Soluciones para firewall + router (100fwdz)

Objetivo (intención de este trabajo)

Este trabajo solo tiene la intención de investigar (adquirir y/o actualizar conocimientos) respecto al estado actual (*al 22/03/2025*) de soluciones (principalmente del tipo software) para implementar firewall sobre redes basadas en TCP/IP (sean estas redes LAN o que puedan utilizarse en la frontera de redes WAN - LAN). Esta documentación, intenta aportar a realizar algunas implementaciones a modo de laboratorio o prototipos reales que puedan evolucionar a implementaciones con funcionalidad de firewall + route. El principal objetivo a cubrir por las soluciones aquí introducidas, deberían cubrir estar orientadas a ser firewall y router para LAN y DMZ o también gestión de segmentación de red, reglas de filtrados y redirección de paquetes en redes LAN (Local Adress Network/Redes de Area Local).

Nota del autor: La mayoría de soluciones presentadas en este documento (el cual para nada pretende ser un trabajo completo) puede ser utilizada con el fin que quien lo consulte lo crea necesario.

Alternativas como firewall y router

Windows Defender Firewall (Tecnología Windows)

Base: Basado en la tecnología del firewall integrado de Windows.

Funcionalidad: Filtrado de paquetes y control de conexiones entrantes y salientes.

Interfaz: Integración con el Centro de seguridad de Windows, accesible desde el Panel de Control y Configuración.

Ventajas: Integración nativa con el sistema operativo, políticas de grupo y reglas avanzadas de firewall.

Windows Server (Tecnología Windows, incluyendo 2025)

Base: Sistema operativo servidor para gestión de redes y servicios empresariales.

Funcionalidad: Gestión de usuarios y equipos mediante Active Directory, DHCP, DNS, administración de roles de servidor.

Interfaz: Admin Center (web) y herramientas clásicas (Server Manager, MMC).

Ventajas: Alta capacidad de integración y escalabilidad en entornos empresariales.

RRAS e IPsec

Base: Rol de servidor en Windows Server para servicios de enrutamiento y acceso remoto.

Funcionalidad: Conexiones VPN seguras, enrutamiento dinámico y políticas IPsec para comunicaciones seguras.

Interfaz: Administración vía RRAS Management Console y PowerShell.

Ventajas: Integración con Active Directory para autenticación y control de acceso centralizado.

URL: Documentación oficial de Microsoft; Windows Server Blog

pfSense y OPNsense

Distribuciones basadas en FreeBSD (con Packet Filter (pf) como principal motor de filtrado), poseen muy buenas capacidades y performance para tareas de firewall, router y DMZ, y muchas otras caracteristicas. Por indicar algo estas:

- pfSense: Mayor comunidad y más recursos, pero algunas características avanzadas son de pago.
- OPNsense: Fork de pfSense con enfoque en seguridad, interfaz moderna y completamente gratuito.

Base: Packet Filter (pf) (personalizado/compilado por cada uno de los desarrolladores según corresponda) con base en el sistema operativo FreeBSD.

Funcionalidad: DHCP Server y DHCP Relay, DNS Resolver y Forwarder, NTP, Failover de WAN, Load Balancing, WireGuard (principalmente en OPNsense), etc.

Interfaz: Principalmetne Web. Aunque posee CLI totalmente usable, es necesario un conocimiento muy avanzado tanto de pf como del sistema operativo Unix FreeBSD.

Ventajas: Se enfocan principalmente en la seguridad de red, gestión de amenazas y segmentación, utilizando principalmente el motor de filtrado packet filter.

URL: pfSense; OPNsense

F5 BIG-IP (solución comercial de firewall avanzado)

Base: Hardware y software propietarios con sistema operativo TMOS (Traffic Management Operating System).

Motor de filtrado: AFM (Advanced Firewall Manager) para gestión de firewall avanzado.

Interfaz: GUI (interfaz web), CLI (tmsh) y API REST.

