



Carrier-Grade Security for the Mobile Core, from RAN to Internet

6WIND turns mobile security into software, so MNOs, MVNOs and MVNEs can encrypt RAN backhaul, protect the Gi/N6-LAN and scale CGNAT on infrastructure they control.

Challenges

- ▶ *Encrypting the RAN at scale*
- ▶ *The Gi/N6-LAN is the exposed surface*
- ▶ *IPv4 exhaustion and the IPv6 transition*
- ▶ *Hardware dictated by the vendor*

The Solution

- ▶ *One platform, purpose-built functions.*
- ▶ *Carrier-grade scale.*
- ▶ *Built for availability*
- ▶ *Standards-aligned.*

Use Cases

- ▶ *RAN-to-core IPsec backhaul (Mobile Security Gateway)*
- ▶ *Gi/N6-LAN firewall and CGNAT*
- ▶ *Secured interconnection with mobile and value-added service partners*
- ▶ *Secure IoT backhaul*
- ▶ *Extension: distributed and local UPF*

Mobile traffic keeps climbing. 5G adoption and bandwidth-intensive applications such as video and gaming push more data through the mobile core every year — and every gigabit that reaches the core has to be encrypted, inspected or translated on its way.

At the same time, the threat has changed. Mobile networks are critical infrastructure: they carry emergency services, utilities, transport and payments, and they are targeted accordingly — DDoS floods at the internet edge, exposed RAN transport links, and partner interconnects used as a way into the core. Regulators are responding, and the EU's NIS2 directive brings telecom operators into its scope. Protection is moving from best practice to obligation.

Operators have to do all of this while cutting cost. The traditional answer — security appliances and hardware chassis sized for peak and refreshed on the vendor's schedule — scales in expensive hardware steps and ties the roadmap to a single supplier.

Software changes the equation: security that grows with the cores you allocate, on servers you choose, deployed wherever the core runs. One caveat: an unoptimized stack consumes the savings it was meant to create, so throughput per core decides whether the economics work.

The Challenges

- ▶ **Encrypting the RAN at scale.** 3GPP TS 33.501 requires every gNB to implement IPsec and allows a security gateway to terminate it in the core; turning it on is left to the operator, and regulation increasingly makes that call. The gateway must hold tens of thousands of tunnels, authenticate against the operator's PKI from day one, and survive failures without dropping sessions.
- ▶ **The Gi/N6-LAN is the exposed surface.** Untrusted internet traffic, DDoS flooding and tens of millions of concurrent sessions hit the core's internet edge at hundreds of Gbps — with stateful inspection and audit-grade logging enforced at line rate.

- ▶ **IPv4 exhaustion and the IPv6 transition.** Devices outnumber available IPv4 addresses, making CGNAT mandatory. IPv6-only cores still need NAT64 and 464XLAT to reach IPv4 content, and every translation has to be recorded.
- ▶ **Hardware dictated by the vendor.** A telco cloud strategy collides with security appliances on proprietary hardware. As traffic grows, some operators that virtualized are pushed back to boxes by their incumbent vendor, losing the flexibility and cost model they moved to software for.

The 6WIND Solution

6WIND secures both ends of the mobile user plane from one software platform. 6WIND Virtual Service Router delivers purpose-built IPsec security gateway, stateful firewall and CGNAT functions as virtualized or containerized network functions on standard servers — the same software on bare metal, in a VM, on Kubernetes or OpenShift, on a telco cloud or at any hyperscaler.

- ▶ **One platform, purpose-built functions.** vSecGW, vFW and vCGNAT share one VSR foundation — data plane, management model and tooling. Each is deployed and sized where it belongs, at RAN aggregation or on the Gi/N6-LAN, so internet-edge peaks never compete with RAN encryption for cores.
- ▶ **Carrier-grade scale.** Up to 800 Gbps validated and 100M+ sessions on the Gi/N6-LAN firewall; 100k+ IPsec tunnels with high, linear throughput per core.
- ▶ **Built for availability.** Stateful high availability on the security gateway and firewall, with active and backup tunnels per remote site.
- ▶ **Standards-aligned.** IKEv1/v2 with PSK, EAP or X.509, the latest algorithms, NAT44, NAT64 and 464XLAT, L3/L4 firewalling, DDoS flooding protection and session-aware routing.

