MKR

TECHNOLOGY SOLUTIONS

- Cloudflare Tunnel + Double Caddy
- UDM Pro + Firewall + VPN
- Proxmox + Backup Server + DRBD
- FreeIPA + Keycloak
- NAS: FreeIPA + Samba
- Cloud: Nextcloud + Apps
- Cyber Security

Enterprise-Grade Security Infrastructure

Cloud | Security | Virtualization | Identity | Collaboration

A complete IT infrastructure buildout solution for small businesses through enterprise teams

Security, stability, and scalability - all in one

Solution Overview

A complete IT infrastructure built from 7 core solution layers

01 **Cloudflare Tunnel + Double Caddy**
Secure external access channel & reverse proxy

02 **UDM Pro + Firewall + VPN**
Zone-based firewall & user access control

03 **Proxmox + PBS + DRBD**
Virtualization server & auto-recovery storage

04 **FreeIPA + Keycloak**
Integrated identity & single sign-on (SSO)

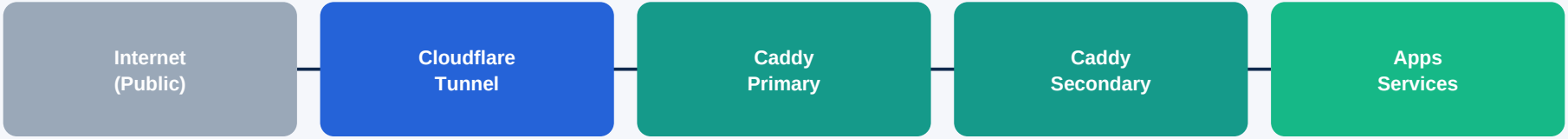
05 **NAS: FreeIPA + Samba**
Permission-based network storage

06 **Cloud Workspace**
Nextcloud, OpenProject, Vaultwarden, and more

07 **Cyber Security**
Multi-layer security architecture & attack defense

Cloudflare Tunnel + Double Caddy

A secure channel for safely accessing internal services from the public internet



Cloudflare.com

- One of the world's largest CDN and security networks
- Network across 330+ cities in 120+ countries
- DDoS protection, WAF, and bot management
- Free plan: DDoS + basic managed WAF ruleset (advanced WAF/bot scoring is paid)

Cloudflare Tunnel Benefits

- No open ports required - safely expose servers behind the firewall
- External access without a public IP address
- End-to-end encryption (TLS)
- Enables a Zero Trust security model

Double Caddy Benefits

- Role separation: primary handles TLS termination & auto-cert management
- Automatic HTTPS certificate issuance and renewal
- Secondary handles internal app routing & access control
- Edge attack-blocking is performed by the Cloudflare layer

UDM Pro + Zone-Based Firewall + VPN

Segment the network precisely with zones and secure remote access through VPN

Zone-Based Firewall Benefits

- Segment the network into role-based security zones
- Control traffic between zones with detailed policies
- Automatically apply policies when new devices are added
- Granular L3 traffic filtering

VPN + Firewall User Control

- VPN authenticates against FreeIPA via RADIUS
- Limit accessible network zones by user / group
- Apply the same internal security model to remote workers
- Log connection history and monitor in real time
- Advanced per-user policy & MFA via UniFi Identity

Proxmox Virtualization Server + PBS + DRBD

Enterprise-grade virtualization, automatic recovery, and efficient backup for stability

PVE Firewall - Complements UDM Pro

- Host/VM-level firewall (no per-VM hardcoding)
- Application-level policy management simplifies upkeep
- Software-based rules - flexible and version-controlled
- Defense-in-depth with the UDM Pro network firewall

ZFS - Automatic Disk Recovery

- Automatic mirroring across disks (mirror / RAIDZ)
- Self-healing: restores corrupt blocks from a good copy
- Data integrity verification using checksums
- Enterprise reliability without a hardware RAID card

DRBD - Real-Time Server Replication

- Servers replicate the same data in real time
- 2 diskful + 1 diskless quorum node (anti split-brain)
- Auto failover via DRBD Reactor / Pacemaker (brief I/O pause)
- DRBD / LINSTOR maintained & supported by LINBIT
- Packaged separately - not bundled with Proxmox

