Principales características pfSense

pfSense® es una distribución, **open source** basada en **FreeBSD**, personalizada para ser un **firewall** y **router**. Encima de ser una potente plataforma **firewall** y **router**, incluye una gran lista de paquetes que permiten expandir facilmente las funcionalidades sin comprometer la seguridad del sistema.

pfSense® es un proyecto abundantemente probado, cuenta con más de 1.000.000 usuarios e **innumerables instalaciones** en todo el mundo, desde el uso casero hasta la **grande empresa**, **autoridades públicas**, **privadas** y **universidades**.

Características principales

pfSense® incluye casi todas las funcionalidades de los costosos **firewall** comerciales y en muchos casos incluye en más. La siguiente es una lista de las funciones actualmente disponibles. Todas las funciones que siguen son administrables con interfaz web, sin la ayuda de la consola (sin líneas de comando).

Esta página incluye también la descripción de las limitaciones que actualmente conocemos. Por nuestra experiencia y por la experiencia de miles de usuarios sabemos muy bien lo que **pfSense®** puede o no puede hacer. Cualquier software tiene limitaciones. Nosotros nos distinguimos de otros porque comunicamos este concepto. Son bienvenidas todas las personas que quisieran contribuir a eliminar estas limitaciones. Muchas de estas limitaciones son las mismas de otros productos comerciales.

Firewall

Filtrado de origen a destino de IP, protocolo IP, puerto de origen y destinación para TCP y UDP tráfico
Habilitación de límites para conexiones simultaneas con reglas de base
pfSense® utiliza p0f, una avanzada herramienta de red para huellas dactilares digitales que habilita la **filtración** a través el sistema operativo al inicio de la conexión Option to log or not log traffic matching each rule Politicas de enrutamiento con alta flexibilidad para la seleccion del gateway sobre las reglas de base para el equilibrio de banda, failover, WAN multiple, backup sobre mas ADSL, etc…
Posibilidad de creacion de Alias de grupos de IP y nombres de IP, networks y puertas. Estas caracteristicas ayudan a mantener la configuracion limpia y facil de entender, especialmente con configuraciones con varios IP publicos y numerosos Servers
Filtracion transparente Layer 2. Posibilidad de puentear interfaces y filtrar el trafico entre estas
Normalización de paquete. Descrito en la documentación de pf Scrub. (Mira la documentación). Habilitado de norma. Es posible desactivarlo si es necesario
Posibilidad de inhabilitar la **filtración** (firewalling) para utilizar **pfSense®** como solo **router**

Digital – Mind
+52 (722) 2276149
info@digitalmind.com.mx
www.digitalmind.mx

State Table (tabla de estado)

La tabla de estado del **firewall** mantiene informaciones de las conexiones abiertas. **pfSense®** es un stateful firewall, por defecto todas las reglas son stateful. Muchos firewall No tienen la capacidad de controlar la tabla de estados. pfSense® tiene muchas funciones en grado de hacer un control granular de la tabla de estado, gracias a las caracteristicas de OpenBSD's pf.

Regulacin del tamaño de la tabla de estado – existen muchas **instalaciones de pfSense®** que usan diferentes cientos de estados. De norma la tabla de estado varía segun la RAM instalada en el sistema, pero puede ser aumentada en tiempo real a la dimension deseada. Cada estado ocupa aproximadamente 1 KB de RAM, este parámetro viene mantenido en la mente cuando se deve dimensionar la memoria.

