WireGuard VPN Configuration Guide
AWS EC2 ↔ OPNsense ↔ Home Lab

Architecture

Internet → AWS EC2 (Ubuntu) → WireGuard Tunnel → OPNsense → LAN (192.168.1.0/24).

Prerequisites

AWS EC2 Ubuntu, OPNsense with WireGuard plugin, UDP 51820 allowed, LAN subnet 192.168.1.0/24.

OPNsense Configuration

Create WireGuard instance, create peer, assign wg1 to interface AWS_Email, enable interface, IPv4 type None.

Ubuntu Configuration

Install WireGuard, create wg0.conf, assign 10.20.20.2/24, configure endpoint and AllowedIPs, start wg-quick.

Firewall

Create Pass rule on AWS_Email interface: IPv4, Any protocol, Source Any, Destination Any, Direction In, then Apply Changes.

Verification

Use: wg show, ifconfig wg1, pfctl -sr | grep wg1, tcpdump, ping 10.20.20.1, ping 192.168.1.10.

Troubleshooting

Main issue was missing pass rule on AWS_Email interface. After adding and applying the rule, tunnel traffic passed correctly.

Validation

AWS EC2 successfully pinged OPNsense and DC01 through the VPN.

Next Steps

Configure Postfix SMTP relay, Exchange Receive Connector, monitoring, backups.