# Laboratorio 28

Políticas permisivas:

| Política de Firewall | Descripción | Ejemplo / Caso de uso |
|---|---|---|
| **Política de control de contenido** | Bloquea ciertos tipos de contenido web. | Denegar acceso a Facebook, YouTube, etc., pero permitir navegación general. |
| **Política de bloqueo temporal o condicional** | Se bloquea algo solo bajo ciertas condiciones (como horarios o volumen). | Bloquear descargas grandes durante el horario laboral. |
| **Política de bloqueo reactivo (por eventos)** | Se activa cuando se detecta un evento sospechoso. | Bloquear una IP si genera muchas conexiones fallidas. |
| **Políticas de red global** | Se aplican a toda la red, permitiendo el tráfico en general con restricciones específicas. | En una universidad, permitir acceso general a internet, pero bloquear puertos como Telnet. |
| **Políticas de red regional** | Aplican a subredes específicas, con reglas más detalladas. | En una empresa, la sede de I+D tiene acceso más libre que la sede administrativa. |
| **Políticas de primera y última ejecución** | Definen el orden en que se evalúan las reglas: primero se aplican bloqueos, luego reglas permisivas. | Bloquear todo acceso externo a la base de datos, luego permitir tráfico web general. |
| **Políticas basadas en identidad** | Permiten/deniegan acceso según el usuario autenticado (VPN, LDAP, certificados). | Solo empleados autenticados por VPN pueden acceder a recursos internos. |
| **Políticas basadas en tiempo** | Restringen conexiones después de cierto tiempo de inactividad o en horarios específicos. | El acceso a servidores está limitado al horario laboral (8:00 a.m. a 6:00 p.m.). |
| **Políticas basadas en aplicación o servicio** | Permiten o bloquean tráfico según la aplicación o protocolo usado. | En una escuela, solo se permite HTTP/HTTPS y plataformas educativas; se bloquea P2P y redes sociales. |

**Políticas Restrictivas:**

| Tipo de Política | Descripción | Ejemplo Práctico |
|---|---|---|
| **Política de denegación por defecto** | Bloquea todo el tráfico a menos que haya una regla explícita que lo permita. | Se bloquea todo y se permite solo acceso HTTP/HTTPS al servidor web corporativo. |
| **Reglas de entrada** | Controlan el tráfico que intenta ingresar a la red. | Solo se permite tráfico entrante al puerto 443 (HTTPS) desde IPs de confianza. |
| **Reglas de salida** | Controlan el tráfico que sale de la red. | Se permite todo el tráfico de salida excepto FTP y puertos no autorizados. |
| **Políticas jerárquicas** | Permiten aplicar reglas de forma centralizada y organizada en toda la organización. | Un grupo de políticas se aplica a todos los firewalls de sucursales desde la sede. |
| **Políticas basadas en roles** | Restringen quién puede ver o modificar las reglas del firewall, según su rol o perfil. | Solo los administradores de red pueden cambiar las reglas; los técnicos solo visualizan. |
| **Políticas basadas en grupos de recursos** | Asocian reglas de firewall a recursos agrupados (servidores, subredes, etc.). | Se aplican reglas específicas a todos los servidores del grupo “Producción Web”. |
| **Políticas perimetrales** | Filtran el tráfico entre la red interna y externa, actuando como primera línea de defensa. | Se bloquea todo el acceso externo salvo VPN y correo corporativo cifrado. |
| | | |
| **Política basada en aplicaciones** | Permite solo ciertas aplicaciones (como DNS, HTTPS) y bloquea otras. | bloquear juegos en línea o redes P2P. |
| **Política de tráfico saliente restrictiva** | Solo se permite salir a ciertos destinos o servicios. | permitir que los usuarios solo accedan a ciertos sitios web o servicios de correo. |
| **Política de segmentación interna** | Restringe el tráfico entre subredes o departamentos internos. | no permitir que la red de usuarios acceda directamente a la red de servidores. |