

Studio PiKVM

This document details the network architecture, perimeter/host firewall projections, Authentik Single Sign-On (SSO) integration, mutual TLS (mTLS), Nginx reverse proxy configuration for the Studio PiKVM device, and the complete technical specification for the **Studio Control Gateway** (`scontrol.drheck.dev`).

1. Network & DNS Architecture

Clean separation between administrative direct terminal access and Authentik-gated browser access is maintained across dedicated DNS records and network flows:

Hostname	Target IPs	Purpose	Protection Mechanism
<code>studio-kvm-ssh.drheck.dev</code>	<code>10.0.0.7</code> <code>fd77:7777:5010:0:e65f:1ff:fee4:8911</code>	Direct hardware & SSH administration	SSH Key Authentication (<code>id_ultra</code> / <code>id_scontrol</code>)
<code>studio-kvm-web.drheck.dev</code>	<code>10.0.0.100</code> <code>fd77:7777:5010:0:1337:f1ac:d00d:aaaa</code>	Authentik-protected browser Web UI	Authentik SSO + ForwardAuth + mTLS
<code>scontrol.drheck.dev</code>	<code>10.0.0.100</code> <code>fd77:7777:5010:0:1337:f1ac:d00d:aaaa</code>	Studio One-Touch Orchestration Gateway	Authentik SSO ForwardAuth (Group <code>studio</code>)
<code>bmo95.drheck.dev</code>	<code>10.0.0.6</code> <code>fd77:7777:5010:0:a236:9fff:fe29:bc72</code>	Studio Recording PC	Subnet Isolation & SSH Key Auth

2. Security Projections & Layered Defense

Layer 1: Outbound Gateway Isolation on Host `ul` (`nftables`)

Unprivileged SSH users logged into host `u1` are blocked by the kernel from directly connecting to PiKVM web ports (TCP 80/443) or Studio Control backend (TCP 8000). Only Nginx worker processes (`http`, UID 33), rootless Podman containers (`docker-data`, UID 1100, so `scontrol` can query the PiKVM ATX API), and administrative users (`root`, UID 0; `akadmin`, UID 1101) are permitted outbound connections:

Rules in `/etc/nftables.conf` (`chain output`):

```
# Studio PiKVM (Direct KVM Access Protection – permits root 0, nginx 33, docker-data 1100,
akadmin 1101)
ip daddr 10.0.0.7 tcp dport { 80, 443 } meta skuid != { 0, 33, 1100, 1101 } reject with tcp
reset comment "Block direct local access to Studio PiKVM IPv4"
ip6 daddr fd77:7777:5010:0:e65f:1ff:fee4:8911 tcp dport { 80, 443 } meta skuid != { 0, 33,
1100, 1101 } reject with icmpx admin-prohibited comment "Block direct local access to Studio
PiKVM IPv6"

# Studio Control Gateway Isolation
ip6 daddr fd77:7777:5010:0:1337:flac:d00d:5c01 tcp dport 8000 meta skuid != { 0, 33, 1101 }
reject with icmpx admin-prohibited comment "Block direct access to Studio Control backend"
```

Layer 2: Pre-Shared Proxy Secret Header (X-Proxy-Secret)

- A high-entropy pre-shared token is stored in `/etc/nginx/certs/studio_secret.conf` (mode `0600`, owned by `http:http`).
- Nginx injects this header alongside `X-KVMD-User: $authentik_username` when proxying upstream requests to PiKVM.

Layer 3: Mutual TLS (mTLS) Client Certificate

- Dedicated internal CA certificate: `/etc/nginx/certs/pikvm_ca.crt`
- Nginx client certificate: `/etc/nginx/certs/pikvm_client.crt`
- Nginx client private key: `/etc/nginx/certs/pikvm_client.key` (mode `0600`, owned by `http:http`)
- Nginx presents this client certificate to PiKVM during TLS handshake (`proxy_ssl_certificate`).

