

Global Architecture and Request Flow

Purpose

The Bytek homelab provides privately hosted identity, collaboration, documentation, monitoring, project-management, and infrastructure services.

The environment is hosted on Proxmox VE and follows these design principles:

- One major service per VM or LXC.
- Public services enter through a VPS instead of direct home-router port forwarding.
- WireGuard transports public traffic securely from the VPS to the home network.
- Traefik terminates HTTPS and routes requests according to the requested hostname.
- Authentik provides centralized authentication, multi-factor authentication, and application-access policies.
- Pi-hole provides LAN DNS, split DNS, and DHCP reservations.
- Data-bearing applications use a dedicated LVM-thin storage pool.
- Proxmox backups are stored on a separate internal HDD.
- Management interfaces remain accessible only from the LAN or a trusted VPN whenever practical.
- Critical services retain an authentication or console path that does not depend on Authentik.

Main Components

Component	Address	Primary Role
Public VPS	38.29.213.101	Public HTTPS entry point
WireGuard gateway	192.168.2.64	VPS-to-home tunnel gateway

Pi-hole	192.168.2.65	DNS, split DNS, and DHCP reservations
Nextcloud AIO	192.168.2.100	File storage and collaboration
Uptime Kuma	192.168.2.115	Service monitoring
Vikunja	192.168.2.121	Project and task management
Authentik	192.168.2.162	Identity, authorization, and MFA
Traefik	192.168.2.182	HTTPS reverse proxy
Proxmox VE	192.168.2.254	Hypervisor
BookStack	Confirm current IP	Infrastructure documentation

Core Infrastructure Roles

Proxmox VE

Proxmox VE hosts the Bytek VMs and LXC's.

Proxmox provides:

- Virtual-machine and container isolation.
- Virtual networking.
- Proxmox firewalling.
- LVM-thin storage.
- Scheduled backups.
- Short-term snapshots.
- VM and LXC restoration.
- Emergency console access.

Proxmox management address:

[Open Proxmox VE](#)

Proxmox is intended for LAN or trusted VPN access only.

Public VPS

The VPS is the public entry point for applications hosted at home.

The VPS receives public HTTPS traffic at `38.29.213.101` and forwards permitted traffic through WireGuard.

The VPS prevents each home service from requiring its own public router port forwarding rule.

WireGuard Gateway

The home WireGuard gateway connects the VPS tunnel to the home LAN.

The gateway performs:

- WireGuard tunnel termination.
- Controlled traffic forwarding.
- Firewall filtering.
- Network address translation where required.
- Delivery of public HTTPS traffic to Traefik.

Pi-hole

Pi-hole provides:

- LAN DNS.
- DNS filtering.
- Split-DNS records.
- DHCP reservations.
- Internal application-name resolution.

Pi-hole allows the same application hostname to work both inside and outside the home network.

Traefik

Traefik is the central HTTPS reverse proxy.

Traefik provides:

- HTTPS termination.
- Let's Encrypt certificate management.
- Hostname-based application routing.
- Communication with private application backends.

- Authentik ForwardAuth for selected administrative services.
- Dashboard visibility into routers, services, and certificates.

Authentik

Authentik is the central identity provider.

Authentik provides:

- Central user accounts.
- Multi-factor authentication.
- OpenID Connect.
- Proxy Providers.
- ForwardAuth.
- Group-based authorization.
- Email-domain policies.
- Embedded outpost services.

External Application Traffic

When an external user opens an application, traffic moves through the following components:

1. The user enters an application hostname such as `ccloud.bytek.ca`.
2. WHC public DNS resolves the hostname to the VPS at `38.29.213.101`.
3. The VPS accepts the HTTPS connection on TCP port 443.
4. The VPS forwards the traffic through the WireGuard tunnel.
5. The home WireGuard gateway receives the tunneled traffic.
6. The gateway forwards the request to Traefik at `192.168.2.182`.
7. Traefik examines the requested hostname.
8. Traefik forwards the request to the correct internal application.

Nextcloud Example

A public Nextcloud request follows this path:

1. The browser opens `ccloud.bytek.ca`.
2. WHC DNS returns `38.29.213.101`.

3. The VPS receives the connection.
4. The VPS forwards the connection through WireGuard.
5. The home gateway forwards the request to Traefik.
6. Traefik forwards the request to Nextcloud at `192.168.2.100` on TCP port 11000.

BookStack Example

A public BookStack request follows this path:

1. The browser opens `docs.bytek.ca`.
2. WHC DNS returns `38.29.213.101`.
3. The VPS receives the connection.
4. The VPS forwards the connection through WireGuard.
5. The home gateway forwards the request to Traefik.
6. Traefik forwards the request to the BookStack VM on TCP port 6875.

