AZBLINK NFV Platform —

Secure Multi-OS Workspaces at the Network Edge

以虛擬化與 NFV 為核心，在單一 Edge 平台上，
同時提供隔離式多作業系統工作環境、精細的網路控管，
以及防火牆、路由、VPN 與 SBC 的整合虛擬化能力

導入「單一安全主機」，企業戰力全開，
安全升級、簡化管理，大幅縮減成本

alanl@azblink.com
https: //www.azblink.com
https://www.ucchats.com

解決方案架構：Dedicated Secure Workspace Node

- 以 x86 Edge Appliance 為基礎，透過 KVM Hypervisor / Container Runtime 提供多 VM / Container 隔離環境。
- 使用者端 PC 僅作為存取終端，不直接承載高風險或高負載應用，透過 RDP / HTML5 等協定連入。
- AI / 批次工作可在專屬 VM 上配置 vCPU / RAM / Disk，避免影響 Endpoint 效能與穩定度。

Azblink NFV 平台：核心功能一覽

- 在單一 x86 平台上，同時執行多台 Windows / Linux 虛擬主機與網路安全功能（防火牆、路由、VPN、SBC 等）。
- 以區域（Zone）與虛擬橋接器（br0 / br1 / br2 / br3…br11）精準劃分內外網、DMZ、訪客網與管理網，避免不同安全等級的業務彼此干擾。
- 內建 Port Forwarding、IP 負載平衡（Load Balancer）、HTTP Proxy、IP Policy Routing、HTTP 反向代理等邊界控制能力，在同一台機器上完成「多盒合一」。
- 提供 Client-to-Site / Site-to-Site VPN 與憑證式 VPN，內建簡易 CA，延伸企業與家庭的安全邊界。
- 支援 RIPv2、OSPF、PIM 等動態路由與常見 SD-WAN 情境，在單一平台整合 WAN 邊緣服務與 Always-On 工作負載。

技術導向的關鍵價值

- 以 VM / Container 隔離取代傳統 AV / EDR (End Point Detection Response) 白名單堆疊，降低 Policy 維護複雜度。
- 主機 OS 工作負載極簡化，減少 Patch / Driver 依賴與軟體衝突風險。
- 透過 Snapshot / Rollback 機制支援 Dev / Test / UAT 多階段環境共存。
- 在每個 VM 層級實作 VLAN / VRF / ACL / QoS 等 NFV 策略，做到細緻化微分段。
- 可針對 AI / 高負載任務建立 Dedicated VM，搭配 CPU Pinning 與 I/O 限速確保 QoS。
- 降低實體 Server / Desktop 數量，簡化硬體採購與 OS / Hypervisor 授權管理。
- 提供集中管理介面，簡化 VM Profile、映像版本與安全策略的維護。
- 支援以策略路由與 Multi-WAN 實作 per-VM 路由 / VPN Breakout 與 Split-DNS，滿足資料落地與合規要求。
- 內建橋接式防火牆與多區域設計：透過預先定義的 br0（WAN / 管理）、br1（內部受限區）、br2（DMZ）、br3（內部信任區）等橋接器，將不同安全等級的服務與設備清楚分區，降低橫向移動風險。
- 單一平台整合防火牆與 SBC 虛擬化：在同一台 NFV 平台上同時承載防火牆、SBC、VPN、動態路由等網路功能，虛擬機透過不同橋接器與 Zone 隔離，簡化實體設備數量與機櫃配置。
- 統一出口 NAT 與 Split-DNS 策略：所有來自 br1 / br2 / br3~br11 的對外流量，統一經由 br0 出口並套用 NAT 與策略路由，支援 per-VM VPN、Multi-WAN、Split-DNS 等合規需求。

主要技術利害關係人

- **負責 Terminal / Admin Console / Legacy App 的 IT Operations / Infrastructure Team。**
- **著重 Endpoint Attack Surface 與 Micro-Segmentation 的 Security / SOC / Blue Team。**
  - (SOC / 藍隊 = 負責日常資訊安全監控與防禦的團隊)
- **需隔離高權限工具與憑證的 SRE / DBA / Network Engineers。**
  - (SRE / DBA = 負責系統穩定與資料庫可靠性、安全性的人。)
- **提供託管服務與集中更新能力的 MSP / MSSP / Telco / SI。**
  - (MSP / MSSP = 代管客戶 IT 或資安服務的外包服務商（通路合作對象)
- **需要在同一硬體上跑多種 OS（Windows / Linux / 專用 OS）的 Lab / PoC / 測試團隊。**
- **需配合 PCI / ISO / SOC2 等稽核，縮小 Endpoint 範圍的 Compliance / GRC 團隊。**
  - PCI / ISO / SOC 2 = 與支付、資訊安全管理、雲端服務控制相關的國際合規標準。
- **Internet-facing PC that is completely isolated from their internal business systems.**
  - 面向 Internet 的工作桌面（Internet-facing PC）與內部業務系統完全隔離，僅透過 NFV Node 上的虛擬機上網。
- **進階個人用戶 / 小型工作室 / SOHO / Home Lab 使用者：**
  - 需要一台專門處理「對外連線與對內服務」的第二台機器，集中承載網路服務、實驗環境與自架伺服器，避免把日常工作 PC 暴露在高風險服務之中。

