global-options
        dos-protection
            cookie-threshold 0
            ..
        threads 128
        sa-table-size 2048
        sa-table-segments 256
        sp-hash-ipv4 local 16
        delete-rekeyed-delay 0
        make-before-break true
        interface-use loopback0
        ..

    ike-policy-template demo-ike-policy
        ike-proposal 1
            aead-alg aes256-gcm-128
            prf-alg hmac-sha384
            dh-group ecp384
            ..
        rekey-time 0
        ..

    ipsec-policy-template initiator-ipsec-policy
        esp-proposal 1
            aead-alg aes256-gcm-128
            dh-group ecp384
            esn true
            ..
        start-action none
        close-action none
        dpd-action clear
        replay-window 4096
        rekey-time 8h
        ..

    vpn initiator-tunnel
        ike-policy
            template demo-ike-policy
            ..
        ipsec-policy
            template initiator-ipsec-policy
            ..
        description “IPSec Management”
        local-address 65.123.252.10
        local-id 6wind.virtz.net
        remote-id *clt
        vip-pool VIP-Pool
        security-policy initiator-mgmt
            local-ts subnet 192.169.0.0/16
            ..
        ..
    ..
```

In order to monitor the vSecGW performance, the system is configured to export the different KPIs to an external InfluxDB time series database:

