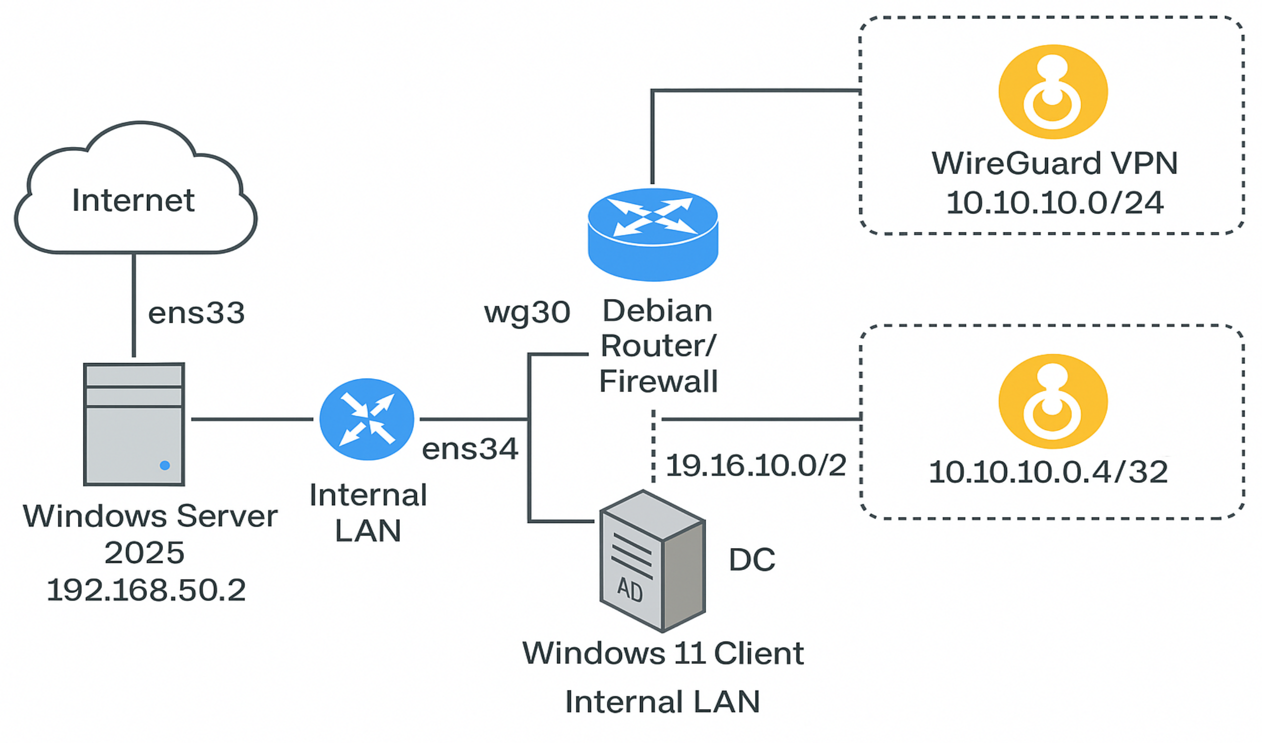
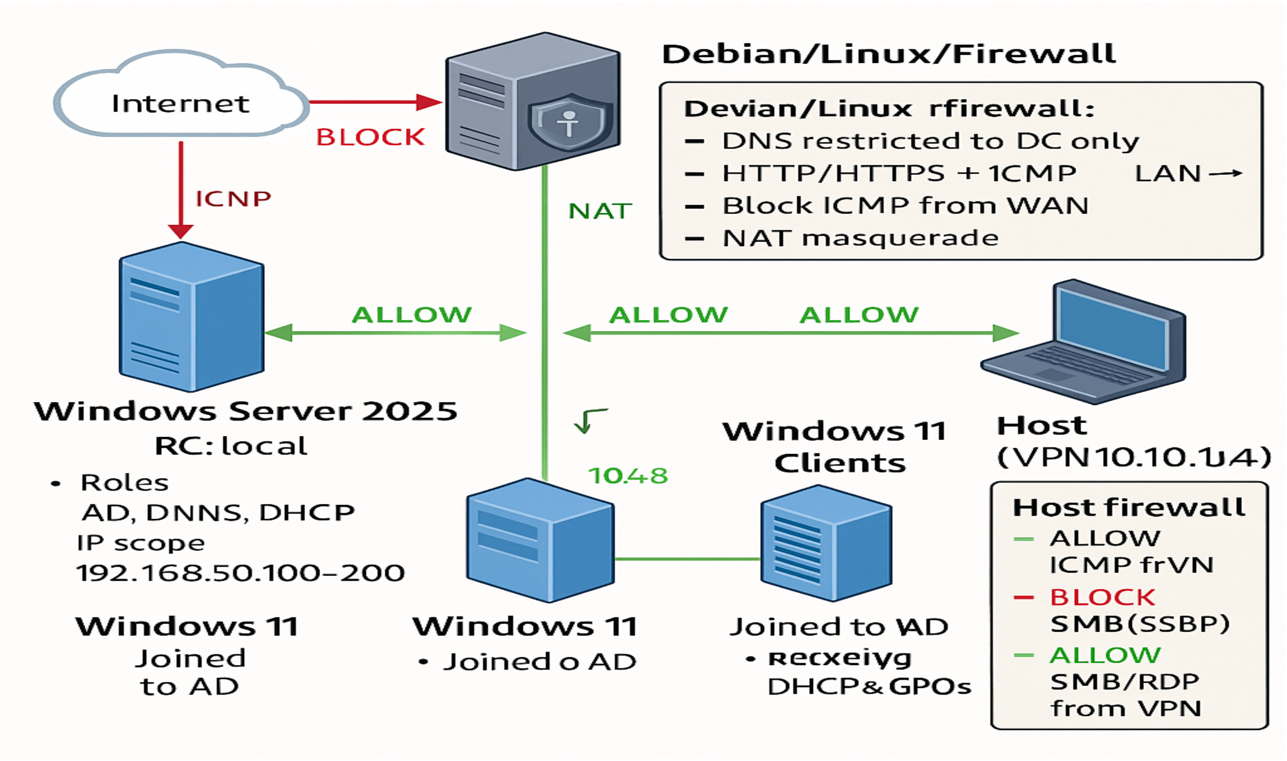
Corporate Lab – Security Map & Topology

