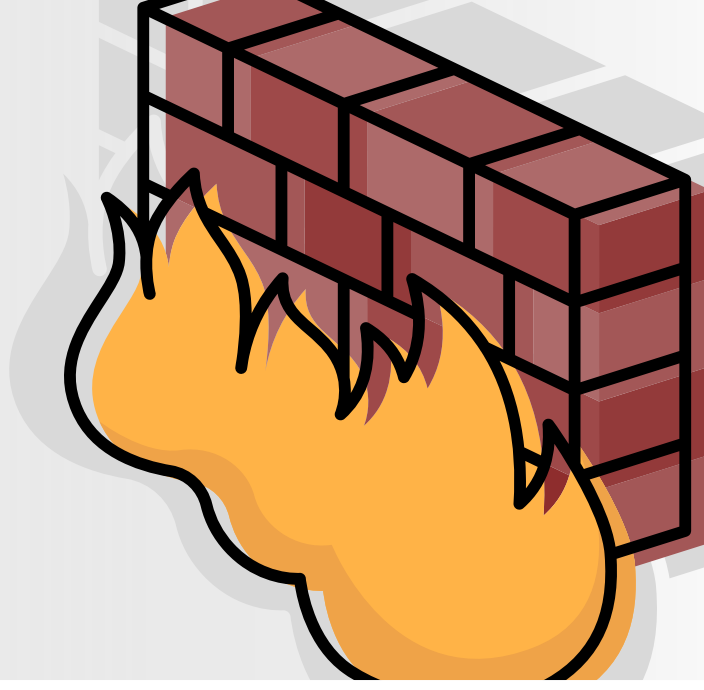
Infografía.

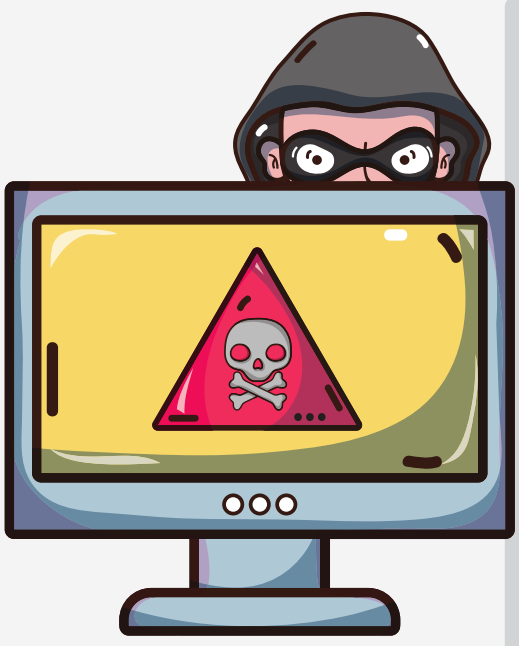
Cortafuegos

y Zonas Desmilitarizadas



Subvenciona
Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Desarrolla
ATA AUTÓNOMOS



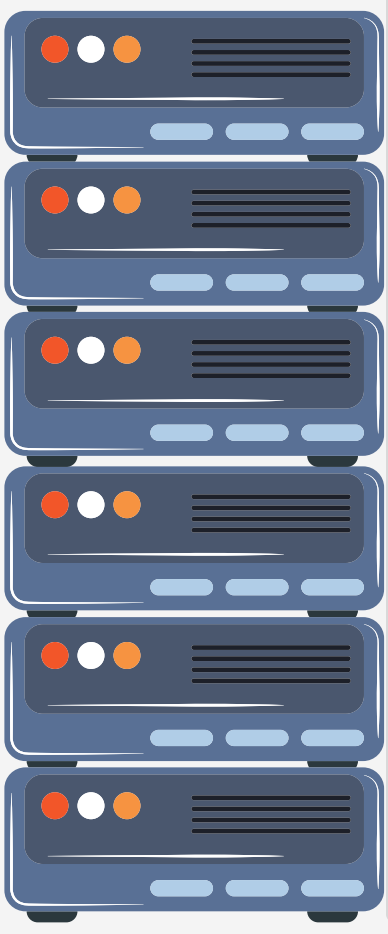
01

Con el rápido avance de las tecnologías de la información y la comunicación, se han desarrollado en paralelo y, a gran velocidad las ciberamenazas, por lo que el número de filtraciones de datos aumenta cada año. Esto significa que la seguridad de redes se ha vuelto fundamental para salvaguardar la información de las empresas.

