



Netzwerk-Zonenplan

Eine Firewall, mehrere Zonen, ein Blatt · gehört zu Kapitel 4 · Firewall: _____ · Stand: _____

Trennen statt hoffen. Ein unverändertes Heimnetz ist eine flache Fläche: Was der Smart-TV oder das billige IoT-Gerät einfängt, erreicht den Rechner. Zonen (VLANs) auf einer eigenen Firewall trennen das. Dieses Blatt hält fest, welche Zone wofür da ist, was darin hängt, wohin sie darf und wie sie ins Internet geht. Es nennt keine Menüpfade, denn Oberflächen altern, aber die Regeln bleiben. Wer den Plan einmal ausfüllt, weiß später, warum ein Gerät wo hängt.

1 · MEINE ZONEN

Zone	VLAN-ID / Subnetz	Zweck	Geräte (was hängt hier)	Internet über (VPN-Tunnel / Clearnet / kein Internet)	DNS (VPN-DNS / NextDNS / Filter)	erreicht welche Zonen
Management		Nur Router- und Switch-Konfiguration, von keiner anderen Zone erreichbar				
Privat + VPN		Rechner, Smartphone. Gesamter Verkehr zwingend durch den VPN-Tunnel, VPN-DNS				
Clearnet		Banking, Streaming-Dienste, die VPN blockieren. NextDNS				
Gast		Besucher, kein Zugriff auf interne Netze				
IoT		Smart-Home, stark eingeschränkter Internetzugang, kein Zugriff auf andere Zonen				

2 · WER DARF ZU WEM

Zeile = von, Spalte = nach. Standard ist blockiert, nur was hier ein Kreuz hat, wird per Firewall-Regel erlaubt. Die eingetragenen Kreuze sind der Vorschlag aus dem Buch, eigene Zonen und Ausnahmen trägst du mit Stift ein.

von ↓ / nach →	Management	Privat + VPN	Clearnet	Gast	IoT	Internet
Management		X	X	X	X	
Privat + VPN						X nur über VPN-Tunnel
Clearnet						X
Gast						X
IoT						eingeschränkt

3 · KILL-SWITCH AUF FIREWALL-EBENE: DIE KONTROLLE

Punkt	OK	Notiz
Der gesamte Verkehr der VPN-Zone ist an das VPN-Gateway gebunden, nicht an das Standard-Gateway der Firewall. Die Regel zeigt auf das einzelne VPN-Gateway, nicht auf eine Gateway-Gruppe.		
Die Durchlass-Regel verfällt, wenn das VPN-Gateway tot ist (in OPNsense derzeit die globale Firewall-Einstellung „Skip rules when gateway is down“). Ohne diese Option leitet die Firewall den Verkehr stillschweigend ans Standard-Gateway, also ins Clearnet.		
Eine nachgelagerte Block-Regel sperrt den gesamten ausgehenden Verkehr der VPN-Zone. Sie greift, sobald die Durchlass-Regel weggefallen ist.		
Getestet: VPN-Tunnel absichtlich getrennt. Aus der VPN-Zone geht nichts mehr raus, keine DNS-Antwort, keine IP-Exposition, keine stille Umleitung ins Clearnet.		Test am: _____

4 · DNS JE ZONE

Punkt	OK	Notiz
Die VPN-Zone nutzt ausschließlich die DNS-Server des VPN-Anbieters. Kein personalisiertes DNS-Profil durch den Tunnel: Das Profil ist mit deinem Konto verknüpft, sein Antwortmuster macht dich identifizierbar (Fingerprint-Paradoxon).		
Die Clearnet-Zone nutzt den verschlüsselten Filter-Resolver (NextDNS). Über die Heim-IP bist du dort ohnehin identifizierbar, das Profil verrät nichts Neues.		
Der Resolver der Firewall spricht DNS over TLS mit dem Upstream. Das Feld für die Server-Verifikation (Hostname des Resolvers) ist nie leer, sonst bleibt ein Man-in-the-Middle-Angriff auf DNS möglich.		Upstream-Resolver: _____

Hardware-Kriterien: Hardware-beschleunigte Verschlüsselung (AES-NI für OpenVPN und IPsec, für WireGuard ein moderner Prozessor mit SIMD-Befehlen), sonst bricht die Geschwindigkeit mit VPN drastisch ein. Mehrere physische Netzwerkports für saubere Zonen. Lüfterlos für den geräuschlosen Dauerbetrieb. Darauf ein quelloffenes Firewall-System, das Buch empfiehlt OPNsense. Keine Consumer-Firmware.

⚠ Ein VPN ohne Kill-Switch auf Netzwerkebene schützt weniger als angenommen. Verbindungsabbrüche passieren, und genau dann ist die ungeschützte IP sichtbar. ⚠ Was in der IoT-Zone kompromittiert wird, darf die VPN-Zone nie erreichen. Die Matrix oben ist die Regel, nicht die Ausnahme. ⚠ Keine Passwörter, WLAN-Schlüssel oder VPN-Schlüssel auf dieses Blatt. VLAN-IDs und Subnetze sind kein Geheimnis, Zugangsdaten schon.