Publicado en CDMX el 27/06/2023

# [Las 4 mejores prácticas que toda empresa que utiliza firewalls en su red debe conocer: Hillstone Networks](http://www.notasdeprensa.es)

## Tanto las PYMES como las grandes empresas confían en los firewalls para controlar el tráfico y el acceso a la red. Pero ningún firewall es perfecto. De hecho, un firewall será tan efectivo como las prácticas y políticas que lo soportan

 Hillstone Networks considera que se puede maximizar la protección del firewall siguiendo algunas de las mejores prácticas, todas ellas son fáciles de implementar y no requieren gran inversión de tiempo y recursos. A continuación, se comparten cuatro de estas prácticas: 1. Mantener las actualizaciones al díaLa estrategia más sencilla suele ser una que las empresas más descuidan: mantener las actualizaciones al día. Las amenazas evolucionan constantemente y para responder a ellas, los fabricantes de hardware y los desarrolladores de software lanzan actualizaciones periódicas de firmware. Cada nueva versión de firmware hace que un firewall sea más seguro. Las organizaciones no deben esperar a que una amenaza se convierta en un problema para buscar nuevas versiones. La forma más eficaz de garantizar que las amenazas no traspasen el firewall es asegurarse de que siempre se está ejecutando el firmware más reciente. Un retraso de una sola versión puede dejar vulnerable la red. 2. Parches actualizadosLos proveedores de firewalls lanzan parches de seguridad para solucionar vulnerabilidades entre las principales versiones de firmware. Siempre que un proveedor publique un parche de seguridad o hotfix, debe ser aplicado inmediatamente. Sin excepciones. Muchos parches de seguridad se publican debido a una amenaza inminente, se ha detectado una amenaza o se ha expuesto una vulnerabilidad. Entonces, es importante actuar con rapidez. 3. Utilizar políticas de autenticación avanzadasUn firewall es tan seguro como su capacidad para mantener alejadas a las partes no autorizadas. Los nombres de usuario y contraseñas ya no son suficientes; en su lugar, el acceso administrativo debe controlarse mediante políticas de autenticación avanzada. La autenticación multifactor es una buena opción. Puede evitar los intentos de pirateo por fuerza bruta cerrando cualquier oportunidad de iniciar sesión en el sistema de forma malintencionada. Otra buena opción es la contraseña de un solo uso. Otra alternativa es definir diferentes roles para la administración del firewall. El control de acceso basado en roles limita el acceso de los distintos administradores al sistema. Se pueden asignar privilegios a cada rol, mientras que a los administradores se les asignan roles basados en las tareas que es más probable que realicen. 4. Habilitar sólo los servicios necesariosLa mayoría de los firewalls ofrecen una gran lista de servicios y cada que uno está habilitado representa una posible vía de entrada. Así que, si los servicios no son necesarios, no deben ser habilitados; deben estar en trabajando sólo aquellos que  sean absolutamente necesarios para funcionar correctamente. Hillstone insta a las organizaciones a deshabilitar la administración remota siempre que sea posible. Incluso la administración remota mediante HTTPS y SSH puede ser innecesariamente arriesgada. Si la administración remota es necesaria, el acceso debe limitarse sólo a unas pocas personas elegidas en las que se pueda confiar para ocuparse del negocio. El firewall de una organización es la mejor línea de defensa contra una serie de amenazas diferentes. No seguir las mejores prácticas básicas para un firewall significa que las organizaciones no están obteniendo la máxima protección de su solución.

**Datos de contacto:**

Carlos Soto

Comunicación en Movimiento

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/las-4-mejores-practicas-que-toda-empresa-que](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Telecomunicaciones Programación Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)