Azblink NFV Platform

Secure Multi-OS Workspaces at the Network Edge

Virtualization- and NFV-first edge platform that delivers isolated multi-OS workspaces,fine-grained network control, and integrated , routing, VPN and SBC capabilities on a single node.

Introduce a single secure host to boost security, simplify operations and cut cost

alanl@azblink.com
www.azblink.com
www.ucchats.com

Solution Architecture: Dedicated Secure Workspace Node

- Built on an x86 edge appliance with a Linux host OS running KVM hypervisor and container runtime.
- User PCs act only as access terminals and no longer host high-risk or high-load applications directly.
- Access into the node is via RDP, HTML5 and similar protocols, exposing controlled workspaces instead of raw servers.
- AI and batch workloads run inside dedicated VMs with their own vCPU / RAM / disk, so they do not degrade endpoint performance or stability.

Azblink NFV Platform: Core Capabilities

- Run multiple Windows and Linux virtual machines alongside network security functions (firewall, routing, VPN, SBC) on a single x86 node.
- Use zones and virtual bridges (br0, br1, br2, br3…br11) to precisely segment WAN, internal, DMZ, guest and management networks.
- Built-in edge controls: port forwarding, IP load balancing, HTTP proxy, IP policy routing and HTTP reverse proxy – consolidating many edge boxes into one.
- Provide client-to-site, site-to-site and certificate-based VPN with a built-in lightweight CA to extend the secure perimeter to branches and homes.
- Support RIPv2, OSPF, PIM and common SD-WAN patterns so WAN edge services and always-on workloads can be consolidated on the same platform.

Key Technical Value Propositions

- Replace complex AV / EDR whitelisting stacks with VM and container isolation to simplify policy management at the endpoint layer.
- Keep the host OS lean and focused, reducing patch, driver dependency and software conflict risk on the physical node.
- Use snapshot and rollback to support Dev / Test / UAT and multiple environment stages on the same hardware.
- Apply NFV policies such as VLAN, VRF, ACL and QoS at the per-VM level to achieve fine-grained micro-segmentation.
- Spin up dedicated VMs for AI or high-load tasks and combine them with CPU pinning and I/O throttling to guarantee QoS.
- Reduce the number of physical servers and desktops, simplifying hardware procurement and OS / hypervisor licensing.
- Use a centralized management interface to maintain VM profiles, image versions and security policies.
- Implement per-VM routing and VPN breakout with policy routing and Multi-WAN, and support Split-DNS for data residency and compliance.
- Leverage built-in bridge firewall and multi-zone design: br0 (WAN / management), br1 (restricted internal), br2 (DMZ), br3 (trusted internal) and beyond.
- Consolidate firewall and SBC virtualization on the same NFV node so VMs attach to different bridges and zones instead of separate appliances.
- Apply unified outbound NAT and Split-DNS at br0 for flows from br1 / br2 / br3, enabling consistent policy enforcement and audit.

Primary Technical Stakeholders

- IT operations and infrastructure teams responsible for terminals, admin consoles and legacy applications.
- Security teams / SOC / blue teams focused on endpoint attack surface reduction and micro-segmentation.
- SREs, DBAs and network engineers who must isolate high-privilege tools and credentials from general-purpose desktops.
- MSPs, MSSPs, Telcos and SIs delivering managed services, secure connectivity and centralized update capabilities to customers.
- Lab, PoC and test teams who need to run multiple OS types (Windows, Linux and specialized OSes) on shared hardware without interference.
- Compliance and GRC teams working under PCI, ISO 27001, SOC 2 and similar audits who want to shrink endpoint scope and prove least privilege.
- Internet-facing PCs that must be fully isolated from internal business systems by placing browsing desktops inside NFV VMs.
- Advanced users, small studios, SOHO and home lab owners who need a second machine dedicated to external access and internal services, keeping their daily PC out of harm’s way.