Ventajas: Firewall de aplicaciones avanzado (WAF), balanceo de carga y control granular del tráfico. Integración profunda con otros módulos F5 (DNS, SSL VPN, etc.).

URL:

- URL principal de F5.

Nota importante: En el sitio https://www.f5.com/labs, el fabricante pública tanto una extensa documentación de sus tecnologías, y también hace disponible descargas de ciertas soluciones, para estudio de las mismas. El URL es interesante de revisar para quien quiera profundizar en una de las soluciones mas prestigiosas del momento a nivel mundial. Recordemos que F5 es definitivamente una de las soluciones más prestigiosas y avanzadas en el mercado de firewalls de aplicaciones y balanceadores de carga. Su producto F5 BIG-IP se utiliza ampliamente en grandes empresas y proveedores de servicios debido a su capacidad para manejar tráfico a gran escala y ofrecer funciones avanzadas, compiendo actualmente con sus homólogas tales como: Citrix ADC, A10 Networks Thunder ADC, Barracuda Web Application Firewall, Imperva, AWS WAF y Google Cloud Armor.

IPFire

Base: Linux, derivada de iptables y adaptada como firewall dedicado.

Funcionalidad: Firewall avanzado, NAT, DMZ, VPN (OpenVPN, IPsec), QoS, proxy y filtrado de contenido.

Interfaz: Web fácil de usar.

Ventajas: Se enfoca principalmente en la seguridad de red, gestión de amenazas y segmentación.

URL: IPFire

VyOS

Base: Debian, sucesor de Vyatta (que fue comercializado por Brocade).

Funcionalidad: Firewall, router avanzado, NAT, DMZ, VPN (OpenVPN, WireGuard, IPsec), balanceo de carga.

CLI y Web GUI: Mayor control y flexibilidad en configuración avanzada.

Ventajas: Similar a equipos de red empresariales, ideal para entornos híbridos.

URL: Vyos

Untangle NG Firewall

Base: Debian.

Funcionalidad: Firewall, NAT, DMZ, VPN (OpenVPN y IPsec), filtrado de contenido, prevención de intrusiones.

Interfaz: Gráfica muy amigable.

Nota: Tiene versión gratuita, pero algunas características avanzadas son de pago.

URL: Untangle NG Firewall

Smoothwall Express

Base: Smoothwall Express se basa en el sistema operativo Linux.

Funcionalidad: Smoothwall es una familia de productos de seguridad para Internet diseñada para proteger a sus usuarios y su red de ataques externos. Smoothwall incluye un subconjunto reforzado del sistema operativo GNU/Linux, por lo que no es necesario instalar un sistema operativo independiente. Diseñado para facilitar su uso, Smoothwall se configura mediante una interfaz gráfica de usuario web y no requiere conocimientos de Linux para su instalación o uso. Esta solución posee varias de las características y servicios propios de Firewall.

Interfaz: Principalmente GUI Web, interface simple e intuitiva.

URL: Descarga de Smoothwall

Firewalld (nativa en RHEL, CentOS, AlmaLinux, Fedora, etc)

Base: Linux, interfaz más amigable y modular sobre iptables/nftables.

Interfaz: CLI (firewall-cmd) y GUI (firewalld-config en entornos gráficos).

Ventajas: Integración nativa con distribuciones derivadas RHEL y/o Fedora (AlmaLinux, Rocky Linux, Oracle Linux, etc). Actualmente ya se encuentra disponible en para sistemas derivados de Debian (ejemplo: Ubuntu), Linux Arch, etc.

URL: El sitio oficial de firewalld oficial con documentación, tutoriales y desarrollo.

iptables y nftables (disponibles en todas las distribuciones Linux)

Base: Linux, herramientas de filtrado de paquetes en espacio de usuario para netfilter (kernel).

Interfaz: CLI (iptables/nft y frontends como ufw o Shorewall).

Ventajas: Control granular y detallado del tráfico. `nftables` simplifica la sintaxis y mejora el rendimiento.

