White Paper

CSP, Enterprise
Telecom 5G/Wi-Fi Access

Wipro N3IWF Reference Delivers 100Gbps[1] Throughput to 5G Core

In tests, the Wipro N3IWF reference for secure access of untrusted Wi-Fi-devices to 5G core networks, delivered 100Gbps throughput running on 4th Gen Intel® Xeon® Scalable processors with integrated Intel® QuickAssist Technology (Intel® QAT) and Intel® Ethernet 800 Series Network Adapters

Table of Contents

The Promise of 5G

The rapid expansion of mobile network users and devices across different technologies, new and legacy, as well as vertical adoption of industrial communications technologies such as Internet of Things (IoT), drive the need for 5G mobile networks, which address capacity, coverage and data congestion challenges raised by these new use cases.

Because it is built on a service-based architecture (SBA) and has a software-defined network structure, 5G is highly flexible and offers the promise of ubiquitous access-agnostic connectivity, as defined by the 3rd Generation Partnership Project (3GPP). As such, 5G services can be available over the 5G core network (5GCN), even for non-3GPP user equipment (UE) and networks, whether trusted or non-trusted, wireline or wireless, such as those for wireless LAN (WLAN) access points and residential gateways.

Seamless integration of non-3GPP access networks with 5G minimizes operational costs, and benefits include Enhanced Mobile Broadband (eMBB) for increased bandwidth; Massive Machine Type Communications (mMTC) for high connection density, and Ultra-Reliable Low Latency Communication (URLLC) for reduction in end-to-end latency.

Untrusted, non-3GPP networks and devices are those that the mobile network operator (MNO) does not have direct control over, such as enterprise and home Wi-Fi or public hotspots, and therefore does not control device or network security. To integrate untrusted networks and devices into the 5GCN, 3GPP developed a gateway, the Non-3GPP Interworking Function (N3IWF). Some of the use cases for the gateway include:

- Access to a 5G core from an untrusted Wi-Fi connection
- Supporting multi access PDU sessions
- Provide Wi-Fi access for edge computing

N3IWF supports both N2 (control plane) and N3 (user plane) interfaces to 5GCN, and secure connections with support for internet protocol security (IPsec) via encrypted tunnels (NWu), between untrusted UE and the 5GCN. By enabling N3IWF with secure convergence between untrusted non-3GPP networks and devices, access networks gain the following benefits:

- Avoid data congestion and reduce backhaul costs with increased capacity and intelligent traffic offloading

- Provide better coverage and connectivity in high density traffic environments and indoor environments
- Enable new business opportunities with value added services, innovative mobility solutions and mobile engagement
- Reduce operator capital and operational costs with increased capacity and unified management
- Deliver enhanced services to customer in a cost-efficient manner

Wipro N3IWF Virtual Gateway

Wipro's N3IWF virtual gateway reference solution (Figure 1) allows a UE to access a 5GCN from an untrusted WLAN through secure registration and authentication via IPsec tunneling.

The untrusted WLAN interworking with the 5GCN supports the following interfaces:

- NWu reference point between the UE and N3IWF for establishing secure tunnel(s) between the UE and N3IWF so that control-plane and user-plane traffic between the UE and the 5GCN is transferred securely over untrusted non-3GPP access
- Y1 reference point between the UE and the WLAN
- Y2 reference point between the WLAN and the N3IWF for the transport of NWu traffic
- N1 reference point between the UE and the access and mobility function (AMF)
- N2 reference point between the N3IWF and the AMF
- N3 reference point between the N3IWF and the UPF

