# Síntesis conceptual

| |
|---|
| **Grado**: Administración de Sistemas Informáticos |
| **Asignatura**: Seguridad y alta disponibilidad |
| **Unidad**: 4. El cortafuegos |

## Resumen

Cortafuegos: Analiza todos los paquetes de datos que entran y salen por sus interfaces y, apoyándose en un conjunto de reglas, determinan de qué manera actuar con cada uno de ellos, es decir, aceptando o rechazando el mensaje. Los routers contienen sus propios cortafuegos de tipo *hardware* los cuales emplean un software particular, el *firmware.*

Es conveniente poseer unos determinados conocimientos sobre el funcionamiento de netfilter e iptables para que nos sirvan de base en su configuración a nivel profesional.

- Conexiones de red: tráfico de paquetes que se establece entre una dirección IP origen y destino respectivamente utilizando el protocolo TCP o UDP.
- Reglas, cadenas y políticas de cadena: Las reglas se organizan en un sistema que llamamos cadena(chain). Una cadena es un conjunto de reglas que se calculan para cada paquete. Si el paquete cumple cierta condición, se le aplica la acción definida en esa regla y se interrumpe su ejecución. Si, por el contrario, no cumple con ninguna regla determinada, el kernel asigna a dicho paquete la acción por defecto establecida, llamada política de la cadena. En cualquier cortafuegos siempre encontraremos 3 cadenas predefinidas: INPUT, OUTPUT y FORWARD.
- Tablas: Las cadenas se organizan en tablas. Contiene 4 tablas, cada una con un conjunto de cadenas predefinidas.
    - Tabla filter: Todos los paquetes pasan por esta tabla. Aquí podemos filtrar dichos paquetes para adoptar políticas pertinentes, ya sea para permitir o denegar un paquete su camino.
    - Tabla nat: El primer paquete de conexión pasa por esta tabla, aunque su uso es para reescribir los paquetes y alterar su destino.
    - Tabla mangle: Conjunto de reglas que pretendan modificar cualquiera de sus campos. Su principal uso es la implantación de calidad del servicio (QoS).
    - Tabla raw: Reglas que se aplican a los paquetes antes de que pasen por una evaluación o reciban cambios por cadenas de otras tablas.

Linux se incluye un módulo del kernel que se llama netfilter, el cual actúa de cortafuegos.

De manera predeterminada, todos los equipos Linux tienen “deshabilitado” el cortafuegos, es decir, a todos los paquetes se le aplica la acción ACCEPT. No ocurre lo mismo en equipos Windows. La configuración del cortafuegos de Linux se realiza con el comando iptables.

Iptables es una utilidad de línea de comandos para configurar el firewall del kernel de Linux que se implementó como parte del proyecto Netfilter. El término iptables también se usa

comúnmente para referirse a un firewall de kernel. Es un firewall altamente configurable y flexible como la mayoría de las herramientas de Linux.

Firewall Builder es una herramienta de administración de firewall multiplataforma que le permite agrupar y administrar firewalls para diferentes sistemas operativos, brindando la opción de control remoto. Algunas de las características que podemos destacar de Firewall Builder son:

- Objetos: con él, puede especificar las direcciones de los dispositivos en los que desea aplicar el firewall y también administrarlos a través de este software.
- Nuevo Objeto: menú a través del cual se pueden crear nuevos clusters, hosts, redes, nuevo rango de direcciones, servicios IP, servicios ICMP, etc.
- Crear un nuevo cortafuegos: puede crear un nuevo firewall después de seleccionar el dispositivo y el enrutador al que desea aplicar el firewall.
- Reglas: puede crear reglas de firewall personalizadas para cada dispositivo al que desee aplicar el firewall.

Windows posee su propio *firewall* Windows Defender, el cual es suficiente para una conexión doméstica. Windows permite activar o desactivar el *firewall*, tanto a nivel general como para aplicaciones específicas. Podemos llevar a cabo una configuración mucho mayor entrando en el menú contextual, botón derecho, como los tipos de reglas predeterminadas o los tipos de reglas de seguridad de conexión.

## Conceptos fundamentales

- **Timeout**: Tiempo transcurrido con una conexión activa sin que ocurra nada, tras un tiempo de esto la conexión se finaliza sola.

- **INPUT**: Una conexión entrante, implica que el primer paquete es recibido desde otro equipo.

- **OUTPUT**: Una conexión saliente, implica que el primer paquete es originado por el propio equipo y enviado hacia el exterior.

- **FORWARD**: conexiones enrutadas, paquetes de datos que entran por alguna de las interfaces, pero vuelven a salir por otra ya que el destino es otro equipo diferente

- **Webmin**: En Linux, es un servidor web al que se acede por el puerto 10.000. Permite a cualquier administrador del sistema gestionar de una manera centralizada, gráfica y remota una cantidad de funcionalidades y servicios.