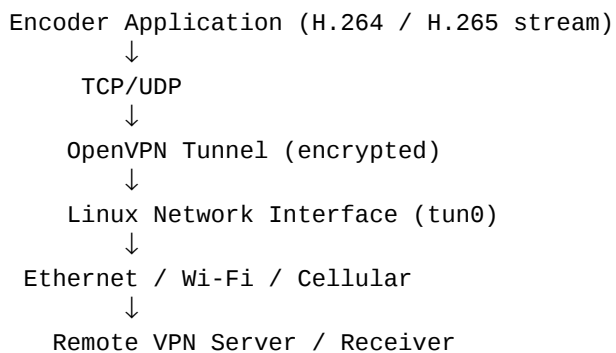


Guide: Hosting OpenVPN on i.MX8 to Secure Encoder Streams

1. Overview

This guide outlines how to host OpenVPN on an i.MX8-based platform to secure video streams from an encoder. The i.MX8 runs a Linux-based operating system, on which OpenVPN operates as a software service.

2. System Architecture



3. Requirements

Hardware: i.MX8 platform with network interface (Ethernet/Wi-Fi/Cellular).

Software: Embedded Linux OS, OpenVPN, OpenSSL/mbedTLS, and TUN/TAP support.

4. Installation & Setup

Enable TUN/TAP:

```
ls /dev/net/tun
```

Install OpenVPN (example):

```
apt install openvpn
```

Run OpenVPN:

```
openvpn --config /etc/openvpn/client.ovpn
```

5. Operating Modes

Client mode is recommended for most deployments. Server mode is less common and more resource intensive.

6. Routing Video Streams

Option 1: Full tunnel (all traffic via VPN).

Option 2: Selective routing (recommended for performance).

7. Performance Considerations

OpenVPN is CPU-based and may impact performance depending on bitrate, CPU capability, and encryption method.

8. Reliability

Implement auto-start, auto-reconnect, watchdog monitoring, and secure certificate storage.

9. Security

Use certificate-based authentication, protect keys, and restrict VPN access.

10. Alternatives

WireGuard (faster), IPsec (hardware acceleration), OpenVPN (most compatible).

11. Summary

OpenVPN runs on Linux on the i.MX8 and secures encoder traffic via encrypted tunnels.