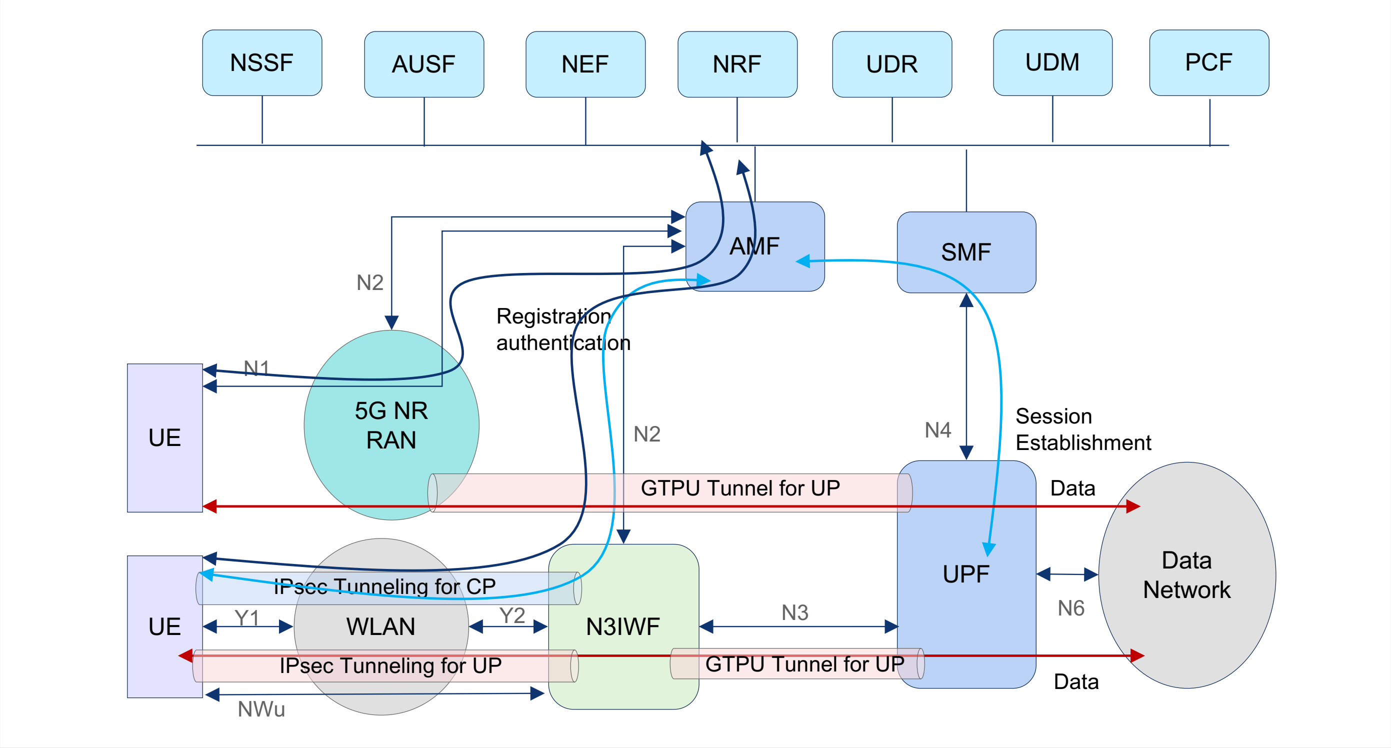

Figure 1. Architecture for untrusted WLAN internetworking with a 5GCN; diagram shows the data path for both a trusted and untrusted UE to access the 5GCN.

Wipro's N3IWF virtual gateway reference maintains secure access to the 5GCN from untrusted WLAN with high throughput, up to 100Gbps (see test results later in this paper) and supporting IPsec acceleration (Figure 2). The gateway can utilize open source functionality to improve performance. Wipro regularly utilizes the Intel-developed open source Data Plane Development Kit (DPDK) to improve virtual networking throughput, and the Vector Packet Processing (VPP) platform to provide layer three switching functionality.

The CP protocol stacks provide protocols used in UE, WLAN, N3IWF and AMF establish initial registration and authentication, NAS mobility and session management, and establish UP between N3IWF and UE.

