Confidential Documentation Vault

> ⚠ **Confidentiality Notice:** All content in this vault is **confidential and proprietary**. Unauthorized distribution, reproduction, or disclosure is strictly prohibited and may result in legal action.

Enterprise Infrastructure Blueprint

This document provides a complete deployment blueprint for our enterprise clients, detailing the end-to-end infrastructure design. It covers everything from physical layout to network architecture, ensuring a robust, scalable, and secure setup. The blueprint includes detailed network diagrams and hardware specifications to guide installations in a **server room or data center environment**.

An example of a secure server room setup with dedicated racks, cooling, and access control. The Enterprise Infrastructure Blueprint outlines how to achieve such a professional, organized environment.

Overview: Our enterprise infrastructure is designed with **privacy, reliability, and performance** in mind. Key elements of the blueprint include segregated network zones (e.g. **DMZ, internal LAN, and guest network**), high-availability server clusters, and on-site data storage using TrueNAS SCALE. All critical systems are on-premises to keep sensitive data under client control (no reliance on external cloud for core services). The blueprint also emphasizes redundant power and cooling, robust firewalling, and secure remote access via VPN (see WireGuard VPN section).

Physical Layout & Environment: We specify requirements for a dedicated, climate-controlled server room. For example:

- **Secure Location:** A lockable server room with solid-core or metal door (optional biometric access), surveillance cameras, and a fireproof safe for backups and sensitive materials.
- **Power & Cooling:** Redundant 20A power circuits with UPS backup and generator integration for power outages. Independent cooling (AC or ventilation) to maintain optimal temperature for equipment.
- **Rack and Cabling:** Standard 19-inch equipment racks with proper cable management. All servers, storage arrays, and network gear are rack-mounted. Cables are labeled and routed through patch panels for a clean layout. This minimizes signal interference and simplifies maintenance.
- **Environmental Monitors:** Temperature and humidity sensors, smoke detectors, and automated alerts for any environmental anomalies.

Network Architecture: The enterprise network diagram (provided in this document) illustrates a multi-tier architecture:

- **Edge Firewall/Router:** A high-performance firewall (e.g. pfSense or Cisco NGFW) at the network perimeter. It connects to the ISP and manages traffic into a **Demilitarized Zone (DMZ)** for any traffic.

- **DMZ Segment:** Hosts external services (if any, such as a web server or a VPN endpoint) isolated from the internal network. This adds an extra layer of security—external clients can reach the DMZ servers but have no direct path to the internal LAN.
- **Internal Network Segments:** The internal LAN is segmented into VLANs or subnets by function (e.g. corporate PCs, IoT devices, servers, IP cameras). For enterprise clients, we recommend VLANs like *Workstations*, *Servers*, *VoIP/IoT*, and *Guest Wi-Fi*. Internal switches (Layer 2/3) handle VLAN tagging and inter-VLAN routing is tightly controlled (only allow necessary traffic between segments).
- **Core Services:** Core infrastructure like directory services (AD/LDAP), DNS/DHCP, and monitoring systems reside on the secure server VLAN. They are only accessible to authorized segments. Storage systems (NAS/SAN) connect to a storage network for high throughput and are also isolated from client subnets except via specified file-sharing protocols.
- **Remote Access:** No direct exposure of internal services to the internet. All remote access for administrators or clients is tunneled through a VPN (see WireGuard section) or other secure gateway in the DMZ. This ensures that even maintenance is done through encrypted channels with strict authentication.

Server & Storage Design: The blueprint calls for at least two server-grade machines for redundancy and load distribution:

- **Primary Server Node:** A powerful rackmount server (multi-core CPUs, ample RAM) running a hypervisor (Proxmox VE) to host critical VMs and containers. This primary node might run services like virtualization for business apps or AI workloads (see On-Prem AI Deployment Scripts), and potentially house an instance of our password vault or management VMs.
- **Secondary Server Node:** Another server (or high-end workstation) to run auxiliary services and provide failover. It might handle tasks like home automation controllers, media servers, or act as a hot spare for critical VMs (replicated from the primary).
- **GPU Acceleration:** If AI or heavy computation is required (as in many enterprise scenarios), one server is equipped with an **NVIDIA GPU** (configured via GPU passthrough on Proxmox). This allows VMs to leverage the GPU for machine learning inference, data analysis, or any GPU-intensive applications internally.
- **Storage Array (NAS):** Enterprise-grade storage is provided by TrueNAS SCALE on a dedicated NAS server or as a VM with direct disk access. The design uses ZFS with RAID for data protection (e.g. RAID-Z2 or mirrored vdevs with hot spares). At least 60–100TB raw capacity is recommended for heavy data users, using enterprise HDDs and SSD caches for performance. All sensitive data stays on this NAS; cloud backup is optional and encrypted if used. Local backup drives (encrypted external disks) are rotated off-site periodically and kept in the fireproof safe.

High-Level Diagram: The included network diagram visualizes the above components. It shows the internet feeding into a firewall, which then connects to a switch that feeds multiple VLANs (with example devices on each). Servers and the NAS are on the secure server VLAN. A management station (or laptop) can access the systems via an out-of-band management network or the VPN. The diagram also highlights how the WireGuard VPN server in the DMZ grants remote admins access to the management VLAN only, not the entire network.

