TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 4 – UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

Lección 4: Firewalls

Un firewall es un componente esencial en la seguridad informática diseñado para monitorear y controlar el tráfico de red que entra y sale de un sistema o red. Funciona como una barrera entre redes confiables e inseguras, como Internet, permitiendo o bloqueando paquetes de datos según un conjunto de reglas predefinidas. Los firewalls pueden ser hardware, software o una combinación de ambos, y su principal objetivo es prevenir accesos no autorizados mientras permiten la comunicación legítima.

En un entorno corporativo, los firewalls ayudan a resguardar información sensible, impedir intrusiones y limitar el alcance de posibles ataques. También se utilizan para segmentar redes, permitiendo que diferentes departamentos operen en áreas protegidas de la red para reducir el impacto de posibles brechas. Los usuarios individuales pueden beneficiarse de los firewalls instalados en sus dispositivos personales, asegurándose de que solo las aplicaciones autorizadas se conecten a Internet e intercambien datos.

Además, soluciones modernas como los firewalls de próxima generación (NGFW) combinan capacidades tradicionales con funciones avanzadas, como inspección profunda de paquetes y detección basada en inteligencia artificial.

El principal beneficio de usar un firewall es su capacidad para prevenir accesos no autorizados a redes y dispositivos. Además, permiten una gestión centralizada de la seguridad en redes complejas, simplificando la implementación de políticas de seguridad. Los firewalls también mejoran el rendimiento de la red al bloquear tráfico innecesario o malicioso y garantizan el cumplimiento de normativas específicas al proteger datos sensibles.

El firewall funciona inspeccionando las cabeceras HTTP de los paquetes que entran a una red o a un dispositivo. Al analizar las cabeceras HTTP encuentran las direcciones IP de origen y de destino, los puertos a los que una comunicación va dirigida y los datos. De esta forma se puede identificar un ataque o una serie depaquetes sospechosos. La forma en la que se determina qué paquetes se deja pasar y cuales se bloquean es por medio de reglas.

Cada regla o política de firewall es definida por la persona que administra una red. En las políticas se describe qué protocolos puede usar una comunicación (TCP o UDP) qué paquetes son permitidos y cuales no y qué orígenes se admiten o bloquean.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT

El análisis que realiza un firewall puede ocurrir en diferentes niveles del modelo OSI. Un firewall tradicional opera principalmente en las capas de red y transporte, evaluando direcciones IP y puertos. Por otro lado, un firewall de próxima generación (NGFW) también puede operar a nivel de la capa de aplicación, analizando el contenido de los datos para identificar amenazas más complejas, como malware o intentos de phishing. En cualquier caso, el firewall actúa como un guardián que asegura que solo el tráfico legítimo pase al sistema o red protegida

.

Los puertos son un concepto fundamental en la comunicación TCP/IP, ya que representan puntos virtuales de conexión en un dispositivo. Cada puerto está asociado con un número único que identifica un tipo específico de servicio o aplicación en la red. Por ejemplo, el puerto 80 se utiliza comúnmente para tráfico HTTP, mientras que el puerto 443 está reservado para HTTPS. Cuando un dispositivo quiere comunicarse con otro, envía datos a una dirección IP específica y un puerto determinado, asegurando que los datos lleguen al servicio correcto.

En el contexto de un firewall, los puertos desempeñan un papel clave en la creación de reglas de filtrado. Un administrador puede decidir bloquear o permitir tráfico en ciertos puertos para limitar el acceso a servicios específicos. Por ejemplo, podría cerrar el puerto 23 (usado para Telnet) por motivos de seguridad y permitir solo el puerto 22 (usado para SSH) para conexiones remotas seguras. Esta capacidad de gestionar puertos permite un control granular del tráfico y ayuda a mitigar riesgos asociados con servicios vulnerables o no utilizados.

- La gestión de puertos y el filtrado de tráfico son esenciales para la seguridad de la red, ya que muchos ataques aprovechan puertos abiertos o mal configurados para infiltrarse en un sistema. Configurar un firewall para supervisar y restringir el uso de puertos según las necesidades de la red es una de las mejores prácticas para reducir la superficie de ataque y proteger tanto los dispositivos como la información.

Algunos puertos que se han estandarizado para comunicaciones de forma arbitraria o por motivos de uso histórico son:

- 20: FTP (Protocolo de Transferencia de Archivos, canal de datos).
- 21: FTP (Protocolo de Transferencia de Archivos, canal de control).
- 22: SSH (Secure Shell, conexiones remotas seguras).
- 23: Telnet (Conexiones remotas inseguras, no recomendado).
- 25: SMTP (Protocolo para envío de correos electrónicos).
- 53: DNS (Sistema de Nombres de Dominio, resolución de nombres).
- 67: DHCP (Protocolo de Configuración Dinámica de Host, servidor).
- 68: DHCP (Protocolo de Configuración Dinámica de Host, cliente).
- 80: HTTP (Protocolo de Transferencia de Hipertexto, navegación web).
- 110: POP3 (Protocolo de oficina de correos, recepción de correos).

- 123: NTP (Protocolo de Tiempo de Red, sincronización de tiempo).
- 143: IMAP (Protocolo de Acceso a Mensajes de Internet, correos).
- 161: SNMP (Protocolo Simple de Administración de Red).
- 443: HTTPS (HTTP seguro, navegación web cifrada).
- 465: SMTP sobre SSL/TLS (Envío seguro de correos).
- 514: Syslog (Registro de eventos y logs).
- 993: IMAP sobre SSL/TLS (Acceso seguro a correos).
- 995: POP3 sobre SSL/TLS (Recepción segura de correos).
- 1433: Microsoft SQL Server.
- 1521: Oracle Database.
- 3306: MySQL.
- 3389: RDP (Protocolo de Escritorio Remoto).
- 5432: PostgreSQL.
- 5900: VNC (Virtual Network Computing, acceso remoto).
- 5985: WinRM (Microsoft Remote Management sobre HTTP).
- 5986: WinRM sobre HTTPS.
- 8080: HTTP alternativo o proxies web.
- 8443: HTTPS alternativo (servidores y aplicaciones).
- 5000: Servicios web y aplicaciones locales (Docker, Flask).
- 6379: Redis (almacenamiento en memoria).
- 8086: InfluxDB (base de datos de series temporales).
- 9000: MinIO (almacenamiento S3 compatible).
- 9200: Elasticsearch (búsqueda y análisis).
- 27017: MongoDB.

Dependiendo de las configuraciones que un equipo o una red requiera, se pueden permitir las salidas y entradas por algunos de los puertos listados y se bloquean todas las demás. La regla generalmente es ser estricto en el bloqueo ya que, si algo falla, los usuarios suelen reportar. Sin embargo, si hay más puertos abiertos que los necesarios, casi nunca hay reportes de estas situaciones favoreciendo que atacantes tengan la oportunidad de intentar vulnerar una red o un equipo.

Los firewalls ayudan a evitar el escaneo de puertos por parte de atacantes y a prevenir ataques DoS y DDoS bloqueando las solicitudes provenientes de direcciones IP identificadas como maliciosas. De esta forma no se sobrecarga la capacidad de cómputo creando respuestas, sino que se usa una pequeña porción rechazando las solicitudes.