Características de integración de Firewall

Balanceo de Carga

- Balanceo de carga entrante: Es usado para la distribución de carga entre múltiples servidores. Esta característica es comúnmente usada en servidores web, de correo DNS y otros. De esta forma se puede hacer un clúster para conseguir una alta disponibilidad y/o un gran rendimiento.
- Balanceo de cargas saliente: Se usa para enviar el tráfico por distintos enlaces WAN para proveer calidad de servicio o redundancia. El trafico pude se distribuido a nivel de regla de firewall.

Firewall

- Filtrado por dirección IP origen y destino, por origen y destino de protocolos.
- Capaz de limitar las conexiones simultáneas por regla.
- Utiliza p0f, un avanzado sistema de detección de sistemas Operativos basados en el fingerprinting OS, el cual permite por ejemplo, para elevar la seguridad, solo los usuarios que se conecten mediante maquinas Linux o Unix se puedan conectar a los sistemas críticos y denegando usuarios que usen versión de Windows; o por cuestiones de soporte técnico solo permitir Sistemas Operativos aprobados etc.
- Habilitar el log para el tráfico que concuerda con una regla del firewall.
- Ruteo flexible para elegir a una puerta de enlace (Gateway) función del estado de una regala (por balanceo de carga, failover, múltiples rutas WAN etc.)
- Alias que permiten agrupar y nombrar IPs, Redes, y puertos. Esto ayuda a mantener su conjunto de reglas de cortafuegos limpio y fácil de entender, especialmente en entornos con múltiples IPs públicas y varios servidores. Por ejemplo si se tiene múltiples servidores de bases de datos, uno en mysql que corre en el puerto 3306 , Postgresql con el puerto 5432 y Oracle con el 1521, se puede crear una agrupación que incluya a todos estos servidores con un nombre de bases_datos.
- Capaz de filtrara en capa 2.
- Normalización de paquetes el cual protege a sistemas operativos que no manejan bien la fragmentación de paquetes.
- Deshabilitar el filtrado para fungir únicamente como Router.

NAT

- Reenvió de puertos, 1:1 NAT, NAT saliente etc.

Portal Cautivo

El portal cautivo permite forzar la autenticación de los usuarios redirigiéndolos a una página especial de autenticación y/o para aceptar los términos de uso, realizar un pago etc. para poder tener acceso a la red. El portal cautivo es usado comúnmente para contro de accesos a la red en lospuntos de accesos inalámbricos de los hoteles, restaurantes, parques y kioscos.

Las características que pfsense ofrece para la implementación de portales cautivos son:

- Limitar el número de conexiones concurrentes de una misma IP, para evitar denegación de servicio por clientes que envían tráfico repetidamente sin autenticación.
- Desconexion de a usuarios que se mantienen inactivos por un numero de minutos predefinidos.
- Redirección de URL, para llevar a los usuarios a una página predefinida antes durante y después de la autenticación.
- Filtrado de MACs.
- Múltiples métodos de autenticación, usuarios locales, Radius, y Microsoft Active Directory.
- El portal soporta ambos protocolos HTTP o HTTPS.
- Pagina web personalizable.

PPPoE Server

- pfSense incorpora un servidor para PPPoE. Los usuarios son autenticados por una base local, o vía Radius el cual ofrece auditoria.

Reduncia

La redundancia se logra por dos componentes:

- Por el protocolo de redundancia de dirección común (Common Address Redundancy Protocol) CARP, el cual permite que múltiples host en una red compartan un dirección cumun. Así dos o más firewalls pueden ser configurados como un grupo de conmutación por error (failover group). Si una de las interfaces falla en el firewall primario o por alguna razón deja de reponder, el firewall secundario toma el control de las

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

operaciones y se declara como primario. pfSense también sincroniza la configuración hacha en el firewall primario a todos los miembros de del grupo.

- Pfsync: asegura que la tabla de estado sea replicado a todos los firewall dentro del grupo de conmutación por error, el cual es importante para prevenir las interrupciones de servicios.
- Balanceo de carga saliente: Distribuye el tráfico hacia varias conexiones WAN.
- Balanceo de cargas entrante: Distribuye la carga hacia varios servidores. Comúnmente balanceando de tráfico web hacia múltiples servidores web. Si un servidor deja de responder se remueve del pool y automáticamente se agrega si se recupera

Reportes y Monitoreo

Graficas Históricas con RDD

- Las graficas RDD mantienen un historial con la siguiente información:
- Utilizacion de CPU
- Total throughput
- Estado del Firewall
- Throughput individual para todas las interfaces
- Paquetes enviados y recibidos por todas las interfaces
- Tiempos de respuestas
- Manejo de tráfico y ancho de banda

Información de Tiempo Real

- Uso de la memoria, CPU, memoria, throughput, por medio de graficas SVG, páginas construido en AJAX muestran el estado del funcionamiento en tiempo real del estado del firewall.

Servidor DHCP

Tabla de estado

- pfSense es un stateful firewall, el cual como característica principal guardad el estado de las conexiones abiertas en una tabla.

La mayoría de los firewall no tienen la capacidad de controlar con precisión la tabla de estado. pfSense tiene una enorme número de características que permiten una granularidad muy fina para el manejo de la tabla de estado.

- Tabla de estado ajustable. El tamaño por defecto de la tabla es de 10000 pero se puede incrementar en tiempo de ejecución dependiendo a los requerimientos. Cada estado ocupa 1 KB de RAM, tener en cuenta la memoria disponible a la hora de incrementar el tamaño.
- Limites por regla:
- Limitar las conexiones simultaneas por cliente
- Limitar el estado por host
- Limite de conexiones por segundo.
- Definir el tiempo de cada conexión
- Definir el tipo de estado
- Tipos de estado
- Mantener el estado
- Módulos de estado para fuertes números de secuencia inicial (ISN).
- Synproxy: Protege de ataques de TCP S
- Opciones de optimización de estado:
- Normal – El algoritmo por defecto
- Alta latencia - Útil para enlaces de alta latencia, como las conexiones por satélite. Expira conexiones inactivas después de lo normal.
- Agresivo - Expira conexiones inactivas más rápidamente. Un uso más eficiente de los recursos de hardware, pero pueden interrumpir las **conexiones legítimas.**
- Conservadora - Trata de evitar que se caiga las conexiones legítimas a expensas de aumentar el uso de memoria y la utilización de la CPU.

VPN

- Ofrece capacidad para realizar conexiones VPN con distintos protocolos IPSec, PPTP, VPN sobre SS

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