垂直場域的技術落地型態

- **Finance：在同一 NFV Node 上以 VLAN / VRF 分區部署 Trading VM、Back-Office VM 與 Audit VM。**
  - **VLAN = 虛擬區域網路**，在交換器層把一條實體網路切成多個邏輯網段。
  - **VRF = 虛擬路由與轉送**，在路由層把不同客戶／業務的路由邏輯隔離開。
- **Healthcare：醫療系統 VM 透過 per-VM VPN 與醫院核心系統連線，端點僅呈現 RDP / HTML5 介面。**
- **Gov / Public：Critical VM 置於獨立 VRF，並透過集中 Log Shipping 導入 SIEM / SOC 平台。**
  - **SIEM = 資安事件與資訊管理平台**，就是集中的「資安眼睛＋記錄庫」。
  - **SOC = 資安營運中心**，負責每天盯 SIEM、處理告警與事件的那群人。
- **Legal / Compliance：eDiscovery / Case Management VM 與一般辦公環境完全隔離，降低資料外洩風險。**
- **Media / Content：Rendering / AI Pipeline VM 分流至獨立 Storage / Network，避免影響剪輯工作站。**
- **Manufacturing / OT：Production VM 與 Office VM 採不同 Security Zone，只能透過 Jump Host 互通。**
- **Retail / PoS：PoS VM 與 Back-Office VM 由獨立 VLAN 控管，對外流量經過 Proxy / VPN；落地遵循 PCI-DSS。**
  - **PCI-DSS（信用卡產業資料安全標準）：Payment Card Industry Data Security Standard.**
    針對所有「處理、儲存或傳輸信用卡資料」的機構所制定的資安要求，用來保障持卡人資料安全。若你提供收款、代收或與刷卡資料有關的雲端／主機服務，客戶通常會問你「有沒有符合 PCI-DSS？」
- **Telco / ISP / Channel：NFV Node 可作為 CPE 或 Edge Node，與 BSS / OSS 整合計費與監控。**
  - BSS: Business Support System, OSS: Operation Support System
- **Education / Research：Lab VM 快速建立 / 回收，支援多版本 OS 與工具並與校務系統隔離。**
- **Property / Hospitality**：NVR VM、PMS VM、Portal VM 分區，並透過 Multi-WAN 控制外聯路徑與 Failover。
- **Government: Front Desk 對外上網風險高，需要「上網專用、安全隔離桌面」與日常辦公機分離。**
- **Home / SOHO / 個人實驗室：NFV 平台作為「智慧家用主機」與安全中樞，集中承載 IoT / Smart Home 控制、監視與錄影、門禁與感測器平台，為兒童裝置建立獨立網段，並提供回家的 VPN、私有雲與影音媒體伺服器，同時兼作可快照還原的實驗環境。**

單一安全主機：企業與家庭共同的 NFV 基礎

企業與組織

- 在一台 NFV 平台上整合多個關鍵服務（防火牆、WAN Edge、SBC、應用伺服器），提升資源使用率、降低設備與機櫃成本。
- 可先在虛擬化環境中做 PoC / 測試，成熟後再擴充到多節點或雲端，縮短導入週期。

辦公室環境

- NFV 平台作為一站式安全網路中心：集中管理 VPN、檔案服務、內部系統與開發測試環境。
- 使用者終端機只負責連線，不必在個人 PC 上承載高風險服務與敏感資料，降低資安風險。

住家 / SOHO / 個人實驗室

- 把 Azblink NFV 當作家庭的「智慧家用主機」與安全中樞：承載 IoT / Smart Home 控制、監視與錄影、門禁與感測器平台。
- 為兒童裝置建立獨立網段，提供回家的 VPN、私有雲與影音媒體伺服器。
- 同時作為可快照還原的實驗環境，方便安裝各種新系統與服務，不影響家用電腦與日常工作。

定位為企業與家庭的『安全第二台電腦』

市場與技術環境變化

- LLM / GPU / AI Pipelines 對單機資源需求大幅提高，傳統 Fat Client 架構難以維持良好體驗。
- Zero Trust / Micro-Segmentation 架構普及，對 Endpoint 的可視性與可控性要求提升。
- 低功耗多核心 x86 平台（例如 Intel N 系列）讓 Edge Hypervisor Node + NFV 成為具成本效益的選項。

