6WIND | Virtualized Networking Software

Powering Mobile Network Security with Virtualized Security Gateway

Disaggregate and distribute Mobile Security Gateways

Mar 12, 2024

Intel® Network Builders PARTNER networkbuilders.intel.com intel.

Webinar Speaker

Karim MCHIRKI

VP of Product Management,
6WIND

As VP of Product Management, Karim is leading the 6WIND product roadmap definition and is helping the product committee, in accordance with the company business strategy, in cultivating product vision and enriching the product solutions

Company Profile

6WIND is a **global networking software company**, with Headquarters in Paris, France, Singapore and in Santa Clara California USA.

We are specialized in delivering **high performance and secure networking software solutions** to support customers with new applications for **5G, IoT and SD-WAN**.

We deliver **Virtualized**, **Cloudified** and **Secure** network solutions that offer the **lowest TCO** in the market with **best cost-performance functionality ratio**.

6WIND's leading edge solutions are used by CSPs, MNOs, NHPs, Cloud Providers, Datacenters, and Enterprises around the world.

20+ Years
Experience

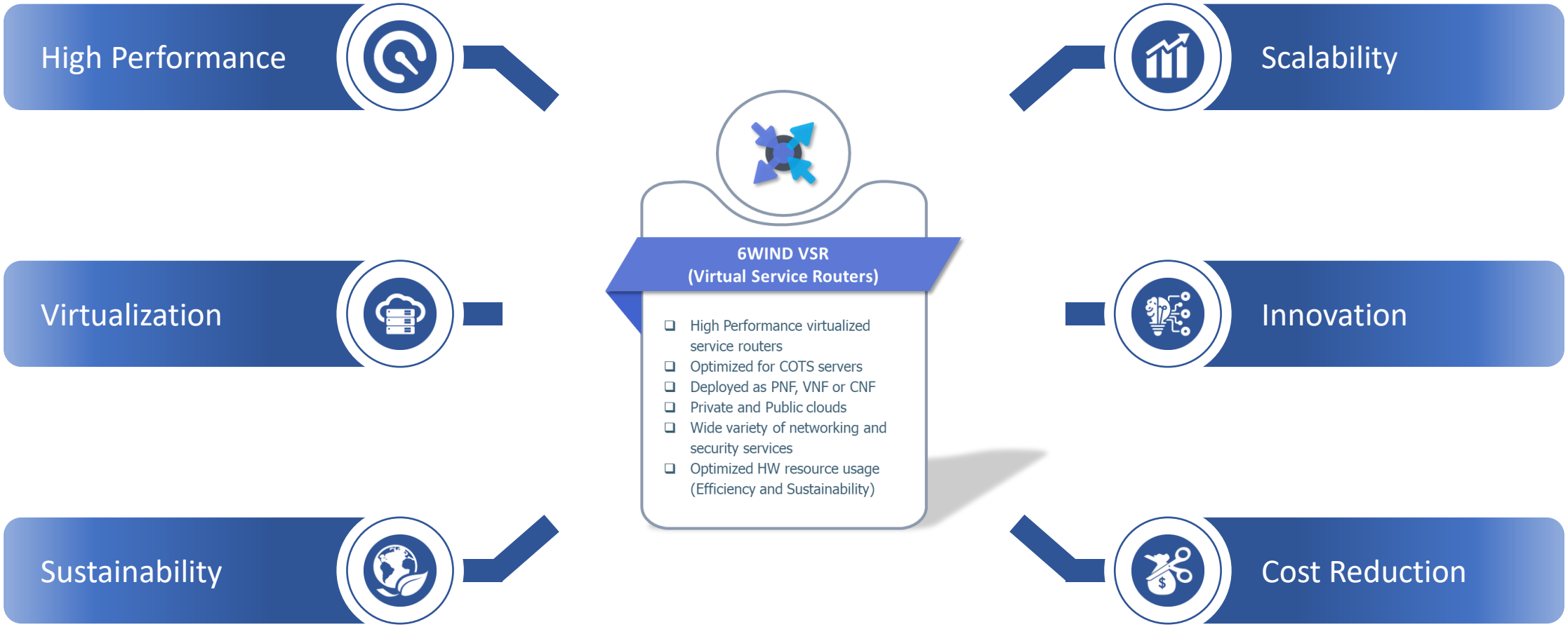
200+
Customers

WW
Deployments

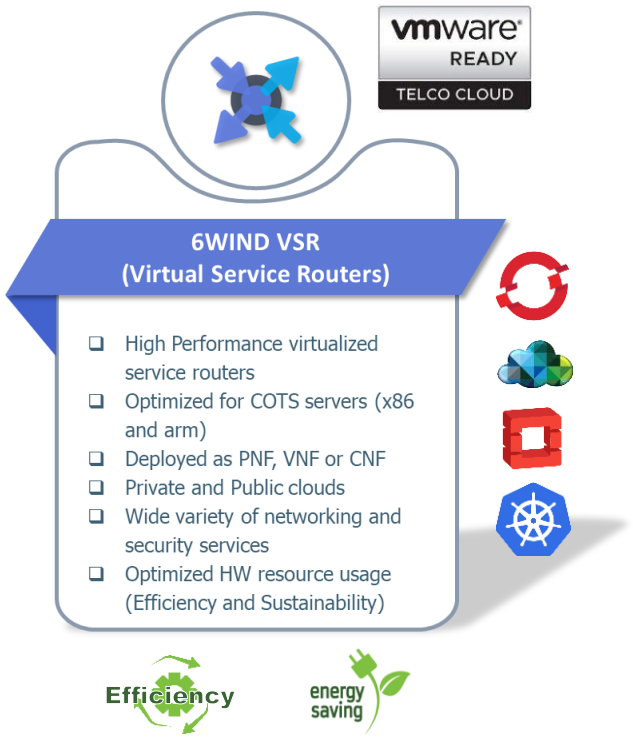
Green-Tech

Meeting Our Customers' Challenges

Best-in-Class Virtualized Network Solutions



6WIND Virtual Service Router Product Family



- 6WIND Virtual Provider Edge Router (vPE)
- 6WIND Virtual Security Gateway Router (vSecGW)
- 6WIND Virtual Cell Site Router (vCSR)
- 6WIND Virtual CG-NAT Router (vCG-NAT)
- 6WIND Virtual Border Router (vBorderRouter)
- 6WIND Virtual CPE router (uCPE)
- 6WIND Virtual FW Router (vFW)
- 6WIND Virtual BNG/AGF Router (vBNG)
- 6WIND User Plane Function (UPF)

Higher Performance

- Optimized for multicore Processors
- Linear Scalable performance
- Lockless implementation for High performance and low latency.

