**Firewalla**

**Boîtier de sécurité réseau compact avec interface mobile/tablette et fonctionnalités DPI,.**

**Firewalla – Présentation rapide**

| **Caractéristique** | **Détail** |
| --- | --- |
| **Origine** | **🇺🇸 USA (créé par ex-ingénieurs Cisco, Broadcom)** |
| **Format** | **Petit boîtier (type Raspberry Pi amélioré, fanless)** |
| **Fonctionnalités** | **Pare-feu, VPN, IDS, contrôle parental, monitoring, DPI, tunnel SSH** |
| **Interface** | **Application mobile/tablette (iOS/Android), accès web limité** |
| **Cible** | **Particuliers, TPE, bureaux distants, familles** |
| **Pas de cloud imposé** | **Mode local possible (sans dépendance Cloud obligatoire)** |
| **Mode bridge** | **Oui, possible d’intégrer dans un réseau existant sans routage direct** |

**Prix des modèles (juillet 2025 – valeurs courantes)**

| **Modèle** | **CPU/RAM** | **Débit recommandé** | **Prix approx. TTC €** |
| --- | --- | --- | --- |
| **Firewalla Red** | **ARM v7 / 512Mo** | **< 100 Mbps** | **95–115 €** |
| **Firewalla Blue+** | **ARM v8 / 1 Go** | **< 500 Mbps** | **140–160 €** |
| **Firewalla Purple** | **Quad-core / 2 Go** | **1 Gbps filaire / WiFi** | **220–250 €** |
| **Firewalla Gold** | **x86 4C / 4 Go** | **3 Gbps (4 ports RJ45)** | **420–450 €** |

**⚠️ *Ce sont des boîtiers physiques (pas des VM), donc destinés à être branchés en ethernet dans un réseau local.***

**🧩 À quoi ça sert vraiment dans ton cas ?**

| **Besoin** | **Firewalla utile ?** |
| --- | --- |
| **Séparer des flux métier (visio, doc, etc.)** | **✅** |
| **Limiter les connexions sortantes** | **✅** |
| **Identifier des connexions anormales** | **✅ (DPI + alertes)** |
| **Analyser les flux HTTPS** | **⚠️ partiellement (sans MITM complet)** |
| **Gérer des ACL par utilisateur ou device** | **✅** |
| **Superviser discrètement** | **✅ (application mobile configurable)** |
| **Jouer à l'admin réseau avec logs clairs** | **✅ pédagogique** |

**🧠 Conclusion**

* **C’est un peu cher pour un usage personnel, mais extrêmement compact, silencieux, efficace et pédagogique.**
* **L’on peut tout voir sans bruit ni log système visible sur ta VM. Ce n’est pas un IDS local, c’est une sonde silencieuse.**

**Rappel : Exemple d’architecture : Sécurisation d’un serveur Jitsi**

**Internet**

**│**

**[ Firewall ]**

**│**

**├── Port 443 → Reverse proxy (TLS certbot)**

**├── Port 10000/UDP → Jitsi bridge**

**└── Port 9090+ → Prometheus / Grafana / Exporters**

**↓**

**[Serveur Ubuntu / Jitsi]**

**À insérer :**

* **pfSense = firewall + NAT + reverse proxy**
* **Raspberry Pi = monitoring en VLAN isolé**
* **Firewalla = surveillance passive simple (mode bridge ou nat)**

**Conseil pédagogique**

**Puisque tu veux valider un titre RNCP niveau licence avec option cybersécurité, voici un projet valorisable :**

**Titre : Architecture sécurisée et supervisée pour la visio-conférence Jitsi**

**Objectifs :**

**- Déploiement sécurisé (TLS, ports limités)**

**- Supervision (Prometheus, Grafana, Blackbox)**

**- Filtrage réseau (pfSense ou Firewalla)**

**- Analyse passive autorisée (nc -vz + journaux)**

**Options :**

**- Comparatif Firewall matériel/virtuel**

**- Script de test Bash sans scan actif**

**face à un choix critique d'architecture sécurité entre :**

* **🔒 Boîtiers tout-en-un comme Firewalla**
* **🧱 Solutions professionnelles comme pfSense/opnSense**
* **🧰 Montages DIY type Raspberry Pi + Linux durci**

**Tableau comparatif — Firewalla vs pfSense/opnSense vs DIY Linux (Raspberry Pi)**

| **Critère** | **🔴 Firewalla (Red / Purple)** | **⚙️ pfSense / OPNsense** | **🛠️ DIY Linux durci (Raspberry Pi)** |
| --- | --- | --- | --- |
| **📦 Type** | **Boîtier propriétaire prêt à l’emploi** | **Distribution BSD/Linux pour pare-feu dédiés** | **Machine autonome à configurer (Debian, Alpine…)** |
| **🎯 Usage cible** | **TPE, familles, réseaux simples** | **Entreprises, écoles, SI critiques** | **Administrateurs expérimentés ou étudiants avancés** |
| **🧠 Courbe d’apprentissage** | **Très facile (app mobile, tableau simple)** | **Moyenne à élevée (interfaces web très complètes)** | **Haute (scripts, durcissement manuel, shell)** |
| **🔐 Firewall/ACL** | **Oui (préconfiguré)** | **Oui (pf, stateful, ACL NAT/DMZ complexes)** | **Oui (iptables, nftables, firewalld)** |
| **📡 IDS/IPS intégré** | **Basique (alertes de flux suspects)** | **Oui avec Suricata, Snort, plugins** | **Oui si installé (Suricata, Falco, etc.)** |
| **📈 Monitoring réseau** | **Oui (trafic, device tracking, alertes)** | **Avancé avec plugins + logs syslog** | **Via Prometheus, iptraf, iftop, etc. (à configurer)** |
| **🛡️ DPI (Deep Packet Inspection)** | **Oui (limité), sans MITM** | **Oui (avec configuration), possible MITM HTTPS** | **Possible avec sslstrip, Wireshark, Zeek** |
| **🔧 Reverse proxy / TLS** | **Non natif** | **Oui (HAProxy, nginx en DMZ)** | **Oui via nginx/apache + certbot** |
| **🌐 Accès distant** | **App mobile (VPN, contrôle cloud optionnel)** | **WebGUI ou SSH sécurisé** | **SSH/VPN/Tmux – selon config** |
| **🧰 Maintenance** | **Automatique** | **Manuelle ou semi-automatisée** | **Entièrement manuelle** |
| **💵 Prix** | **95 € (Red) → 250 € (Purple)** | **Gratuit (install ISO) – machine à fournir** | **~60 € pour un Pi 4 + SD + alim + boîtier** |
| **⚙️ Virtualisable** | **❌ Non** | **✅ Oui (VM, KVM, Proxmox, VirtualBox)** | **✅ Oui (cloud-init, QEMU, Docker, etc.)** |

**Recommandation selon ton projet Jitsi + Sécurité + Monitoring**

| **Profil** | **Choix recommandé** | **Justification technique** |
| --- | --- | --- |
| **🔰 Débutant / Audit passif** | **Firewalla Purple** | **Zéro maintenance, DPI simple, alertes automatiques** |
| **⚙️ Étudiant Bachelor + projet SI** | **pfSense / OPNsense + Suricata** | **Tu apprends tout : DMZ, IDS, NAT, VPN, failover** |
| **🧪 Passionné / Autonomie totale** | **Raspberry Pi + Linux durci + Grafana** | **Pour tester scripts Bash, monitoring, déploiement léger** |