系統構成（簡化技術視角）

- Host OS：以 Linux 為基礎，整合 KVM Hypervisor 與 Container Runtime（如 LXC）。
- NFV：透過虛擬交換 / 路由元件（如 Linux Bridge / OVS / FRR）實作 VLAN / VRF / PBR。
  - PBR – Policy-Based Routing:政策式路由，依「政策條件」決定要走哪條路，而不只是目的地。
- Security Chain：可插入 vFirewall、IDS / IPS、Proxy / VPN 等虛擬服務，並由 Policy 驅動流量走向。
  - IDS (Detection): 入侵偵測系統，只偵測與告警，不一定主動阻擋。
  - IPS (Prevention):入侵防禦系統，在流量路徑中直接阻擋惡意行為。

橋接器防火牆：
br0 / br1 / br2 / br3 ~ br11 安全區域設計

- Azblink NFV 平台透過預先定義的虛擬橋接器與防火牆規則，將虛擬網路切成多個安全區域：
  · 所有對外流量統一由 br0 出口與 NAT 控管
  · br2 作為 DMZ 專用區，承載對外服務
  · br1 / br3 ~ br11 對應不同層級的內部網段與信任區 (br4–br11 可依實際專案需求規劃額外內部網段或區域)

br0 — WAN / 管理區	作為 NFV 平台對外出口與管理網。
	所有來自 br1 / br2 / br3~br11 的對外流量都經由 br0，統一套用 NAT、Multi-WAN 與 Policy Routing 策略。
	來自 br0 的一般主機不得任意掃描或連線內部橋接器，只允許必要的管理流量。
br1 — 內部受限區	放置高風險、需嚴格控管的內部設備（如實驗環境、舊系統、某些 OT 裝置）。
	不允許主動連線其他 IP 子網，只能被動接受經過防火牆允許的連線。
br2 — DMZ 區	專門承載對外服務（Web / Mail / Portal / API Gateway…）。
	與 br1 / br3~b11高度隔離，只開啟必要的後端通道（例如資料庫或內部 API）。
br3 ~br11 — 內部信任區	放置內部業務系統、管理工具與開發 / 測試 VM。
	可與 br1 雙向通訊，但預設不接受來自外部網段的主動連入。

Always-On Workloads：技術實作觀點

- 為特定 VM 配置固定 vCPU / RAM / Storage，設定開機自動啟動並監控健康狀態。
- 可透過 Watchdog / Health Check 機制與多台 NFV Node 的備援架構或接手機制，設計成高可用（HA）的 Edge 解決方案（進階部署選項）。
- 使用 I/O 限速與 QoS 控制，避免背景工作影響其他互動式 Session 的體驗。
- 定期對關鍵 VM 進行 Snapshot / Backup，支援快速復原與版本回退。
- 可將 Monitoring Agent / Log Forwarder 預載於 VM 模板中，方便集中監控。

Per-VM NFV 拓樸與策略控制

- 支援以 IP 策略路由與 Multi-WAN 實作「per-VM 路由與 VPN Breakout」，讓不同 VM 走不同的 WAN / VPN 通道。
- 利用虛擬 Switch 與 VLAN / VRF 將不同 VM 放入不同 Security Zone，隔絕東西向橫向移動。
- 對每個 VM 設定 ACL 與 E-W / N-S 流量策略，搭配 Log 以利 Incident 分析。
  - N-S「內部 ↔ 外部」的流量，E-W「內部 ↔ 內部」之間橫向跑的流量
- 透過 QoS / Rate Limit 控制高流量 VM（如 NVR / Backup）的頻寬使用。
- 以 PBR / Multi-WAN 技術，將特定 VM 的流量導向指定 ISP 或 VPN Tunnel。
- 對需合規的 VM 啟用 per-VM VPN 與 Split-DNS，確保目的地與解析行為符合規範。
  - **Split-DNS = 依「查詢來源（內／外）」對同一個網域回覆不同 IP 的 DNS 架構。**常用在企業、VPN、混合雲，讓內外部存取同一網域時，走不同且較安全／有效率的路徑。
- 支援 Service Chaining，將流量依序導入 vFirewall、IDS / IPS、Proxy / VPN 等元件。

實例：單一 VM 的 NFV Service Chain

VM（應用）透過 vFirewall、IDS / IPS、Proxy / VPN 等虛擬網路功能串接後，再由 WAN A / B 對外。每個節點可套用對應的 Security Policy 與 Log，形成最小權限、可稽核且易於調整的 Service Chain。

分級套件與技術能力差異

- SSM-Pro：
  - 3–5 VM，支援 per-VM VPN、Multi-WAN、Service Chaining 與 Resource Pinning。