Lower Cost

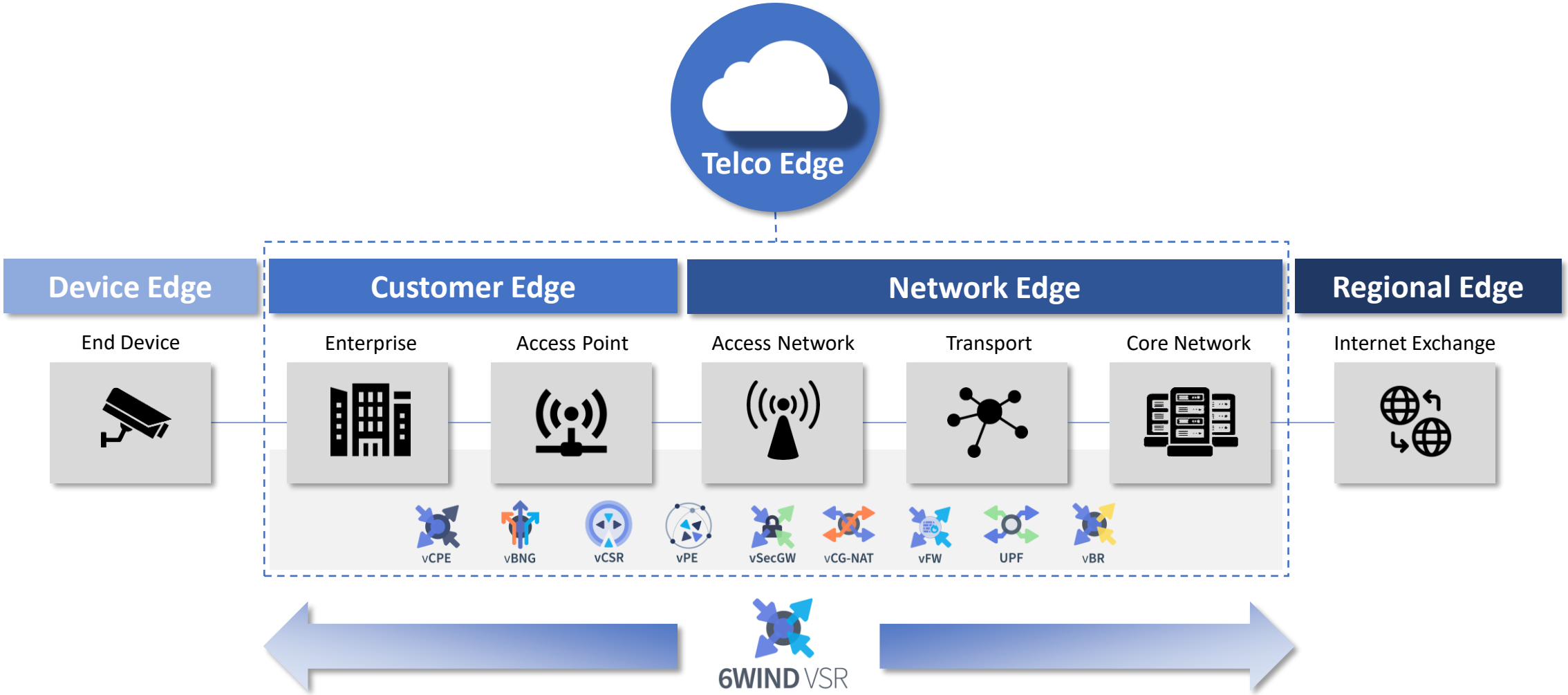
- Optimized resource usage
- Automation - Simple operations
- Hardware agnostic
- Runs on COTS servers

Rapid Service Innovation

- Software based solutions
- Easy feature enhancements
- Faster build new services
- TTM & Competitiveness

Pave the way for the Edge transformation

Network Virtualization and Cloudification



Performance, Agility, flexibility and Efficiency

5G: The need for Security

Security in 5G Specifications

- EU Security
- Access Network Security
- Core Network Security
- Application Network Security

5G Security : Cybersecurity of 5G - EU Toolbox Measures

EU 5G Cybersecurity policy

EU toolbox conclusions: key measures

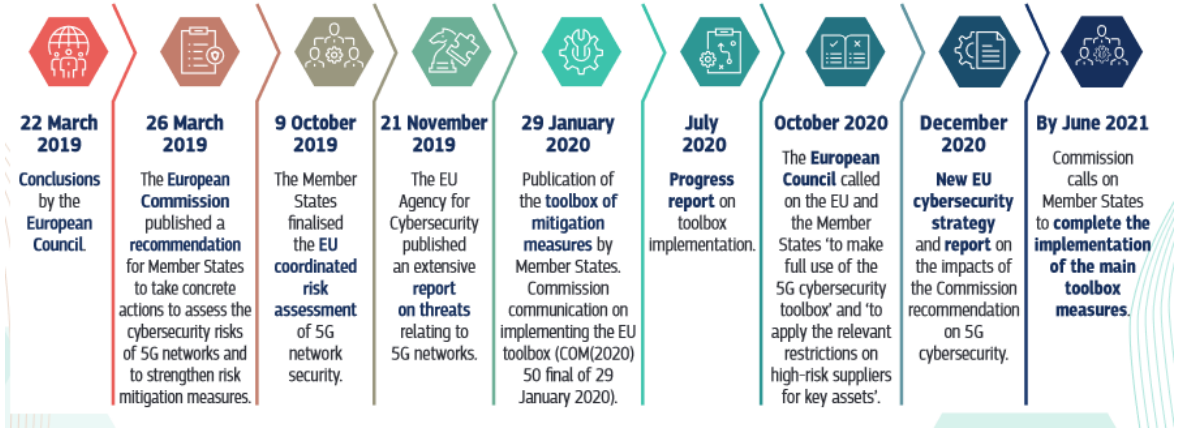
Member States should have measures in place and powers to mitigate risks. In particular they should:

- strengthen **security requirements** for **mobile network operators**;
- assess the risk profile of suppliers; apply relevant **restrictions for suppliers considered as high risk**, including necessary exclusions for key assets;
- ensure that each operator has an appropriate **multi-vendor strategy** to **avoid** or **limit** any **major dependency** on a single supplier and avoid dependency on suppliers considered to be high risk.

The **European Commission**, together with Member States, should take measures to:

- maintain a **diverse** and **sustainable 5G supply chain** in order to avoid long-term dependency, including by:
  - making full use of the existing EU tools and instruments (foreign and direct investment screening, trade defence instruments, competition),
  - further strengthening EU capacities in the 5G and post-5G technologies by using relevant EU programmes and funding;
- facilitate coordination between Member States regarding **standardisation** to achieve specific security objectives and develop relevant EU-wide **certification schemes**.

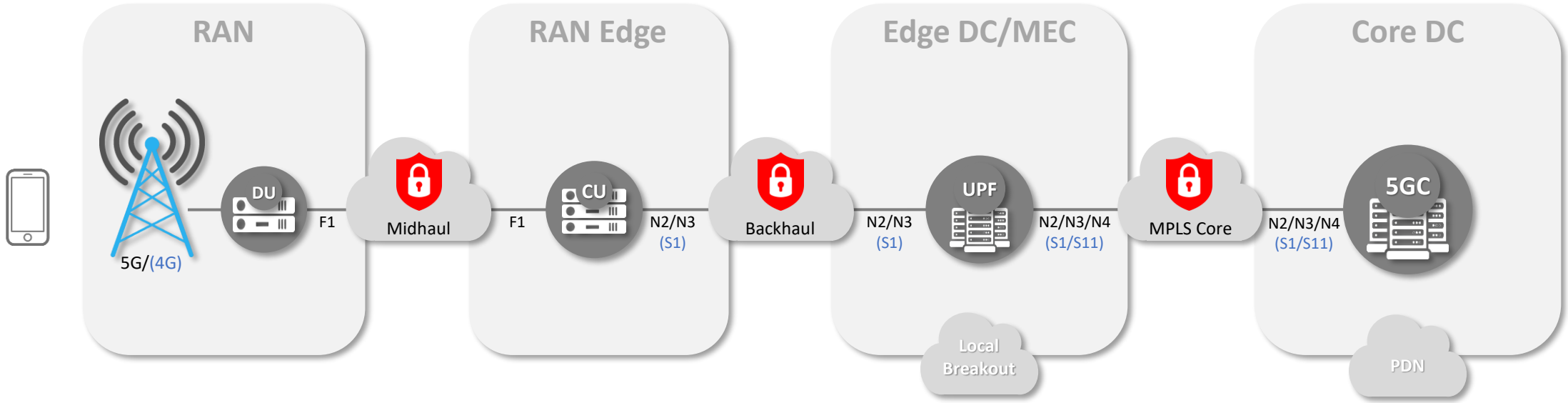
Timeline of the EU 5G cybersecurity policy



