Network Security

Transcribed on July 25, 2025 at 4:41 PM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de las bases que forman una red de datos.

Este paso es fundamental para después poder tener éxito a la hora de securizar nuestras diferentes arquitecturas de red.

En concreto nos centraremos en los Security Program o los programas de seguridad y también daremos un repaso a diferentes dispositivos que forman parte de todas esas redes de datos.

Bien, pues un programa de seguridad o un Security Program es un conjunto de diferentes procedimientos y también políticas que se aplican a la hora de definir la seguridad de un tipo de arquitectura.

Quizás el más conocido es el NIST que es el National Institute of Standards and Technology que fue creado por el Departamento de Comercio de los Estados Unidos y éste integra entre otros muchos apartados dedicados a la seguridad, algunos que son específicos sobre la seguridad de redes, en concreto son los de la serie 800, por ejemplo el segundo que podéis ver ahí que es el NIST SP es un procedimiento especial de NIST que se centra en los BGP que son los Border Gateway Protocol y también a los packets de denegación de servicio distribuido o DDOS.

Es posible que tengamos que decidir o incluso utilizar una amplia variedad de Security Programs y no solamente ir a uno específico.

Por ejemplo la GDPR o RGDPD que es el Reglamento General de Protección de Datos, se centra en la protección como bien dice de datos personales de las personas físicas y por ejemplo en Estados Unidos existen otras como la HIPAA que es el Health Information Privacy que se centra sobre todo en lo relativo a la salud.

En definitiva un Security Program nos puede ayudar igual que el TRIP Modeling a decidir qué aplicaciones o qué servicios o qué implementaciones nos van a ayudar a la hora de securizar nuestra red.

Lo que pasa que el Security Program está enfocado a un punto de vista mucho más práctico, aquí ya va directamente a actuaciones sobre la arquitectura.

Bien, antes de continuar es importante repasar qué es la capa OSI, porque haremos referencia continua a qué capa está trabajando por ejemplo un dispositivo concreto.

Bien pues la capa OSI lo que nos puede ayudar es a servir como modelo de referencia para describir cómo las aplicaciones de se pueden comunicar a través de una computadora o de una red de ordenadores.

Como podéis ver está dividido en siete capas, cada una con una función específica.

Tenemos la capa física que es la capa 1 que se encarga de la transmisión física de los datos a través del medio de comunicación, definiendo aspectos como los voltajes, conectores y también por ejemplo la velocidad de transmisión.

Después tenemos en la capa 2 la capa de enlace o de datos, aquí se gestiona el flujo de datos entre dispositivos que están cercanos en la red y se asegura que la transmisión sea confiable.

La capa 3 que es la capa de red, se encarga de determinar la ruta que deben de seguir los paquetes de datos a través de la así como también de la gestión del direccionamiento y del enrutamiento.

La capa 4 es la capa de transporte, aquí se proporciona una entrega de datos extremo a extremo que sea confiable y también controla el flujo de datos entre los dispositivos finales.

La capa 5 es la capa de sesión, establece, administra y también finaliza las conexiones entre aplicaciones de diferentes dispositivos.

La capa 6 es la capa de presentación, ésta se encarga de traducir, de comprender y de cifrar por ejemplo los datos para garantizar que se puedan interpretar correctamente por las aplicaciones.

Y finalmente tenemos la capa 7 que es la capa de aplicación, esta es la capa más cercana al usuario final y proporciona los servicios de red directamente al usuario, como por ejemplo el acceso a recursos compartidos, transferencia de archivos o o incluso el email entre otros.

El primer dispositivo del que vamos a hablar son los routers o los enrutadores que ofrecen una cantidad de opciones muy enfocadas a la seguridad.

Aparte de sus funciones específicas como por ejemplo el cifrado, crear una VPN, también podemos encontrar algunos modelos que implementan incluso protocolos como por ejemplo el OSPF que es el Open Shortest Path First o el IGP que es el Interior Gateway Routing los cuales optimizan el enrutamiento de la información en caso de caída de los nodos que conforman nuestra red.

También tenemos que recordar que los router funcionan dentro de la capa 3 del modelo OSI.

Todos los routers actuales implementan una característica de seguridad que se llama ACL que es el Access Control List que veremos más adelante implementado en el software de PFSense.

Entonces elegir un modelo concreto de route así como los protocolos o funciones de seguridad que nos puede ofrecer es básico para establecer unos cimientos de las futuras implementaciones que se relacionen con la seguridad.