- Service Chaining（服務鏈 / 服務串接）：
  - Decide in what order a flow must pass through multiple network / security functions,
  - especially in a virtualized (NFV) environment.
  - 定義特定流量「依序」要經過哪些虛擬防火牆、IDS / IPS、Proxy / VPN 等虛擬網路 / 資安服務。

- Resource Pinning（資源釘選）：
  - 將 vCPU / 記憶體 / NIC Queue 等資源釘選給關鍵 VM 或租戶，確保效能穩定與租戶之間的資源隔離。

面向 MSP / Telco 的技術與營運能力

- 提供 API / Portal 管理 Tenant / Node / VM，支援版本控管與批次更新。
- 可透過 Syslog / Agent / Webhook 等方式整合既有 NMS / SIEM / SOC 平台。
- 映像檔可預載通路自有 Agent（監控 / 資安 / 計費），達成白牌與深度整合。

現況常見技術與營運問題

- 依賴 AV / EDR / DLP 的例外導向控制，使 Endpoint Policy 複雜度與維護成本不斷上升。
  - AV（Antivirus）防毒軟體/EDR 端點偵測與回應/ DLP（Data Loss Prevention）資料外洩防護
- Legacy App / 專用 Client 經常與 OS / Driver 更新衝突，造成相容性問題。
- Vendor Access 多以共享帳號 / 通用 VPN 實作，Audit Trail 不清楚且風險偏高。
- Split-Tunnel VPN 在多 SaaS / Multi-Cloud 環境下愈來愈難正確配置與維護。
- Endpoint 環境差異大，導致 Patch Management 與 Vulnerability Management 複雜度增加。
- 在 PCI / ISO / SOC2 等稽核中，難以有效證明端點隔離與最小權限控制。
  - **PCI-DSS**：信用卡產業資料安全標準（保護持卡人資料）。
  - **ISO（通常指 ISO 27001）**：資訊安全管理系統標準。
  - **SOC 2**：針對雲端／服務供應商，評估 Security / Availability / Confidentiality 等控制是否到位的稽核報告。
- 缺乏對應 Edge / Branch 環境的專用 Hypervisor / NFV 方案，只能勉強沿用資料中心工具。
- 對 AI / 高負載應用缺乏資源隔離與網路控管，容易影響其他關鍵業務。

技術與場景：Azblink NFV 與 VMware /VirtualBox /Proxmox 的差異

- VMware / VirtualBox 偏向一般虛擬化與開發 / 測試用途；Azblink NFV 聚焦 Edge Appliance + NFV + Security。
- Proxmox 強於資料中心 / 叢集 Hypervisor；Azblink 專注於小體積、Network-First 的現場盒裝方案。
- Azblink 內建 per-VM NFV 策略、Multi-WAN 與 per-VM 路由 / VPN Breakout、Service Chaining，簡化邊緣場景網路與資安設計。
- Management Plane 以通路多租戶管理為前提，支援批次佈署、預設 Profile 與簡化運維流程。
- 支援白牌與品牌客製，讓 Telco / MSP 可無縫整合既有 Portal / 計費與服務包裝。
- 以 Edge / Branch 實務場景為優先，預設提供適合 NVR、AI、PoS、Admin Console 等型態的 Profile。
- 相較於通用 Hypervisor，Azblink NFV 更適合作為「安全第二台電腦」與 Always-on Edge 工作負載平台。
- Azblink NFV 平台也被設計成任何 PC 擁有者都能運用的「第二台機器」，從中小企業到 SOHO 與個人實驗室，都可以在一台小型 x86 主機上整合多種服務與網段。

Desktop vs Datacenter Hypervisor vs Edge NFV Appliance

功能面比較

Criteria	Azblink NFV Edge	VMware (Desktop/ESXi)	VirtualBox	Proxmox VE
Deployment focus	Edge appliance • second, secure workspace ★	Enterprise/desktop hypervisor	Desktop hypervisor	Datacenter/cluster hypervisor; not an edge appliance by default
Networking (NFV)	Per-VM policies, service chaining, per-VM VPN, multi-WAN built-in ★	Advanced (ESXi) but heavier to set up/licensed; desktop editions limited	Basic virtual networking; lacks per-VM VPN/multi-WAN out of box	Advanced virtual networking; no built-in per-VM VPN/multi-WAN policy
Ops & profiles	Opinionated templates, quick snapshots & easy rollback ★	Powerful but complex (vCenter, policy stacks)	Manual setup; fewer enterprise profiles	Powerful but DIY; strong clustering, more admin overhead
Always-on workloads	Yes — dedicate VMs with resource pinning and watchdogs	Yes (ESXi strong), desktop variants vary	Possible, but desktop-oriented	
AI waiting-room pattern	Supported pattern on separate workspace	Not a native pattern; depends on user setup	Not a native pattern; user-managed	
Channel/white-label	Yes — MSP/MSSP ready ★	Enterprise licensing; less white-label focus	Not channel-centric	