Layer 4: Inbound Host Firewall on PiKVM (`studio-kvm-ssh`)

On PiKVM itself, firewall rules reject all incoming HTTP/HTTPS connections unless sourced from host `ul`:

```
iptables -A INPUT -p tcp -m multiport --dports 80,443 -s 10.0.0.100 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 -j DROP

ip6tables -A INPUT -p tcp -m multiport --dports 80,443 -s fd77:7777:5010:0:1337:f1ac:d00d:aaaa -j ACCEPT
ip6tables -A INPUT -p tcp -m multiport --dports 80,443 -j DROP
```

3. Authentik SSO Configuration

- **Applications:**

- **Studio PiKVM (`studio-kvm-web`):** URL `https://studio-kvm-web.drheck.dev/` (with secondary alias `scontrol.drheck.dev` redirecting cleanly via `301` to `https://scontrol.drheck.dev/`)
- **Studio Control (`scontrol`):** URL `https://scontrol.drheck.dev/`

- **Proxy Provider:** ForwardAuth Single Mode with `cookie_domain='drheck.dev'` and explicit callback redirect URIs.
- **Authorization Flow:** `default-provider-authorization-implicit-consent` (transparent single-click launch).
- **Access Control:** Bound to Authentik Group `studio` (members: `luke`, `ikura`) via `PolicyBinding`. Non-members receive access denied.

4. Studio Control Gateway (`scontrol.drheck.dev`)

4.1 Architecture & Implementation

- **Git Repository:** `/home/luke/git/scontrol` (tracked with `.gitignore`, `build.sh`, and `Dockerfile`).
- **Deployment Location:** `/data/docker/scontrol` (`scontrol.container` and `scontrol.network`, symlinked into `/home/docker-data/.config/containers/systemd/` under rootless Podman `docker-data`, UID 1100).
- **Network Binding:** Dedicated ULA IPv6 address `[fd77:7777:5010:0:1337:f1ac:d00d:5c01]:8000`.
- **Dedicated Service Key:** `/data/docker/scontrol/id_scontrol` (ed25519 key registered in `luke@studio-kvm-ssh.drheck.dev:~/.ssh/authorized_keys`).

4.2 Building & Restarting

```
# Build image in rootless Podman store and restart Quadlet service
(cd /data/docker/scontrol && sudo -u docker-data HOME=/home/docker-data
XDG_RUNTIME_DIR=/run/user/1100 podman build -t localhost/scontrol:latest
/data/docker/scontrol)
sudo systemctl --user -M docker-data@ restart scontrol.service
```

4.3 Orchestration Execution Pipeline (`/api/stream/on`)

1. **RF Power Outlets (YARD Stick One on PiKVM):**
 - Connects to `studio-kvm-ssh.drheck.dev` via SSH using `id_scontrol`.
 - Runs `sudo /home/luke/git/studio_yardstick/bin/studio-power all on` to power Moroccan Lamp (`mrc`), Recording Rack (`rack`), Studio Computer (`computer`), Subwoofer (`sub`), Main PA Speakers (`pa`), TV Monitor (`tv`), and Neewer LED Lights (`neewer`).
2. **Motherboard ATX Power Ignition:**
 - Queries PiKVM ATX state via `GET https://studio-kvm-ssh.drheck.dev/api/atx`.
 - If power rail is off, triggers `POST https://studio-kvm-ssh.drheck.dev/api/atx/click?button=power` and polls for rail confirmation.
3. **Studio Computer Boot Verification (`bmo95.drheck.dev`):**
 - Probes DNS hostname `bmo95.drheck.dev` with a 100-second boot timeout.
4. **Soundcards & Audio Readiness:**
 - Audits 4x Echo AudioFire 12 interfaces (`hw:AudioFire12,0` through `hw:AudioFire12_3,0`) and Emagic Uinitor8 USB MIDI interface.
 - Confirms `jackd`, `zita-a2j`, `zita-j2a`, `a2jmidid`, and `ardour.service` DAW readiness.

4.4 Strict Error Gating & Real-Time SSE Console

- If any step fails, the sequence immediately aborts and transitions the UI to `ERROR / FAILED`.
- Real-time progress is streamed live via Server-Sent Events (`/api/stream/on` and `/api/stream/off`).
- Monospace console displays colored tags for `[RF]`, `[ATX]`, `[HOST]`, `[AUDIO]`, `[SYSTEM]`, and `[ERROR]`.
- Secondary actions allow querying live hardware state (`Refresh Status`) and one-touch shutdown (`Power Off All`).

Revision #2

Created 2026-08-25 02:21:09 UTC by admin

Updated 2026-10-20 03:46:24 UTC by luKe