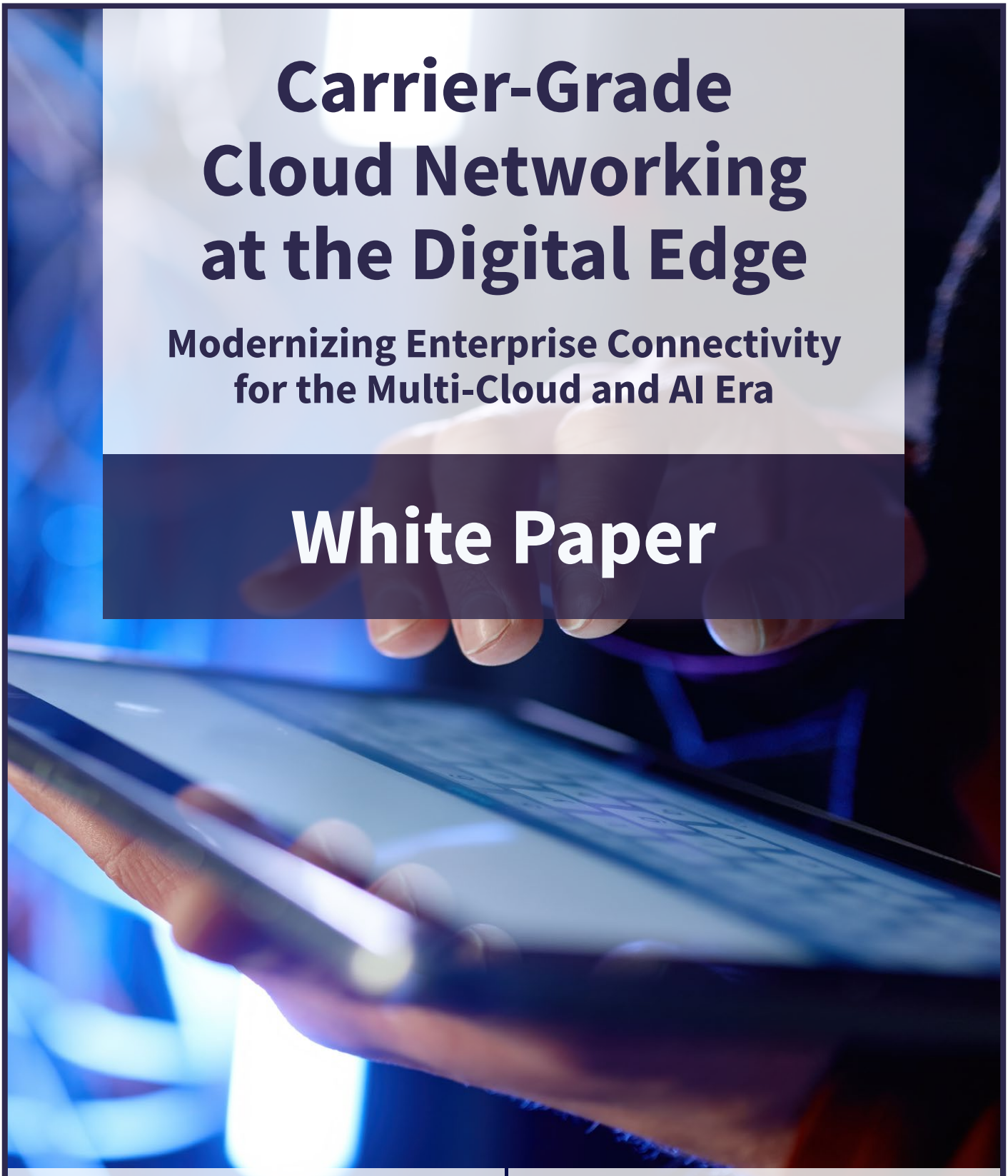
Carrier-Grade Cloud Networking at the Digital Edge

