

Public VPS Ingress

Purpose

The public VPS is the internet-facing entry point for applications hosted on the Bytek home network.

The VPS prevents individual home services from being exposed directly through the Bell router. Public HTTPS traffic reaches the VPS first, then travels through an encrypted WireGuard tunnel to the home network.

The VPS provides:

- A stable public IPv4 entry point.
- Public TCP port 443.
- An encrypted path to the home network.
- Separation between the public internet and private service backends.
- A recovery console independent of the home network.
- A controlled point for public firewalling.

Service Information

Setting	Value
Public IPv4 address	38.29.213.101
Primary purpose	Public HTTPS ingress
Public application port	TCP 443
Home-network transport	WireGuard
Administration	SSH key authentication
SSH port	Confirm current hardened SSH port

Operating system	Confirm current Linux distribution
Hosting provider	Confirm current VPS provider
Public DNS provider	WHC cPanel
Monitoring	Uptime Kuma

Architecture Role

The VPS does not host the main Bytek applications.

The VPS forwards approved traffic to the home network.

The primary traffic path is:

1. A client opens a public application hostname.
2. WHC DNS resolves the hostname to 38.29.213.101.
3. The client establishes HTTPS to the VPS on TCP port 443.
4. The VPS forwards the permitted connection through WireGuard.
5. The home WireGuard gateway receives the traffic.
6. The gateway forwards the request to Traefik at 192.168.2.182.
7. Traefik selects the correct application backend.

The VPS must not have direct access to all home-LAN services unless a specific rule requires it.

Public Hostnames

The following public DNS records point to the VPS:

Service	Hostname	Public Destination
Nextcloud	cloud.bytek.ca	38.29.213.101
BookStack	docs.bytek.ca	38.29.213.101
Authentik	portal.bytek.ca	38.29.213.101
Vikunja	projects.bytek.ca	38.29.213.101
Traefik dashboard	proxy.bytek.ca	38.29.213.101

Uptime Kuma	status.bytek.ca	38.29.213.101
-------------	-----------------	---------------

The public hostname `pve.bytek.ca` must not point to the VPS.

Proxmox remains available only through the LAN or a trusted remote-access method.

Public HTTPS Flow

External HTTPS requests follow this sequence:

1. WHC public DNS returns `38.29.213.101`.
2. The incoming connection reaches the VPS on TCP port 443.
3. VPS firewall rules verify that the connection targets an approved public entry point.
4. The VPS forwards the traffic through the WireGuard tunnel.
5. The home WireGuard gateway forwards the connection to Traefik.
6. Traefik terminates HTTPS or processes the forwarded connection according to the configured design.
7. Traefik routes the request by hostname.

The VPS does not need separate public ports for every HTTPS application because Traefik distinguishes applications by hostname.

WireGuard Connection

The VPS maintains a WireGuard peer relationship with the home WireGuard gateway.

The tunnel is used for:

- Public HTTPS ingress.
- Approved management traffic where explicitly configured.
- Connectivity testing between the VPS and home gateway.
- Delivery of traffic to Traefik.

The existing VPS tunnel must remain separate from any future laptop or phone VPN.

Do not reuse:

- The same WireGuard client keys.
 - The same peer address.
 - The same interface configuration.
 - The same subnet for road-warrior clients without deliberate routing design.
-

WireGuard Health

Review the tunnel using:

```
sudo wg show
```

Verify:

- The home peer is listed.
- A recent handshake exists.
- Transfer counters are increasing.
- The expected tunnel addresses appear.
- Allowed IPs contain only intended routes.
- The endpoint and keepalive settings match the deployment.

A recent handshake confirms peer connectivity but does not prove that application forwarding works.

Test the complete application path separately.

VPS Firewall Policy

The VPS firewall should allow only required public and administrative traffic.

Required Public Access

- TCP 443 for hosted HTTPS applications.
- The required WireGuard UDP port.
- The hardened SSH management port.

Traffic That Must Remain Private

Do not expose the following home ports through the VPS:

Service	Port
Proxmox VE	TCP 8006
Pi-hole DNS administration	Private management port
Nextcloud AIO management	TCP 8080
Nextcloud AIO backend	TCP 11000
Uptime Kuma backend	TCP 3001
Authentik backend	TCP 9000
Vikunja backend	TCP 3456
BookStack backend	TCP 6875
Docker API	Any Docker API listener
Home service SSH	TCP 22

New public ports must be documented before being added.

