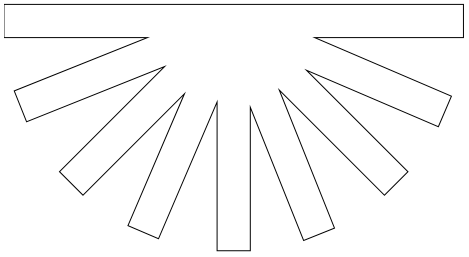
SISTEMAS OPERATIVOS

PFSENSE Y SU IMPLEMENTACION DE FREEBSD



PRESENTADO POR:

Perez Osorio Luis Euardo

Flores Garcia claudio

PROFESOR:

Ing. Gunnar Eyal Wolf Iszaevich

1. Introducción a pfSense

● ¿Qué es pfSense?

pfSense es una solución de software de código abierto basada en el sistema operativo ***FreeBSD*** que proporciona funciones avanzadas de firewall y enrutamiento para redes. Se distribuye bajo la licencia BSD, lo que permite su uso, modificación y distribución sin restricciones. pfSense está diseñado para ser instalado en hardware dedicado o en máquinas virtuales, lo que lo convierte en una opción flexible y accesible para empresas y usuarios individuales que requieren una solución robusta para la gestión de redes.[1.1]

Desarrollado originalmente por ***Electric Sheep Fencing LLC***, pfSense ha crecido en popularidad debido a su interfaz de usuario amigable, su flexibilidad, la abundancia de características y su constante evolución con mejoras y actualizaciones. Es ampliamente utilizado en entornos empresariales, hogares y entornos educativos por su capacidad para manejar grandes volúmenes de tráfico, proteger redes y ofrecer funcionalidades de red avanzadas.[1.1]

● pfSense como firewall y router

1. **Firewall de estado**: pfSense utiliza un firewall de inspección de estado que monitorea el estado de las conexiones activas y permite o bloquea el tráfico basado en reglas predefinidas. Esto le otorga una seguridad avanzada y granular.[1.1]

2. **Enrutamiento avanzado**: pfSense es capaz de manejar una variedad de configuraciones de enrutamiento, incluyendo enrutamiento estático, dinámico y basado en políticas, lo que lo convierte en una opción muy versátil para configuraciones de red complejas.[1.1]

3. **VPN (Virtual Private Network)**: pfSense ofrece compatibilidad con varios protocolos de VPN, como IPsec y OpenVPN, lo que permite a los usuarios conectarse de forma segura a redes remotas o proporcionar acceso seguro a su red a través de Internet.[1.1]

4. **Balanceo de carga y conmutación por error**: pfSense admite el balanceo de carga entre múltiples conexiones WAN, lo que permite distribuir el tráfico de Internet entre diferentes enlaces para mejorar el rendimiento. También ofrece conmutación por error en caso de que una conexión WAN falle, garantizando la continuidad del servicio.[1.1]

5. **Soporte para VLANs (Redes de Área Local Virtual)**: pfSense admite la creación y gestión de VLANs, lo que permite segmentar el tráfico de red de manera eficiente y mejorar la seguridad y el rendimiento en redes más grandes.[1.1]

6. **Gestión de tráfico y QoS (Calidad de Servicio)**: pfSense puede priorizar el tráfico de red utilizando reglas de QoS, lo que garantiza que aplicaciones críticas, como la voz sobre IP (VoIP) o los servicios de video, tengan prioridad sobre otras actividades menos urgentes.[1.1]

7. **Extensible**: pfSense soporta una amplia gama de complementos (plugins) que amplían sus funcionalidades, incluyendo servicios como el filtrado de contenido, sistemas de detección de intrusiones (IDS/IPS), y servidores DHCP, DNS y NTP.[1.1]

- **Comparación con alternativas propietarias (Cisco, Juniper, etc.)**

pfSense vs. Cisco ASA (Adaptive Security Appliance)

Cisco ASA es un firewall empresarial de alto rendimiento, ampliamente utilizado en grandes organizaciones. Aunque ofrece una excelente seguridad y rendimiento, Cisco ASA es un producto propietario y costoso, lo que limita su accesibilidad para pequeñas y medianas empresas o usuarios domésticos. Además, requiere experiencia técnica considerable para configurarlo y gestionarlo correctamente.[1.2]

Ventajas de pfSense sobre Cisco ASA:

- Costo: pfSense es gratuito y de código abierto, mientras que Cisco ASA es un producto de alto costo.[1.2] [1.3]
- Facilidad de uso: pfSense tiene una interfaz gráfica web mucho más intuitiva y fácil de usar en comparación con Cisco ASA, que a menudo requiere configuración mediante la línea de comandos.[1.2] [1.3]
- Flexibilidad: Al ser de código abierto, pfSense permite una mayor personalización y tiene una amplia gama de complementos que pueden adaptarse a las necesidades de una red específica.[1.2] [1.3]

Desventajas de pfSense:

- Rendimiento: Cisco ASA suele ser superior en rendimiento, especialmente en entornos de alto tráfico o donde se requiere un alto nivel de encriptación y análisis de paquetes.[1.2] [1.3]
- Soporte técnico: Aunque existen comunidades activas para pfSense, Cisco ofrece un soporte técnico profesional y especializado, algo crucial para entornos críticos.[1.2] [1.3]

pfSense vs. Juniper SRX

Juniper SRX es otra solución de firewall empresarial que compite con Cisco ASA. Es conocido por su escalabilidad y su integración con otras soluciones de red de Juniper. También es una opción cara y generalmente está orientada a grandes empresas y proveedores de servicios.[1.2]

Ventajas de pfSense sobre Juniper SRX:

- Costo: Nuevamente, la mayor ventaja de pfSense es su costo cero, en comparación con Juniper SRX, que es costoso tanto en términos de licencia como de mantenimiento.[1.2] [1.3]
- Personalización: pfSense es altamente personalizable, mientras que Juniper SRX, al ser un sistema propietario, no ofrece tanta flexibilidad para adaptaciones o personalizaciones fuera de lo que permite el fabricante.[1.2] [1.3]
- Compatibilidad con hardware genérico: pfSense puede instalarse en una amplia gama de hardware, desde PCs hasta servidores dedicados, mientras que Juniper SRX requiere dispositivos específicos de la marca.[1.2] [1.3]

