Network Architecture Design Document

Version: 2.0
Date: 2026-01-06
Status: PENDING APPROVAL
Author: Infrastructure Automation

Open Items

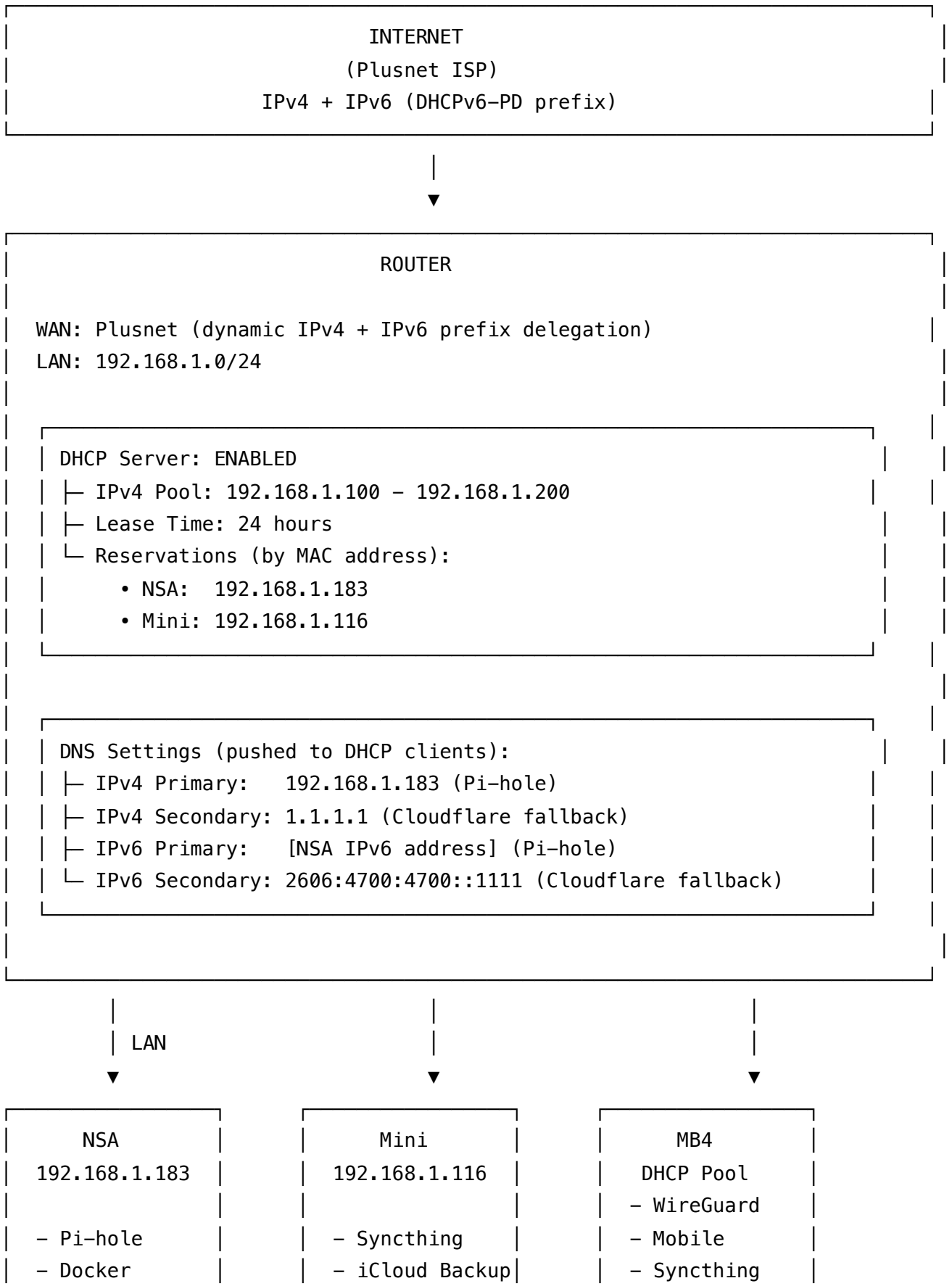
- [ ] Obtain NSA IPv6 address (check router DHCPv6-PD prefix, then run `ip -6 addr` on NSA or assign static)
- [ ] Update IPv6 placeholders at sections 2, 3.1, and 9
- [ ] Complete implementation checklist (section 9)
- [ ] Obtain approval signatures (section 10)