SSH Administration

VPS management uses SSH key authentication.

Recommended SSH controls include:

- Disable password authentication.
- Disable direct root login where the administration model permits.
- Restrict accepted users.
- Use an Ed25519 key.
- Store the private key securely.
- Use Fail2ban or equivalent rate limiting.
- Keep the VPS provider console available for recovery.
- Restrict SSH using the VPS firewall where practical.

Confirm the current SSH listener using:

```
ss -lntp
```

Confirm SSH service health using:

```
systemctl is-active ssh
```

Expected result:

- active

Do not place the private SSH key in BookStack.

Public DNS Management

Public DNS records are managed through WHC cPanel.

When adding a new public application:

1. Create an A record for the new hostname.
2. Point the record to 38.29.213.101.
3. Use a short TTL during the initial deployment.
4. Create the matching Pi-hole split-DNS record.
5. Create the Traefik router and service.
6. Confirm the application backend is reachable from Traefik.
7. Confirm certificate issuance.
8. Test internally.
9. Test externally using cellular data or another external network.
10. Add Uptime Kuma monitoring.
11. Update BookStack documentation.

Do not point public DNS directly to:

- A private home address.
 - The application VM.
 - Traefik's private IP.
 - Proxmox.
 - Nextcloud AIO management.
-

Public Application Onboarding Checklist

Before exposing a new application through the VPS, confirm:

- The application works directly on its private backend.
 - The application VM has a reserved IP.
 - The Proxmox firewall allows Traefik to reach the backend.
 - The public WHC record points to `38.29.213.101`.
 - Pi-hole points the hostname to `192.168.2.182`.
 - A Traefik route exists.
 - The Traefik backend uses the correct current IP.
 - A valid HTTPS certificate is issued.
 - Authentik is configured if the application requires SSO.
 - The application does not expose an administrative backend unintentionally.
 - Uptime Kuma monitors the routed service.
 - The VM is covered by the Proxmox backup job.
-

Service Validation

Confirm the VPS Public Address

Verify that public DNS resolves application hostnames to:

- `38.29.213.101`

Confirm the WireGuard Tunnel

Use:

```
sudo wg show
```

Expected:

- Recent handshake.
- Increasing transfer counters.

Confirm Public Port 443

Use:

```
ss -lntp
```

Confirm that the intended ingress service or forwarding mechanism is listening on TCP port 443.

Confirm Routing to the Home Network

Test the intended WireGuard peer or private tunnel address.

A successful tunnel ping confirms network reachability but not application-level routing.

Confirm an Application Through the VPS

From an external connection, open a public application such as:

[Open Authentik](#)

The request should reach Authentik without exposing the private backend port.

External Testing

External testing must use a network outside the home LAN.

Suitable test methods include:

- A phone with Wi-Fi disabled.
- A laptop connected through a mobile hotspot.
- A remote trusted network.
- A public external monitoring service.

Testing from the home LAN may use Pi-hole split DNS and therefore bypass the VPS.

To validate public ingress, confirm the client resolves the hostname to `38.29.213.101`.

Monitoring

Recommended Uptime Kuma monitors include:

Monitor	Target
VPS host	Public VPS address
Public HTTPS	TCP 443 on the VPS
WireGuard peer	Home tunnel peer
Authentik external route	<code>portal.bytek.ca</code>
Nextcloud external route	<code>cloud.bytek.ca</code>
BookStack external route	<code>docs.bytek.ca</code>
Vikunja external route	<code>projects.bytek.ca</code>

Monitoring should distinguish:

- VPS host availability.
- Public port availability.
- WireGuard tunnel availability.
- Traefik routing.
- Application health.

A successful ping does not prove HTTPS or WireGuard forwarding is functioning.

Logging

Review logs for:

- SSH authentication failures.
- Firewall drops.
- WireGuard handshake loss.
- Forwarding failures.

- Unexpected public-port listeners.
- Repeated scans or brute-force attempts.
- Kernel networking errors.

Useful sources may include:

- System journal.
- SSH journal.
- Firewall logs.
- WireGuard status.
- Reverse-proxy or forwarding logs, depending on the VPS design.

Do not copy active tokens, private keys, or full authentication headers into BookStack.