Desventajas de pfSense:

- Seguridad de nivel empresarial: Juniper SRX ofrece características de seguridad de nivel empresarial, como análisis profundo de paquetes y seguridad a nivel de aplicación, que pueden superar lo que ofrece pfSense en ciertos entornos.[1.2] [1.3]
- Rendimiento en redes grandes: Aunque pfSense puede manejar grandes volúmenes de tráfico, las soluciones de Juniper están diseñadas para escalar en entornos de telecomunicaciones y grandes empresas de manera más eficiente.[1.2] [1.3]

pfSense vs. Fortinet FortiGate

Fortinet es otro competidor importante en el mercado de firewalls con su serie FortiGate, que ofrece una amplia gama de características de seguridad avanzadas, como el filtrado web, protección antivirus y control de aplicaciones. Fortinet también es conocido por su enfoque en la seguridad unificada (UTM, por sus siglas en inglés), que agrupa múltiples servicios de seguridad en un solo dispositivo.[1.2]

Ventajas de pfSense sobre FortiGate:

- Costo: pfSense sigue siendo gratuito, mientras que FortiGate requiere una inversión inicial significativa, además de suscripciones continuas para acceder a sus características avanzadas de seguridad.[1.2] [1.3]
- Comunidad y soporte: Aunque Fortinet ofrece soporte empresarial, pfSense tiene una comunidad activa que genera guías, plugins y foros para ayudar a resolver problemas de configuración y optimización.[1.2] [1.3]

Desventajas de pfSense:

- Seguridad avanzada: FortiGate incluye características como filtrado antivirus y control de aplicaciones, que, si bien se pueden implementar en pfSense con complementos, no están integradas de forma nativa.[1.2] [1.3]
- Soporte y actualizaciones profesionales: Fortinet ofrece soporte técnico dedicado y actualizaciones constantes como parte de su oferta comercial, mientras que el soporte de pfSense depende principalmente de su comunidad de usuarios.[1.2] [1.3]

2. FreeBSD

- **¿Qué es FreeBSD?**

FreeBSD es un sistema operativo de código abierto derivado de Unix, específicamente de la línea BSD (Berkeley Software Distribution). Es conocido por su estabilidad, rendimiento y seguridad, lo que lo convierte en una opción popular tanto para servidores como para soluciones de red y sistemas embebidos. A diferencia de otros sistemas operativos, FreeBSD ofrece un núcleo (kernel) y un conjunto de herramientas desarrolladas de forma conjunta, lo que garantiza una mayor coherencia y optimización del sistema. [2.1]

- **Por qué pfSense utiliza el sistema operativo FreeBSD**

pfSense es una plataforma de firewall y enrutamiento de código abierto, muy popular en soluciones de seguridad de red. El motivo principal por el que pfSense utiliza FreeBSD como su sistema operativo base es por la robustez y flexibilidad que ofrece en entornos de red. Algunas razones clave son:

  - **Estabilidad**: FreeBSD es ampliamente reconocido por su estabilidad, lo cual es esencial para aplicaciones críticas como firewalls y routers, que requieren un tiempo de actividad prolongado sin fallos.[2.2]

  - **Rendimiento en Redes**: FreeBSD cuenta con una pila de red extremadamente eficiente y avanzada, optimizada durante décadas de desarrollo, lo que lo hace adecuado para gestionar un alto tráfico de red sin comprometer el rendimiento.[2.1] [2.2]

  - **Licencia BSD**: FreeBSD utiliza una licencia BSD que es menos restrictiva en comparación con otras licencias de código abierto, como la GPL (Licencia Pública General). Esto permite a proyectos como pfSense personalizar y distribuir el sistema con mayor libertad sin tener que liberar el código fuente de sus modificaciones, lo que es atractivo para desarrolladores comerciales.[2.3]

  - **Soporte para tecnologías avanzadas**: FreeBSD admite muchas tecnologías avanzadas que son útiles para la creación de soluciones de red, como el soporte de múltiples procesadores, redes virtuales y sistemas de archivos avanzados como ZFS.[2.1]

  - **Seguridad**: FreeBSD tiene un fuerte enfoque en la seguridad, lo que es primordial para una plataforma como pfSense. Incluye características de seguridad robustas como el control de acceso basado en roles, el sistema de archivos seguro y una política de seguridad coherente a nivel del sistema operativo.[2.1] [2.2]

- **Características de FreeBSD para soluciones de red.**

➔ **Pila de red avanzada**: FreeBSD tiene una de las pilas de red más maduras y optimizadas del mundo Unix, lo que permite un manejo eficiente del tráfico, soporte para redes de alta velocidad y múltiples protocolos de enrutamiento. Además, soporta un gran conjunto de controladores de red, lo que garantiza compatibilidad con diversos dispositivos de hardware.[2.1]

➔ **Escalabilidad**: FreeBSD puede escalar desde pequeñas aplicaciones embebidas hasta grandes infraestructuras de red. Su kernel es altamente configurable, lo que permite personalizar el sistema para aplicaciones específicas, desde servidores web hasta soluciones de firewall y VPN.[2.1] [2.2]

➔ **Jails**: FreeBSD incluye una tecnología llamada "jails", que es similar a los contenedores en Linux. Esto permite a los administradores de sistemas ejecutar aplicaciones aisladas unas de otras, proporcionando seguridad adicional y facilitando la administración de múltiples servicios en un solo sistema.[2.1]

➔ **Soporte para ZFS**: FreeBSD soporta ZFS, un avanzado sistema de archivos que proporciona integridad de datos, replicación y snapshots, lo que es crucial para la administración de sistemas de red grandes y complejos.[2.1]