Source: https://ec.europa.eu/newsroom/dae/redirection/document/64577

Security in Mobile Networks

From Access to Core network



E2E security requirements

Security for 5G systems

IPsec ESP & IKEv2 as a requirement

9.2 Security mechanisms for the N2 interface

N2 is the reference point between the AMF and the 5G-AN. It is used, among other things, to carry NAS signalling traffic between the UE and the AMF over 3GPP and non-3GPP accesses.

The transport of control plane data over N2 shall be integrity, confidentiality and replay-protected.

In order to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 certificates-based authentication as specified in sub-clause 9.1.2 of the present document. IPsec is mandatory to implement on the gNB and the ng-eNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

9.3 Security requirements and procedures on N3

N3 is the reference point between the 5G-AN and UPF. It is used to carry user plane data from the UE to the UPF.

The transport of user data over N3 shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the N3 reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec is mandatory to implement on the gNB and the ng-eNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

9.1.2 Implementation requirements

IPsec ESP implementation shall be done according to RFC 4303 [4] as profiled by TS 33.210 [3]. For IPsec implementation, tunnel mode is mandatory to support while transport mode is optional.

IKEv2 certificate-based authentication implementation shall be done according to TS 33.310 [5]. The certificates shall be supported according to the profile described by TS 33.310 [5]. IKEv2 shall be supported conforming to the IKEv2 profile described in TS 33.310 [5].

9.4 Security mechanisms for the Xn interface

Xn is the interface connecting NG-RAN nodes. It consists of Xn-C and Xn-U. Xn-C is used to carry signalling and Xn-U user plane data.

The transport of control plane data and user data over Xn shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the Xn reference point, it is required to implement IPsec ESP and IKEv2 certificate-based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec shall be supported on the gNB and ng-eNB.

9.8.2 Security mechanisms for the F1 interface

The F1 interface connects the gNB-CU to the gNB-DU. It consists of the F1-C for control plane and the F1-U for the user plane. The security mechanisms for the F1 interface connecting the IAB-node to the IAB-donor-CU are detailed in clause M.3.3 of this document.

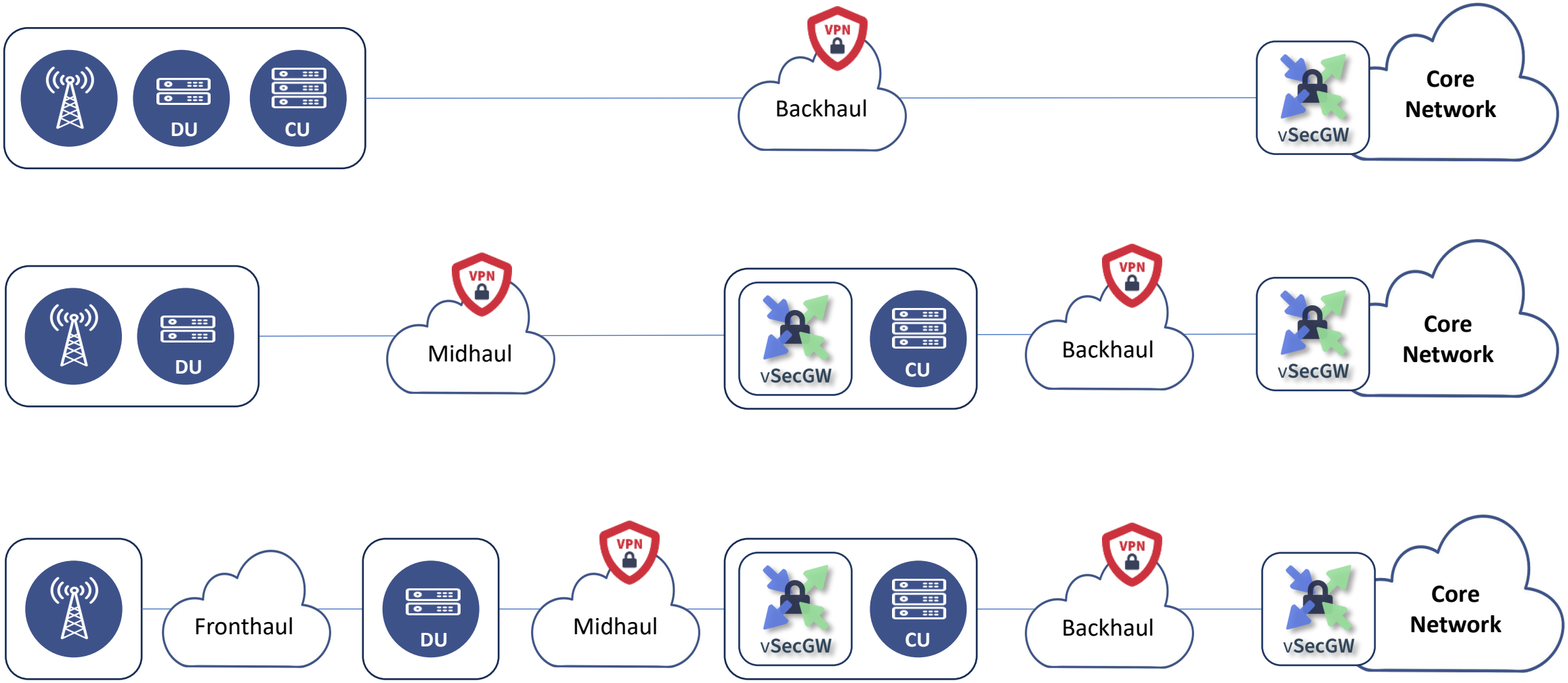
In order to protect the traffic on the F1-U interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In order to protect the traffic on the F1-C interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

IPsec is mandatory to implement on the gNB-DU and on the gNB-CU. On the gNB-CU side, a SEG may be used to terminate the IPsec tunnel.