```
kpi
     interface vlan11
     interface vlan21
     interface vlan30
     interface ntfp1
     interface ntfp2
     telegraf
          influxdb-output url http://behemoth.dev.6wind.com:8086 database telegraf
          ..
     ..
..
```

Collected KPIs are displayed through a Grafana graphical backend (Figure 6).

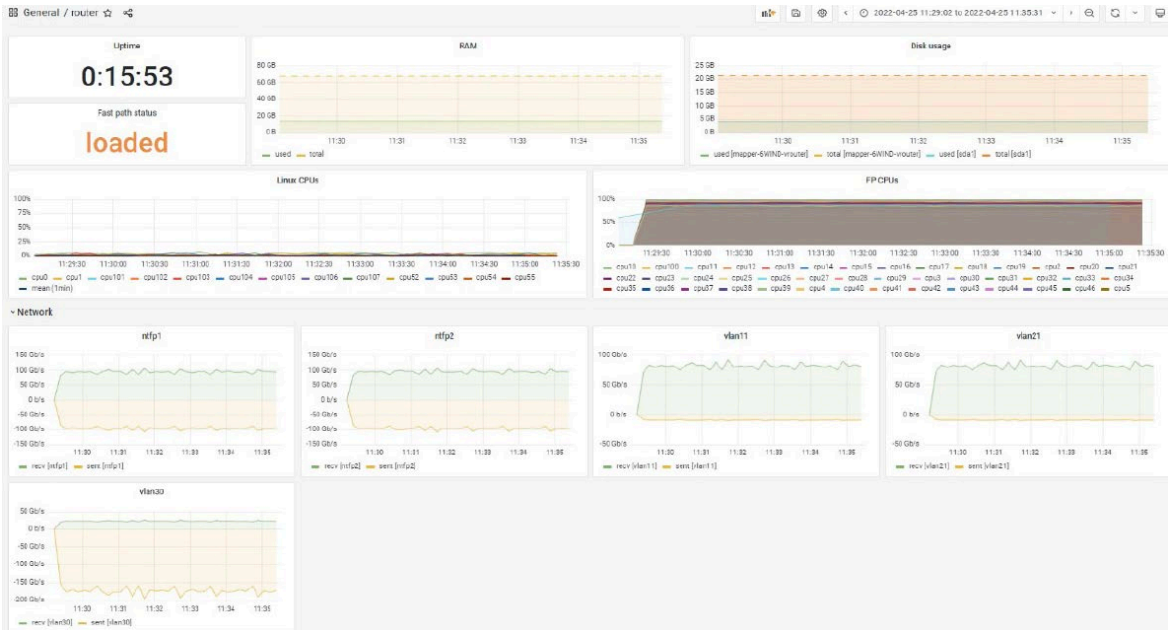

Figure 6: 6WIND vSecGW KPIs - Grafana dashboard.

The IPsec throughput performance of the system presented in Figure 4 is illustrated in the figure below.

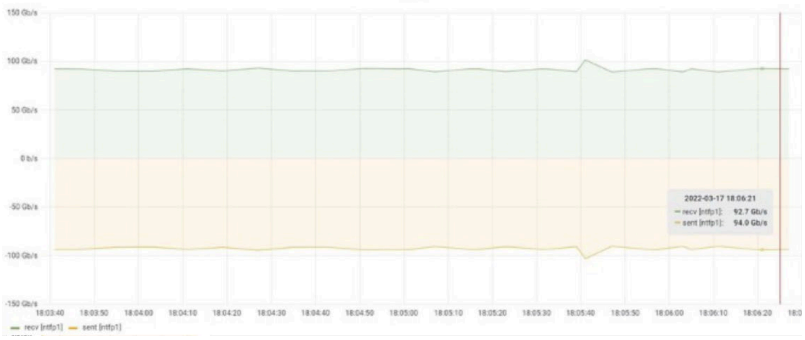

Figure 7: traffic sent and received through interface NTFP1.

Figure 7 shows that the average aggregate throughput on interface NTFP1 of the DUT is approximately 187Gbps, and the peak throughput is 200Gbps. A similar picture emerges at interface NTFP2 (not shown).

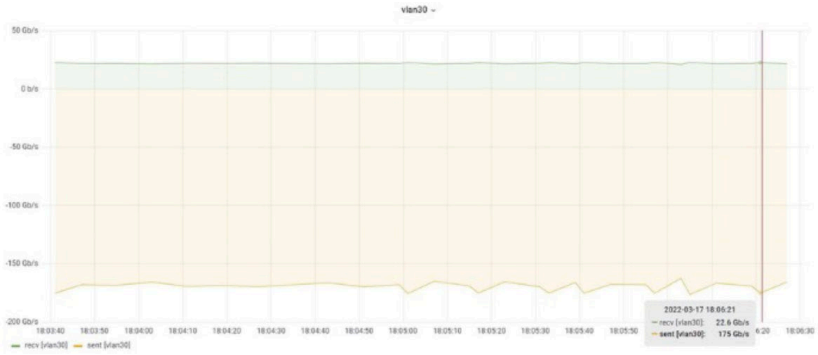

Figure 8: encrypted traffic throughput between the vSecGW and the RAN simulator.

Figure 8 shows the volume of encrypted IPsec traffic flowing between the vSecGW and the RAN simulator.

In this figure, the green plot represents the 10% uplink traffic, in the order of 23Gbps, and the yellow plot represents the 90% downlink traffic, in the order of 175Gbps. The aggregate IPsec traffic that is handled by the DUT averages close to 198Gbps.

5. Conclusion

The demonstration illustrated in this white paper proves that the 6WIND vSecGW Virtual Security Gateway can comfortably support 200Gbps of IPsec traffic on a plain, general-purpose COTS server, without leaning on any hardware acceleration.

The performance scalability of the 6WIND vSecGW can be achieved regardless of the used packet size with an IPsec throughput capacity of more than 7.6Gbps per CPU core @ IMIX and up to 23.75Gbps per CPU core @ 1500B packets. Depending on the number of allocated CPU cores and the traffic packet size distribution, vSecGW has the potential to digest way more than 200Gbps of aggregate IPsec payload on a single server instance.

The Intel x86 COTS server used in this demonstration includes enough CPU cores to scale the performance beyond the 200Gbps illustrated in this white paper. An enhanced demonstration setup is planned in the near future to push the platform to its limits and prove that a 6WIND vSecGW running as a VNF can reliably deliver more than 400G IPsec @ IMIX.