La tecnología de protección de redes está integrada por varias capas de defensa en el perímetro y la propia red. En cada área de la empresa, se recomienda implementar las políticas y controles para evitar el paso de amenazas que puedan atacar vulnerabilidades del sistema, mientras se permite el acceso a personas autorizadas.

02

Riesgos de utilizar Servidores Propios



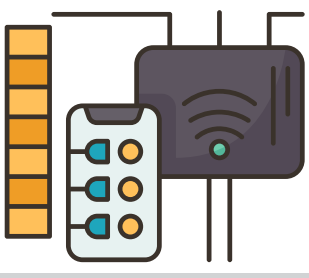
Los servidores son los principales responsables de garantizar el éxito en los accesos a los servicios de la empresa. Estos se encuentran en el centro de toda la actividad de la compañía; intercambio de datos, optimización de procesos de trabajo y servicios asociados con tareas individuales. Puesto que son tan necesarios para el correcto funcionamiento del trabajo cotidiano de una empresa, los servidores son un atractivo objetivo para los hackers.

Si un servidor falla, toda la compañía se paraliza:

- Caídas de la IT, interrupción de los procesos de negocio.
- Pérdidas de datos y acceso limitado a los mismos.
- Aplicaciones defectuosas o deshabilitadas.
- Impedimentos en el acceso a los servicios.
- Sanciones contractuales por plazos perdidos o incumplimiento.

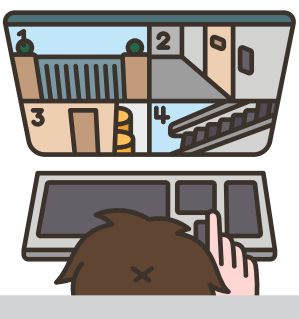
Medidas de Seguridad para Servidores

Seguridad de las salas de servidores



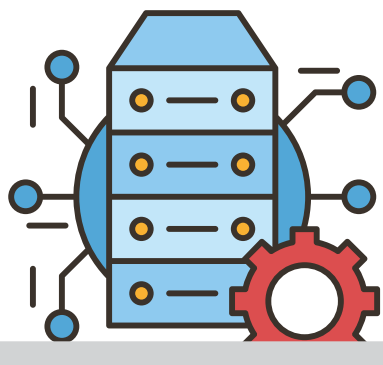
Asegurar los alrededores

Peligros naturales

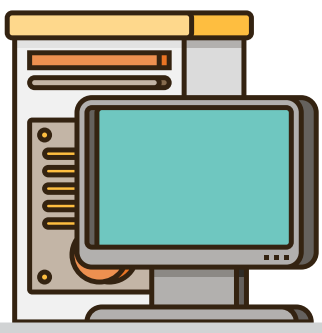


Limitar el acceso

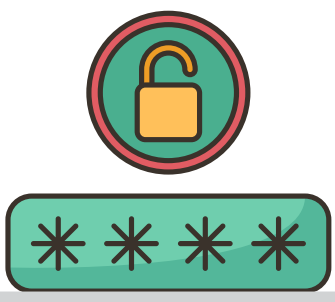
Permiso de acceso: saber cuándo y cómo otorgarlo