➔ **Soporte de hardware**: FreeBSD tiene un excelente soporte para hardware de red y ofrece una amplia gama de controladores, asegurando que puede funcionar bien en una variedad de entornos de hardware sin problemas de compatibilidad.[2.1] [2.3] [2.4]

3. Historia y desarrollo de pfSense

- **Origenes**

pfSense se originó en 2004 como un fork del proyecto m0n0wall, creado por Manuel Kasper. m0n0wall fue una solución de firewall diseñada específicamente para dispositivos embebidos con recursos de hardware limitados. Sin embargo, algunos usuarios necesitaban una plataforma más robusta para equipos más grandes y servidores. Así, Chris Buechler y Scott Ullrich decidieron desarrollar pfSense, que mantendría la facilidad de uso de m0n0wall, pero con una gama más amplia de funciones y capacidades para hardware más potente.[3.1] [3.2]

- **m0n0wall.**

m0n0wall se centraba en ofrecer un firewall para dispositivos embebidos y utilizaba FreeBSD como su sistema operativo subyacente. Con el tiempo, el equipo de pfSense añadió nuevas funcionalidades como soporte para VPN, detección y prevención de intrusiones (IDS/IPS), y capacidades de balanceo de carga, expandiendo su utilidad tanto para redes pequeñas como para grandes infraestructuras empresariales. [3.2] [3.3]

En 2015, Kasper anunció el fin de m0n0wall, recomendando a los usuarios migrar a pfSense, lo que solidificó la relevancia de pfSense en el mercado de software de firewall.[3.1]

- **Contribuyentes.**

pfSense ha crecido gracias a una activa comunidad de desarrolladores y a la empresa Netgate, que proporciona soporte comercial y desarrollo continuo. Actualmente, Netgate gestiona el proyecto, ofreciendo versiones gratuitas (pfSense CE) y comerciales (pfSense Plus). La comunidad también ha contribuido significativamente al desarrollo, garantizando que pfSense se mantenga actualizado y competitivo frente a soluciones comerciales. [3.4]

Este crecimiento ha permitido que pfSense se utilice en una amplia gama de aplicaciones, desde redes domésticas hasta entornos empresariales y educativos, gracias a su flexibilidad, escalabilidad y eficiencia.[3.1] [3.3]

4. Arquitectura de pfSense

- **Interacciones entre pfSense y el kernel de FreeBSD.**

pfSense es una distribución de firewall basada en FreeBSD, lo que significa que utiliza el kernel de FreeBSD como base para su funcionamiento. La interacción entre pfSense y el kernel de FreeBSD es fundamental para entender cómo opera este sistema de seguridad de red.

El kernel de FreeBSD proporciona las funcionalidades de bajo nivel que pfSense aprovecha para implementar sus características de firewall y enrutamiento. Algunas de las interacciones clave incluyen:

1. **Gestión de red**: pfSense utiliza las capacidades de red del kernel de FreeBSD para manejar las interfaces de red, tanto físicas como virtuales. Esto incluye la configuración de direcciones IP, enrutamiento y manejo de protocolos de red. [4.1]

2. **Filtrado de paquetes**: pfSense hace uso intensivo del sistema de filtrado de paquetes PF (Packet Filter) integrado en FreeBSD. PF se ejecuta a nivel del kernel, permitiendo un filtrado de paquetes de alto rendimiento.[4.2]

3. **Gestión de estado**: El kernel de FreeBSD proporciona mecanismos para el seguimiento de estado de las conexiones, que pfSense utiliza para implementar su firewall con estado.[4.3]

4. **Virtualización**: pfSense aprovecha las capacidades de virtualización del kernel de FreeBSD, como las jaulas (jails), para proporcionar aislamiento y seguridad adicional.[4.4]

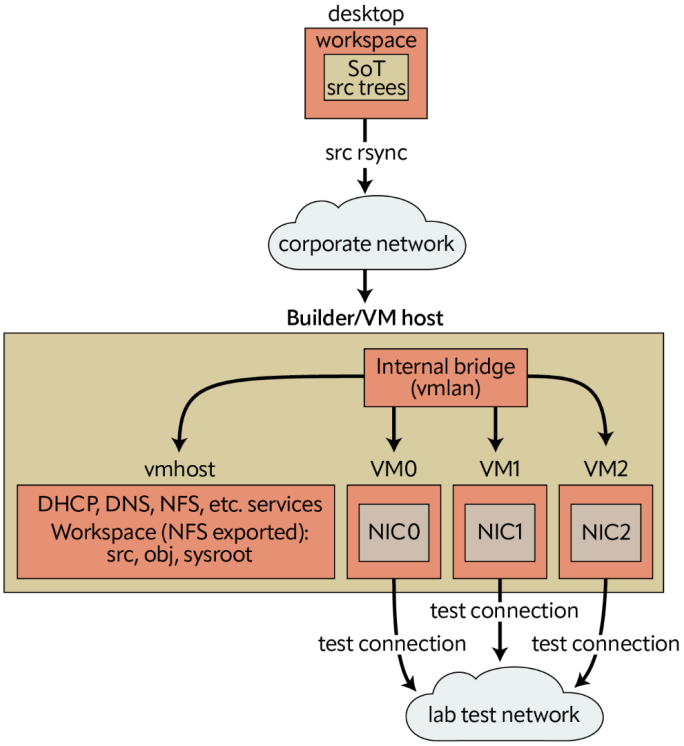


Imagen 1.- FreeBSD Kernel Development Workflow [4.5]

- **El diseño modular de pfSense.**

pfSense está diseñado con una arquitectura modular, lo que permite una gran flexibilidad y extensibilidad. Esta modularidad se refleja en varios aspectos del sistema:

1. **Sistema de paquetes**: pfSense utiliza el sistema de paquetes de FreeBSD, permitiendo la instalación, actualización y eliminación de componentes de software de forma independiente.[4.6]

2. **Interfaz web modular**: La interfaz web de pfSense está construida de manera modular, con diferentes secciones para distintas funcionalidades. Esto permite una fácil expansión y personalización de la interfaz.[4.7]