Vikunja Example

A public Vikunja request follows this path:

1. The browser opens `projects.bytek.ca`.
2. WHC DNS returns `38.29.213.101`.
3. The VPS receives the connection.
4. The VPS forwards the connection through WireGuard.
5. The home gateway forwards the request to Traefik.
6. Traefik forwards the request to Vikunja at `192.168.2.121` on TCP port 3456.

Internal Application Traffic

LAN devices do not need to leave the home network and return through the VPS.

Pi-hole resolves public application hostnames directly to Traefik.

Hostname	Internal Address
<code>cloud.bytek.ca</code>	<code>192.168.2.182</code>
<code>docs.bytek.ca</code>	<code>192.168.2.182</code>
<code>portal.bytek.ca</code>	<code>192.168.2.182</code>

projects.bytek.ca	192.168.2.182
proxy.bytek.ca	192.168.2.182
status.bytek.ca	192.168.2.182

An internal request follows this path:

1. The LAN client queries Pi-hole.
2. Pi-hole returns 192.168.2.182.
3. The client connects directly to Traefik.
4. Traefik routes the request to the private application backend.

This internal route provides:

- Lower latency.
- No unnecessary public internet path.
- No dependence on router hairpin NAT.
- The same HTTPS hostname inside and outside the home network.
- Valid Let's Encrypt certificates for internal and external access.

Proxmox Private Access

Proxmox does not sit behind Traefik.

Pi-hole resolves:

- pve.bytek.ca to 192.168.2.254.

The administrative path is:

1. The administrative workstation queries Pi-hole.
2. Pi-hole returns 192.168.2.254.
3. The workstation connects to Proxmox on TCP port 8006.

The Proxmox host itself uses Quad9 at 9.9.9.9 rather than Pi-hole.

This prevents the hypervisor from depending on Pi-hole for its own DNS resolution.

Native OIDC Authentication

The following services use native Authentik OpenID Connect:

- Nextcloud.
- Vikunja.
- BookStack.
- Proxmox VE.

The authentication sequence is:

1. The application redirects the browser to `portal.bytek.ca`.
2. Authentik requests credentials and MFA.
3. Authentik evaluates application group and policy bindings.
4. Authentik redirects the browser to the application callback.
5. The application validates the returned token.
6. The application creates or matches the local user.
7. The application applies its own internal permissions.

OIDC Callback Reference

Application	Callback
Nextcloud	<code>https://cloud.bytek.ca/apps/user_oidc/code</code>
Vikunja	<code>https://projects.bytek.ca/auth/openid/authentik</code>
BookStack	<code>https://docs.bytek.ca/oidc/callback</code>
Proxmox VE	<code>https://pve.bytek.ca:8006</code>

Proxy Authentication

Some services do not support native OIDC.

Authentik Proxy Providers or ForwardAuth are used for:

- Traefik dashboard.
- Uptime Kuma dashboard.

Traefik Dashboard

The dashboard request follows this sequence:

1. The administrator opens `proxy.bytek.ca`.
2. Traefik invokes the Authentik ForwardAuth middleware.
3. The embedded Authentik outpost validates the user.
4. Authentik requires membership in `bytek-admin`.
5. The authenticated request returns to the Traefik dashboard.

Uptime Kuma

The Uptime Kuma request follows this sequence:

1. The administrator opens `status.bytek.ca`.
2. Traefik forwards the request to the Authentik embedded outpost.
3. Authentik validates the user and policies.
4. The outpost forwards the request to Uptime Kuma.
5. Selected public status-page paths may bypass authentication when intentionally configured.

Standard User Access

The Authentik group `bytek-users` grants access to:

- Nextcloud.
- Vikunja.
- BookStack.

These applications also apply the `Allow bytek.ca users` policy.

Policy engine mode is set to `ALL`.

A user must therefore:

- Belong to `bytek-users`.
- Pass the `Allow bytek.ca users` policy.

Administrator Access

The Authentik group `bytek-admin` grants access to:

- Proxmox VE.
- Traefik dashboard.
- Uptime Kuma dashboard.

Administrative applications also apply the `Allow bytek.ca users` policy.

An administrator may belong to both `bytek-admin` and `bytek-users`.

