Firewall rule:

WAN interface:

| **Priority** | **Action** | **Protocol** | **Source** | **Destination** | **Port(s)** | **Description** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Pass | TCP | any | Web server IP | 80, 443 | Allow HTTP/HTTPS to web server |
| 2 | Block | any | any | any | any | Block all other inbound |

Alright — if you’ve simplified to just:

**LAN** → 192.168.80.0/24 (your internal network with all VMs, including Wazuh, Prometheus, DB, Web, Jenkins, etc.)

**WAN** → connected to the hotspot/internet

No DMZ, no mail server (using Gmail SMTP instead)

Then the firewall rules can be cleaner but still secure.

## ****OPNsense Firewall Rules for This Setup****

### ****WAN Interface Rules****

(These protect you from the outside world)

| **Priority** | **Action** | **Protocol** | **Source** | **Destination** | **Port(s)** | **Description** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Pass | TCP | any | <WebServer\_IP> | 80, 443 | Allow HTTP/HTTPS traffic to your web server from the internet |
| 2 | Block | any | any | any | any | Block everything else inbound |

💡 This ensures **only the web server** is reachable from the internet — no one can directly touch Wazuh, DB, Jenkins, or Prometheus.

### ****LAN Interface Rules****

(Controls outbound traffic from inside your network)

| **Priority** | **Action** | **Protocol** | **Source** | **Destination** | **Port(s)** | **Description** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Pass | TCP | any | any | 53, 80, 443 | Allow LAN devices to browse web and resolve DNS |
| 2 | Pass | TCP | <Internal\_Service\_IP> | <Allowed\_IP> | <Service\_Port> | Allow only specific internal services to talk to each other (e.g., web server → DB) |
| 3 | Pass | TCP | any | smtp.gmail.com | 465, 587 | Allow outbound email via Gmail SMTP |
| 4 | Block | any | any | any | any | Deny all other LAN → WAN traffic by default |

💡 Rule #4 means that unless you **explicitly allow** it, nothing can leave your LAN to the internet — this is very strong security.

### ****Best Practices for Strengthening Security****

**Change the default LAN allow rule** — by default OPNsense allows all LAN → anywhere traffic; replacing it with a whitelist is far safer.

**Segment critical services** — if possible, put Wazuh, DB, Prometheus on different VLANs or virtual networks and control their access.

**Enable Suricata IDS/IPS** on both WAN and LAN to detect suspicious traffic.

**Enable outbound NAT** so your LAN IPs are hidden from the internet.

**Block private networks on WAN** — stops spoofed traffic coming from non-public IPs.

**Use GeoIP filtering** if your site only serves certain regions.

If you want, I can **give you the exact OPNsense click-by-click configuration** so you can set these rules in the GUI without guessing, and I can add diagrams so you see exactly how packets flow and where they get blocked.

Do you want me to prepare that step-by-step config?