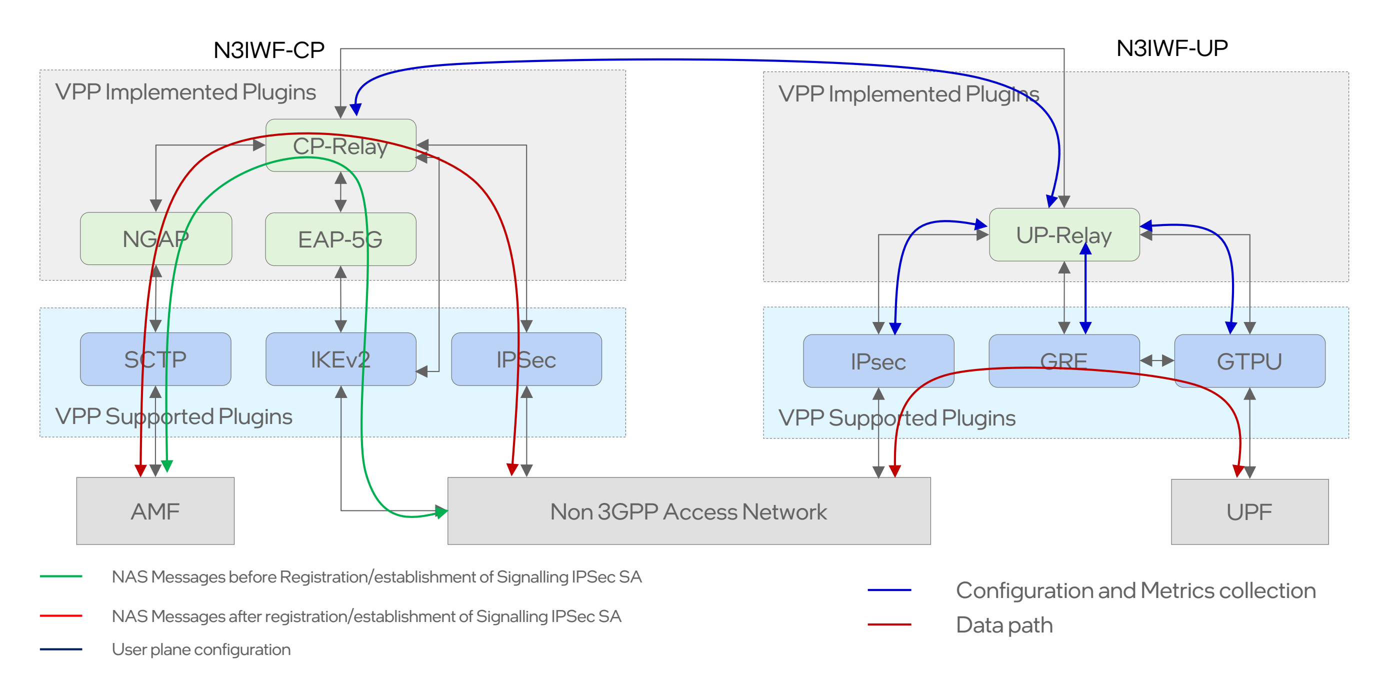

Figure 2. Control plane and user plane configuration, metrics collection, and data path.

N3IWF Functionality

The N3IWF control plane and user functionality for accessing the 5GCN from an untrusted WLAN includes:

Control Plane

- Support of IPsec tunnel establishment with UE over NWu using IKEv2/IPsec protocols
- Establishment of signaling IPsec security association (SA) for non-access stratum (NAS) messages and protocol data unit (PDU) session traffic
- Termination of N2 interface using NG application protocol (NGAP) and stream transmission control protocol (SCTP) to AMF
- Relaying uplink/downlink control plane NAS (N1) signaling between UE and selected AMF
- NAS messages to authenticate and register UE, authorize access to 5GCN, and establish PDU sessions
- Handling N2 signaling from SMF relayed by AMF related to PDU sessions and quality of service (QoS)

User Plane

- Termination of N3 interface using GTPU protocol to UPF
- Relaying uplink/downlink user plane packets between UE and UPF
- Decapsulation/encapsulation of packets for IPsec and GTPU tunnelling
- N3 user plane packet marking in uplink
- Enforcing QoS corresponding to N3 packet marking

Speed and Scalability with Intel

Wipro is an Intel® Network Builders ecosystem partner and recommends the use of servers based on 4th Gen Intel® Xeon® Scalable processors with integrated Intel® QAT and Intel® Ethernet 800 Series Network Adapters for N3IWF deployments. 4th Gen Intel Xeon Scalable processors are based on a balanced, efficient architecture that increases core performance, memory, and I/O bandwidth to accelerate diverse workloads from the data center to the network edge.

