



Network Zone Plan

One firewall, several zones, one sheet · belongs with Chapter 4 · Firewall: _____ · Date: _____

Separate instead of hope. An unchanged home network is a flat surface: whatever the smart TV or the cheap IoT gadget catches reaches your computer. Zones (VLANs) on a dedicated firewall separate that. This sheet records which zone is for what, what lives in it, where it may go and how it reaches the internet. It names no menu paths, because interfaces age but the rules stay. Fill in the plan once and you will know later why a device sits where it does.

1 · MY ZONES

Zone	VLAN ID / subnet	Purpose	Devices (what lives here)	Internet via (VPN tunnel / clearnet / no internet)	DNS (VPN DNS / NextDNS / filter)	reaches which zones
Management		Router and switch configuration only, unreachable from any other zone				
Private + VPN		Computer, smartphone. All traffic forced through the VPN tunnel, VPN DNS				
Clearnet		Banking, streaming services that block VPNs. NextDNS				
Guest		Visitors, no access to internal networks				
IoT		Smart home, heavily restricted internet access, no access to other zones				

2 · WHO MAY TALK TO WHOM

Row = from, column = to. Everything is blocked by default, and only what has a cross here is allowed by a firewall rule. The crosses already entered are the book's suggestion. Your own zones and exceptions go in with a pen.

from ↓ / to →	Management	Private + VPN	Clearnet	Guest	IoT	Internet
Management		X	X	X	X	
Private + VPN						X only via VPN tunnel
Clearnet						X
Guest						X
IoT						restricted

3 · KILL SWITCH AT THE FIREWALL LEVEL: THE CHECK

Item	OK	Note
All traffic of the VPN zone is bound to the VPN gateway, not to the firewall's default gateway. The rule points to the single VPN gateway, not to a gateway group.		
The pass rule lapses when the VPN gateway is dead (in OPNsense currently the global firewall setting "Skip rules when gateway is down"). Without this option the firewall silently routes the traffic to the default gateway, that is, into the clearnet.		
A downstream block rule shuts off all outbound traffic of the VPN zone. It takes effect as soon as the pass rule has lapsed.		
Tested: VPN tunnel deliberately disconnected. Nothing leaves the VPN zone any more, no DNS reply, no IP exposure, no silent redirect into the clearnet.		Tested on: _____

4 · DNS PER ZONE

Item	OK	Note
The VPN zone uses exclusively the VPN provider's DNS servers. No personalized DNS profile through the tunnel: the profile is tied to your account, and its response pattern makes you identifiable (DNS fingerprint paradox).		
The clearnet zone uses the encrypted filter resolver (NextDNS). Your home IP makes you identifiable there anyway, so the profile reveals nothing new.		
The firewall's resolver speaks DNS over TLS with the upstream. The server verification field (Verify CN, the resolver's hostname) is never empty, otherwise a man-in-the-middle attack on DNS remains possible.		Upstream resolver: _____

Hardware criteria: Hardware-accelerated encryption (AES-NI for OpenVPN and IPsec, for WireGuard a modern processor with SIMD instructions), otherwise speed drops drastically with the VPN active. Several physical network ports for clean zones. Fanless for silent continuous operation. On top of that an open-source firewall system (the book recommends OPNsense). No consumer firmware.

⚠ A VPN without a kill switch at the network level protects less than assumed. Connection drops happen, and at that very moment the unprotected IP is visible. ⚠ What gets compromised in the IoT zone must never reach the VPN zone. The matrix above is the rule, not the exception. ⚠ No passwords, Wi-Fi keys or VPN keys on this sheet. VLAN IDs and subnets are no secret, but credentials are.