Primary Use Cases

6WIND VNF	Use Case	Challenge Addressed	What It Delivers
vSecGW	RAN-to-core IPsec backhaul (Mobile Security Gateway)	Every gNB, eNB and small cell crossing untrusted transport must be encrypted. Tunnel counts grow with the RAN, and appliance gateways cap out on tunnel scale.	A security gateway terminating 10k+ tunnels per instance, IKEv2 with X.509 against the operator's PKI from day one, and stateful high availability.
vFW + vCGNAT	Gi/N6-LAN firewall and CGNAT	The internet edge of the mobile core carries untrusted traffic, DDoS flooding and IPv4 exhaustion at hundreds of Gbps, with every session logged.	Stateful L3/L4 firewall, flooding protection and NAT44, NAT64 and 464XLAT — up to 800 Gbps validated, 100M+ sessions, optimized logging.
vSecGW + vFW	Secured interconnection with mobile and value-added service partners	Partner operators and VAS providers connect directly to the mobile core. Every link has to be encrypted and filtered without a gateway stack per partner.	vSecGW and vFW on one platform and one operating model — 100k+ tunnels, a minimal footprint and consistent policy per partner.
vSecGW + vFW + NAT	Secure IoT backhaul	Thousands of remote sites per control center need redundant, encrypted tunnels with very demanding availability, in public or private cloud.	Route-based VPN with active and backup tunnels per site, with firewall and NAT from the same 6WIND platform and one operating model.
UPF	Extension: distributed and local UPF	Private 5G, fixed wireless access and edge breakout need the user plane close to users, integrated with a third-party 5G core.	3GPP Release 16 UPF (N3, N4, N6, N9; IP and Ethernet PDU), up to 300 Gbps validated and 1M GTP tunnels, on x86 or ARM.

STRATEGIC BENEFITS

Price to Performance

Up to 800 Gbps validated from 6WIND software on standard servers. Capacity scales with the cores you allocate.

Ubiquitous Deployment

The same software on bare metal, VM, container, Kubernetes, OpenShift, telco cloud or any hyperscaler. Same behavior everywhere.

Flexibility

A flexible licensing model and functions that scale up, down or out per site. Add a gateway, a firewall or a region without adding a platform.

Efficiency

High throughput per core at a minimal footprint means more protected traffic per server, less rack space and lower power per gigabit.

No Vendor Lock-In

European-engineered software on the infrastructure you choose. Hardware and software disaggregated, no vendor-dictated end-of-life.

Cutting Edge

Cloud-native and API-first, 5G-ready, with the latest IPsec algorithms and IPv6 transition mechanisms in a data plane under continuous development.

Proven in Production

6WIND secures the user plane of mobile operators, virtual operators and their partners.

Anonymized profiles:

- ▶ **A French mobile network operator** encrypted RAN traffic between its cell sites and mobile core with 6WIND vSecGW against a regulatory deadline — 10k+ IPsec tunnels per gateway, PKI-compliant from day one, and hardware-software disaggregation that scales with the RAN.
- ▶ **A Belgian MVNO and MVNE** kept its Gi/N6-LAN virtualized when its incumbent vendor pushed it to hardware. 6WIND vFW delivers advanced firewall and CGNAT at high throughput in a virtualized environment, on a flexible business model and with software ready for its future plans.
- ▶ **A Tier-1 North American operator** selected 6WIND vSecGW to replace 376 in-house security gateways for mobility and small-cell backhaul, with stateful and geo-redundant HA; migration in progress.
- ▶ **An OEM in Israel serving utilities** embedded 6WIND vSecGW in its IoT solution: thousands of sites per SCADA control center, active and backup tunnels per site, and firewall and NAT capabilities from the same 6WIND platform.
- ▶ **An Italian ISP** extended its fixed wireless access to 5G with a green-field, distributed 6WIND UPF integrated with a third-party 5G core, on a very small x86 or ARM footprint.

Learn more at 6wind.com or contact us at sales@6wind.com.