AZBLINK NFV プラットフォーム

ネットワークエッジにおけるセキュアなマルチOSワークスペース

仮想化とNFVを核としたエッジ・プラットフォーム

単一のエッジプラットフォーム上で、「隔離されたマルチOSワークスペース」、「精細なネットワーク制御」、そして**「ファイアウォール、ルーター、VPN、SBCの統合仮想化機能」**を同時に提供します。

1台のセキュアなエッジサーバーが、企業の競争力を引き出す。強固な防御、管理コストの最小化、そして圧倒的なコストパフォーマンスへ。

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

解決策のアーキテクチャ:
Dedicated Secure Workspace Node

- **x86 Edge Appliance**を基礎とし、**KVM Hypervisor / Container Runtime**を通じて多VM / Container隔離環境を提供します 。
- ユーザー側PCは単なるアクセス用端末として機能し、高リスクまたは高負荷のアプリケーションを直接承載せず、**RDP / HTML5**などのプロトコルを通じて連入します 。
- **AI / 批次工作（バッチ処理）**は専用VM上でvCPU / RAM / Diskを配置でき、エンドポイントの性能と安定性に影響を与えません 。

Azblink NFV プラットフォーム：コア機能一覧

- 「多台・多機能」の統合： 単一の x86 プラットフォーム上で、複数の Windows / Linux 仮想マシン（VM）とネットワークセキュリティ機能（ファイアウォール、ルーティング、VPN、SBC など）を同時に実行できます。
- 精密なネットワーク分離： ゾーン（Zone）と仮想ブリッジ（br0 / br1 / br2 ... br11）を活用し、内部・外部ネットワーク、DMZ、ゲストネットワーク、管理用ネットワークを正確に切り分けます。これにより、異なるセキュリティレベルの業務間での相互干渉を防ぎます。
- 高度な境界制御（エッジコントロール）：ポートフォワーディング、IP ロードバランサー（負荷分散）、HTTP プロキシ、IP ポリシールーティング、HTTP リバースプロキシなどの機能を内蔵。1 台のデバイスで「マルチボックス（多機能集約）」を実現します。
- セキュアなリモート接続： Client-to-Site / Site-to-Site VPN および証明書ベースの VPN を提供。簡易認証局（CA）を内蔵しており、企業や家庭のネットワーク境界を安全に拡張します。
- SD-WAN と動態ルーティングのサポート：RIPv2、OSPF、PIM などの動的ルーティングプロトコルと一般的な SD-WAN シナリオに対応。WAN エッジサービスと Always-On（常時稼働）ワークロードを単一プラットフォームに統合します。

技術指向の鍵となる価値

- VM / Container隔離を採用し、従来のAV/EDR（ホワイトリストの積み重ね）に代わることで、ポリシー保守の複雑さを軽減します 。
- ホストOSのワークロードを極小化し、パッチ、ドライバーへの依存、およびソフトウェアの衝突リスクを減少させます 。
- **Snapshot / Rollback**メカニズムにより、Dev / Test / UATの多段階環境の共存をサポートします 。
- 各VMレベルで**VLAN / VRF / ACL / QOS**などのNFV策略を実装し、緻密なマイクロセグメンテーションを実現します 。
- AI / 高負荷タスク向けに**Dedicated VM**を構築し、**CPU Pinning**とI/O制限でQoSを確保します 。
- 物理サーバーやデスクトップの数を減らし、ハードウェア調達とOS / ハイパーバイザーのライセンス管理を簡素化します 。
- 集中管理インターフェースを提供し、VMプロファイル、映像（イメージ）バージョン、セキュリティポリシーの維持を容易にします 。
- 策略（ポリシー）ルーティングとMulti-WANにより、per-VMルーティング / VPN Breakout、Split-DNSを実装し、データのローカライゼーションと合規要件を満たします 。