Vertical Deployment Patterns

- Finance: deploy trading, back-office and audit VMs on the same NFV node with isolation via VLAN and VRF.
- Healthcare: connect clinical and medical system VMs back to core hospital systems through per-VM VPN, exposing only RDP / HTML5 front-ends.
- Government / public sector: place critical VMs into separate VRFs and forward logs into SIEM / SOC platforms for centralized monitoring.
- Legal and compliance: run eDiscovery and case management VMs in isolated zones away from general office desktops to limit data leakage.
- Media and content: separate rendering / AI pipeline VMs with their own storage and network paths so they do not impact editing workstations.
- Manufacturing and OT: separate production VMs from office VMs into different security zones, only interconnected via hardened jump hosts.
- Retail and PoS: isolate PoS and back-office VMs into their own VLANs, enforce Proxy / VPN for outbound traffic and meet PCI-DSS requirements.
- Telco / ISP / channels: use NFV nodes as CPE or edge nodes tightly integrated with OSS / BSS for billing and monitoring.
- Education / research: rapidly spin up and recycle lab VMs while keeping them logically separated from administrative systems.
- Property / hospitality: isolate NVR, PMS and portal VMs and manage WAN egress and failover using Multi-WAN and policy routing.
- Government front-desk: provide a dedicated, hardened internet-facing desktop VM separate from daily office PCs.
- Home / SOHO / labs: treat the NFV node as a smart-home controller and security hub, hosting IoT / smart home, surveillance, access control and sensor platforms with child and guest networks and VPN access back home.

Single Secure Host: A Shared NFV Foundation for Enterprise and Home

- Enterprise and organization use case: consolidate firewall, WAN edge, SBC and application servers onto one NFV node to increase utilization and reduce rack and device sprawl.
- Start in a virtualized PoC, then scale out to multiple nodes or cloud once the pattern has been validated, shortening project cycles.
- Office use case: use the NFV platform as a one-stop secure network core, centralizing VPN, file services, internal systems and dev / test environments.
- Keep user endpoints as simple terminals that connect into NFV workspaces instead of hosting high-risk services and sensitive data locally.
- Home / SOHO / personal lab use case: run Azblink NFV as a smart-home hub and security center hosting IoT / smart home control, surveillance and access systems.
- Create dedicated segments for children’s devices, expose VPN back home, and host private cloud and media servers on the same node.
- Use snapshots to test new systems and services safely without impacting family machines or daily productivity.
- Overall positioning: a “secure second computer” that serves both enterprise and home scenarios.

Market and Technology Trends

- LLMs, GPUs and AI pipelines significantly increase per-node resource demands, making traditional fat clients struggle to keep user experience smooth.
- Zero Trust and micro-segmentation frameworks raise expectations for how visible and controllable endpoints and east–west traffic must be.
- Low-power, multi-core x86 platforms (for example, Intel N-series) have made edge hypervisor nodes plus NFV both technically viable and cost-effective.

System Composition (Simplified Technical View)

- Host OS: Linux-based, integrating KVM hypervisor and a container runtime such as LXC for workload isolation.
- NFV data plane: virtual switching and routing using Linux bridge / OVS and FRR to implement VLANs, VRFs and policy-based routing (PBR).
- Security chain: vFirewall, IDS / IPS, proxy and VPN functions are inserted as virtual services, with policies steering flows through the appropriate chain.
- IDS focuses on detection and alerting; IPS is inline and actively blocks malicious behaviour in the traffic path.

Bridge Firewall: br0 / br1 / br2 / br3…br11 Security Zones

- Azblink NFV uses pre-defined virtual bridges plus firewall rules to carve the virtual network into multiple security zones.
- All outbound traffic is funneled through br0 for NAT and egress policy enforcement.
- br2 is reserved as a DMZ for externally exposed services, keeping them away from internal workloads.
- br1 and br3–br11 map to different levels of internal and trusted segments; br4–br11 can be customized per project for additional internal networks or tenant zones.
- This design drives clear logical boundaries and reduces the risk of lateral movement within the node.

Always-On Workloads: Implementation View

- Allocate fixed vCPU, RAM and storage to specific VMs and mark them as auto-start with continuous health monitoring.
- Use watchdogs and health checks to detect failures and automatically restart VMs or applications when needed.
- Apply I/O throttling and QoS controls so background jobs cannot starve interactive sessions of bandwidth or IOPS.
- Regularly snapshot and back up critical VMs to support fast recovery and controlled rollbacks.
- Preload monitoring agents and log forwarders into VM templates to simplify central monitoring and observability.
- In advanced topologies, deploy multiple NFV nodes with failover or handover strategies to achieve higher availability at the edge.