Reglas de base:
Limites de conexiones simultáneas de clientes
Limites de estado para host
Limites de nuevas conexiones al segundo
Definir el estado de timeout
Definir el tipo de estado

Tipos de estado – **pfSense®** ofrece numerosas opciones para la gestion del estado.
Keep state – Trabaja con todos los protocolos. De norma con todas las reglas
Modulate state – Trabaja solo con TCP. **pfSense®** generará ISNs (Initial Sequence Numbers) por cuenta de el host
Synproxy state – Los Proxy inician las conexiones TCP para ayudar los server de spoofed TCP SYN floods
None – No se mantiene ninguna informacion sobre el estado

Opciones de optimización de la tabla de estado – **pfSense®** ofrece cuatro estados para la optimización de la tabla de estado
Normale – de norma
Hight latency – usada para links de alta latencia, como enlaces por satélite
Aggressive – fecha límite del estado de idle mas veloz. Mas eficiente usando mas recursos hardware, pero puede eliminar conexiones correctas
Conservative – Trata de evitar la cancelación de conexiones correctas a costa de mayor utilizo de CPU y RAM

NAT: Network Address Tranlation

El Port forwards incluye un rangos y uso de IP publicos múltiple
NAT 1:1 para IP individuales o enteras subredes
Outband NAT
Impostado de norma, todo el trafico en salida al IP de la WAN. En configuraciones con WAN múltiples, vendra usado el trafico en salida al IP de la interfaz WAN
Advanced Outbound NAT
NAT Reflection – en alguna configuracion, NAT Reflection es utilizado para servicios que pueden acceder con IP publicos desde redes internas

Digital – Mind
+52 (722) 2276149
info@digitalmind.com.mx
www.digitalmind.mx

NAT Limitation

PPTP / GRE Limitation – El monitoreo del estado de colas en **pfSense®** para el protocolo GRE puede monitorar una sola sesion por IP publico para **server** externo. Esto significa que si usan conexiones PPTP VPN, solo una máquina interna podra conectarse simultáneamente al PPTP server en internet. Miles de máquinas pueden conectarse simultáneamente con miles de server PPTP, pero solo uno simultáneamente podra conectarse a un server PPTP. El unico modo para evitar el problema es utilizar IP publicos diferentes en el **firewall**, uno para el client, o usar ip publicos múltiples para los PPTP server. Este problema No existe para conexiones VPN con diferentes protocolos. La solucion a este problema es actualmente en desarrollo.

Redundancia

El protocolo CARP de OpenBSD gestiona el hadware failover. Dos o mas grupos de **firewall hardware** pueden ser configurados como un grupo de failover. Si una interfaz se malogra en el dispositivo primario o el dispositivo primario pasa a offline, el segundo dispositivo se activa. pfSense® incluye tambien capacidad de sincronización automatica entre el dispositivo primario y el secundario. pfsync asegura que la tabla de estado del **firewall** sera reproducida en todos los firewall inseridos en el failover. Esto significa que las conexiones existentes seran mantenidas en caso de falla(failure).

Limitaciones

Funciona solo con IP publicos estáticos, No funziona con stateful fileover usando DHCP, PPPoE o PPTP en la red WAN.

Balance de Cargo

Balance de cargo en salida: (Outbound)
El load balancing en salida es usado en red WAN múltipla para brindar balanceo y failover. El trafico es directo a un gateway designado o a un pool de balanceo de cargo definido en las reglas de base del **firewall**.

Inbound Load Balancing

El balanceo de cargo en entrada es usado para distribuir el cargo entre los servers. Es comúnmente usado para **server web**, **server de posta electronica** y otros. Los server que No responden al ping o conexiones TCP en la puerta definida seran excluidos por el pool.

VPN

pfSense® ofrece tres opciones para la conectividad VPN, IPsec, OpenVPN, e PPTP.

IPsec

IPsec consiente conectividad con todos los dispositivos que soportan el standard IPsec. Esto es de uso comun en las configuraciones site to site con otros dispositivos **pfSense®**. Otros **firewall** open source como m0n0wall y muchos otros **firewall**comerciales como Cisco, Juniper, etc... la implementan. Es usada a menudo en las conexiones client mobile.

Digital – Mind
+52 (722) 2276149
info@digitalmind.com.mx
www.digitalmind.mx

OpenVPN

OpenVPN es una flexible, potente solucion SSL VPN que soporta una ampla gama de sistemas operativos client. Para mas informacion lee mas: OpenVPN.