主要な技術利害関係者

- **IT Operations / Infrastructure Team**: 端末、管理コンソール、レガシーアプリを担当 。
- **Security / SOC / Blue Team**: エンドポイントの攻撃対象領域とマイクロセグメンテーションを重視 。
- **SRE / DBA / Network Engineers**: 高権限ツールと証明書の隔離が必要なエンジニア 。
- **MSP / MSSP / Telco / SI**: 委託管理サービスと集中更新能力を提供 。
- **Lab / PoC / テストチーム**: 同一ハードウェアで多種のOS（Windows / Linux / 専用OS）を実行する必要があるチーム 。
- **Compliance / GRCチーム**: PCI / ISO / SOC2等の監査に対応し、エンドポイントの範囲を縮小する必要があるチーム 。
- **インターネット接続PC**: 内部業務システムから完全に隔離され、NFV Node上の仮想マシンを通じてのみネット接続します 。

垂直領域における技術の着地型態

業界	実装の詳細
金融	同一NFV Node上でVLAN / VRFを用いて、取引VM、バックオフィスVM、監査VMを分区分散
医療	医療システムVMはper-VM VPNを通じて病院のコアシステムと接続し、端末にはRDP / HTML5のみを表示 。
政府 / 公共	重要VMを独立したVRFに配置し、集中Log Shippingを通じてSIEM / SOCプラットフォームへ導入 。
法務 / 合規	eDiscovery / ケース管理VMを一般のオフィス環境から完全隔離し、漏洩リスクを低減 。
メディア / コンテンツ	レンダリング / AI Pipeline VMを独立したStorage / Networkに分流し、編集作業への影響を回避 。
製造 / OT	生産VMと事務用VMで異なるSecurity Zoneを採用し、Jump Host経由でのみ通信可能 。
小売 / POS	POS VMと事務用VMを独立したVLANで管理し、外部通信はProxy / VPNを経由。PCI-DSSに準拠 。
通信 / ISP	NFV NodeをCPEまたはEdge Nodeとして使用し、BSS / OSSと統合して計量と監視を実施 。
教育 / 研究	Lab VMを迅速に構築 / 回収し、多バージョンのOSをサポート。校務システムと隔離 。
不動産 / 宿泊	NVR VM、PMS VM、Portal VMを分画し、Multi-WANで外部接続経路とFailoverを制御 。
政府 (Front Desk)	外部ネット接続のリスクが高い受付窓口に、安全な隔離デスクトップを提供 。

単一のセキュリティホスト:
企業と家庭に共通の NFV 基盤

企業・組織向け

- **リソース効率の最適化とコスト削減** 単一の NFV プラットフォーム上に、複数の重要サービス（ファイアウォール、WAN Edge、SBC、アプリケーションサーバー）を統合。リソースの利用効率を最大化し、ハードウェア導入コストやデータセンターのラックスペース費用を大幅に削減します。
- **導入サイクルの短縮** まずは仮想化環境で PoC（概念実証）やテストを実施し、環境が整った段階でマルチノードやクラウドへ拡張可能。これにより、システム導入までの期間を劇的に短縮します。

オフィス環境（Office Environment）

- **ワンストップ・セキュアネットワークセンターとしての NFV プラットフォーム** VPN、ファイルサービス、社内システム、そして開発・テスト環境を一つのプラットフォームで集中管理。NFV がオフィスのあらゆるネットワークとサービスの中約拠点となります。
- **エンドユーザー端末の負荷軽減とセキュリティ強化** ユーザー端末は「接続」のみを担当。個人の PC に高リスクなサービスや機密データを保持させない運用を実現し、情報漏洩などのセキュリティリスクを大幅に低減します。