With support for higher memory speeds, enhanced memory capacity, and up to four-socket scalability, 4th Gen Intel Xeon Platinum processors deliver improved performance, enhanced memory capabilities, hardware-enhanced security, and workload acceleration. These processors are optimized for demanding mainstream data center, multi-cloud compute, and network and storage workloads. 4th Gen Intel Xeon Platinum Scalable processors support up to 52 cores per processor and up to eight memory channels at up to 4800 MT/s, driving enhanced performance, throughput, and CPU frequencies compared to previous-gen processors.

The 100GbE Intel Ethernet 800 Series Network Adapters offer exceptional compatibility, interoperability, and performance to meet the requirements of a demanding range of communications workloads. The Intel Ethernet Network Adapter E810-CQDA2 improves N3IWF application efficiency and network performance with its dual-port configuration and 100/50/25/10GbE per port data rates, packet-classification, and sorting optimizations, and a fully programmable pipeline. Features include network data throughput up to 100 Gbps per adapter for high-performance virtual radio access networks (vRANs), network functions virtualization (NFV) forwarding plane, storage, high performance computing (HPC), cloud and content delivery networks (CDN).

The integrated Intel® QAT provides hardware acceleration to assist with the performance demands of applications such as N3IWF. The integrated Intel® QAT provides up to 50 Gbps of IPsec crypto acceleration in the uplink/downlink N3IWF data plane with an aggregate of up to 100Gbps IPsec crypto acceleration.

Test Network Set Up

The goal of this test is to show the bi-directional data path throughput from various packet sizes by testing gateway performance when the N3IWF with minimal number of CPU cores augmented with Intel® QAT.

The system under test (SUT) server was based on an Intel® Xeon® Platinum 8470N processor with integrated Intel® QAT, which also utilized the Intel® Ethernet Network Adapter E810-CQDA2 with two ports operating at 100 Gbps (Figure 3).

Performance Drivers

- SUT server with dual Intel® Xeon® Platinum 8470N processors
- Using a 52-core CPU with optimized hyperthreading (108 threads) and memory cache for optimized stateful flow processing
- Integrated Intel® QAT for hardware acceleration of cryptographic functions
- Intel single root I/O virtualization (SR-IOV) mode for creating virtual functions
- DPDK and Vector Packet Processing (VPP) were leveraged for fast packet processing
- Total memory was 256 GB DDR5, DCPMM

