UDS

Mi Universidad

Super Nota

Sofia Pereyra Orantes
Seguridad en redes
Unidad 3
Seguridad en la información
Reyes Molina Andres Alejandro
Ingeniería en Sistemas Computacionales
Cuatrimestre 9

Comitan de Dominguez, Chiapas a 7 de Junio 2025

SEGURIDAD EN REDES

ASPECTOS DE SEGURIDAD EN LAS COMUNICACIONES

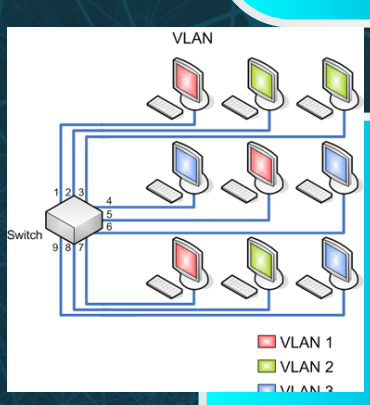
Seguridad en las comunicaciones se incluye la encriptación, la tokenización y otras prácticas sobre la gestión de claves. Gracias a todas ellas se protegen los datos en cualquier aplicación o plataforma de una empresa.

DEBILIDADES DE LOS PROTOCOLOS TCP/IP

TCP/IP no está diseñado para ser intrínsecamente seguro, lo que significa que la seguridad en las comunicaciones a través de TCP/IP depende de medidas adicionales como el cifrado y la autenticación. Esto lo hace vulnerable a ataques como la intercepción y la manipulación de datos

TRANSMISION DE PAQUETES Y PROMISCUIDAD

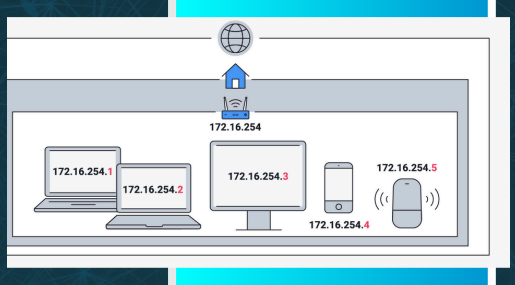
En el modo promiscuo, una máquina intermedia captura todos los paquetes, que normalmente desecharía, incluyendo los paquetes destinados a él mismo y al resto de las máquinas. Resulta a destacar que las topologías y hardware que se usen para comunicar las redes, influye en su funcionamiento, ya que las redes en bus, redes en anillo, así como todas las redes que obliguen a que un paquete circule por un medio compartido, al cual todos tienen acceso, los modos promiscuos capturarán muchos más paquetes que si están en una red con topología en árbol.



REDES LOCALES (VLAN) Y AMPLIAS (VPN)

Una VLAN (acrónimo de virtual LAN, «red de área local virtual») es un método de crear redes lógicamente independientes dentro de una misma red física.1 Varias VLANs pueden coexistir en un único conmutador físico o en una única red física

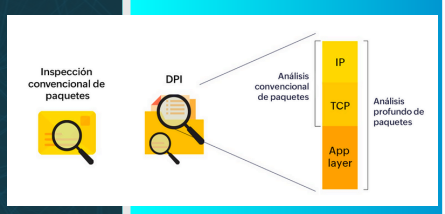
Una VPN es una red privada que utiliza un red pública (generalmente Internet) para conectar varios lugares o usuarios remotos entre ellos. En vez de utilizar una conexión dedicada o líneas alquiladas, una VPN usa una "conexión virtual" a través de Internet desde la red privada de la compañía hasta el sitio o empleado remoto



DOMICILIOS IP

Etiqueta numérica que identifica de forma única y jerárquica a un dispositivo conectado a una red, como una computadora, un teléfono inteligente o un servidor.

- **Identificación**:
- Las direcciones IP identifican de forma única a cada dispositivo en una red.
- **Comunicación**:
- Facilitan la comunicación entre dispositivos al permitir que se envíen y reciban datos entre sí.
- **Locación**:
- Permiten identificar la ubicación de un dispositivo en la red.
- **Tipos**:
- Existen diferentes tipos de direcciones IP, incluyendo IP públicas (accesibles desde Internet) y IP privadas (utilizadas en redes internas).



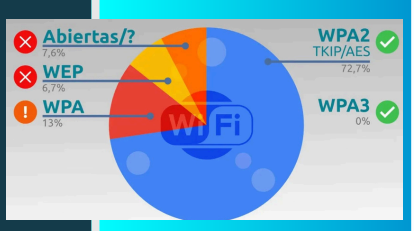
VIGILANCIA DE PAQUETES

Proceso de interceptar y analizar los paquetes de datos que se transmiten a través de una red. Esto se puede hacer mediante software o hardware que intercepta y registra la información de los paquetes, incluyendo su origen, destino, protocolo y contenido.