3. **Servicios independientes**: Muchas de las funcionalidades de pfSense se implementan como servicios independientes que pueden ser habilitados o deshabilitados según sea necesario. Esto incluye servicios como DHCP, DNS, VPN, entre otros.[4.8]

4. **Sistema de plugins**: pfSense soporta un sistema de plugins que permite a los usuarios extender las funcionalidades del sistema sin modificar el núcleo del software.[4.9]

- **Como pfSense implementa características de FreeBSD (jails, PF packet filter, etc.).**

pfSense hace un uso extensivo de las características avanzadas que ofrece FreeBSD:

1. **Jaulas (Jails)**: pfSense utiliza las jaulas de FreeBSD para proporcionar entornos aislados para ciertos servicios, mejorando la seguridad y el aislamiento. Por ejemplo, se pueden utilizar jaulas para aislar servicios de proxy o sistemas de detección de intrusiones.[4.10]

2. **PF (Packet Filter)**: Como se mencionó anteriormente, pfSense utiliza intensivamente el sistema de filtrado de paquetes PF de FreeBSD. PF proporciona capacidades avanzadas de filtrado, NAT y gestión de tráfico que son fundamentales para las funcionalidades de firewall de pfSense.[4.11]

3. **ALTQ (Alternate Queueing)**: pfSense aprovecha ALTQ, el sistema de gestión de colas de FreeBSD, para implementar QoS (Quality of Service) y control de ancho de banda.[4.12]

4. **GEOM**: pfSense utiliza el framework GEOM de FreeBSD para la gestión de dispositivos de almacenamiento y la implementación de funcionalidades como el cifrado de disco.[4.13]

5. **IPsec**: Para las funcionalidades de VPN, pfSense hace uso de la implementación de IPsec de FreeBSD, que está bien integrada con el kernel para un rendimiento óptimo.[4.14]

5. Características importantes de pfSense

- **Filtrado de paquetes y firewall.**

pfSense es conocido por sus robustas capacidades de filtrado de paquetes y cortafuegos, que son fundamentales para la seguridad de la red.

1. **Filtrado de paquetes con estado**: pfSense utiliza el sistema de filtrado de paquetes PF (Packet Filter) de FreeBSD, que proporciona un filtrado de paquetes con estado. Esto significa que pfSense puede rastrear el estado de las conexiones y tomar decisiones de filtrado basadas en el contexto de cada paquete dentro de una conexión.[5.1]

2. **Reglas de firewall flexibles**: pfSense permite a los administradores crear reglas de firewall complejas y detalladas. Estas reglas pueden basarse en una variedad de criterios, incluyendo direcciones IP de origen y destino, puertos, protocolos, y más.[5.2]

3. **Alias y tablas**: Para simplificar la gestión de reglas complejas, pfSense soporta el uso de alias (que permiten agrupar múltiples direcciones IP o puertos bajo un solo nombre) y tablas (que pueden contener grandes conjuntos de direcciones IP).[5.3]

4. **Inspección profunda de paquetes**: pfSense puede realizar inspección profunda de paquetes, permitiendo un filtrado más granular basado en el contenido de los paquetes.[5.4]

- **Network Address Translation (NAT) y redirección de puertos.**

Las capacidades de NAT y reenvío de puertos de pfSense son esenciales para la gestión eficiente del tráfico de red y la exposición segura de servicios internos.

1. **NAT saliente (Source NAT)**: pfSense puede realizar NAT saliente, permitiendo que múltiples dispositivos en una red privada compartan una única dirección IP pública. Esto es crucial para la conservación de direcciones IP y la seguridad de la red interna.[5]

2. **NAT entrante (Destination NAT)** y reenvío de puertos: pfSense soporta NAT entrante y reenvío de puertos, permitiendo que los servicios internos sean accesibles desde Internet de manera controlada.[6]

3. **1:1 NAT**: Para escenarios más complejos, pfSense soporta NAT 1:1, que mapea una dirección IP pública a una dirección IP privada específica.[7]

4. **UPnP y NAT-PMP**: pfSense incluye soporte para UPnP (Universal Plug and Play) y NAT-PMP (NAT Port Mapping Protocol), que permiten a los dispositivos en la red configurar automáticamente el reenvío de puertos cuando sea necesario.[8]

- **Soporte para VPNs (IPsec, OpenVPN, WireGuard).**

pfSense ofrece un amplio soporte para tecnologías VPN, permitiendo conexiones seguras entre redes y usuarios remotos.

1. **IPsec**: pfSense incluye una implementación completa de IPsec, permitiendo crear túneles VPN sitio a sitio y conexiones de acceso remoto. Soporta una variedad de algoritmos de cifrado y autenticación, así como IKEv1 e IKEv2.[5.9]

2. **OpenVPN**: pfSense integra OpenVPN, una solución VPN flexible y de código abierto. Soporta tanto conexiones sitio a sitio como de acceso remoto, y ofrece opciones avanzadas como autenticación de dos factores.[5.10]

3. **WireGuard**: Desde la versión 2.5, pfSense incluye soporte para WireGuard, un protocolo VPN moderno conocido por su simplicidad y rendimiento. Aunque inicialmente se ofreció como un paquete experimental, ahora está completamente integrado en pfSense.[5.11]

4. **Configuración y gestión de clientes**: pfSense proporciona herramientas para la generación de configuraciones de cliente y la gestión de certificados, simplificando la configuración de conexiones VPN.[5.12]

- **ID (Intrusion Detection) e IP (Intrusion Prevention) (Snort, Suricata).**

pfSense integra sistemas de detección y prevención de intrusiones (IDS/IPS) para proporcionar una capa adicional de seguridad.