Modernizing Enterprise Connectivity for the Multi-Cloud and AI Era

White Paper



6WIND
Cloud Networking for AI

EQUINIX

www.6wind.com

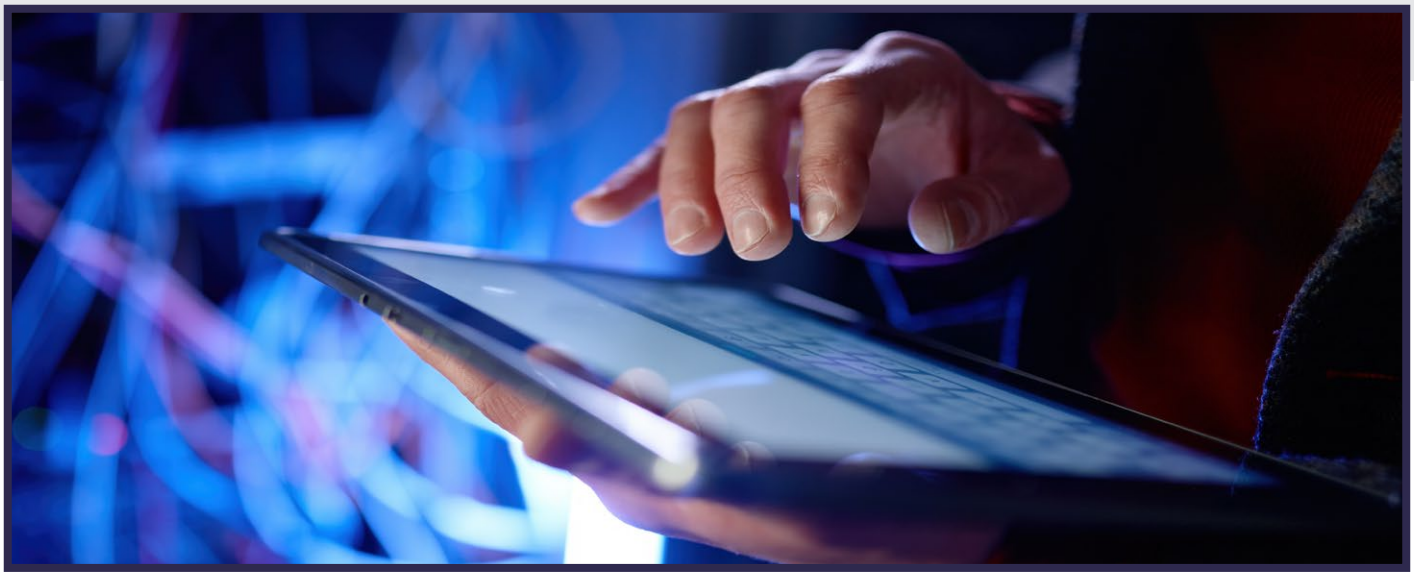


Table of Content

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

6WIND Copyright © 2026. All rights reserved.

Executive Summary

Enterprise networking is undergoing a structural transformation. Applications, users, and data are increasingly distributed across multiple public clouds, private infrastructure, SaaS ecosystems, edge locations, and emerging AI-driven environments.

Traditional WAN architectures and hardware-centric networking models were not designed for this level of distribution, scale, or operational agility. As a result, many enterprises are reassessing how connectivity, security, and interconnection services are delivered in cloud-first environments.

At the same time, infrastructure priorities continue to evolve. According to Flexera's 2025 State of the Cloud Report, managing cloud spend remains a top challenge for organizations operating in multi-cloud environments, even as cloud adoption continues to expand. This highlights the growing importance of networking architectures that support not only performance and agility, but also cost visibility and operational governance.

Modern enterprises now support increasingly complex requirements, including multi-cloud application environments, AI and data-intensive workloads, real-time analytics, edge computing, secure hybrid connectivity, distributed workforces, and dynamic partner ecosystems.

In response, a new model is emerging: **software-defined networking at the digital edge**, where networking and security functions are deployed closer to points of interconnection.

By combining the global interconnection capabilities of **Equinix Network Edge** with high-performance virtual networking software such as **6WIND Virtual Service Router (VSR)**, enterprises can deploy carrier-grade networking and security functions in software across global metros—reducing reliance on traditional hardware-centric deployments.