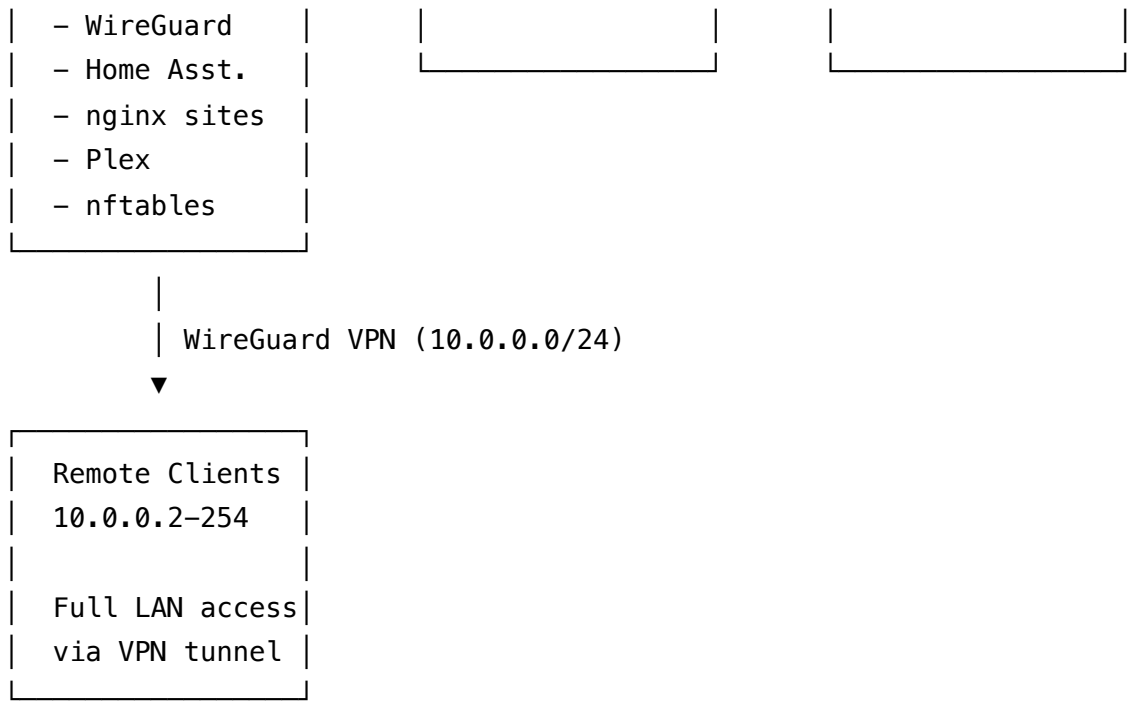
1. Executive Summary

This document defines the network architecture for the home infrastructure, covering DNS resolution, DHCP assignment, firewall rules, and service discovery. The design prioritises:

- **Reliability**: Router handles DHCP with fallback DNS
- **Security**: All DNS routed through Pi-hole with ad-blocking
- **Visibility**: Complete DNS query logging
- **Simplicity**: Single DNS server, clear separation of concerns

2. Network Topology





3. Component Specifications

3.1 Router Configuration

Setting	Value	Notes
DHCP Server	Enabled	Primary IP assignment for all LAN devices
DHCP Pool	192.168.1.100 - 200	~100 addresses for dynamic clients
Lease Time	24 hours	Standard for home network

DHCP Reservations

Device	MAC Address	Type	Reserved IP
NSA	7c:83:34:b2:c1:33	Eth	192.168.1.183
Mini	14:98:77:78:d6:46	Wifi	192.168.1.116

DNS Settings (Pushed via DHCP)

Setting	Value	Purpose
IPv4 Primary	192.168.1.183	Pi-hole (ad-blocking DNS)
IPv4 Secondary	1.1.1.1	Fallback if NSA offline
IPv6 Primary	[NSA IPv6]	Pi-hole IPv6
IPv6 Secondary	2606:4700:4700::1111	Cloudflare IPv6 fallback

Note: Secondary DNS provides resilience but may bypass ad-blocking when NSA is unavailable.

3.2 NSA Server (192.168.1.183)

3.2.1 Pi-hole (Docker Container)

Setting	Value
Container Name	pihole
Image	pihole/pihole:latest
DNS Port	53 (TCP/UDP)
Web UI Port	8080
DHCP	Disabled (router handles)
Upstream DNS	1.1.1.1, 8.8.8.8

Local DNS Records (custom.list):

```
# NSA Services
192.168.1.183 nsa
192.168.1.183 ha
192.168.1.183 pihole
192.168.1.183 plex
192.168.1.183 laya
192.168.1.183 hopo
192.168.1.183 etc

# Other Hosts
192.168.1.116 mini
```

3.2.2 Existing dnsmasq

Setting	Value
Status	DISABLED
Action	Stop and disable service
Reason	Replaced by Pi-hole (includes FTLDNS)

```
# Commands to disable
sudo systemctl stop dnsmasq
sudo systemctl disable dnsmasq
```

3.2.3 Avahi (mDNS)

Setting	Value
Status	ENABLED
Purpose	mDNS responder for .local domains

Provides (NSA only):

Service	Type	Description
`nsa.local`	Hostname	Primary hostname resolution
`_ssh._tcp`	DNS-SD	SSH service discovery

Service	Type	Description
`_http._tcp`	DNS-SD	HTTP services (nginx, Pi-hole UI, Home Assistant)

Note: Each host runs its own Avahi daemon. Mini advertises `mini.local` via its own Avahi instance. mDNS is LAN-only (multicast doesn't traverse routers) - VPN clients must use Pi-hole DNS names (`nsa` , `ha` , `mini`) instead of `.local` domains.