1. **Snort**: pfSense soporta Snort, un potente sistema de detección y prevención de intrusiones basado en reglas. Snort puede analizar el tráfico en tiempo real y alertar o bloquear actividades maliciosas basándose en una extensa base de datos de firmas.[5.13]

2. **Suricata**: Como alternativa a Snort, pfSense también soporta Suricata, otro sistema IDS/IPS de alto rendimiento. Suricata ofrece capacidades similares a Snort, pero con algunas ventajas en términos de rendimiento en ciertas configuraciones.[5.14]

3. **Integración con el firewall**: Tanto Snort como Suricata se integran estrechamente con las capacidades de firewall de pfSense, permitiendo una respuesta automatizada a las amenazas detectadas.[5.15]

4. **Actualización de reglas**: pfSense facilita la gestión y actualización de las reglas de IDS/IPS, permitiendo a los administradores mantener sus sistemas de detección de intrusiones actualizados contra las últimas amenazas.[5.16]

- **Load balancing y failover.**

pfSense ofrece capacidades avanzadas de balanceo de carga y failover para garantizar la alta disponibilidad y el rendimiento óptimo de las redes.

1. **Balanceo de carga de servidores**: pfSense puede distribuir el tráfico entrante entre múltiples servidores backend, mejorando el rendimiento y la disponibilidad de los servicios. Soporta varios algoritmos de balanceo, incluyendo round-robin, menor número de conexiones y menor tiempo de respuesta.[5.17]

2. **Balanceo de carga de enlaces WAN**: Para redes con múltiples conexiones a Internet, pfSense puede balancear el tráfico saliente entre estas conexiones, maximizando el ancho de banda disponible y proporcionando redundancia.[5.18]

3. **Failover de enlaces WAN**: pfSense puede configurarse para detectar fallos en las conexiones WAN y redirigir automáticamente el tráfico a enlaces alternativos, garantizando la continuidad del servicio.[5.19]

4. **Alta disponibilidad (CARP)**: Utilizando el protocolo CARP (Common Address Redundancy Protocol), pfSense puede configurarse en un clúster de alta disponibilidad, donde un firewall secundario puede tomar el control si el primario falla.[5.20]

- **Traffic shaping y Quality of Service (QoS).**

Las capacidades de modelado de tráfico y QoS de pfSense permiten a los administradores optimizar el uso del ancho de banda y priorizar el tráfico crítico.

1. **Limitación de ancho de banda**: pfSense puede limitar el ancho de banda para ciertos tipos de tráfico o para direcciones IP específicas, evitando que un solo usuario o aplicación consuma todos los recursos de red disponibles.[5.21]

2. **Priorización de tráfico**: Mediante el uso de colas de prioridad, pfSense puede asegurar que el tráfico crítico (como VoIP o aplicaciones de negocio) reciba prioridad sobre el tráfico menos importante.[5.22]

3. **ALTQ (Alternate Queueing)**: pfSense utiliza ALTQ, el sistema de gestión de colas de FreeBSD, para implementar sus funcionalidades de QoS. ALTQ soporta varios algoritmos de planificación, incluyendo HFSC, CBQ y PRIQ.[5.23]

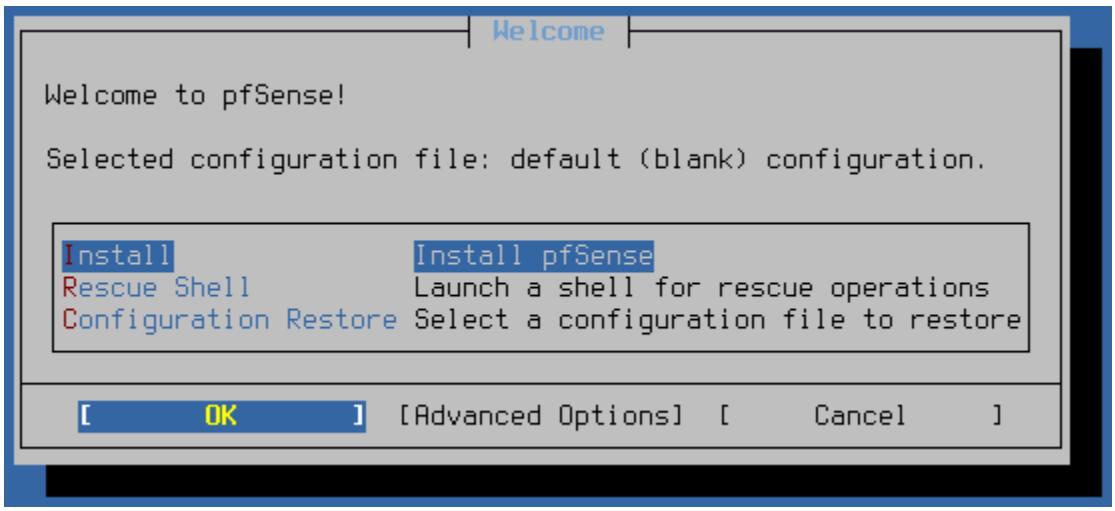
4. **Clasificación de tráfico**: pfSense puede clasificar el tráfico basándose en diversos criterios, incluyendo protocolo, puerto, dirección IP y más, permitiendo una gestión de QoS muy granular.[5.24]

5. **Monitoreo y análisis**: pfSense proporciona herramientas para monitorear y analizar el uso del ancho de banda, ayudando a los administradores a identificar patrones de tráfico y ajustar las políticas de QoS según sea necesario.[5.25]