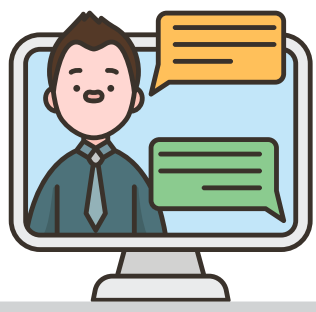
Precauciones para prevenir ataques



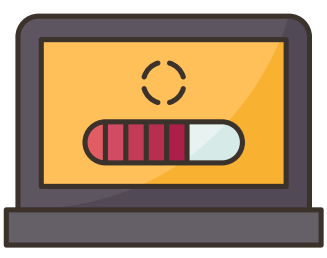
Sistemas mínimos



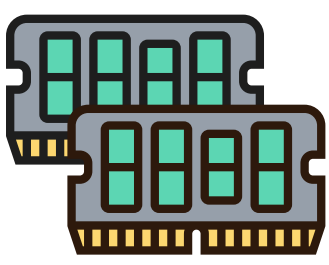
Gestión de permisos



Formación para el personal



Actualizaciones de software

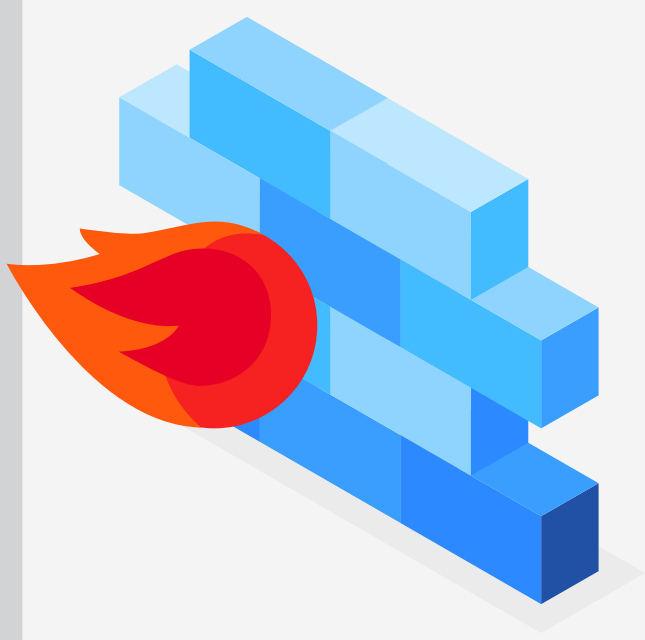


Dispositivos de protección y aleatoriedad de memoria

La protección de conexiones remotas

03 ¿Qué es un Cortafuegos

Un cortafuegos, o también denominado “Firewall”, es un sistema de seguridad digital que comprueba todo el tráfico entrante y saliente de una red de acuerdo con un conjunto de reglas definido. Mantiene fuera el tráfico no autorizado y solo deja entrar las comunicaciones que se consideran seguras.



Para proteger las comunicaciones de la empresa, éstas suelen utilizar un cortafuegos de software en todos los ordenadores, junto con cortafuegos de hardware, más grandes para proteger toda la red. Eso significa que, cada solicitud de datos, tiene que atravesar al menos dos cortafuegos.

Funcionamiento del Cortafuegos

Un cortafuegos filtra los datos que entran en su red, los analiza y comprueba la dirección del remitente, la aplicación a la que van destinados y el contenido de los datos. Combinando estos puntos de datos definidos, un cortafuegos puede decir qué es dañino y qué no lo es. Entonces, el cortafuegos abre o cierra la puerta de la red.

Ningún esfuerzo es demasiado cuando se trata de la seguridad del servidor.

