Dispositivos de red: configuración en el ámbito local y doméstico

Una red local (también conocida habitualmente como red de área local o LAN) consiste en un grupo de ordenadores y otros dispositivos que se encuentran conectados entre sí a través de una red, encontrándose todos en una misma ubicación, ya sea dentro de una casa o una oficina con cientos o miles de dispositivos distintos.

La función principal de este tipo de redes consiste básicamente en enlazar los ordenadores entre sí y proporcionar acceso compartido a archivos, impresoras y otros servicios.

Los distintos dispositivos se encuentran conectados a un servidor central (un PC con Windows Server), en el que se gestiona el acceso a los dispositivos, aplicaciones, el tráfico de la red y al almacenamiento de los archivos.

A diferencia de las versiones normales de Windows, Windows Server se ha diseñado para brindar capacidades y características adicionales que son esenciales para administrar redes empresariales y proporcionar servicios a múltiples usuarios de manera eficiente y segura.

- Redes MAN. Red de Área Metropolitana, ya que se trata de una red de alta velocidad que brinda cobertura a un área geográfica más extensa que una LAN (de hecho, contiene varias de ellas), como una porción de una ciudad.

Ejemplos de redes MAN: Una red interministerial, Una red entre sucursales, Una red en un campus universitario, …

Una Red de Área Amplia (WAN) es un tipo de red que existe en un área geográfica de gran escala. Tu módem envía y recibe información hacia y desde Internet mediante su puerto WAN. Se trata de redes de amplio alcance y alta velocidad, que echan mano a satélites, cableados, microondas y nuevas tecnologías para cubrir una extensa porción geográfica.

Ejemplos: Internet, sin duda alguna, es una WAN de proporciones globales, Una red bancaria nacional, las redes empresariales trasnacionales, las redes satelitales militares, Las redes de la TV pago, …

Red pública o privada en Windows:

La red privada es el tipo de configuración de red para cuando eres tú quien controla la red y los dispositivos que se van a conectar entre ellos a través de ella. Por lo tanto, es el tipo de red que vas a tener en tu casa o en una pequeña oficina en la que sois varias personas, y tú lo administras todo.

Si configuras tu red como privada, Windows entenderá que tienes el control de todos los dispositivos, y por lo tanto no establecerá una seguridad tan férrea entre ellos. Esto va a permitir que todos los dispositivos que estén conectados a esta red puedan conectarse entre ellos.

La Red Pública: cuando configuras una red con este parámetro, le estás diciendo a Windows que no tienes el control de la red o de todos los dispositivos que haya conectados a ella, y que por lo tanto, prefieres que haya una mayor seguridad. Esto puede pasar, por ejemplo, en redes de hoteles, restaurantes estaciones, y otros sitios públicos. Esta configuración no te va a proteger de todos los peligros, por eso es recomendable usar una VPN para evitar ataques de malware.

Tipos de seguridad de red

Protección mediante cortafuegos

Un cortafuegos es un programa de software o un dispositivo de hardware que evita que los usuarios no autorizados accedan a la red, detiene el tráfico sospechoso y permite el tráfico legítimo. Existen varios tipos de cortafuegos con diferentes niveles de seguridad, que van desde cortafuegos sencillos que solo filtran los paquetes, hasta servidores proxy o cortafuegos complejos de última generación que utilizan IA y machine learning *(aprendizaje automatizado de máquinas)* para comparar y analizar la información que intenta llegar.

Detección y prevención de intrusiones

Los sistemas de detección y prevención de intrusiones (IDPS) se pueden desplegar directamente detrás de un cortafuegos para proporcionar una segunda capa de defensa contra agentes peligrosos.

Control de acceso de red (NAC)

El control de acceso de red. El NAC, que se suele utilizar para «comprobaciones de estado de punto final», puede filtrar un dispositivo de punto final, como un portátil o un smartphone, para comprobar que tiene la protección antivirus adecuada, el nivel apropiado de actualización del sistema y la configuración correcta antes de dejarlo acceder.

Seguridad del cloud

La seguridad en cloud protege los recursos en línea (como los datos confidenciales, las aplicaciones, las IP virtualizadas y los servicios) ante filtraciones, pérdidas o robos.

Redes privadas virtuales (VPN)

Una red privada virtual (VPN) es software que protege la identidad de un usuario cifrando sus datos y enmascarando su dirección IP y su ubicación. Usar una VPN permite acceder a sitios que de otra manera estarían inaccesibles, Lo más recomendable es usar la versión gratuita de una VPN de pago, que son más fiables.

Prevención de pérdida de datos (DLP)

La prevención de la pérdida de datos consta de una serie de estrategias y herramientas que se implementan para asegurarse de que los usuarios de punto final no compartan información confidencial de forma accidental o deliberada fuera de una red corporativa.

Pasarela web segura

Esta tecnología de seguridad impide la entrada de tráfico de red no autorizado a la red interna red y protege a los usuarios y empleados ante un potencial acceso a sitios web maliciosos que contengan virus o malware.