6. Instalación y configuración

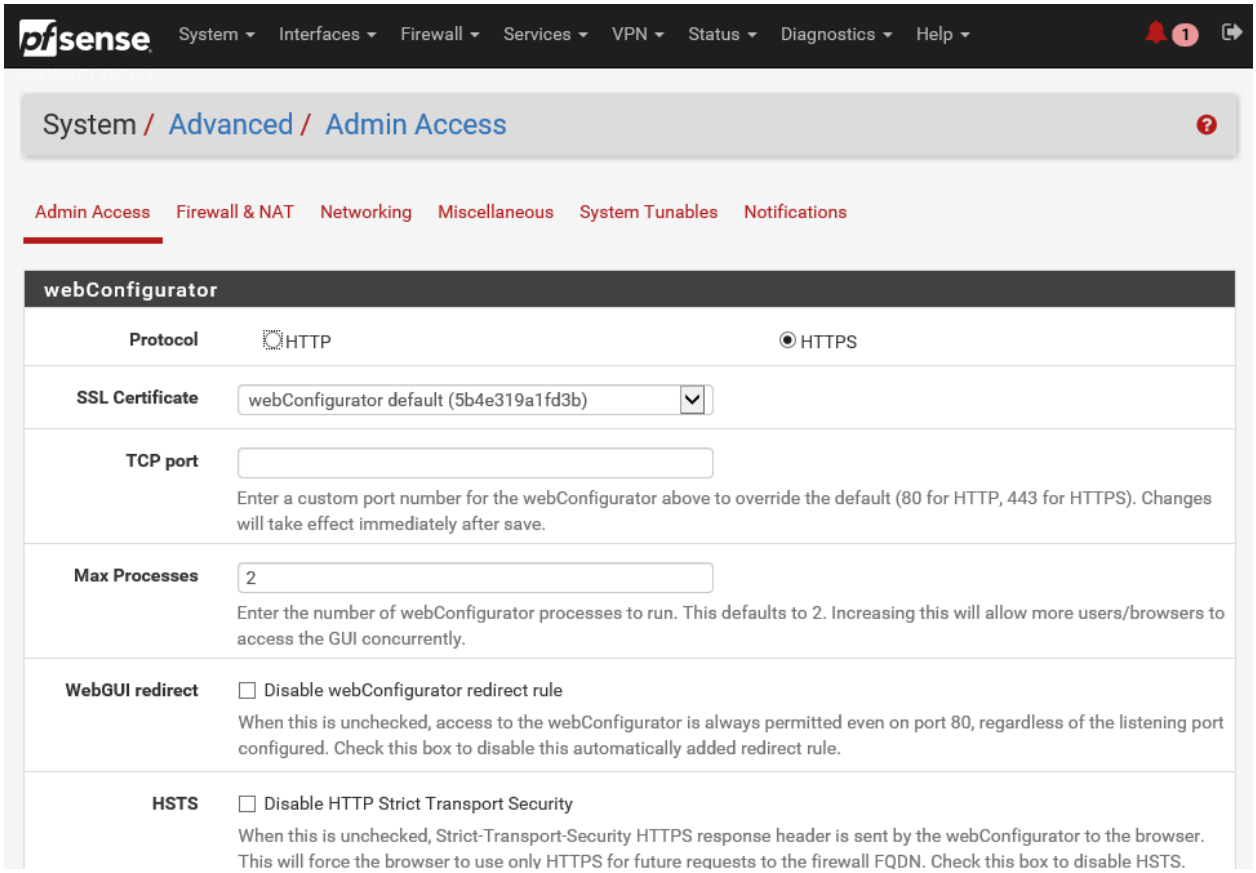
- **Requisitos de hardware**
  - ➔ CPU de 64 bits amd64(x86-64)
  - ➔ 1GB+ de RAM
  - ➔ 6GB+ de disco
  - ➔ Una o más tarjetas de red compatibles
  - ➔ Un dispositivo USB de arranque o disco óptico (DVD)[6.1]
- **Proceso de instalación:**

pfSense puede ser instalado en hardware dedicado o mediante una máquina virtual para instalarlo es necesario descargar una imagen apropiada de la tienda de netgate y preparar el medio de instalación, una vez iniciada la computadora con el medio de instalación conectado se iniciará el instalador del sistema.



Desde aquí pueden modificarse varios aspectos del sistema operativo FreeBSD sobre el cual está escrito pfSense tales como el sistema de archivos(pfsense soporta ZFS y UFS como sistemas de archivos) el esquema de partición (GPT o MBR), configuración de interfaces de red, entre otras.

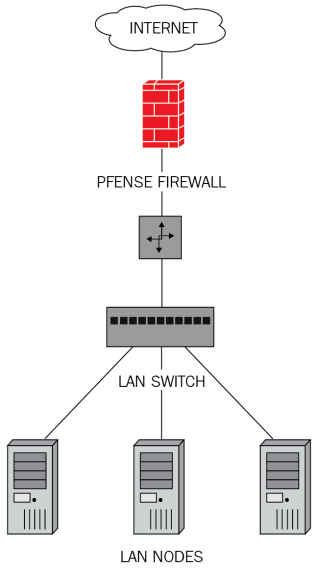
Después de esto el instalador hará las modificaciones necesarias al sistema operativo, aplicará las configuraciones específicas para pfSense y se reiniciará, si se configuraron las interfaces de red correctamente a partir de este punto se puede hacer la gran mayoría del manejo del software a través de la interfaz web proporcionada por pfSense. [6.2]


pfsense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
1
System / Advanced / Admin Access
Admin Access
Firewall & NAT
Networking
Miscellaneous
System Tunables
Notifications
webConfigurator
Protocol
HTTP
HTTPS
SSL Certificate
webConfigurator default (5b4e319a1fd3b)
TCP port
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
Max Processes
2
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.
WebGUI redirect
Disable webConfigurator redirect rule
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.
HSTS
Disable HTTP Strict Transport Security
When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS.

7. Casos de uso [7.1] [7.2]

- **Firewall perimetral**

Uno de los usos más comunes de pfSense es como firewall perimetral, permite el uso de múltiples conexiones a internet y múltiples redes LAN, esta capacidad le permite ser útil para casos como la seguridad de una red doméstica hasta la seguridad de redes empresariales de gran escala.