Diferencia clave: `nftables` reemplaza a `iptables` con una sintaxis unificada, tablas más simples y gestión centralizada de reglas. Reduce la complejidad al manejar IPv4, IPv6, ARP y bridges bajo una misma sintaxis.

URL:

- Wiki oficial de nftables con documentación detallada y recursos.
- Página oficial dentro del proyecto Netfilter, responsable del desarrollo de iptables.

Otras soluciones

En este apartado se quiere nombrar al menos una de las soluciones que si bien inicialmente la funcionalidad principal a cubrir no es la de firewall, con el agregado de extensiones o complementos o similar es que se amplian sus funciones a este elemento de seguridad. Mas soluciones de este tipo pueden ser consultadas en sitios como Distrowath, por si el lector esta motivado por este tipo de soluciones.

Zentyal

Base: Ubuntu 22.04 LTS en la versión Zentyal 8.0.

Funcionalidad: Zentyal puede cumplir perfectamente la función de firewall y router para LAN y DMZ, y/o segmentación de red. (Esta solución está más enfocada a la gestión de servidores de infraestructura como controladores de dominio, correo, VPN, etc).

Ventajas: Interface Web muy completa, intuitiva, aunque puede resultar abrumadora al principio. Completa administración para CLI, por tratarse de un sistema Linux.

URL: Zentyal Server Development Edition

Tabla Comparativa

Solución	Base	GUI	Complejidad	Firewall Avanzado	DMZ	VPN	Gratuita
Zentyal	Ubuntu	Sí	Baja	Sí	Sí	OpenVPN, IPsec	Parcial
pfSense	FreeBSD	Sí	Media	Sí	Sí	OpenVPN, IPsec	Parcial
OPNsense	FreeBSD	Sí	Media	Sí	Sí	OpenVPN, WireGuard	Sí
IPFire	Linux	Sí	Media	Sí	Sí	OpenVPN, IPsec	Sí
VyOS	Debian	CLI/Web (pago)	Alta	Sí	Sí	OpenVPN, WireGuard	Parcial

Solución	Base	GUI	Complejidad	Firewall Avanzado	DMZ	VPN	Gratuita
Untangle	Debian	Sí	Baja	Sí	Sí	OpenVPN, IPsec	Parcial
Smoothwall	Linux	Web	Baja	Sí	Sí	OpenVPN, IPsec	Sí
Firewalld	Nativo en RHEL/Fedora y derivados	CLI y GUI	Media	Básico	Limitado	IPsec	Sí
iptables	Linux	CLI (ufw, Shorewall)	Alta	Avanzado	Sí	IPsec	Sí
nftables	Linux	CLI	Media	Avanzado	Sí	IPsec	Sí
Windows Defender Firewall	Windows	Powershell y GUI	Baja	Orientado a la protección de PC	N/A	--	No
RRAS/IPsec	Windows Server	Powershell y GUI	Media	Media	Sí	Sí	No

Recomendación según contexto / resumen adicional

- Entornos híbridos y avanzados: VyOS o OPNsense.
- Entornos simples o educativos: Zentyal o IPFire.
- Integración con Linux de servidor: Firewalld.
- Hardware muy limitado o de bajo recursos (sea real o virtual): Smoothwall.
- Compatibilidad y disponibilidad: Tanto iptables, nftables y firewalld están presentes en todas las distribuciones Linux modernas. Aunque firewalld es más común en RHEL/Fedora, también se encuentra en Debian, Ubuntu y Arch Linux.
- Evolución: nftables es la evolución natural de iptables, permitiendo gestionar reglas de forma centralizada, simplificada y más eficiente.

Referencias

- Documentación oficial de Microsoft
- Windows Server Blog

Glosario

RRAS: Routing and Remote Access Service, permite gestionar conexiones remotas y enrutamiento de red.

IPsec: Protocolo para asegurar comunicaciones IP mediante autenticación y cifrado.

Active Directory: Servicio para administración centralizada de usuarios y políticas de seguridad.

MMC: Consola de administración de Microsoft para gestionar componentes de Windows.