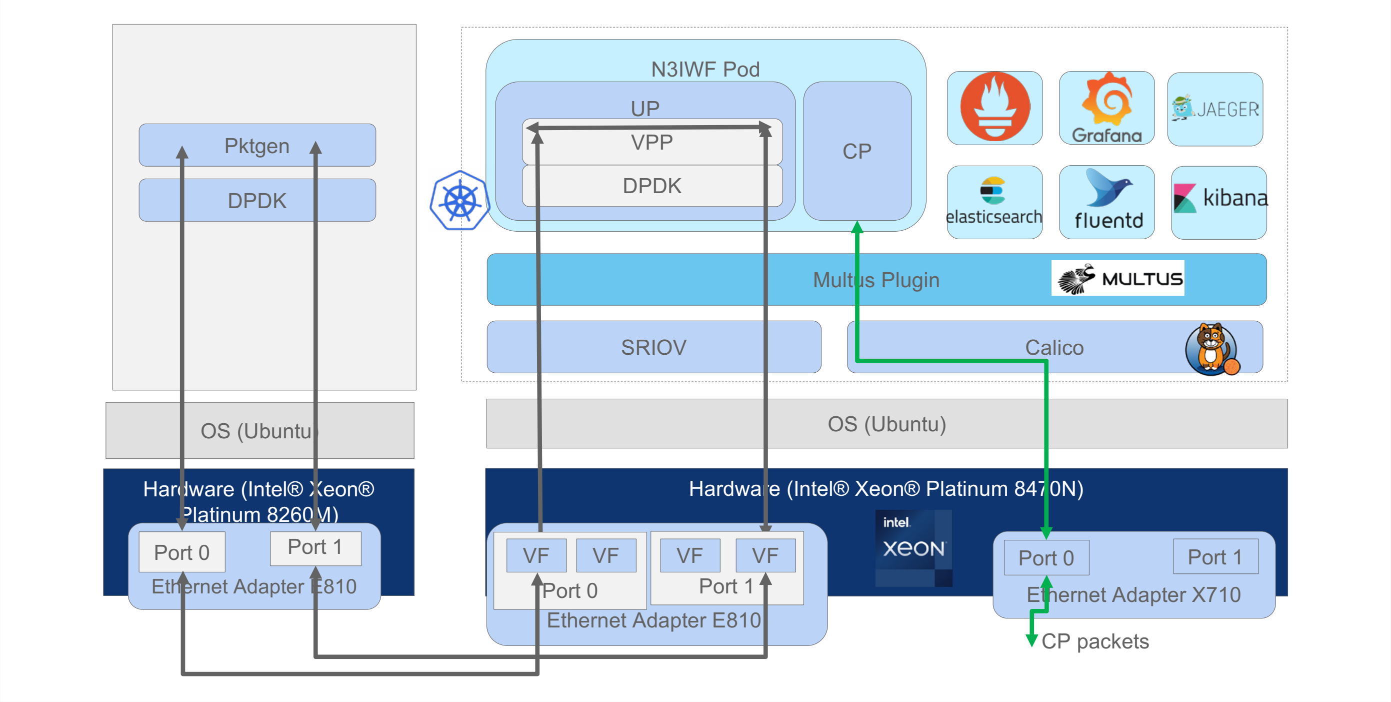

Figure 3. N3IWF is run in a container with the packet generator in another server. N3IWF runs with one core for the main thread and two worker threads each with one core, one Rx, and one Tx queues. DPDK's Pktgen packet generator ran using five cores – one core for main and two cores each for two ports.

Software Configuration

The SUT utilized the Wipro N3IWF software configuration including Ubuntu operating system (OS) and the 5.15.0-87-generic kernel. The N3IWF is based on VPP and DPDK stack for fast path processing utilizing SRIOV VFs for input and output. The N3IWF was deployed as pod in a Kubernetes cluster along with required plugins as a cloud native function in cloud native environment with EFK stack for logging and Prometheus and Grafana for monitoring. The N3IWF was deployed utilizing one core for the main thread and two worker threads each with one core, one Rx, and one Tx queues along with two Intel® QAT VFs.

Pktgen was deployed in another server and used to send the uplink/downlink packets through the N3IWF and utilized one core for main thread and two cores each for two ports.

Test Results

The test results (Figure 4) show that the N3IWF based on a 4th Gen Intel® Xeon® Platinum Processor with integrated Intel® QAT enables customers to support Wi-Fi clients that can securely access the 5GCN through untrusted Wi-Fi access networks using IPsec security with bi-directional throughput up to 100Gbps (Figure 5). For large packet sizes, maximum throughput for the user plane is approximately 98 Gbps. Because of the integrated Intel® QAT accelerator engines throughput is minimally impacted by processing IPsec data.