PPTP Server

PPTP es un sistema VPN muy popular porque instalado en casi todos los sistemas operativos client incluidos todos los sistemas operativos Windows a partir de Windows 95 OSR2. Mira la documentacion para mayor informacion. El server **pfSense®** PPTP puede usar un database locale o un RADIUS server para la autenticación. La compatibilidad RADIUS es tambien soportada.

PPPoE Server

pfSense® ofrece un **server** PPPoE. para mayor informacion sobre protocolo PPPoE, mira la documentacion. Los usuarios locales del database pueden ser usados para la autenticación y la autenticación RADIUS con opciones de accounting es tambien soportada.

Reportes y Monitoreo

Gráficos RRD. Los gráficos RRD en **pfSense®** ofrecen las seguientes informaciones:
Utilizo de la CPU
Tráfico total
Estado del **firewall**
Tráfico individual de las interfaces
Packets por second-rates para todas las interfaces
Tiempo de respuesta a el ping del gateway de la interfaz WAN
Cola de tráfico shaper sobre el sistema si el tráfico shaper esta abilitado

Real Time Information

Las informaciones sobre la historia del sistema son importantes, pero a veces son mas importantes las informaciones en tiempo real. Los gráficos SVG muestran el tráfico en tiempo real para todas las interfaces. La pagina inicial incluye gráficos AJAX que muestran en tiempo real el cargo de la CPU, memoria, swap y espacio disco usado y la tabla de estado.

Digital – Mind
+52 (722) 2276149
info@digitalmind.com.mx
www.digitalmind.mx

DNS Dinámica

El client de DNS Dinámica activa la registracion mediante uno de los siguientes servicios:

- DynDNS
- DHS
- DNSexit
- DyNS
- EasyDNS
- FreeDNS
- HE.net
- Loopia
- Namecheap
- No-IP
- ODS.org
- OpenDNS
- ZoneEdit

Captive Portal

El captive portal permite de forzar la autenticacion o redirigir el tráfico de red a una pagina de autenticación de red. Esto es comunmente usado en las conexiones de red hot spot, ampliamente usada tambien para niveles de seguridad adicionales en el acceso de redes internet a travez sistemas wireless. Para mayor informacion sobre Captive Portal se vea esta pagina. La que sigue es una lista de funciones y caracteristicas del Captive Portal.
conexiones maximas competidoras - Límite al numero de conexiones competidoras para cada IP client. Esta funcionalidad impide ataques DOS
Idle timeout – Desconecta los client que No efectuan conexiones por mas de un cierto numero de minutos
Hard timeout – Fuerza la desconexión de client conectados por mas de un numero definido de minutos
Pop up de logon – Opcion de pop up de la ventana con pulsante de desconexión
URL Redirection – despues de la autenticación los usuarios pueden ser direccionados a una pagina definida de norma
MAC Filtering – de norma **pfSense®** usa el **filtración** direcciones MAC
Opciones de autenticación – existen tres metodos de autenticación
Ninguna autenticación: habilita la navegacion sin la inserción de ningun dato
Usuarios locales – el database de los usuarios locales puede ser configurado y usado para la autenticación
Autenticación RADIUS – Este es el metodo preferido por las empresas, entes y ISP. Puede ser usado con la autenticación de Microsoft Active Directory y numerosos otros server RADIUS
Capacidad de RADIUS
Forzar la re-autenticación
Activacion a el actualización de cuentas de usuarios
Autenticación MAC RADIUS habilita el Captive Portal en la autenticación de client usando el MAC address, username y password
Acepta configuraciones redundante de RADIUS Server
http e HTTPS – La pagina del portal puede ser configurada sea en http que en https
Pass-through MAC and IP addresses – Direcciones MAC y IP pueden ser inseridas en una white list sin pasar por el portal
File manager – Esto permite de cargar imagenes que pueden ser utilizadas en la pagina inicial del captive portal

DHCP Server and Relay

pfSense® incluye DHCP Server y funcionalidad Relay.