Application Access Matrix

Service	Authentication	Intended Group
Nextcloud	Native Authentik OIDC	<code>bytek-users</code>
Vikunja	Native Authentik OIDC	<code>bytek-users</code>
BookStack	Native Authentik OIDC	<code>bytek-users</code>
Proxmox VE	Native Authentik OIDC	<code>bytek-admin</code>
Traefik dashboard	Authentik ForwardAuth	<code>bytek-admin</code>
Uptime Kuma dashboard	Authentik Proxy Provider	<code>bytek-admin</code>
Pi-hole	Local authentication	Administrators on LAN
Nextcloud AIO	AIO local authentication	Administrators on LAN
WireGuard gateway	SSH key authentication	Administrators
VPS	SSH key authentication	Administrators

Service URLs

Service	URL	Access Scope
Authentik	Open Authentik	Public through Traefik
Nextcloud	Open Nextcloud	Public through Traefik
Vikunja	Open Vikunja	Public through Traefik
BookStack	Open BookStack	Public through Traefik

Uptime Kuma	Open Uptime Kuma	Authentik-protected
Traefik dashboard	Open Traefik	Administrators only
Proxmox VE	Open Proxmox	LAN or VPN only
Nextcloud AIO	<code>https://192.168.2.100:8080/</code>	LAN or VPN only

Break-Glass Access

Central authentication must not be the only recovery path.

Proxmox VE

- **Recovery account:** `root@pam`
- **Access methods:** Private hostname, private IP, or Proxmox console

Authentik

- **Recovery account:** Local Authentik administrator
- **Access methods:** Public portal or direct private backend during recovery

Nextcloud

- **Recovery account:** Local Nextcloud administrator
- **Recovery path:** `/login?direct=1`

BookStack

- **Recovery account:** Dedicated local BookStack administrator
- **Recovery method:** Switch `AUTH_METHOD` from `oidc` to `standard`

Uptime Kuma

- **Recovery account:** Original Kuma administrator

- **Recovery method:** Restore direct private access and re-enable local authentication

Traefik

- **Recovery method:** SSH into the Traefik VM and restore a known-good dynamic configuration
- **Secondary authentication:** Retained Basic Auth while ForwardAuth is being validated

Pi-hole

- **Recovery method:** Private IP, local credentials, and Proxmox console

Critical Dependencies

Function	Dependency Chain
Public applications	WHC DNS, VPS, WireGuard, Traefik, application
Internal applications	Pi-hole, Traefik, application
OIDC login	Application, Traefik, Authentik, Authentik database
Certificate issuance	Traefik, DNS, Let's Encrypt, WHC cPanel API
Monitoring	Uptime Kuma, Pi-hole, monitored services
Backups	Proxmox, mounted backup HDD

Failure Impact

Failed Component	Expected Impact
Pi-hole	Internal hostname resolution may fail
VPS	External access fails; LAN access should continue
WireGuard	External VPS ingress fails
Traefik	HTTPS routing fails
Authentik	New SSO logins fail

Proxmox	VM management fails; running guests may continue
Backup HDD	New backups fail; live services continue
Nextcloud	File and collaboration services fail
Vikunja	Project-management service fails
BookStack	Documentation service fails
Uptime Kuma	Monitoring and alerts fail

Security Boundaries

The following services must not be exposed directly to the public internet:

- Proxmox TCP 8006.
- Pi-hole administration.
- Nextcloud AIO TCP 8080.
- Nextcloud AIO backend TCP 11000.
- Authentik backend TCP 9000.
- Uptime Kuma backend TCP 3001.
- Vikunja backend TCP 3456.
- BookStack backend TCP 6875.
- Traefik internal dashboard service.
- SSH on home service VMs.
- Docker socket or Docker API.

Operational Principles

1. Validate the direct application backend before troubleshooting Traefik.
2. Validate Traefik locally before troubleshooting the VPS.
3. Validate Pi-hole before changing application OIDC settings.
4. Confirm container DNS after a power failure.
5. Preserve local recovery accounts.
6. Do not regenerate OIDC secrets until connectivity is proven.
7. Do not delete Traefik certificate storage during troubleshooting.
8. Do not treat snapshots as backups.

9. Test restored VMs with their network adapter disconnected.
10. Update documentation after each validated infrastructure change.

Document Control

- **Owner:** Bryan Gagne-Plante
- **Last verified:** YYYY-MM-DD
- **Backup coverage:** Partial
- **Recovery tested:** Partial
- **Offsite backup:** Not configured
- **Known limitations:** One Proxmox host and one local backup location

Revision #4

Created 2026-08-17 14:44:42 UTC by Bryan Gagne-Plante

Updated 2026-08-17 15:24:10 UTC by Bryan Gagne-Plante