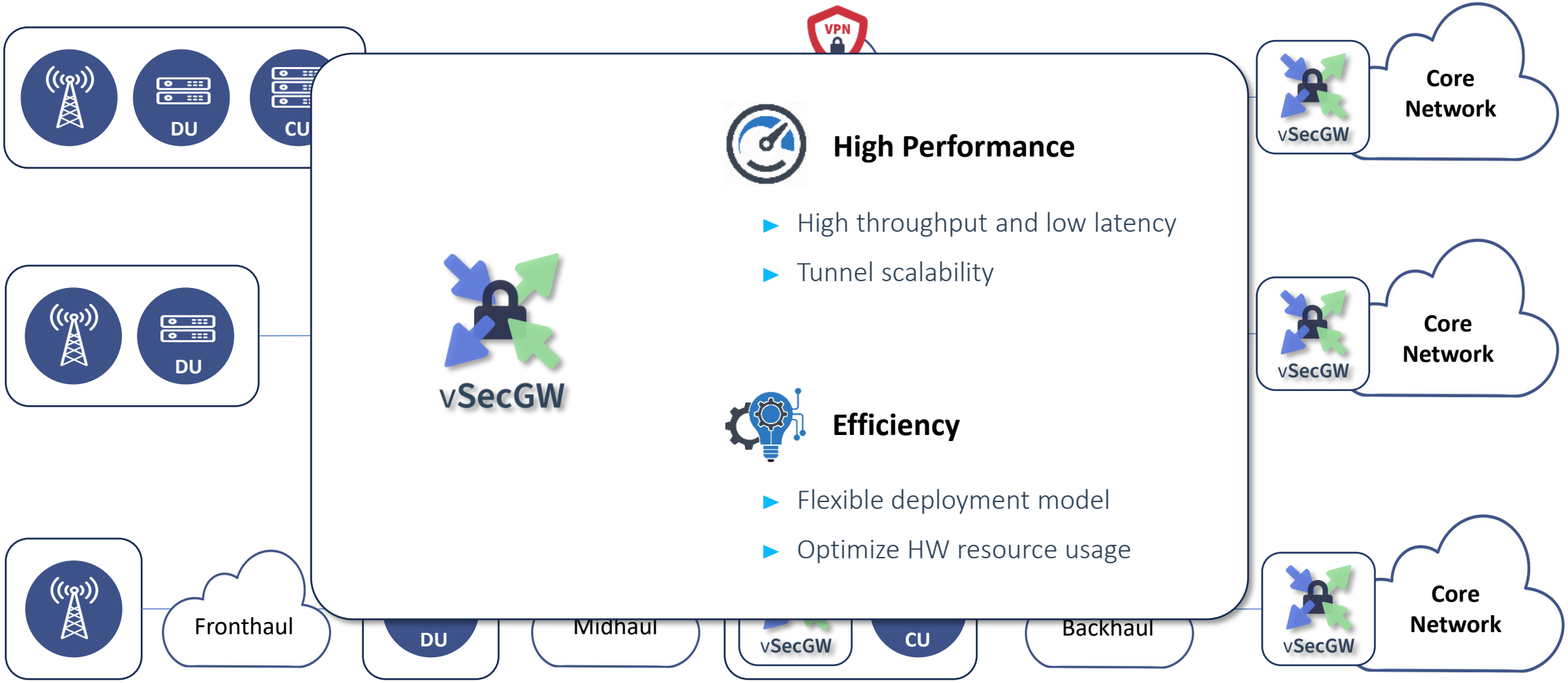
6WIND vSecGW : Securing Mobile Networks

Deployment options



6WIND vSecGW : Securing Mobile Networks

Deployment options



vSecGW

Forwarding and IPsec Performance

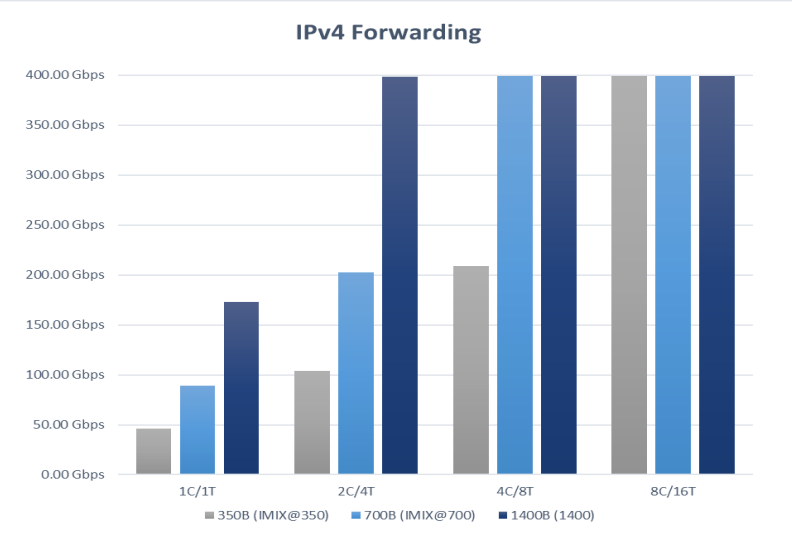
Demo Lab : Leveraging Intel's Power base