This approach enables a more agile, scalable, and operationally efficient networking model aligned with modern digital business requirements.

©2026 6WIND

The Enterprise Networking Challenge Has Changed

For decades, enterprise networking followed a predictable design model built around centralized data centers, fixed WAN topologies, hardware appliances, static routing policies, and relatively limited cloud interconnection requirements. However, that model no longer reflects how enterprises operate today.

Applications and workloads are now increasingly distributed across public cloud providers, SaaS ecosystems, edge environments, remote users, AI compute clusters, partner ecosystems, and hybrid infrastructure. This shift is fundamentally changing traffic flows, performance requirements, and operational expectations.

As a result, interconnection is becoming the new enterprise edge. Rather than traffic flowing through centralized corporate hubs, organizations now require direct, low-latency connectivity between clouds, AI infrastructure, SaaS providers, colocation facilities, partners, customers, and distributed enterprise sites.

As enterprise architectures become more distributed and dynamic, traditional networking approaches are increasingly strained and often introduce a range of operational challenges.

Why Traditional Architectures Are Reaching Their Limits

1. **Hardware-Centric Networking Slows Agility**

   Hardware-centric networking significantly limits agility in modern enterprise environments. Deploying physical routers, firewalls, and VPN appliances across multiple regions typically involves long procurement cycles, capacity planning, staging, and on-site deployment.

   In cloud-driven environments, this results in provisioning timelines measured in weeks or months—no longer aligned with the speed of modern application delivery. Enterprises increasingly require infrastructure that can scale in minutes, not quarters.

2. **Backhauling Increases Latency and Complexity**

   Traditional WAN architectures often rely on centralized security and routing stacks. As workloads move closer to users and across cloud environments, traffic is frequently backhauled through central points for inspection and policy enforcement.

   This introduces increased latency, reduced application performance, higher bandwidth costs, and inefficient traffic paths. The impact is particularly pronounced in AI workloads, real-time analytics, IoT, and high-performance cloud applications.

3. **Multi-Cloud Connectivity Creates Operational Fragmentation**

   Modern enterprises operate across AWS, Microsoft Azure, Google Cloud, Oracle Cloud, private infrastructure, and SaaS ecosystems. Each introduces distinct networking models, security frameworks, and operational tooling.

   The result is fragmented operations, duplicated policy enforcement, and inconsistent

©2026 6WIND

routing and segmentation across environments—creating significant operational overhead and governance challenges.

4 **Cloud Networking Costs Are Becoming Structural**

Cloud networking costs are increasingly material and harder to optimize. The FinOps Foundation's 2025 State of FinOps highlights the expansion of financial governance into "Cloud+" domains, including SaaS, AI workloads, and networking infrastructure.

Costs associated with data egress, NAT gateways, inter-region traffic, and overlay architectures scale rapidly with distributed cloud adoption, making end-to-end cost visibility and optimization increasingly complex.

The Underlying Trend

Across all four areas, a consistent pattern is emerging: traditional networking models are struggling to support cloud-native, distributed, and real-time environments at scale.

The Rise of the Digital Edge

To address these challenges, enterprises are increasingly shifting toward digital edge architectures. This model moves networking, security, and interconnection services closer to where digital activity is generated and consumed, including cloud on-ramps, end users, SaaS ecosystems, AI infrastructure, data-intensive applications, and partner environments. By distributing network functions closer to these interaction points, enterprises can reduce latency, simplify traffic flows, and enable more dynamic and responsive scaling. Rather than relying exclusively on centralized infrastructure, networking capabilities are increasingly being deployed directly at or near points of interconnection, where data exchange and application delivery occur.

This architectural shift is widely reflected across the industry. The Equinix Global Interconnection Index highlights the growing importance of private interconnection, distributed digital ecosystems, and globally connected infrastructure as enterprises modernize their cloud and edge strategies. In parallel, it aligns with broader transformation trends including the adoption of artificial intelligence, distributed application architectures, hybrid cloud environments, edge computing, Network-as-a-Service (NaaS) models, and infrastructure automation.