住宅・SOHO・個人ラボ

- 家庭の「スマートホーム・ハブ」およびセキュリティセンター Azblink NFV を「インテリジェント・ホームサーバー」として活用。IoT やスマートホームの制御、監視カメラの録画（VMS）、入退室管理、センサープラットフォームなどの機能を一台に集約します。
- 家族のためのセキュアなネットワーク環境 子供用デバイスのために独立したネットワークセグメント（網段）を構築。外出先から安全に接続できるリモート VPN、プライベートクラウド、メディアサーバー（動画・音楽）などの機能を提供します。
- 柔軟な実験・検証環境の提供 スナップショット（バックアップ・復元）機能を備えた実験環境としても最適です。日常的な PC作業や仕事に影響を与えることなく、新しい OS やサービスのインストール・テストを自由に行えます。

企業と家庭を支える「第2のセキュア・コンピュータ」

市場と技術環境の変化

- **LLM / GPU / AI Pipelines**による単一デバイスへのリソース需要の大幅増に対し、従来のFat Client架構では良好な体験の維持が困難 。
- **Zero Trust / Micro-Segmentation**架構の普及により、エンドポイントの可視性と制御性への要求が向上 。
- 低消費電力の多核心x86プラットフォーム（Intel N系列等）により、**Edge Hypervisor Node + NFV**がコスト効率の高い選択肢に 。

システム構成（簡略化された技術視点）

- **Host OS**: Linuxを基礎とし、KVM HypervisorとContainer Runtime（LXC等）を統合 。
- **NFV**: 仮想交換 / ルーティングコンポーネント（Linux Bridge / OVS / FRR）を通じてVLAN / VRF / PBRを実装 。
- **Security Chain**: vFirewall、IDS / IPS、Proxy / VPN等の仮想サービスを挿入可能。ポリシーによってトラフィックフローを駆動 。

br0 / br1 / br2 / br3 ～ br11 セキュリティゾーン設計

事前定義された仮想ブリッジとファイアウォールルールにより、ネットワークを複数の安全なゾーンに分割：

- **br0（外部接続・管理）**： すべての外部トラフィックを統合。出口および NAT 管理を担います。
- **br2（DMZ ゾーン）**: 公開サーバーなどの対外サービス専用エリアとして隔離し、保護します。
- **br1 / br3 ～ br11（内部・信頼ゾーン）**: セキュリティレベルの異なる内部ネットワークを構築。 (*注：br4 ～ br11 は、プロジェクトの要件に応じて追加の内部セグメントや特殊なゾーンとして柔軟に拡張可能です。*)

br0 — WAN / 管理ゾーン	br0：WAN ／管理ゾーンの役割
	NFV プラットフォームの外部出口および管理用ネットワークとして機能 すべての br1 / br2 / br3～br11 からの外部トラフィックは br0 を経由し、**NAT、マルチ WAN（Multi-WAN）、およびポリシールーティング（Policy Routing）**の各ルールが統一して適用されます。
	厳格なアクセス制御 br0 側に接続された一般ホストから、内部ブリッジ（内部ネットワーク）への勝手なスキャンや接続は一切禁止されています。許可されるのは、必要最小限の管理用トラフィックのみに制限されます。
br1 — 内部制限ゾーン（受限区）	**高リスク・要厳格管理デバイスの隔離** 実験用環境、レガシーシステム（旧システム）、特定の OT（制御技術）機器など、リスクが高い、あるいは厳格な管理を必要とする内部デバイスを配置します。
	通信の厳格な制御 このゾーンから他の IP サブネットへの自発的な接続（**アウトバウンド**）は一切禁止されています。ファイアウォールによって明示的に許可された接続を受動的に受け入れる（**インバウンド**）のみ可能です。
br2 — DMZ ゾーン	**対外公開サービス専用エリア** Webサーバー、メールサーバー、ポータルサイト、API ゲートウェイなど、外部（インターネット）に公開するサービスを配置します。
	高度なネットワーク隔離 他の内部ゾーン（br1 / br3～br11）とは高度に隔離されています。データベース接続や内部 API 呼び出しなど、業務上不可欠な最小限の**バックエンド通信チャネル**のみを開放する設計です。
br3 ～ br11 — 内部信頼ゾーン	**配置対象:** 内部業務システム、管理ツール、および開発・テスト用 VM。
	通信要件: br1 との双方向通信が可能であること。 **制限事項:** デフォルトでは、外部ネットワークからの能動的なアクセス（主動連入）を受け入れないこと。