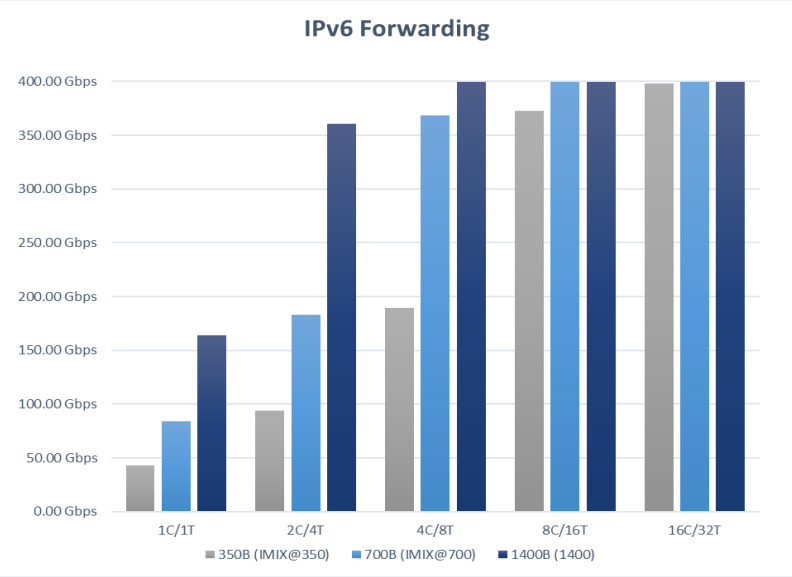
Testbeds

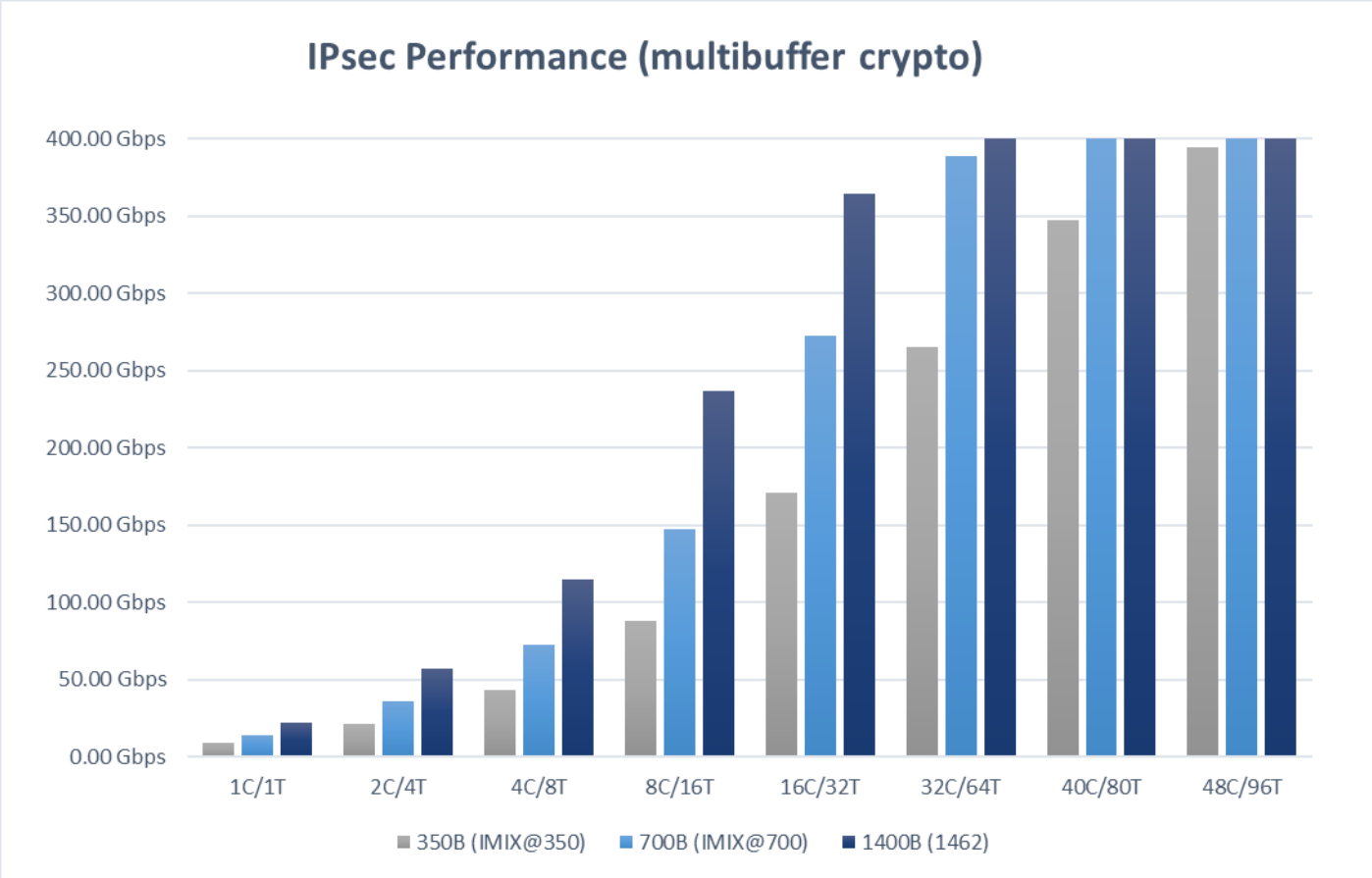
- ✓ Performance Benchmarking
- ✓ Boosting Business Agility
- ✓ Enabling innovation

Performance Benchmarks : Dual Stack (v4/v6) Performance

Pure software performance







Test platform: Intel® Xeon® Gold 6342 CPU @ 2.80GHz
Pure software performance, with no HW acceleration
IPsec performance based on AES-GCM
Line rate performance (400GBps) using 2 x Intel E810

Performance Benchmarks : Dual Stack (v4/v6) Performance

Forwarding Performance

IMIX$_{350B}$	Per Core	46 Gbps
	Line Rate	8 CPU Core
IMIX$_{700B}$	Per Core	90 Gbps
	Line Rate	4 CPU Core
1400B	Per Core	180 Gbps
	Line Rate	2 CPU Core

IPsec Performance

IMIX$_{350B}$	Per Core	9 Gbps
	Line Rate	48 CPU Core
IMIX$_{700B}$	Per Core	14 Gbps
	Line Rate	40 CPU Core
1400B	Per Core	22 Gbps
	Line Rate	32 CPU Core

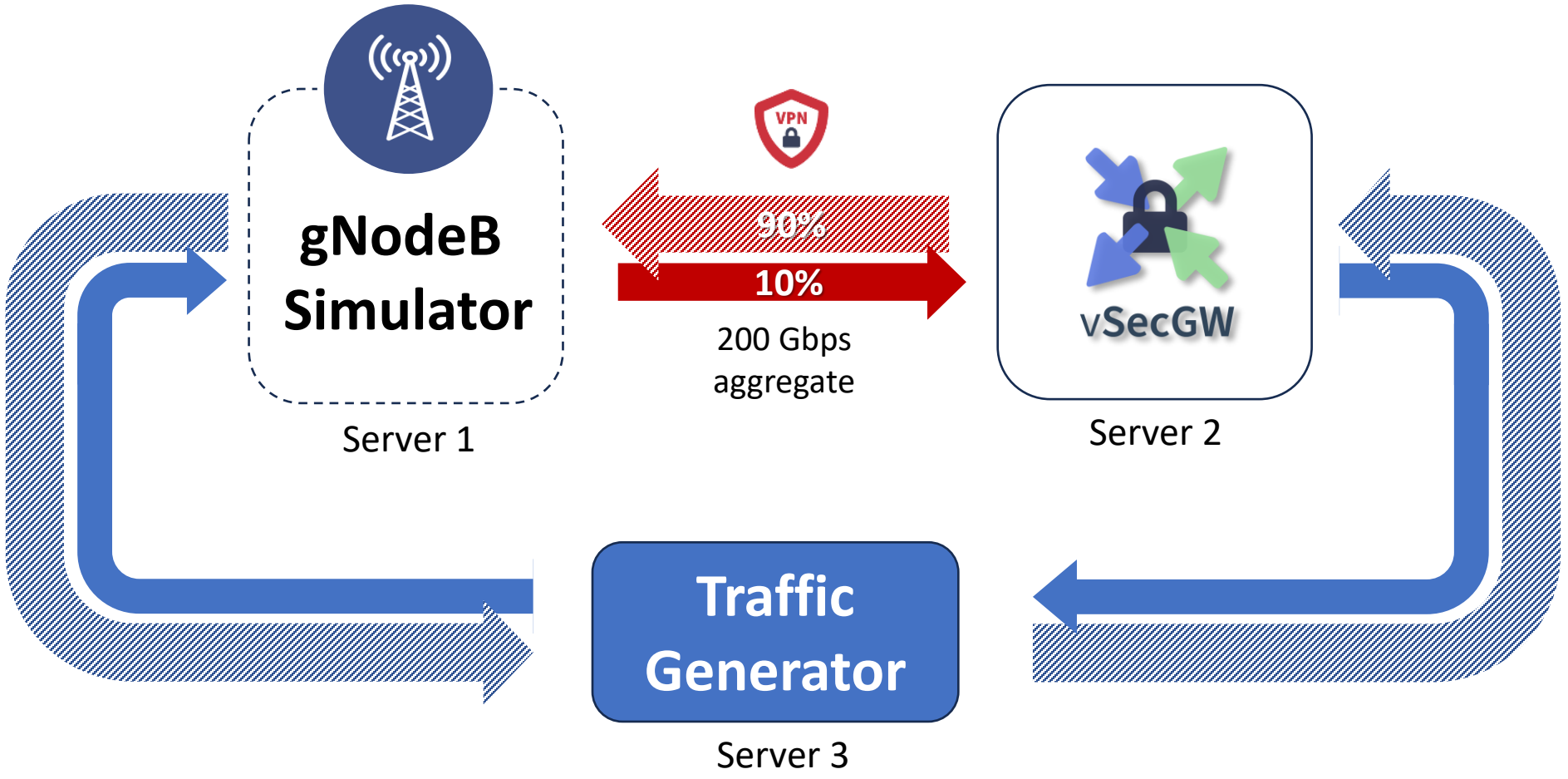
Test platform: Intel® Xeon® Gold 6342 CPU @ 2.80GHz
Pure software performance, with no HW acceleration
IPsec performance based on AES-GCM
Line rate performance (400GBps) using 2 x Intel E810