This document summarizes the lab’s topology and layered security (Debian nftables + Windows Host Firewall).

Technical Topology



Visual Topology


Internet
BLOCK
ICNP
Debian/Linux/Firewall
Devian/Linux rfirewall:
– DNS restricted to DC only
– HTTP/HTTPS + 1CMP LAN →
– Block ICMP from WAN
– NAT masquerade
NAT
ALLOW
ALLOW
ALLOW
Windows Server 2025
RC: local
• Roles
AD, DNNS, DHCP
IP scope
192.168.50.100–200
10.4.8
Windows 11
Clients
Host
(VPN 10.10.1J4)
Host firewall
– ALLOW
ICMP frVN
– BLOCK
SMB(SSBP)
– ALLOW
SMB/RDP
from VPN
Windows 11
Joined
to AD
Windows 11
• Joined o AD
Joined to AD
• Recxeiyg
DHCP & GPOs

Security Map (Rules Overview)

ICMP: Allowed LAN↔LAN and VPN↔VPN; blocked from Internet→LAN.
DNS: Only DC (192.168.50.2) may query external DNS via Debian; clients use DC DNS.
HTTP/HTTPS: Allowed from LAN to Internet for web access.
NAT: Masquerade on Debian (`ens33`) for LAN and VPN outbound traffic.
WireGuard: UDP 51820 allowed; peers: DC (10.10.10.2/32), Win11 (10.10.10.3/32), Host (10.10.10.4/32).
Windows Host Firewall: ICMP allowed only from 10.10.10.0/24; SMB(445)/RDP(3389)/SSH(22, optional) allowed from VPN only.

Defense in Depth

Layer 1 (Debian): perimeter enforcement with nftables, NAT, and VPN termination. Layer 2 (Windows Host): endpoint firewall restricting management services to VPN-only. Together they implement corporate-grade segmentation and least privilege.