Tipología de cortafuegos

Existen cortafuegos de todas las formas y tamaños para proteger estos puntos de contacto. A continuación, se detallan los cortafuegos más relevantes:

Cortafuegos de filtrado de paquetes

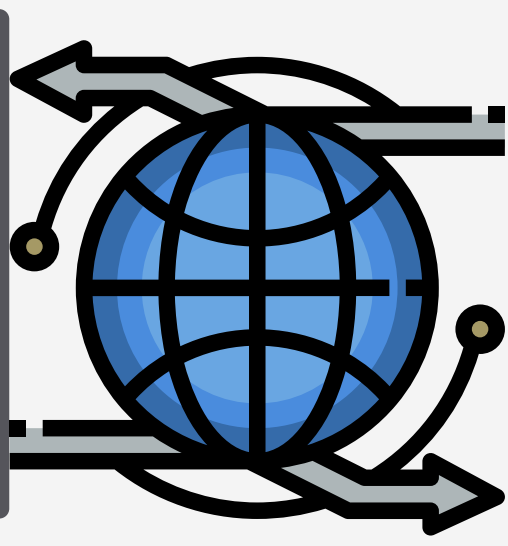
Cortafuegos de nueva generación (NGFW)

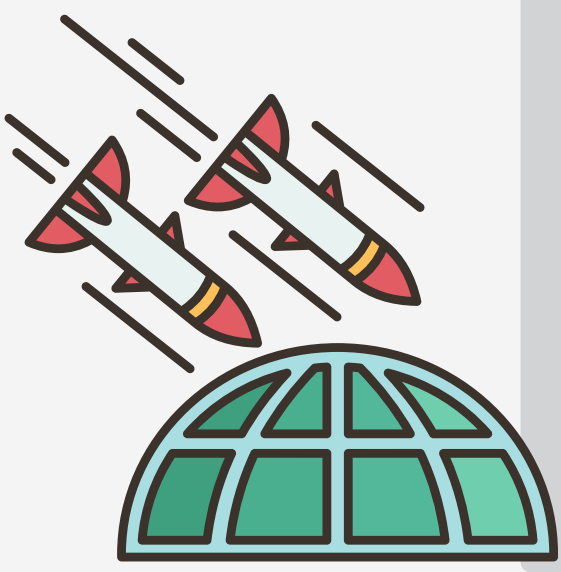
Cortafuegos de traducción de direcciones de red (NAT)

Cortafuegos de inspección multicapa con estado (SMLI)

Ventajas del Cortafuegos

Supervisión del tráfico. Sin un cortafuegos que actúe como resguardo de seguridad del tráfico, la red, dispositivos y sus datos personales, quedan expuestos.





Detener los ataques en línea. Mientras el departamento informático trabaja para asegurar los datos en la red de una empresa y mantener la seguridad de la red de un cortafuegos, puede haber ciberdelincuentes que actúen con malware, troyanos, y otras amenazas destinadas a la obtención de esos datos.

Prevención de hackeos y pérdida de datos. Sin un cortafuegos, las personas ciberatacantes consiguen acceder fácilmente y pueden producirse filtraciones de datos confidenciales, fraudes o, incluso, el robo de la identidad.

04

¿Qué es una Zona Desmilitarizada?

La zona desmilitarizada o DMZ es un mecanismo utilizado, en el ámbito de la seguridad informática, para proteger conexiones de red. Consiste en una red local (IP privada) que se encuentra ubicada entre una red interna de la empresa y la red externa de ella.

Una DMZ es una red aislada dentro de la red interna que actúa como filtro entre la conexión de internet y la red informática de la empresa con el objetivo de verificar que las conexiones, entre ambas redes, están permitidas. La DMZ establece una "zona de seguridad" entre varios equipos conectados a una misma red.

¿Para qué sirve un DMZ?

La principal función de una DMZ es permitir que los equipos informáticos puedan prestar servicios a la red externa como un correo electrónico, funciona como filtro protector de la red interna, actúa como cortafuegos y protege la red de intrusiones maliciosas. Las DMZ se utilizan, comúnmente, para equipos que se usan, posteriormente como servidores, pero que necesitan ser accedidos por conexiones externas utilizando PORT ADDRESS TRASLATION PAT.