ESTANDARES PARA LA SEGURIDAD EN REDES

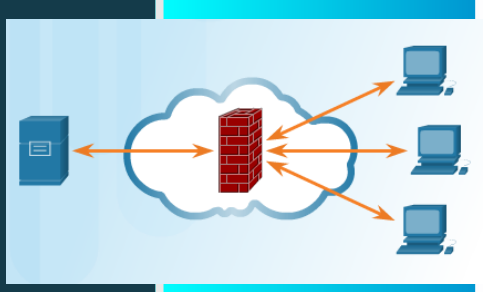
Conjunto de normas y prácticas diseñadas para proteger la información y los sistemas de una red de posibles amenazas cibernéticas. Estos estándares abarcan diferentes aspectos, como la gestión de riesgos, la protección de la información, la implementación de controles técnicos y la formación del personal.

VULNERABILIDAD DE LOS PROTOCOLOS INALAMBRICOS WEP, WPA,WPA2



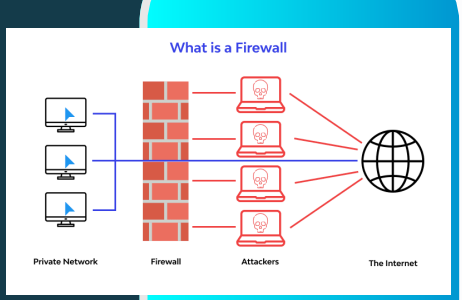
WEP es el más vulnerable debido a sus métodos de cifrado obsoletos y a que puede ser fácilmente descifrado, como la clave compartida. WPA es un avance sobre WEP pero también tiene vulnerabilidades, y WPA2 es el más seguro de los tres, aunque también se ha demostrado que es vulnerable a ciertos ataques

FIREWALL DE CAPAS INFERIORES



Con base en el modelo OSI, también se crearon 7 capas de seguridad, para garantizar la protección de datos, que transitan por la red, que son: Capa Humana, Capa Perimetral, Capa de Red, Capa de Endpoint, Capa de Aplicativo, Capa de Datos y Capa de Misión Urgente

FIREWALL DE CAPA DE APLICACIÓN

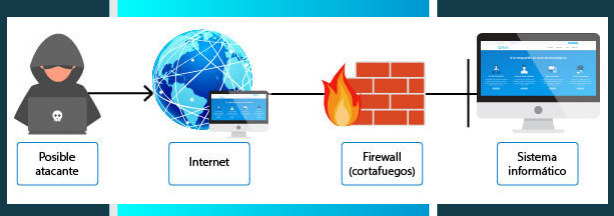


es un tipo de firewall que opera en la capa más alta del modelo OSI, la capa de aplicación. Estos firewalls ofrecen un nivel de seguridad más granular al analizar el tráfico de red en función de las aplicaciones y protocolos específicos, en lugar de simplemente basarse en direcciones IP y puertos.

FIREWALL PERSONAL

Un firewall personal es un programa de seguridad diseñado para proteger dispositivos individuales, como computadoras o teléfonos inteligentes, del acceso no autorizado y de amenazas cibernéticas maliciosas.

VENTAJAS DE UN FIREWALL

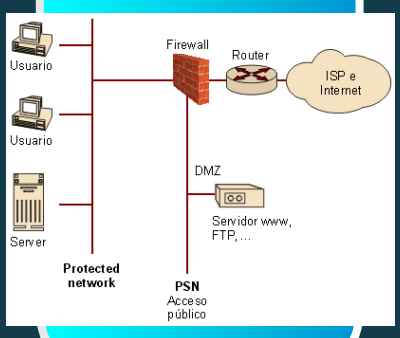


1.Monitorea el trafiuco de red
2.Detiene los ataques de Virus
3.Previene la piratería informática
4.Promueve la privacidad

LIMITACIONES DE UN FIREWALL

Los firewalls solo pueden filtrar el tráfico que entra o sale de la red. No pueden proteger contra amenazas que se originan desde dentro de la red o que no son parte del tráfico de red, como la instalación de software malicioso por parte de un usuario interno o el uso de dispositivos USB infectado

LIMITACIONES DE UN FIREWALL



- Una política de firewall es una declaración que especifica cómo se trata el tráfico de red, basándose en criterios como dirección IP, puertos, protocolos y aplicaciones.

- Función:
- Las políticas de firewall permiten o deniegan conexiones, protegiendo así la red de accesos no autorizados y amenazas.

POLITICAS DEL FIREWALL

conjuntos de reglas que controlan el tráfico de red entrante y saliente, definiendo qué conexiones deben permitirse o denegarse a través del firewall. Estas reglas son esenciales para la seguridad de una red, protegiendo contra el acceso no autorizado y las amenazas cibernéticas

ENLACES EXTERNOS

son **hipervínculos en una página web que apuntan a un sitio web diferente**. Son la contraparte de los enlaces internos, que dirigen a otras páginas dentro del mismo sitio. Están diseñados para dirigir a los usuarios a un contenido externo, proporcionando valor y recursos adicionales.