vSecGW

Mobile Security Gateway

6WIND vSecGW : Demo Setup

High-level design

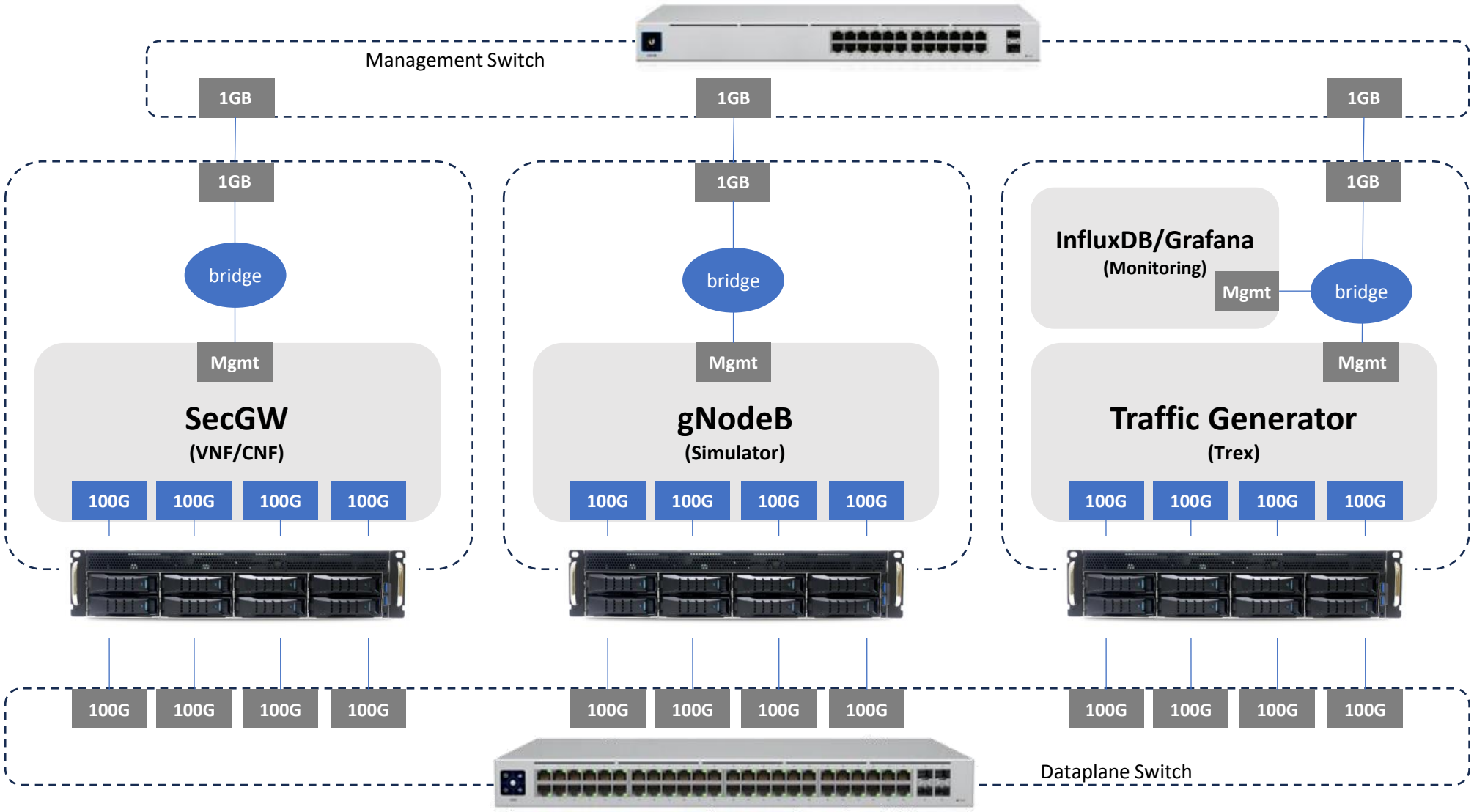


Each server includes:

- 2 x Intel® Xeon® Gold 6342 CPU @ 2.80GHz (24 cores / 48 threads each)
- 2 x Intel® Ethernet Network Adapter E810-2CQDA2 (one dual-port card on each NUMA node)
- 512GB RAM