- A **professional network diagram** (physical and logical) tailored to their environment, printed in a binder and as a high-res PDF.
- A write-up of infrastructure specifications and **standard operating procedures (SOPs)** for routine tasks (e.g. how to start/stop services, replace a drive, etc.).
- Configuration files and credentials (securely stored, with backups in sealed envelopes in the safe).
- A training session and documentation for the client’s IT staff (or family/assistants in a residential case) to understand the setup.

By following the Enterprise Infrastructure Blueprint, we ensure that every deployment is consistent with our high standards of security and reliability, providing a solid foundation for all other services (AI, storage, remote access) to run smoothly.

Advanced Security Protocols (Zero-Trust Architecture)

This document is a comprehensive guide to our **advanced security protocols**, built on a Zero-Trust architecture model. It details how we implement a “**never trust, always verify**” approach across the entire infrastructure, including network segmentation, firewall rules, authentication policies, and monitoring. By following these protocols, we greatly reduce the risk of breaches and ensure client data remains private and secure.

Strict physical security complements our digital security. The vault door and secure safe shown above are examples of how we protect critical hardware and backups from unauthorized access, aligning with our advanced security protocols.

Zero-Trust Principles: In a zero-trust model, no user or device is inherently trusted, even if it’s inside the network. Every access request must be authenticated, authorized, and encrypted. We apply this principle in multiple layers:

- **Identity Verification:** Strong identity and access management (IAM) is mandatory. All user accounts (both for IT admins and end-users) use **multi-factor authentication (MFA)** wherever possible. For example, VPN access via WireGuard requires an SSH key or one-time pass along with the key, and administrative logins to servers require MFA or hardware tokens.
- **Least Privilege Access:** Each user and service is given the minimum privileges needed to perform its function. Admin accounts are separate from regular user accounts. Role-based access control (RBAC) is used on systems like TrueNAS and Proxmox – e.g., a “view-only” role for auditors vs. a “maintainer” role for system engineers. Credentials (passwords, keys) are stored in an encrypted vault (our on-prem password manager) and access to them is logged and limited.

Network Segmentation & Firewalling: Our network is segmented (as described in the Blueprint) and the firewall acts as a gatekeeper between all segments:

- **Firewall Rules:** The firewall configuration is provided as part of this guide. It operates on a **default deny** policy: all inbound **and** internal inter-VLAN traffic is denied unless explicitly allowed. We provide a set of predefined rules, such as: *allow* DNS from VLANs to the DNS server, *allow* web traffic etc. Everything else (e.g., IoT to corporate network, or inbound from internet to LAN) is blocked.

- **Micro-Segmentation:** Even within a VLAN, critical services are further protected. For instance, the NAS shares may have host-based allow-lists (only known IPs can connect), and management interfaces (like the Proxmox web UI or TrueNAS UI) are restricted to a small management subnet or accessible only through VPN. If an attacker somehow lands on one internal machine, they shouldn't freely roam the network.
- **DMZ Isolation:** Any service in the DMZ (like the VPN endpoint or a web server if deployed) is on its own subnet with very limited access back to internal resources. The firewall may allow the DMZ service to query an internal authentication server (like LDAP) but never to initiate arbitrary connections into the LAN. This way, if the DMZ service is compromised, the damage is contained.

Secure Configuration & Protocols: We enforce modern, secure configurations on all systems:

- **Encryption Everywhere:** All data in transit is encrypted using strong protocols (HTTPS/TLS1.3 for web interfaces, WireGuard for VPN, SSH with key authentication for server access, etc.). Within the network, wherever possible, we prefer end-to-end encryption too – for example, if a client application talks to the NAS, it can use NFSv4 with Kerberos or SMB with AES encryption enabled.
- **Secure Defaults:** We disable legacy insecure protocols (e.g., SMBv1, Telnet, older SSL versions) and use hardened configurations (strong ciphers, certificates) across services. Administrative interfaces are not exposed on default ports publicly. We also enable enterprise features like **full-disk encryption** on servers and NAS (so if drives are stolen, data remains inaccessible).
- **Patching and Updates:** A protocol is in place for regular updates of all systems. The guide includes a maintenance schedule recommending at least monthly patching of OS and software (including firewall firmware, hypervisor updates, and application patches). Automatic security updates are enabled where possible, with notifications to admins. Each patch cycle is logged.

Monitoring & Response: Advanced security isn't complete without monitoring and incident response:

- **Logging:** All servers, network devices, and applications send logs to a central log server (or SIEM) where they are stored securely and analyzed for anomalies. For example, the firewall logs all blocked traffic and the VPN logs all connection attempts. Proxmox and TrueNAS logs are collected for any unusual activity (like repeated login failures).
- **Intrusion Detection/Prevention:** We deploy an IDS/IPS (such as **Suricata or Snort**) on the network, typically integrated with the firewall. This system uses updated threat signatures and behavioral analysis to alert or block suspicious traffic (like port scans or known exploit patterns). In our zero-trust setup, even internal traffic can be monitored for lateral movement indications.
- **Alerts:** The guide defines alert rules and contacts. If certain events occur (admin login outside business hours, a new device connecting to the network, etc.), the system sends immediate alerts (email/SMS) to the on-call security engineer. We also set thresholds (e.g., CPU spikes that might indicate crypto-mining malware) to trigger warnings.
- **Incident Response Plan:** Finally, we include a high-level incident response procedure. This covers isolating affected systems, collecting forensic data (from our logs and versioned backups), eradicating threats, and restoring from backups if needed. Because of the layered protections, a breach in one area is contained, but we assume breach and act swiftly whenever any anomaly is detected.