Beneficios de usar una DMZ

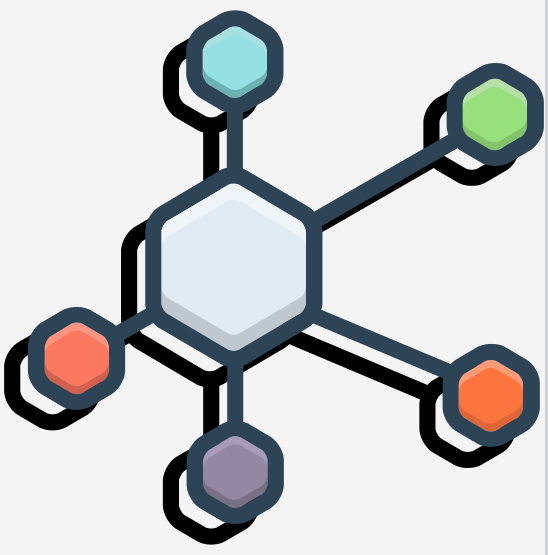
El principal beneficio de una DMZ es proporcionar una red interna con una capa de seguridad adicional al restringir el acceso a los servidores y datos confidenciales. Una DMZ permite que quienes visiten el sitio web obtengan ciertos servicios mientras proporcionan un búfer, entre ellos, y la red privada de la empresa. Como resultado, ofrece también beneficios de seguridad adicionales, tales como:

Habilitación del control de acceso

Prevención del reconocimiento de la red

Bloqueo de suplantación del protocolo de Internet (IP)

Diseño y arquitectura de DMZ



Una DMZ es una “red abierta amplia”, pero existen varios enfoques de diseño y arquitectura que la protegen. Se la puede diseñar de varias maneras, desde un enfoque de cortafuegos único hasta cortafuegos dobles y múltiples. La mayoría de las arquitecturas modernas de DMZ utilizan firewalls dobles que pueden expandirse para desarrollar sistemas más complejos.

Firewall único: con este diseño, una DMZ, requiere tres o más interfaces de red. La primera es la red externa, que conecta la conexión de Internet pública al firewall. La segunda forma la red interna, y la tercera se conecta a la DMZ. Varias reglas monitorean y controlan el tráfico que puede acceder a la DMZ y limitan la conectividad a la red interna.

Firewall doble: La implementación de dos firewalls con una DMZ, entre ellos, suele ser una opción más segura. El primer firewall solo permite el tráfico externo hacia la DMZ, y el segundo solo permite el tráfico que va desde la red interna hacia la DMZ. Quién ataque tendría que poner a ambos firewalls en peligro para obtener acceso a la LAN de la empresa.

¿Es recomendable usar DMZ?

Si bien este tipo de implementaciones son mucho más cómodas de realizar, lo cierto es que son puestas a punto por personas con amplios conocimientos sobre seguridad en redes. El resto de las personas usuarias es mejor que vaya sobre seguro y siga utilizando las características del NAT del router, redirigiendo los puertos a la IP que se necesite cuando sea necesario.

La consecuencia más importante y peligrosa de dejar completamente abiertos todos los puertos del router es que cualquier atacante, simplemente utilizando una conexión a Internet, con las herramientas y conocimientos necesarios puede rastrear vulnerabilidades en los servicios que utilizamos usualmente como por ejemplo FTP o SSH.

Este proyecto está financiado por el Área de Coordinación y Desarrollo Estratégico, Productivo y Social de la Diputación de Cádiz, y surge del Plan Dipuactiva 2023 entre la Diputación Provincial de Cádiz y la Asociación Profesional de Trabajadores Autónomos (ATA) de Andalucía.

Proyecto: *"Seguriza tu actividad. Aprende a utilizar servicios y programas para trabajar de forma segura en la red"*.

Datos de contacto: www.ata.es | ata@ataandalucia.com. 900 100 060 / 956 329 518

Dirección: ATA Jerez (Cádiz) C/ Larga nº 14, 4ª Planta.

Subvenciona

Diputación de Cádiz | COORDINACIÓN Y DESARROLLO ESTRATÉGICO, PRODUCTIVO Y SOCIAL

Desarrolla

ATA AUTÓNOMOS