Always-On Workloads: 技術実装の観点

- 特定のVMに固定のvCPU / RAM / Storageを配置し、自動起動の設定と健康状態の監視を実施 。
- **Watchdog / Health Checkメカニズムによりサービス異常を検知し、VMまたはアプリを自動再起動 。**
- **I/O限速とQoS制御を使用し、バックグラウンドの仕事が他のインタラクティブなセッションの体験に影響するのを回避 。**
- 重要なVMの定期的なSnapshot / Backupにより、迅速な復元とバージョンの回退をサポート 。
- 監視Agent / Log ForwarderをVMテンプレートに事前ロードし、集中監視を容易にします 。
- 多台のNFV Nodeを組み合わせたHA（高可用性）構成のエッジトポロジーを設計可能 。

Per-VM NFV トポロジーと策略制御

- 仮想SwitchとVLAN / VRFを利用して異なるVMを異なるSecurity Zoneに配置し、東西方向の横方向移動を遮断 。
- 各VMにACLと南北 / 東西トラフィック策略を設定し、ログを組み合わせてインシデント分析に活用 。
- **QoS / Rate Limit**により、高トラフィックVM（ NVR / Backup等）の帯域幅使用を制御 。
- PBR / Multi-WAN技術により、特定のVMのトラフィックを指定したISPまたはVPNトンネルへ誘導 。
- 合規が必要なVMに**per-VM VPN**と**Split-DNS**を有効化 。
- **Service Chaining**をサポートし、トラフィックを順次vFirewall、IDS / IPS、Proxy / VPN等に導入 。

実例: 単一VMのNFV Service Chain

フロー: VM（応用） → vFirewall → IDS / IPS → Proxy / VPN → WAN A/B 。
各**ノードに**対応**する**Security Policy**と**Log**を**適用**でき、**最小権限**かつ**可監査**な**Service Chain**を**形成**します** 。

分级パッケージと技術能力の差異

- **SSM-Pro**:
  - 3-5 VMをサポートし、per-VM VPN、Multi-WAN、Service Chaining、Resource Pinningに対応 。
- **Service Chaining**:
  - トラフィックが通過するネットワーク / セキュリティ機能の順序を定義 。
- **Resource Pinning**:
  - vCPU / メモリ等のリソースを特定のVMに釘付けし、性能の安定と資源の隔離を確保 。

MSP・通信事業者向け技術および運用能力

- **API/ポータルによる管理:** API または管理ポータルを通じて、テナント、ノード、VM の管理が可能。また、バージョン管理および一括アップデート（バッチ更新）をサポート。
- **既存プラットフォームとの統合:** Syslog、エージェント、Webhook などの方式により、既存の NMS（ネットワーク管理システム）、SIEM、SOC プラットフォームとの連携が可能。
- **イメージのカスタマイズと深度ある統合:** イメージファイルには、販路（パートナー）独自のカスタムエージェント（監視、セキュリティ、課金用など）をプリインストール可能。これにより、ホワイトラベル化および高度なシステム統合を実現。