Software-Defined Networking at the Digital Edge

Software-defined networking plays a foundational role in enabling this transition by virtualizing critical network functions, including routing, firewalling, IPsec VPN, NAT/CGNAT, and security services. These functions, traditionally delivered through fixed hardware appliances, can now be deployed dynamically as software-based services, providing significantly greater flexibility, scalability, and operational efficiency.

When implemented on global interconnection platforms such as Equinix Network Edge, enterprises gain the ability to deploy networking services globally within minutes, scale capacity elastically in response to demand, reduce reliance on physical infrastructure, automate operational processes, standardize policy enforcement across environments, and optimize end-to-end connectivity paths. This software-defined approach substantially improves operational agility while reducing infrastructure complexity, enabling a more distributed, programmable, and responsive network architecture.

6WIND VSR on Equinix Network Edge

The 6WIND and Equinix joint solution brings together two complementary capabilities: the global interconnection infrastructure of Equinix Network Edge, spanning more than 77+ metros worldwide, and the carrier-grade virtual networking performance of the 6WIND Virtual Service Router.

VSR runs directly on Equinix Network Edge as a software-defined appliance, eliminating the need for physical hardware at each location. Enterprises can deploy any combination of the following virtual network functions, and scale them independently as requirements evolve:

Virtual Border Router (vBR) — high-throughput inter-domain routing with full BGP, MPLS, and SRv6 support

Virtual Firewall (vFW) — stateful security policy enforcement co-located with interconnection points, eliminating the need for centralized backhaul

Virtual Security Gateway (vSecGW) — high-scale IPsec VPN for encrypted connectivity across hybrid cloud, SD-WAN, and partner ecosystems

Virtual Carrier-Grade NAT (vCGNAT) — large-scale address translation for consolidated internet breakout and cloud egress optimization

Why Carrier-Grade Matters

The term “carrier-grade” reflects a specific performance standard: the throughput, availability, and protocol depth required by telecommunications operators serving millions of subscribers. 6WIND VSR was built to that standard — originally for service providers — and brings that same capability to enterprise environments running on Equinix Network Edge.

©2026 6WIND

Core Enterprise Use Cases

Multi-Cloud Routing Hub

Managing routing consistency across multiple cloud providers and regions is one of the most operationally demanding challenges in enterprise networking. Traditional approaches require dedicated routers at each metro, separate provisioning workflows per cloud environment, and fragmented operational domains that are difficult to govern at scale.

Deploying 6WIND vBR on Equinix Network Edge establishes a unified routing hub at each interconnection location, managed through a single software-defined control plane. BGP peering, MPLS interconnection, and traffic engineering policies are configured once and applied consistently. New cloud regions or partner connections can be added by instantiating additional VSR instances — no hardware, no procurement delay. For enterprises managing three or more cloud environments, this architecture materially reduces both operational overhead and the risk of routing policy inconsistency.

High-Performance Cloud Security

Security enforcement has to follow workloads — and workloads are no longer centralized. Backhauling cloud and SaaS traffic through a central firewall stack introduces latency, creates throughput bottlenecks, and concentrates risk in a single point of failure.

6WIND vFW deployed on Equinix Network Edge positions security enforcement directly at the interconnection point, where traffic actually flows. Stateful inspection, segmentation, and policy enforcement happen close to the workload rather than hundreds of milliseconds away. Security capacity scales with demand — additional vFW instances can be deployed at new metros without procurement cycles — and policy management remains centralized regardless of how many locations are active.

Secure Multi-Cloud Connectivity

Encrypted connectivity is foundational for hybrid cloud, partner ecosystems, SD-WAN integration, and cloud-to-cloud networking. The challenge is that the encrypted traffic volumes generated by modern multi-cloud environments frequently exceed what traditional VPN appliances were designed to handle, particularly as AI workloads and data-intensive applications push bandwidth requirements higher.

6WIND vSecGW delivers high-scale IPsec VPN on standard x86 infrastructure, without requiring proprietary encryption hardware. Deployed on Equinix Network Edge, it provides encrypted connectivity between cloud environments, private data centers, and partner networks at the interconnection layer — where traffic paths are shortest and latency is lowest. VPN capacity scales with demand, and enterprises avoid the overprovisioning that fixed appliances require.

