Best practices a la hora de configurar un firewall

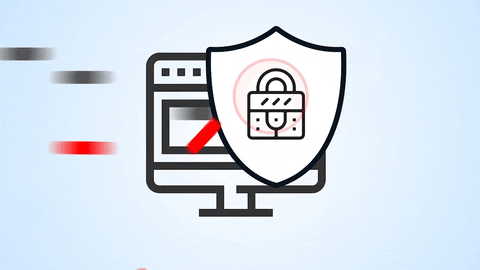
# **Configuraciones del Firewall | ¿Cuáles son las mejores prácticas y desafíos?**

La seguridad de sus usuarios y su red depende en gran medida de cómo esté configurado su cortafuegos. Las configuraciones de los firewalls varían mucho, principalmente debido al tamaño de cada corporación, las pequeñas empresas siguen el modelo de "configúrelo y olvídese", mientras que las grandes empresas suelen tener sus reglas de seguridad creadas una por una o utilizando automatizaciones y DevOps (*conjunto de prácticas que agrupan el desarrollo de software ( Dev ) y las operaciones de TI ( Ops* )).



## **¿Qué es la configuración de firewall?**

Los cortafuegos son un componente central de una estrategia de seguridad corporativa. Los cortafuegos pueden proteger contra ataques cibernéticos, fugas de datos y otras amenazas al monitorear el tráfico de la red y bloquear el tráfico sospechoso.



Los cortafuegos utilizan un conjunto de reglas o políticas predefinidas para determinar si se permite o bloquea una conexión. Estas reglas pueden especificar que se debe permitir o bloquear el tráfico a una dirección IP o puerto en particular. La configuración del firewall es el proceso de configurar estas reglas y configurar otras configuraciones de seguridad.

## **Desafíos de configuración de firewall**

La configuración adecuada del firewall es esencial para la ciberseguridad corporativa. Algunos errores comunes de configuración del firewall incluyen:

* **Políticas generalizadas**: Establecer políticas de firewall amplias puede ayudarlo a configurarlo más rápido, pero deja a su organización vulnerable a los ataques. Las políticas de firewall deben definirse en función de las necesidades comerciales y el principio de privilegio mínimo.
* **Defina sólo reglas de entrada**: A menudo, las políticas de firewall se centran en el tráfico entrante y las amenazas que se originan fuera de la organización. Sin embargo, permitir todo el tráfico saliente puede permitir la fuga de datos, ataques de malware C&C (Command and Control) y otras amenazas.
* **Métodos de autenticación fallidos** : el uso de métodos de autenticación ineficaces e inseguros puede socavar las políticas corporativas de autenticación y seguridad de contraseñas. Los cortafuegos deben configurarse para que sólo permitan métodos de autenticación sólidos, como la autenticación multifactor.
* **Falla al proteger el firewall**: Un firewall está diseñado para restringir el acceso a los recursos corporativos, pero también puede ser un objetivo de ataque. Dejar los puertos y los servicios de gestión de riesgos accesibles puede dar acceso a los ciberdelincuentes a la red corporativa.
* **Monitoreo inadecuado** : la configuración del firewall puede evitar que se bloqueen nuevas amenazas o bloquear nuevos tipos de tráfico comercial legítimo. El monitoreo regular es esencial para garantizar que cualquier intento de ataque se detecte y bloquee correctamente y que la configuración del firewall satisfaga las necesidades del negocio.

## **8 prácticas recomendadas de firewall para proteger su red**

La configuración de seguridad adecuada es esencial para que un firewall sea efectivo. Algunas mejores prácticas importantes son:

* **Asegure y configure adecuadamente el firewall** : si el proveedor aún no lo ha hecho, asegúrese de que el sistema operativo del firewall esté correctamente protegido y actualizado.
* **Planifique su implementación** : los firewalls definen los límites de la red, lo cual es esencial para la segmentación de la red y la seguridad Zero Trust. Las zonas de red deben definirse en función de las necesidades comerciales y, dado que un firewall es un posible punto único de falla, deben implementarse en un clúster de alta disponibilidad (HA) o mediante una solución de seguridad de red de hiperescala.
* **Proteger el cortafuegos** : los cortafuegos son la base de una arquitectura de seguridad de red y son objetivos de ataque comunes. Cambie las contraseñas predeterminadas y otras configuraciones similares para minimizar el riesgo de seguridad y cerrar los vectores de ataque comunes.
* **Cuentas de usuario seguras** : los ciberdelincuentes a menudo usan ataques de apropiación de cuentas para obtener acceso a los sistemas corporativos. Los administradores de firewall deben tener contraseñas seguras, habilitar la autenticación multifactor (MFA) y tener acceso limitado mediante controles de acceso basados ​​en roles (RBAC).
* **Bloquee las zonas de la red para que no accedan al tráfico aprobado** : los firewalls pueden restringir los flujos de tráfico dentro de los límites de la red que definen. Las políticas deben configurarse para permitir solo flujos de tráfico legítimos en función de las necesidades comerciales.
* **Asegúrese de que la política y el uso del cortafuegos se ajusten a los estándares de seguridad** : muchas normas y estándares incluyen requisitos para la configuración y las políticas del cortafuegos. Los reglamentos y normas aplicables deben revisarse para garantizar que las políticas se cumplan.
* **Prueba de política y riesgo** : las reglas de firewall incorrectas o ordenadas incorrectamente pueden bloquear el tráfico legítimo o permitir el tráfico malicioso. Todas las reglas del cortafuegos deben probarse con regularidad para garantizar que cumplen el propósito previsto.
* **Auditoría de software, firmware y registros** : el monitoreo de firewall y el análisis de registros son esenciales para identificar errores de configuración que pueden conducir a detecciones fallidas. Verifique periódicamente si hay actualizaciones de software o firmware y revise los registros en busca de tráfico anómalo.

**Fuente errores y mejores prácticas de configuración de firewall:**

[**HackAda » Errores y buenas prácticas en firewalls**](https://hackada.cl/errores-y-buenas-practicas-en-la-administracion-de-firewalls/) **(revisar en clase)**