Por eso es vital elegir una buena marca y sobre todo una marca que se pueda ampliar y se pueda escalar de una manera sencilla dentro de nuestra arquitectura.

Por supuesto Cisco es la empresa mejor valorada en la calidad de funcionamiento de los routers, pero no es la única, también tenemos otras como Juniper, Fortinet, Dell o HP incluso.

El siguiente elemento son los switches.

Los switches son gestionados, esto quiere decir que nos permiten acceder y configurar sus funciones de forma habitual desde una línea de comandos o desde una interfaz gráfica.

Normalmente todos funcionan dentro de la capa 2 del modelo OSI.

Más adelante entraré un poco más en las diferentes funciones que pueden realizar, pero ya os adelanto que podemos crear por ejemplo lo que se llaman las VLANs que son las Virtual Local Area Network.

También podemos gestionar la seguridad de los puertos, se pueden también monitorizar utilizando protocolos como SNMP por ejemplo, etc.

El switch es el encargado de entregar los diferentes paquetes desde un dispositivo a otro dentro de nuestra red local.

Después tenemos los firewalls o los cortafuegos y estos sí que son unos elementos dedicados exclusivamente a la seguridad de la red.

Por este motivo es muy importante elegir un buen modelo, ya no solo por sus funciones, sino también por lo que hemos comentado antes de la escalabilidad y también que permita un buen mantenimiento.

También la calidad es importante porque esto implica que tiene que gestionar un gran volumen de paquetes de datos, por lo que su rendimiento y capacidad de escalabilidad son fundamentales y críticas para nuestra arquitectura.

Este dispositivo se encarga de gestionar todo el tráfico de entrada, que a partir de ahora también me voy a referir a él como inbound y también el de salida que es el outbound.

Lo que hace es que analiza los paquetes y aplica diferentes reglas para permitir o no el acceso de los mismos.

Este filtrado de puerto es otra de sus funciones principales.

Y bueno, los firewall se encuentran trabajando en la capa 3 del modelo OSI de forma habitual, aunque ya tenemos los NGFW que son los Next Generation Firewall que permiten trabajar en la capa 7 del modelo OSI, es decir, en la capa de aplicación.

Por lo tanto se pueden distinguir por ejemplo usuarios y también se pueden por ejemplo monitorizar los accesos o autorizar que pueda o no a un tipo de usuario o un grupo de usuarios.

Para mostraros cómo funcionan estos elementos en un entorno que podamos simular utilizaremos PFSense.

PFSense es una distribución de software de código abierto que se basa en FreeBSD y además se utiliza para construir por ejemplo cortafuegos y routers.

También tiene otras características muy avanzadas de seguridad y también de tratamiento, incluyendo VPN, balance de carga, filtrado de contenido y mucho más.

Con PFSEN podemos simular varios elementos de red como los firewall, un router una VPN, un proxy, entre muchos otros.

Y esto es importante para aprender a configurar dispositivos de red más caros o complejos porque proporciona una plataforma de práctica segura y flexible.

Así podemos, por ejemplo, experimentar con diferentes configuraciones y escenarios sin riesgo a afectar a una red real.

Además, pcsen ofrece una interfaz de usuario muy intuitiva y una amplia documentación, lo que facilita mucho el aprendizaje y conceptos de redes sociales y de seguridad.

En el siguiente vídeo daremos un paseo por las diferentes funciones y opciones que tiene PFSense.

En conclusión, comprender la seguridad de redes implica familiarizarse con varios marcos y estándares, como por ejemplo el NIST o la serie ISO IEC 27000, y sobre todo con regulaciones como la RGPD.

Estos marcos proporcionan pautas para asegurar la infraestructura de red que cubren aspectos desde la gestión de la identidad hasta la protección contra ataques de denegación de servicio, por ejemplo.

Por otro lado, aprender a configurar dispositivos como los routers, switches y firewall es fundamental, ya que forman la base de la seguridad de la red.

Marcas como Cisco, Juniper, Dell y HP se encuentran entre los principales proveedores de equipos de red, cada uno ofreciendo productos de diferente calidad.

Por último, quiero recalcar que el cumplimiento de las regulaciones como la RGPD es imperativo y tenemos que subrayar la importancia de tomar medidas muy robustas en nuestra seguridad de red para poder cumplimentar y cumplir con esta normativa.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.