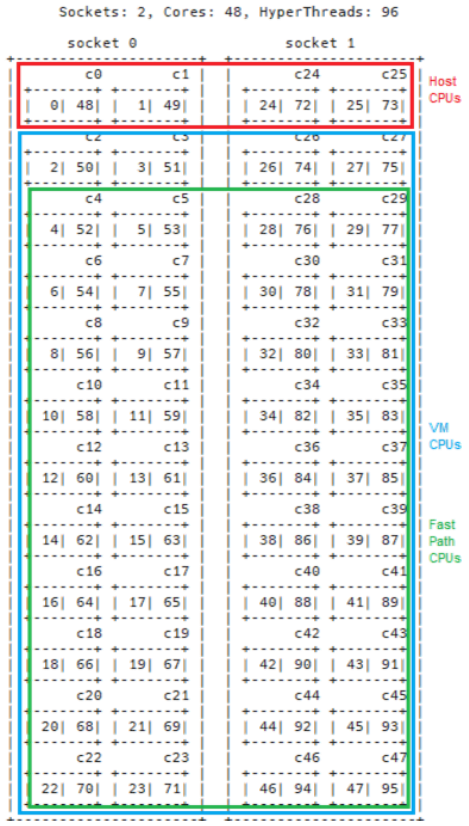
6WIND SecGW : Testbed design

Physical topology

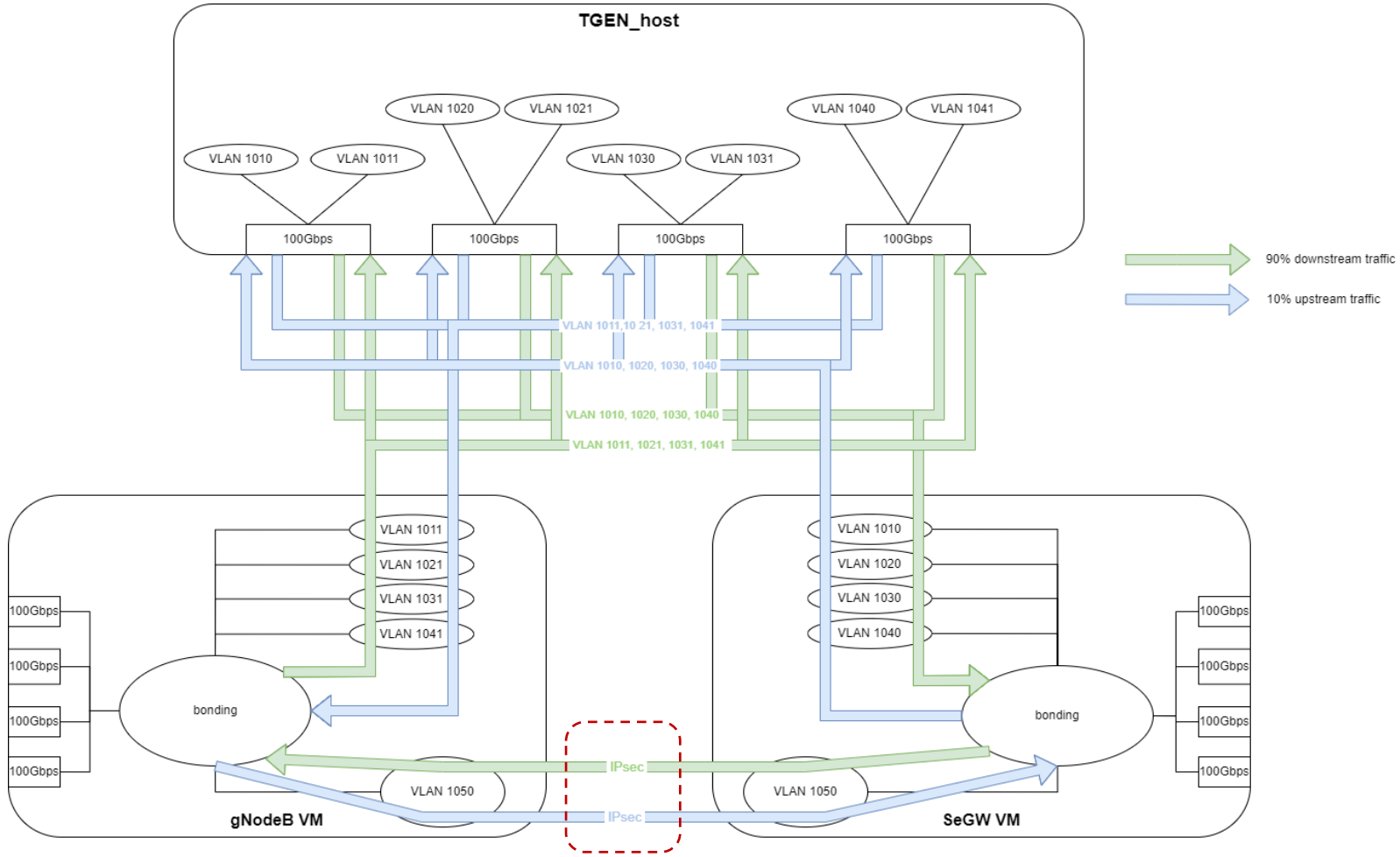


6WIND SecGW : Testbed design

Logical topology



CPU allocation on SeGW-host



6WIND vSecGW : Running the tests

Packet Lengths (Byte)	Downlink	Uplink	Avg. Packet Length
40-79	13%	65%	60
80-159	12%	24%	120
160-319	2%	3%	240
320-639	2%	2%	480
640-1279	2%	2%	960
1280-2559	69%	4%	1500

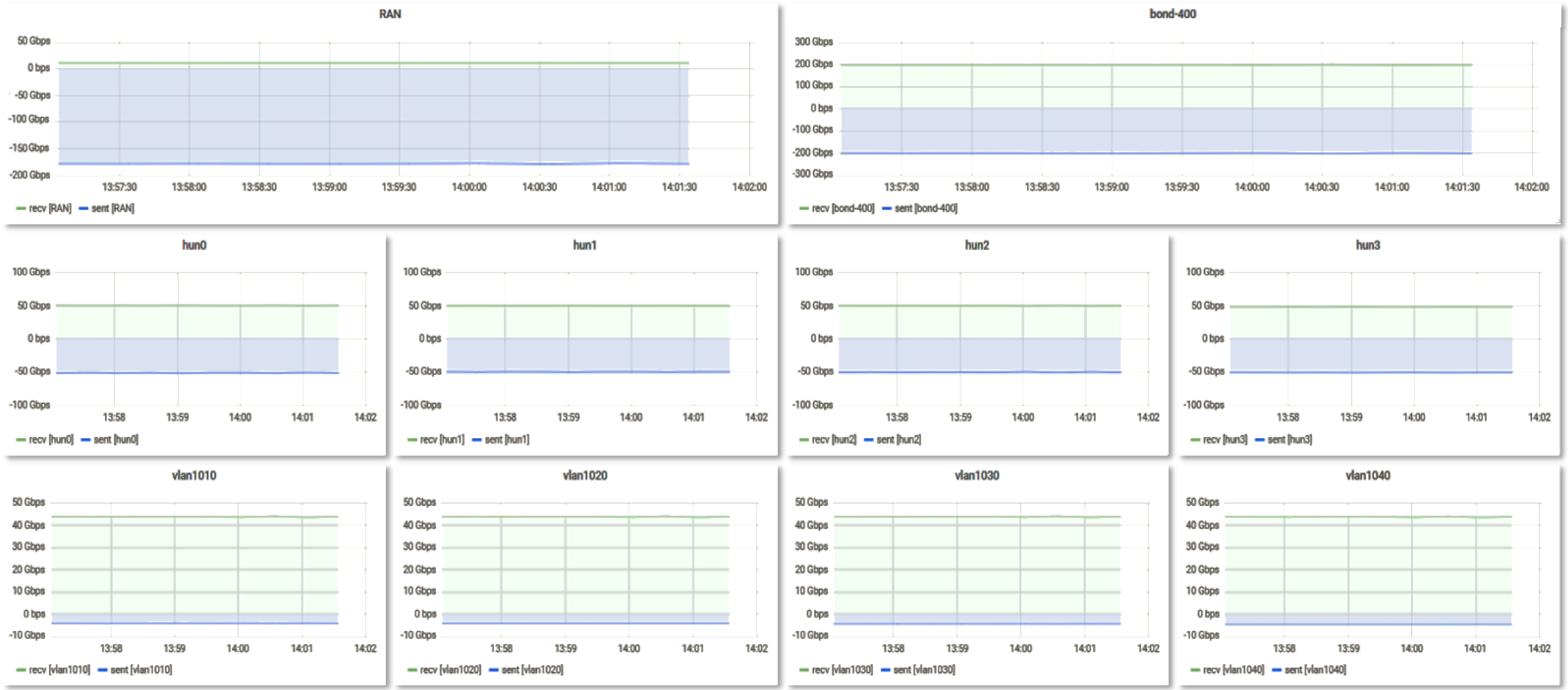
IMIX traffic profile

```
segw> show ike ike-sa-count vrf untrusted
100000

segw> show ipv4-routes summary vrf trusted
Route Source          Routes               FIB  (vrf default)
kernel                100000               100000
connected             4                    4
static                1                    1
------
Totals                100005               100005
```