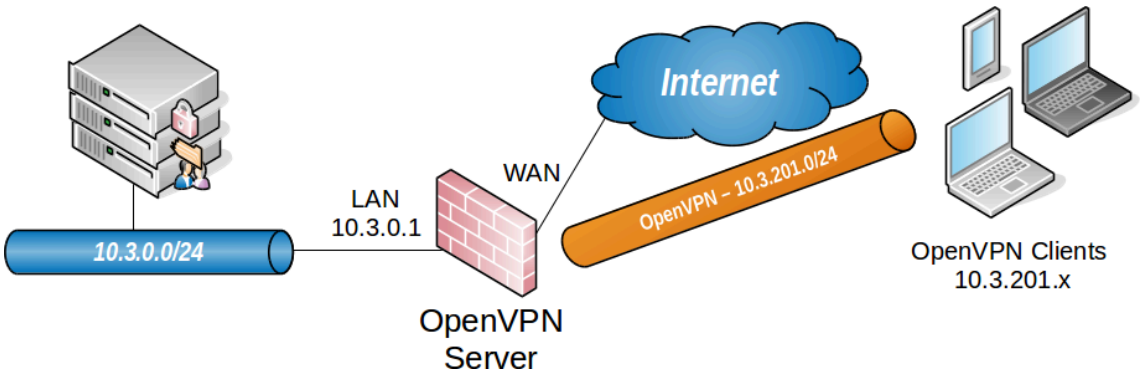
- **Router**

En conjunto con su uso como firewall es común ver pfSense implementado como router para redes WAN y/o LAN, permitiendo conectar múltiples segmentos de red.

pfSense implementa una gran variedad de servicios que pueden ser útiles para todo tipo de usuarios, por ejemplo, permite organizar dispositivos y reglas locales mediante redes virtuales (VLANs), permite equilibrar la carga de red entre diferentes redes WAN (load Balancing), para mantener la disponibilidad en infraestructura crítica es posible configurar un cluster de alta disponibilidad (HA) para evitar el tiempo de inactividad.

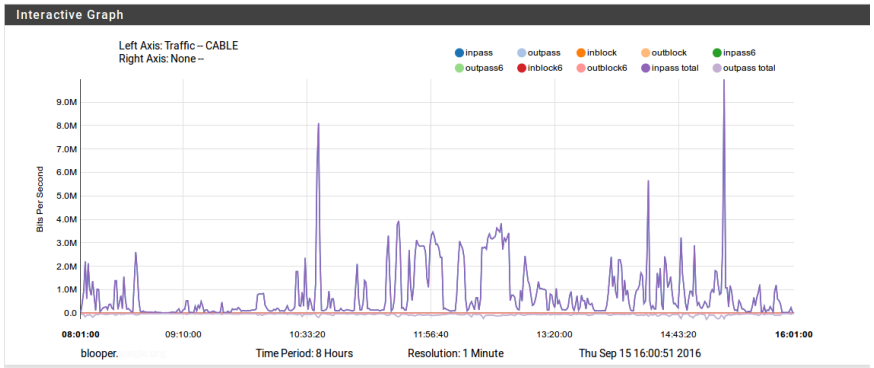
- **Servidor de VPN** [7.3]

pfSense implementa varios servicios de VPN (Ipsec, OpenVPN, WireWard) en conjunto con las funcionalidades anteriores, esto puede usarse para conectarse de manera remota a las redes locales administradas por pfSense o como relay para pasar todo el tráfico de red de un dispositivo remoto a través de la VPN



- **Monitoreo** [7.4]

pfSense permite monitorear el rendimiento y comportamiento de las funcionalidades mencionadas anteriormente, recopila información durante la ejecución de las distintas funcionalidades y guarda bitácoras almacena datos en archivos RRD, a partir de estos archivos el sistema puede generar gráficas para facilitar la visualización de la información, también permite analizar el tráfico de red mediante una interfaz web para el analizador de paquetes tcpdump



Data Summary

	Minimum	Average	Maximum	Last	95th Percentile
inpass	16.52 kb/s	817.76 kb/s	9.96 Mb/s	0.00 b/s	3.12 Mb/s
outpass	12.44 kb/s	56.21 kb/s	262.97 kb/s	0.00 b/s	122.66 kb/s
inblock	0.00 b/s	7.27 b/s	676.90 b/s	0.00 b/s	
outblock	0.00 b/s	0.04 b/s	11.54 b/s	0.00 b/s	
inpass6	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s
outpass6	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s
inblock6	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	
outblock6	0.00 b/s	0.00 b/s	0.00 b/s	0.00 b/s	
inpass total	16.52 kb/s	817.76 kb/s	9.96 Mb/s	0.00 b/s	3.12 Mb/s
outpass total	12.44 kb/s	56.21 kb/s	262.97 kb/s	0.00 b/s	122.66 kb/s

8. Extensión de funcionalidad con paquetes [8.1 8.2]

- **Manejo de paquetes**

pfSense permite extender su funcionalidad mediante la instalación de paquetes de software, algunos de estos paquetes son desarrollados directamente por netgate pero la gran mayoría son desarrollados por la comunidad, esto se puede hacer directamente desde la interfaz web sin que el usuario se involucre directamente con el manejador de paquetes de FreeBSD.

La administración de paquetes para pfSense se realiza a través de la interfaz web, desde aquí se puede instalar, actualizar o eliminar paquetes.

- **Paquetes comúnmente usados**

Algunos paquetes comúnmente utilizados son:

· Opciones de filtrado adicional (pfBlockerNG)

· Detección / prevención de intrusión (Snort)

· VPNs adicionales (Wireguard, Tinc)

· Monitoreo de ancho de banda (ntopng)

· Utilidades de red como nmap, iperf, arping

· Etc.

9. Desventajas y limitantes [9.1] [9.2] [9.3]

- **Soporte limitado**

PfSense es un proyecto de código abierto y no ofrece soporte oficial para usuarios, la ayuda está limitada a aquella que pueda proveer la comunidad de usuarios.

Además del soporte para problemas el soporte de hardware puede llegar a ser limitado, las actualizaciones son poco frecuentes por lo que la compatibilidad con nuevo hardware puede ser un tema complicado.

- **Dificultades con implementaciones a gran escala o de necesidades específicas.**

Dado que pfSense está pensado para funcionar para una gran variedad de usuarios la configuración necesaria para una implementación a gran escala o para aplicaciones muy específicas puede ser muy compleja o simplemente imposible, en este aspecto a veces puede ser más práctico el uso de equipos especializados de compañías como CISCO/HP.