Avahi handles `.local` domain resolution via multicast DNS. This complements Pi-hole which handles unicast DNS.

3.2.4 nftables (Firewall)

DNS Enforcement Rule (Redirect):

All DNS traffic is redirected to Pi-hole, regardless of the destination the client requested. This ensures:

- Smart TVs with hardcoded DNS still use Pi-hole
- Complete visibility of all DNS queries
- Full ad-blocking coverage

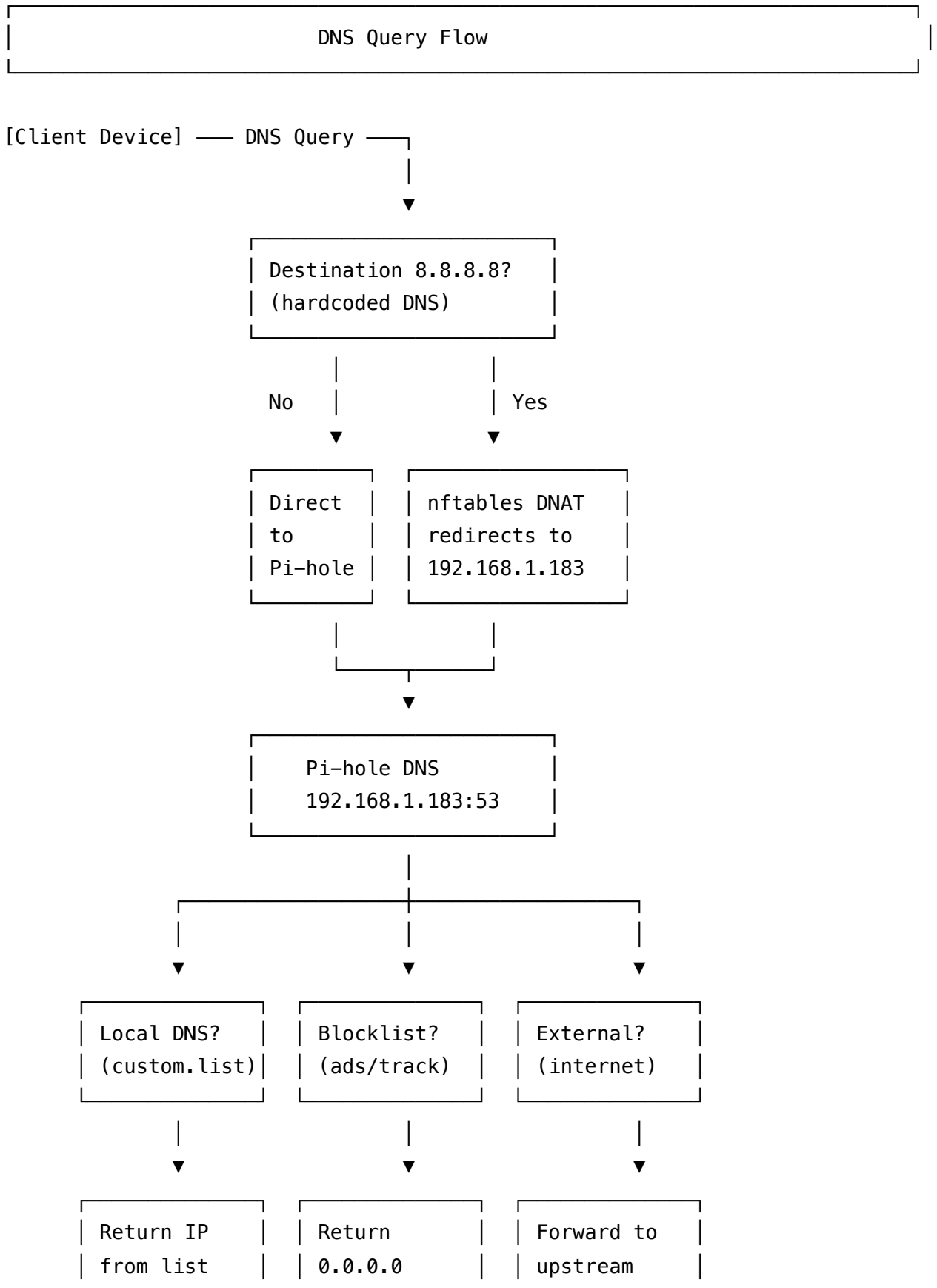
```
table ip nat {
    chain PREROUTING {
        type nat hook prerouting priority dstnat

        # Redirect all DNS to Pi-hole (except from Pi-hole itself)
        ip saddr != 192.168.1.183 udp dport 53 dnat to 192.168.1.183:53
        ip saddr != 192.168.1.183 tcp dport 53 dnat to 192.168.1.183:53
    }
}
```