現状の一般的な技術および運用上の課題

- AV/EDR/DLP の例外設定に依存した制御により、エンドポイントポリシーの複雑化とメンテナンスコストの増大が続いている。
  - AV（Antivirus）: アンチウイルス / 防毒ソフトウェア
  - EDR（Endpoint Detection and Response）: エンドポイントでの検出と対応
  - DLP（Data Loss Prevention）: データ流出防止（情報漏洩対策）
- レガシーアプリや専用クライアントと、OSやドライバーの更新が頻繁に競合し、互換性の問題が発生している。
- ベンダーアクセスの多くが共有アカウントや汎用VPNで運用されており、監査証跡（オーディットトレイル）が不明確で、リスクが高い状態にある。
- SaaSやマルチクラウド環境の普及に伴い、スプリットトンネルVPNの正確な設定と維持管理がますます困難になっている。
- エンドポイント環境の差異（多様性）が大きく、パッチ管理および脆弱性管理の複雑さが増大している。
- PCI / ISO / SOC 2 などの監査において、エンドポイントの隔離や最小権限の原則（Least Privilege）が適用されていることを効果的に証明するのが困難である。
  - PCI-DSS: クレジットカード業界のデータセキュリティ基準（持カード人データの保護）。
  - ISO (主に ISO 27001): 情報セキュリティマネジメントシステム（ISMS）の国際規格。
  - SOC 2: クラウドおよびサービスプロバイダーを対象とし、セキュリティ・可用性・機密性などの統制項目（トラストサービス基準）を評価する監査レポート。
- エッジや拠点（ブランチ）環境に最適化された専用のハイパーバイザーや NFV ソリューションが不足しており、データセンター向けのツールを無理に流用せざるを得ない状況にある。
- AI や高負荷アプリケーションに対して、リソースの隔離やネットワーク制御が不十分なため、他の基幹業務（ビジネス・クリティカルな業務）に影響を及ぼしやすくなっている。

市場における Azblink NFV Edge の位置付け

類別 / 製品群	ネットワークNFV能力	VM / ワークスペース能力	内蔵UCと応用（原生）
Cisco / Juniper / Dell (uCPE)	強	ネットワークVNFに限定	無
Azure Stack / Nutanix	VM間接支援	通用HCI仮想化	外部応用のみ
OPNsense / pfSense	防火牆 / VPN	非通用VMホスト	無
Azblink NFV Edge	電信級 NFV/UCPE	安全多OS空間	Azblink 原生整合

競合製品との差異

- 多項の方案は「ネットワークNFV」か「仮想化/VDI」のいずれか一方に偏っていますが、Azblinkは両者を同時に兼ね備えています 。
- 防火牆 / ルーター設備は完全な安全機能を持ちますが、通用する多OS VMプラットフォームではありません 。
- **Azblink NFV Edge**は、電信級NFV、安全多OSワークスペース、および原生整合されたUC応用を三位一体としています 。

技術とシーン: 既存ハイパーバイザーとの違い

- **VMware / VirtualBox**: 一般的な仮想化や開発テスト用途 。
- **Proxmox**: データセンター / クラスターハイパーバイザー 。
- **Azblink NFV**: Edge Appliance、Network-First、per-VM NFV策略、および通路多租戶（チャネルマルチテナント）管理に特化 。
- 安全な第二のコンピュータおよびAlways-onエッジワークロードプラットフォームとして最適化されています 。

Azblink NFV vs. 汎用ハイパーバイザー 比較

- Azblink NFV は、単なる「仮想マシンの実行環境」ではなく、**通信事業者や MSP がサービスを提供するための「プラットフォーム」**として設計されている点が最大の違いです。

比較項目	Azblink NFV	VMware / Proxmox	VirtualBox
主な用途	MSP/エッジ/通信インフラ	データセンター/エンタープライズ	個人開発/デスクトップ
管理単位	マルチテナント前提 (顧客ごと管理)	クラスタ/サーバー単位	ローカルマシン単位
リソース消費	極めて軽量 (エッジ/ブランチ最適化)	重厚 (DCの豊富な資源を前提)	中程度
運用の容易性	ゼロタッチ・プロビジョニング	専門知識が必要な複雑な設定	手動操作が中心
セキュリティ	高度な隔離と監査証跡の自動化	追加オプションが必要	基本機能のみ
エージェント	通路(パートナー)独自の Agent 統合	汎用的なツールのみ	なし