Proxmox Backup Server (PBS)

- Deduplication (not raw compression): ~5-10x savings
- zstd compression; savings vary by workload
- Incremental dirty-bitmap backups - low impact
- Multiple per day; fast SHA-256-verified restore
- Ransomware-resistant; optional S3 Object Lock

FreeIPA + Keycloak - Integrated Identity System (SSO)

Access every service with one login - enterprise reliability based on Red Hat technologies

SSO Authentication Flow

Strong authentication policy:
Random 4+ word passphrase (15+ chars) + MFA, generated & stored in Vaultwarden - no reuse, no memorization (per NIST SP 800-63B)

FreeIPA (Red Hat)

- Unified ID management for Linux/Unix
- Combines LDAP, Kerberos, DNS, and CA
- Upstream of Red Hat Enterprise Linux IdM
- Centralized user, group & policy management

Keycloak (SSO Broker)

- Supports OIDC, SAML, and OAuth 2.0
- Connects with FreeIPA for web app SSO
- Supports MFA (multi-factor authentication)
- Role-based access control (RBAC)

Integrated Identity Benefits

- One account for all services (protect with MFA)
- Instantly block all access if a credential leaks
- Disable departing employees everywhere at once
- Centralize security audit logs

NAS - FreeIPA + Samba Permission-Based Network Storage

A secure NAS accessible only from authenticated PCs and Macs - high-performance storage

Samba as Domain Member

- Only FreeIPA-authorized PCs/Macs reach shares (Kerberos)
- Unverified devices blocked at the authentication layer
- Granular file access permissions by user and group
- Windows / macOS / Linux compatible (Kerberos-based)
- Access revoked instantly when an account is disabled

High Performance & High Availability

- ZFS local storage enables low-latency access
- High reliability with a Red Hat based OS
- DRBD: standby resumes service within sub-minute
- Quorum-managed failover (DRBD Reactor / Pacemaker)
- Data integrity: ZFS checksum + DRBD replication

Cloud Workspace - Nextcloud, OpenProject, Vaultwarden & More

A unified cloud work platform accessible from anywhere - secured without exposing passwords

Nextcloud

- Flexible shared storage (within underlying disk capacity)
- Group chat, video meetings & recording (Talk)

OpenProject

- Project schedule management
- File sharing, Kanban, and Gantt charts

Paperless

- Document digitization and OCR
- Automatic classification & searchable archive

Vaultwarden

- Self-hosted, Bitwarden-compatible password manager
- A unique strong password per app - none reused

Outline

- Team knowledge base and wiki
- Collaborative documentation platform

Keycloak SSO

- Single login for Nextcloud/OpenProject/Paperless/Outline
- Vaultwarden OIDC SSO (master password still separate)

Cyber Security - Multi-Layer Security Architecture

From the public internet to internal apps - layered defense-in-depth

Authentication flow: FreeIPA -> Keycloak -> all Apps (SSO)

Zero Trust-Aligned Access

Every access request is authenticated via SSO (and Cloudflare Access) - no implicit trust from network location.

Password Exposure Prevention

Vaultwarden stores a unique strong password per app; MFA protects every login.

VPN-Based Data Access

All remote data access travels through a secured VPN tunnel.

Backup & Recovery

PBS ransomware-resistant backups plus DRBD quorum-based failover.

Attack Pattern Defense

Cloudflare bot management and WAF rulesets help block attack patterns at the edge.

Central Audit Logging

Authentication and access events aggregated centrally (e.g., Wazuh / Graylog).

Why MKR?

Enterprise-level security and reliability - achievable for small organizations too

Security

- Multi-layer defense: Cloudflare -> Caddy -> FreeIPA
- Zero Trust-aligned, identity-centric access
- No password reuse with Vaultwarden + MFA

Reliability

- DRBD real-time replication + quorum-based failover (via LINBIT)
- ZFS local storage with self-healing recovery
- PBS deduplication (typ. 5x-10x) + ransomware-resistant backups

Scalability

- Add new services quickly with Proxmox virtualization
- SSO integration with FreeIPA + Keycloak
- Every team member can work securely from anywhere

Contact & Proposal

We analyze your current infrastructure and propose the optimal configuration for your business.

MKR Technology Solutions