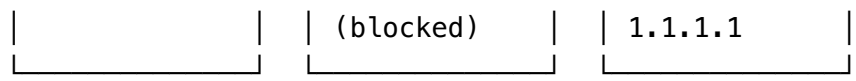
Firewall Rules Summary:

Port	Protocol	Source	Service
22	TCP	LAN, VPN	SSH
53	TCP/UDP	LAN, VPN	DNS (Pi-hole)
80	TCP	LAN, VPN	HTTP (nginx)
1883	TCP	LAN, VPN	MQTT (Mosquitto)

Port	Protocol	Source	Service
8080	TCP	LAN, VPN	Pi-hole Admin
8123	TCP	LAN, VPN	Home Assistant
9090	TCP	LAN, VPN	Cockpit
32400	TCP	LAN, VPN	Plex
51820	UDP	Any	WireGuard VPN

4. DNS Resolution Flow





5. Service Discovery Methods

Method	Domain Format	Handled By	Accessible From
Pi-hole DNS	`nsa` , `mini` , `ha`	Pi-hole custom.list	LAN, VPN
mDNS/Avahi	`nsa.local` , `mini.local`	Avahi daemon	LAN only
FQDN	`nsa.home.arpa`	Pi-hole (optional)	LAN, VPN

6. IPv6 Configuration

Router

- Receives /56 or /64 prefix from Plusnet via DHCPv6-PD
- Advertises prefix to LAN via Router Advertisement (RA)
- Advertises Pi-hole IPv6 address as DNS server

NSA/Pi-hole

- Static IPv6 address within delegated prefix
- Pi-hole listens on both IPv4 and IPv6
- Same filtering rules apply to both

Fallback

- IPv6 secondary DNS: 2606:4700:4700::1111 (Cloudflare)
- Ensures connectivity if NSA temporarily unavailable

7. WireGuard VPN Integration

VPN clients receive full LAN access including DNS:

Setting	Value
VPN Subnet	10.0.0.0/24
DNS Server	192.168.1.183 (Pi-hole)
Allowed IPs	0.0.0.0/0 (full tunnel)

VPN clients can resolve:

- Local hostnames (`nsa` , `mini` , `ha`)
- Internet hostnames (via Pi-hole upstream)
- Ad-blocking applies to VPN traffic

8. Failure Scenarios

Scenario	Impact	Mitigation
NSA offline	Primary DNS unavailable	Secondary DNS (1.1.1.1) takes over
Pi-hole container crash	DNS fails	Docker restart policy: unless-stopped
Router offline	No DHCP, no connectivity	N/A (single point of failure)
Internet outage	External DNS fails	Local DNS still works

9. Implementation Checklist

Router Configuration

- ☐ Create DHCP reservation for NSA (192.168.1.183)
- ☐ Create DHCP reservation for Mini (192.168.1.116)
- ☐ Set IPv4 Primary DNS: 192.168.1.183

- [ ] Set IPv4 Secondary DNS: 1.1.1.1
- [ ] Set IPv6 Primary DNS: [NSA IPv6 address]
- [ ] Set IPv6 Secondary DNS: 2606:4700:4700::1111

NSA Server

- [ ] Stop and disable dnsmasq service
- [ ] Deploy Pi-hole Docker container
- [ ] Configure Pi-hole custom.list with local DNS entries
- [ ] Configure Pi-hole upstream DNS (1.1.1.1, 8.8.8.8)
- [ ] Update nftables with DNS redirect rule
- [ ] Verify Avahi is running for mDNS
- [ ] Assign static IPv6 address to NSA

Testing

- [ ] Verify DNS resolution from LAN client
- [ ] Verify DNS resolution from VPN client
- [ ] Verify ad-blocking is working
- [ ] Test hardcoded DNS redirect (use nslookup to 8.8.8.8)
- [ ] Test failover to secondary DNS (stop Pi-hole temporarily)

10. Approval

Role	Name	Date	Signature
Network Owner			
Reviewer			

Document Control:

- Location: `/infrastructure/docs/network-design.md`
- Related: `README.md`, `nsa.yml`, `files/nsa/nftables.conf`