- **Ediciones Community y Plus**

Desde 2021 netgate comenzó a segmentar su producto en pfSense Community edition (el sujeto de esta investigación) y pfSense Plus, una versión de paga del software orientada a las necesidades del sector empresarial, esto ha puesto en duda la continuidad del proyecto ya que las actualizaciones se han vuelto menos frecuentes.

Fuentes bibliográficas.

- **Por capítulo.**

1. Introducción a pfSense

1.1. https://www.enterprisenetworkingplanet.com/guides/best-firewall-software/#pfsense
1.2. https://www.enterprisenetworkingplanet.com/security/enterprise-firewalls/
1.3. https://www.peerspot.com/products/comparisons/cisco-secure-firewall_vs_fortinet-fortigate_vs_netgate-pfsense

2. FreeBSD

2.1. https://docs.freebsd.org/en/books/handbook/
2.2. https://docs.netgate.com/pfsense/en/latest/
2.3. https://www.bsdnow.tv/
2.4. https://www.reddit.com/r/freebsd/

3. Historia y desarrollo de pfSense

3.1. https://en.wikipedia.org/wiki/PfSense
3.2. https://m0n0.ch/wall/index.php
3.3. https://www.vskills.in/certification/tutorial/history-and-applications/#:~:text=History%20of%20pfSense:%20The%20development%20of%20pfSense%20started%20as%20a
3.4. https://docs.netgate.com/pfsense/en/latest/general/

4. Arquitectura de pfSense

4.1. https://docs.netgate.com/pfsense/en/latest/network/
4.2. https://docs.freebsd.org/en/books/handbook/firewalls/#firewalls-pf
4.3. https://docs.netgate.com/pfsense/en/latest/firewall/
4.4. https://docs.freebsd.org/en/books/handbook/jails/
4.5. https://freebsdfoundation.org/freebsd-kernel-development-workflow/
4.6. https://docs.netgate.com/pfsense/en/latest/packages/
4.7. https://docs.netgate.com/pfsense/en/latest/config/
4.8. https://docs.netgate.com/pfsense/en/latest/services/
4.9. https://forum.netgate.com/category/72/plugin-development
4.10. https://docs.freebsd.org/en/books/handbook/jails/
4.11. https://www.openbsd.org/faq/pf/
4.12. https://man.freebsd.org/cgi/man.cgi?query=altq
4.13. https://man.freebsd.org/cgi/man.cgi?query=geom
4.14. https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/

5. **Características importantes de pfSense**

    5.1. https://docs.netgate.com/pfsense/en/latest/firewall/fundamentals.html
    5.2. https://docs.netgate.com/pfsense/en/latest/firewall/rules.html
    5.3. https://docs.netgate.com/pfsense/en/latest/firewall/aliases.html
    5.4. https://docs.netgate.com/pfsense/en/latest/firewall/layer7.html
    5.5. https://docs.netgate.com/pfsense/en/latest/nat/outbound.html
    5.6. https://docs.netgate.com/pfsense/en/latest/nat/port-forward.html
    5.7. https://docs.netgate.com/pfsense/en/latest/nat/1-1.html
    5.8. https://docs.netgate.com/pfsense/en/latest/services/upnp.html
    5.9. https://docs.netgate.com/pfsense/en/latest/vpn/ipsec/index.html
    5.10. https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/index.html
    5.11. https://docs.netgate.com/pfsense/en/latest/vpn/wireguard/index.html
    5.12. https://docs.netgate.com/pfsense/en/latest/packages/vpn-client-export.html
    5.13. https://docs.netgate.com/pfsense/en/latest/packages/snort.html
    5.14. https://docs.netgate.com/pfsense/en/latest/packages/suricata.html
    5.15. https://docs.netgate.com/pfsense/en/latest/interfaces/index.html
    5.16. https://docs.netgate.com/pfsense/en/latest/packages/snort/updates.html
    5.17. https://docs.netgate.com/pfsense/en/latest/multiwan/load-balance-and-failover.html
    5.18. https://docs.netgate.com/pfsense/en/latest/multiwan/index.html
    5.19. https://docs.netgate.com/pfsense/en/latest/routing/gateways.html
    5.20. https://docs.netgate.com/pfsense/en/latest/highavailability/index.html
    5.21. https://docs.netgate.com/pfsense/en/latest/trafficshaper/limiters.html
    5.22. https://docs.netgate.com/pfsense/en/latest/trafficshaper/index.html
    5.23. https://man.freebsd.org/cgi/man.cgi?query=altq
    5.24. https://www.netgate.com/resources/videos-traffic-shaping-basics-with-priq-on-pfsense
    5.25. https://docs.netgate.com/pfsense/en/latest/monitoring/graphs/index.html

6. **Instalacion y configuracion**
    6.1. https://docs.netgate.com/pfsense/en/latest/hardware/minimum-requirements.html
    6.2. https://docs.netgate.com/pfsense/en/latest/install/index.html#
7. **Casos de uso**
    7.1. https://medium.com/@fahriiyesill/unleashing-the-power-of-pfsense-an-open-source-network-security-platform-b107f5d9d08f
    7.2. https://docs.netgate.com/pfsense/en/latest/general/common-deployments.html
    7.3. https://docs.netgate.com/pfsense/en/latest/vpn/common-deployments.html
    7.4. https://docs.netgate.com/pfsense/en/latest/monitoring/graphs/working.html
8. **Extensión de funcionalidad con paquetes**
    8.1. https://docs.netgate.com/pfsense/en/latest/packages/index.html
9. **Desventajas y limitantes**
    9.1. https://www.itandgeneral.com/the-journey-from-pfsense-ce-to-netgate-pfsense-plus-commercial-use-professional-support-and-migration-help/
    9.2. https://docs.netgate.com/pfsense/en/latest/general/plus.html

9.3. https://docs.netgate.com/pfsense/en/latest/general/help.html