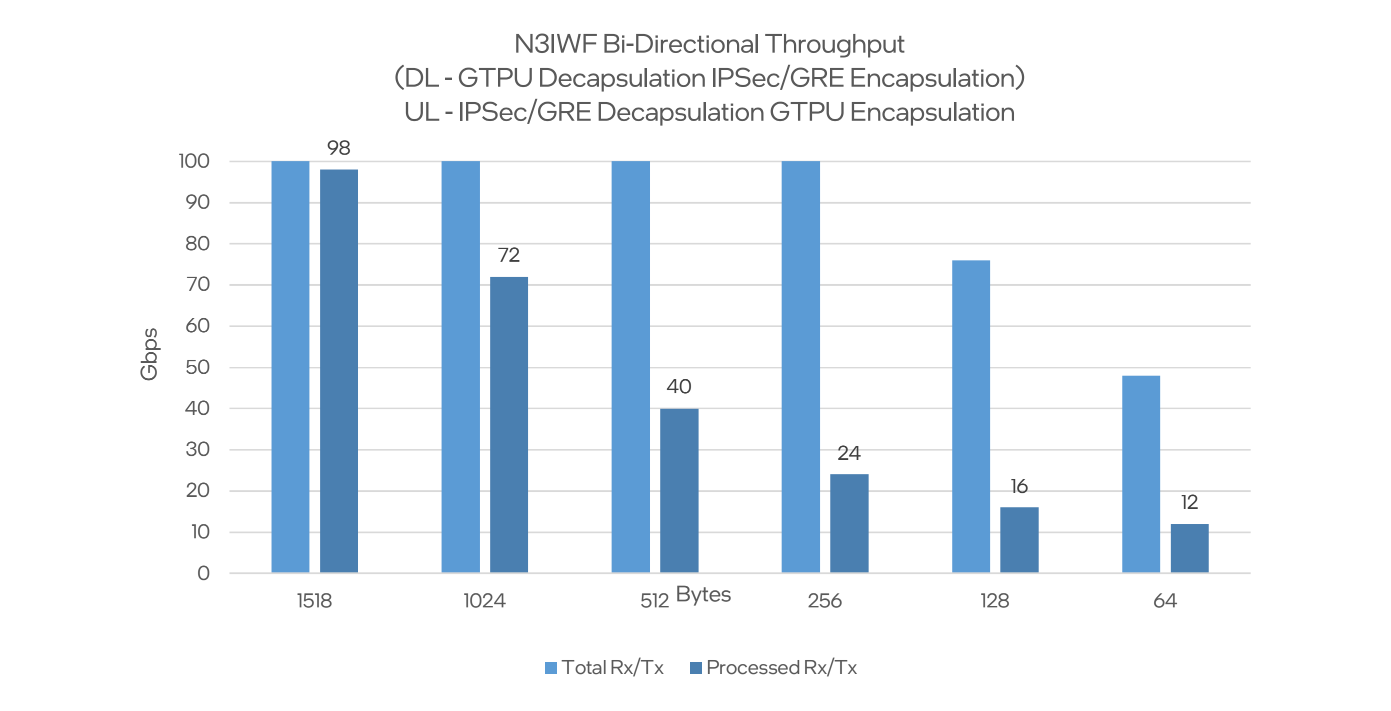

Figure 4. Light blue bars represent total throughput at a variety of packet sizes (higher equals more bandwidth). The dark blue bars represent IPsec processed packets (higher equals more bandwidth).

Conclusion

By implementing the Wipro N3IWF on 4th Gen Intel® Xeon® Platinum CPUs, along with the Intel® Ethernet Network Adapter E810 and Intel® QAT acceleration, untrusted non-3GPP networks and UE can securely access the 5GCN at line speeds. This paves the way for MNOs and enterprises to unify heterogenous access networks to gain all the benefits delivered by 5G.

Learn More

Wipro N3IWF

Wipro

Intel® Xeon® Gold Processors

Intel® Network Builders

Notices & Disclaimers

[1] Test Server: 1-node, 2x 1.7GHz Intel® Xeon® Platinum 8470 with 256 GB (16 slots/16GB)total DDR5 memory, microcode 0x2b0004d0, HT on, Turbo on, dual port 100GbE Intel® Ethernet E810-CQDA2. Operating system was Ubuntu 5.15.0-87-generic, 1x Intel_SSDSC2KG96 960 GB, Wipro UPF and N3IWF compiler is gcc, other software is DPDK and VPP, test by Wipro in Sept. 2023.

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

0124/LV/H09/PDF ♻ Please Recycle 358350-001US