Established IPv4 Routes and IKE SAs

```
Global Statistics

connection   : localhost, Port 4501
version      : STL @ v3.02
cpu_util.    : 4.85% @ 48 cores (24 per dual port)
rx_cpu_util. : 0.0% / 0 pps
async_util.  : 0% / 41.01 bps
total_cps.   : 0 cps

total_tx_L2  : 194.76 Gbps
total_tx_L1  : 200.26 Gbps
total_rx     : 193.95 Gbps
total_pps    : 34.42 Mpps
drop_rate    : 0 bps
queue_full   : 0 pkts

Port Statistics

   port    |         0          |         1          |         2          |         3          |       total
-----------+--------------------+--------------------+--------------------+--------------------+------------------
owner      |               root |               root |               root |               root |
link       |                 UP |                 UP |                 UP |                 UP |
state      |       TRANSMITTING |       TRANSMITTING |       TRANSMITTING |       TRANSMITTING |
speed      |          100 Gb/s  |          100 Gb/s  |          100 Gb/s  |          100 Gb/s  |
CPU util.  |              4.8%  |              4.8%  |              4.89%  |              4.89%  |
--         |                    |                    |                    |                    |
Tx bps L2  |       48.69 Gbps   |       48.69 Gbps   |       48.69 Gbps   |       48.69 Gbps   |     194.76 Gbps
Tx bps L1  |       50.07 Gbps   |       50.07 Gbps   |       50.07 Gbps   |       50.07 Gbps   |     200.26 Gbps
Tx pps     |        8.6 Mpps    |        8.6 Mpps    |        8.6 Mpps    |        8.6 Mpps    |      34.42 Mpps
Line Util. |          50.07 %   |          50.07 %   |          50.07 %   |          50.07 %   |
---        |                    |                    |                    |                    |
Rx bps     |       48.87 Gbps   |       49.16 Gbps   |       48.11 Gbps   |       47.81 Gbps   |     193.95 Gbps
Rx pps     |        8.51 Mpps   |        8.57 Mpps   |        8.55 Mpps   |        8.65 Mpps   |      34.28 Mpps
----       |                    |                    |                    |                    |
opackets   |           47882024 |           47882095 |           47881999 |           47882740 |         191528858
ipackets   |           47370936 |           47669046 |           47583991 |           48126321 |         190750294
obytes     |        33870273544 |        33870339208 |        33870269484 |        33870802264 |      135481684500
ibytes     |        33995371000 |        34196958756 |        33468059840 |        33258611068 |      134919000664
tx-pkts    |       47.88 Mpkts  |       47.88 Mpkts  |       47.88 Mpkts  |       47.88 Mpkts  |     191.53 Mpkts
rx-pkts    |       47.37 Mpkts  |       47.67 Mpkts  |       47.58 Mpkts  |       48.13 Mpkts  |     190.75 Mpkts
tx-bytes   |         33.87 GB   |         33.87 GB   |         33.87 GB   |         33.87 GB   |       135.48 GB
rx-bytes   |           34 GB    |          34.2 GB   |         33.47 GB   |         33.26 GB   |       134.92 GB
-----      |                    |                    |                    |                    |
oerrors    |                  0 |                  0 |                  0 |                  0 |                0
ierrors    |                  0 |                  0 |                  0 |                  0 |                0
```

6WIND vSecGW : Performance Monitoring



vSecGW

Take Aways

Why 6WIND vSecGW?

6WIND vSecGW

Efficiently Enable Security in Mobile Networks

vSecGW

- Flexible and Agile deployment
- Fully virtualized (VNF & CNF)
- High Performance and Scalability
- COTS server based
- No HW acceleration required
- Enhanced Power Efficiency
- Lower TCO

x3 Performance

50% Lower Cost

x3 HW Savings

5G

- ✓ Private and Public
- ✓ Access Network security
- ✓ MEC security
- ✓ Network Slicing
- ✓ Network sharing (MOCN, MORAN)

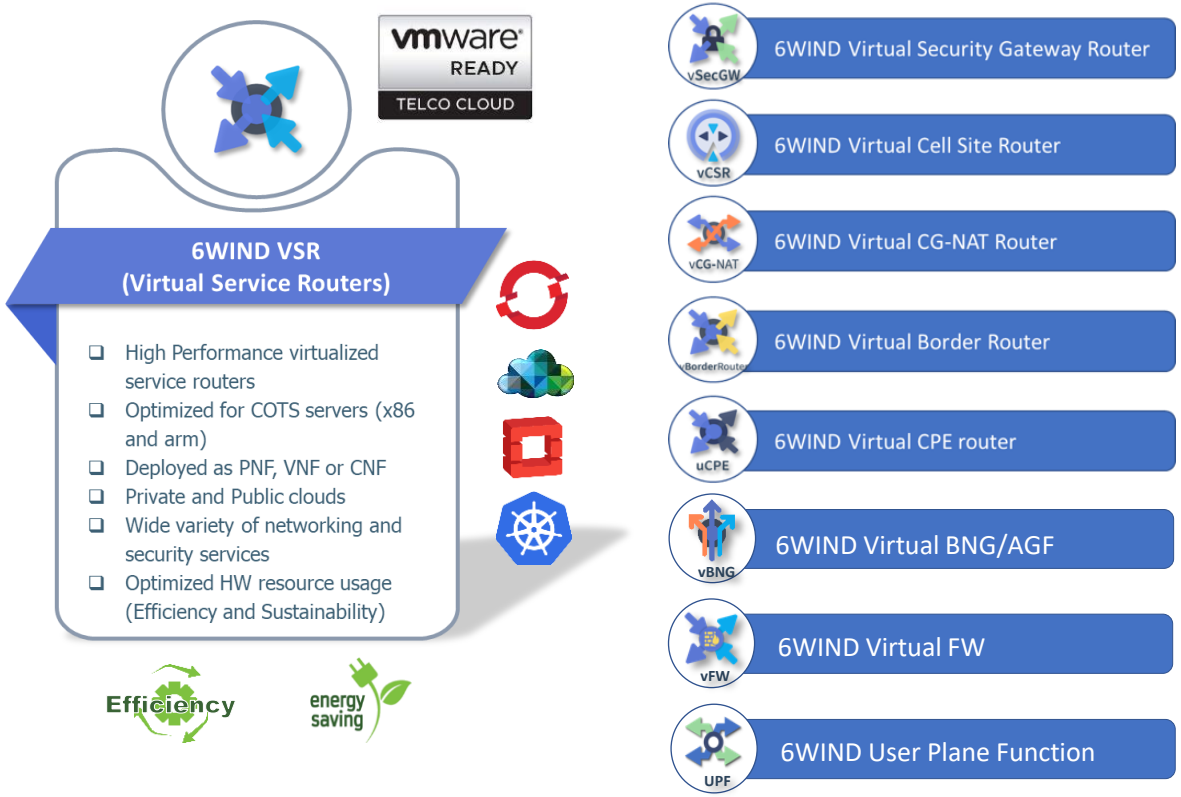
Call to Actions

Assistance

Network Virtualization Journey
Optimizing Network Efficiency
Improving Network Security TCO
Delivering High Performance in the Cloud

Considering Projects

Private Wireless Networks
Multi Access Edge Computing
Open RAN
Virtualization of Network Functions



Register for a free evaluation: https://www.6wind.com/vsr-evaluation

Thank You!

www.6wind.com

6WIND EMEA HQ
Paris, France

6WIND Americas HQ
Santa Clara, USA

6WIND APAC HQ
Singapore