Cloud Egress Cost Optimization

Cloud NAT and egress costs have become significant budget items that are difficult to forecast and control when each cloud environment runs its own NAT gateway configuration. Enterprises operating across multiple clouds frequently find themselves paying for redundant infrastructure, without visibility into aggregate traffic costs or the ability to enforce consistent exit policies.

6WIND vCGNAT on Equinix Network Edge consolidates internet breakout through a common NAT layer at the interconnection point, eliminating per-cloud NAT gateway duplication. Traffic exits through a single, policy-governed path rather than through separate cloud-native gateways. Enterprises gain cost predictability, improved governance, and the ability to optimize internet exit routing through Equinix's interconnection ecosystem — which provides direct access to major CDN providers, internet exchanges, and transit networks.

©2026 6WIND

AI and High-Bandwidth Infrastructure Connectivity

AI workloads are reshaping enterprise networking requirements. GPU clusters running distributed training generate traffic volumes that dwarf traditional enterprise applications. Inference at scale demands consistent low-latency paths between data sources, compute, and endpoints. And as AI adoption accelerates — McKinsey projects dramatic growth in data center demand over the coming decade — the WAN connectivity layer increasingly determines whether AI infrastructure performs as designed or becomes a bottleneck.

VSR is well-suited to serve as the WAN border function for AI-intensive environments, providing the high-throughput routing layer that connects GPU infrastructure to cloud environments, data pipelines, and enterprise networks. Deployed at Equinix — where direct connections to every major cloud provider and internet exchange are available — it enables AI operators to reach the connectivity ecosystem they need without adding networking hardware to already-dense facilities. For enterprises consuming AI services from cloud or co-location providers, the same architecture delivers the consistent, low-latency paths that AI-dependent applications require.

Business Outcomes

OUTCOME	WHAT IT MEANS FOR THE BUSINESS
Speed to Market	Provision carrier-grade networking at any global location in minutes. New cloud regions, partner interconnections, and security policies deploy through software — no hardware procurement, no staging delays.
Cost Efficiency	Eliminate hardware CAPEX, consolidate cloud egress through a single NAT layer, and shift to scalable OPEX consumption. Cloud networking costs become predictable and governable.
Operational Simplicity	Routing, firewalling, VPN, and NAT managed through a unified software-defined architecture. Consistent policy across all cloud environments, enforced from a single control plane.
Performance Without Trade-offs	Carrier-grade throughput and protocol depth on standard x86 infrastructure. No proprietary hardware, no vendor lock-in, no capability gap relative to purpose-built appliances.
Security Governance	Security policies enforced close to workloads rather than through centralized backhaul. Multi-tenant segmentation, encrypted connectivity, and consistent governance across distributed environments.
AI and Cloud Readiness	High-throughput WAN border connectivity for AI infrastructure and bandwidth-intensive cloud workloads, deployed directly at Equinix interconnection hubs.

©2026 6WIND

Conclusion

Enterprise networking is entering a new phase. Multi-cloud environments, AI workloads, and distributed digital ecosystems are redefining what network infrastructure needs to deliver — and exposing the limits of architectures built for a more centralized era.

The organizations best positioned for this shift are those that treat networking not as a fixed-cost infrastructure layer, but as a dynamic capability that can be deployed, scaled, and optimized in step with the business. Software-defined networking at the digital edge — where interconnection happens, where cloud on-ramps live, where partners and ecosystems converge — is the architectural foundation that makes that possible.

By combining the global interconnection capabilities of Equinix with the carrier-grade virtual networking performance of 6WIND, enterprises can modernize their connectivity infrastructure without the constraints of hardware procurement cycles, appliance sprawl, or fragmented operational models. Networking becomes an enabler — not a bottleneck — for the AI and multi-cloud era.

References

1. Flexera — 2025 State of the Cloud Report
2. FinOps Foundation — 2025 State of FinOps Report
3. Equinix — Global Interconnection Index
4. McKinsey & Company — Beyond Compute: Infrastructure That Powers and Cools AI Data Centers