Per-VM NFV Topology and Policy Control

- Use virtual switches plus VLAN / VRF to place each VM into the appropriate security zone and minimize east–west attack paths.
- Apply ACLs per VM and define explicit east–west and north–south traffic policies, with detailed logging to support incident analysis.
- Use QoS and rate limiting to keep high-volume VMs such as NVR or backup under control so they do not affect other services.
- Leverage PBR and Multi-WAN to direct selected VM traffic through specific ISPs or VPN tunnels.
- Enable per-VM VPN and Split-DNS for systems that must meet regulatory requirements around where data flows and how names resolve.
- Support service chaining so flows can pass through a sequence of vFirewall, IDS / IPS, proxy and VPN functions as required.

Example: NFV Service Chain for a Single VM

- Application VM connects to the virtual network through a vFirewall, then flows continue through IDS / IPS and proxy / VPN components.
- Outbound traffic exits via WAN A or B depending on policy, with each hop applying its own security controls and logging.
- This creates a minimum-privilege, auditable and easily adjustable service chain per VM instead of a one-size-fits-all network path.

Tiered Packages and Capability Levels

- Higher-tier packages such as SSM-Pro support 3–5 VMs with per-VM VPN, Multi-WAN, service chaining and resource pinning.
- Service chaining defines the ordered path a flow must take across virtual security and network functions (vFirewall, IDS / IPS, proxy, VPN, etc.).
- Resource pinning lets you bind vCPUs, memory or NIC queues to specific VMs or tenants, ensuring performance isolation and predictable behaviour.
- Lower tiers can start with fewer VMs and simpler network policies while remaining upgradeable to richer configurations.

Capabilities for MSPs and Telcos

- Provide APIs and portals for managing tenants, nodes and VMs, including version control and bulk upgrades across fleets.
- Integrate with existing NMS, SIEM and SOC platforms via syslog, agents and webhooks for monitoring and alerting.
- Ship images pre-loaded with the channel’s own agents (monitoring, security, billing) to achieve deep white-label integration.
- Design the management plane with multi-tenant operations and channel workflows as first-class requirements.

Common Technical and Operational Pain Points Today

- Relying on AV / EDR / DLP exception-driven policies makes endpoint rules increasingly complex and expensive to maintain.
- Legacy applications and proprietary clients often break when OS or drivers are updated, causing compatibility incidents.
- Vendor access is frequently implemented via shared accounts and generic VPNs, leaving poor audit trails and high risk.
- Split-tunnel VPN configurations become hard to manage correctly in multi-SaaS, multi-cloud environments.
- Endpoint diversity complicates patch and vulnerability management across the fleet.
- Under PCI-DSS, ISO 27001 and SOC 2 audits, it is difficult to demonstrate strong endpoint isolation and least privilege with traditional approaches.
- There is a lack of purpose-built hypervisor / NFV solutions for edge and branch environments, leading to forced use of data-center tools.
- AI and high-load applications consume large amounts of compute and network resources, often without proper isolation or controls.

Technology and Scenarios: Azblink NFV vs VMware / VirtualBox / Proxmox

- VMware and VirtualBox focus on general-purpose virtualization and development / test; Azblink NFV focuses on edge appliance + NFV + security use cases.
- Proxmox is excellent for clustered data-center deployments; Azblink NFV is optimized for compact, network-first field appliances.
- Azblink NFV includes per-VM NFV policy, Multi-WAN, per-VM routing and VPN breakout, as well as service chaining tuned for edge scenarios.
- The management plane is designed for channel multi-tenancy, with templates, bulk deployment and simplified operations.
- Supports white-label and brand customization so Telcos and MSPs can integrate with their existing portals, billing and service bundles.
- Predefined profiles align with common edge workloads such as NVR, AI, PoS and admin consoles.
- Compared with generic hypervisors, Azblink NFV is better suited to act as a secure second computer and always-on edge workload platform.
- It is intentionally designed so any PC owner could make use of it as a second machine, from SMEs to SOHO and individual labs on a single small x86 host.

Desktop vs Datacenter Hypervisor vs Edge NFV Appliance

- Desktop virtualization tools excel at providing VMs for individual users or developers but do not address edge network functions or multi-zone security.
- Datacenter hypervisors focus on large clusters, shared storage and traditional server workloads rather than per-site workspaces and network edge roles.
- An edge NFV appliance such as Azblink NFV combines multi-OS workspaces with virtualized firewall, routing, VPN and SBC in one node close to users.
- This lets organizations and homes standardize on a single secure host per site, simplifying architecture while raising the security bar at the edge.