Failure Impact

If the VPS is unavailable:

- External access to hosted applications fails.
- Internal LAN access should continue through Pi-hole and Traefik.
- Proxmox remains available internally.
- Nextcloud AIO management remains available internally.
- Pi-hole remains available internally.
- Authentik may remain available internally.
- Existing local application sessions may continue.

The VPS is therefore critical for external access but not for normal LAN access.

Common Failure Scenarios

Public DNS Resolves Incorrectly

Symptoms:

- External clients connect to the wrong host.
- Certificate issuance fails.
- Application is unreachable externally.

Check:

- WHC A record.
- Public resolver results.
- Record TTL.
- Accidental AAAA record.

WireGuard Handshake Is Missing

Symptoms:

- VPS is reachable.
- Public TCP 443 may be open.
- Home applications are unavailable through the VPS.

Check:

- Home internet connection.
- Home WireGuard gateway.
- Peer keys.
- Endpoint.
- Allowed IPs.
- UDP firewall rules.
- Persistent keepalive.

Tunnel Works but Application Fails

Symptoms:

- WireGuard handshake exists.
- Traffic counters increase.
- Public hostname returns timeout or gateway error.

Check:

- Forwarding rules.
- NAT rules.
- Traefik IP address.
- Traefik firewall.
- Application backend.
- Hostname routing.
- Certificate state.

Internal Access Works but External Access Fails

This usually indicates a problem with:

- WHC public DNS.
- VPS.
- WireGuard.
- Home gateway forwarding.
- Public firewalling.

Internal split DNS bypasses those components.

External Access Works but Internal Access Fails

This usually indicates a problem with:

- Pi-hole.
- Split-DNS records.
- Client DNS settings.
- Browser DNS over HTTPS.
- LAN firewall rules.

Recovery Procedure

If all public applications become unavailable:

1. Confirm the VPS is running through the hosting-provider console.
2. Confirm the public IP is still `38.29.213.101`.
3. Confirm SSH access.
4. Confirm the WireGuard interface.
5. Confirm the latest home-peer handshake.
6. Confirm transfer counters.
7. Confirm IP forwarding and firewall rules.
8. Confirm TCP 443 is listening.
9. Confirm the home WireGuard gateway is running.
10. Confirm Traefik is running.
11. Test one application directly from Traefik.
12. Test the public hostname from an external network.
13. Review logs before changing configuration.

If SSH is unavailable:

1. Use the VPS provider console.
 2. Verify the SSH service.
 3. Verify the VPS firewall.
 4. Verify disk space.
 5. Verify the network interface.
 6. Restore SSH configuration from a known-good backup if required.
-

Backup and Recovery Data

Preserve the following VPS information:

- WireGuard configuration.
- WireGuard public and private keys.
- Firewall rules.
- SSH configuration.
- Authorized SSH keys.
- Network forwarding rules.
- NAT rules.
- Service configuration.

- Provider account and console access.
- Public IP information.
- Recovery procedure.

Private keys must remain in a password manager or encrypted backup.

BookStack should record the location of secrets, not the secret values.

Security Review Checklist

- Only approved public ports are open.
- SSH password authentication is disabled.
- SSH private keys are protected.
- Root SSH behavior matches the hardening policy.
- WireGuard keys are unique.
- WireGuard Allowed IPs are narrow.
- Public TCP 443 reaches only the intended ingress path.
- Proxmox TCP 8006 is not exposed.
- Application backend ports are not exposed.
- The Docker API is not exposed.
- Firewall and authentication logs are reviewed.
- Provider console access works.
- Recovery credentials are stored securely.

Document Control

- **Owner:** Bryan Gagne-Plante
- **Public address:** 38.29.213.101
- **Primary role:** Public HTTPS ingress
- **Home transport:** WireGuard
- **Public DNS provider:** WHC cPanel
- **Last verified:** YYYY-MM-DD
- **Last external-access test:** YYYY-MM-DD
- **Last WireGuard recovery test:** YYYY-MM-DD

- **SSH recovery tested:** Yes / No
 - **Known limitations:** External application access depends on one VPS and one WireGuard tunnel
-

Revision #2

Created 2026-08-17 14:49:54 UTC by Bryan Gagne-Plante

Updated 2026-08-17 15:31:47 UTC by Bryan Gagne-Plante