Network Segmentation

Transcribed on July 29, 2025 at 10:02 AM by Minutes AI

Speaker 1 (00:03)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la segmentación, pero no como lo que hemos visto anteriormente con la segmentación de subnetting.

Esta vez nos centramos en los diferentes tipos, herramientas o arquitecturas que podemos utilizar.

En concreto veremos una segmentación física, una lógica y después nos centraremos en la segmentación wifi o inalámbrica.

Segmentar una red, además de ser una buena práctica que nos permite dividir el tráfico de red y también de esa forma tener mayor control, como ya hemos visto en el subnetting y todo lo anterior, también es clave a la hora de diseñar una arquitectura segura.

Estamos elevando otro nivel de segmentación distinto a lo que hacemos con el subnetting.

Esta vez estamos ya implementando arquitecturas complejas con algoritmos propios y protocolos.

Por ejemplo, utilizando esta técnica se podría bloquear todo el tráfico de red en una zona concreta de la arquitectura en caso de que se vea comprometida.

El concepto de escalabilidad también está muy ligado a esta fase de diseño e implementación.

No olvidemos que la seguridad de un sistema no es solamente su resiliencia a ataques, sino a cualquier otro factor que afecte al rendimiento final de la arquitectura.

Bien, pues comenzaremos por lo que es la segmentación física.

Los elementos físicos son los dispositivos de red que tenemos a nuestra disposición, como por ejemplo los routers, los gateway, los switches, etcétera.

Los cortafuegos o firewall tienen una mención especial en la seguridad de la segmentación ya que si se ubican correctamente y se configuran con las políticas correctas son capaces de proteger desde ataques externos, internos, malware, propagación también de malware o de virus, algún tipo de ataque de movimiento lateral, etcétera.

Es decir, una correcta segmentación de los elementos físicos nos va a permitir monitorizar el tráfico de red.

También nos ofrece una posibilidad de aislamiento si fuera necesario, mayor visibilidad y por lo tanto una forma más sencilla de localizar fallos.

Y aquí en la diapositiva estáis viendo lo que es una DMZ.

Una DMZ es una zona desmilitarizada y tiene que tener una mención especial ya que éstas se implementan utilizando elementos físicos y son clave en la seguridad de la red empresarial o lo que se llama también la red perimetral.

Esta red se ubica exactamente entre las redes internas de la empresa e Internet y en ellas se ubican servidores de la empresa que no tienen acceso directo con las redes internas o la intranet.

Las diferentes políticas de conexión de estos equipos permiten tráfico desde la red interna a Internet y de aquí hasta la DMZ.

En cambio las conexiones desde la DMZ sólo se permiten a Internet, no pueden acceder a la red interna.

En esta ubicación se suelen localizar servidores por ejemplo de correo electrónico, DNS, web, FTP, etc.

Las implementaciones de la DMZ se suelen realizar utilizando un solo cortafuego para gestionar las conexiones o también un diseño con dos cortafuegos.

Quizás este es el más utilizado, en el que uno se dedica a la conexión de la DMZ con la intranet o la red interna o el backend y otro se dedica a la conexión exclusivamente de la DMZ con el frontend.

Es exactamente lo que podéis ver en el gráfico que está en la diapositiva con los elementos External Firewall e Internal Firewall.

Desde el punto de vista de la segmentación lógica, antes ya hemos mencionado por ejemplo las ACL, la lista de control de acceso, pero también es posible utilizar otras listas como por ejemplo las NAC o Network Access Control.

Usar NAC nos permite añadir un nivel más de seguridad, ya que no permite que los elementos de la red se conecten sin antes autenticarse.

Las VLAN son quizás uno de los elementos más utilizados en la segmentación de red, este es el siguiente punto que podéis ver en la diapositiva.

De hecho el objetivo de las VLANs es exactamente separar de forma lógica diferentes redes sociales dentro de una misma red física.

Esto lo veremos más adelante un poco más en detalle.

Otro de los tipos de segmentación lógica más utilizado y más conocido son las VPN o las Virtual Private Networks o Redes privadas virtuales, y éstas permiten enviar información a través de Internet utilizando un canal seguro y cifrado.

Más adelante entraremos un poco más en profundidad con las VPN.

Aquí hago un pequeño inciso con un ejemplo, porque por ejemplo las redes de voz IP, las Voz IP deben estar muy bien segmentadas tanto a nivel físico como lógico, ya que este tipo de redes deben estar segmentadas utilizando dispositivos de red compatibles además de la segmentación que va a realizar la VLAN, y el motivo es que si mezclamos este tipo de tráfico con el de los datos puros y duros pueden llevar a pérdidas de rendimiento global, además de suponer un vector nuevo de ataque para nuestra arquitectura.

Centrándonos ahora en las redes inalámbricas y la segmentación en este tipo de arquitecturas tenemos que tener en cuenta que nos encontraremos unos nuevos retos.

El primero será enfrentarnos a tecnologías que son nuevas y también a dispositivos que no son los habituales, y el segundo es que configurarlos mal o de forma insegura pueda acarrear una gran problemática de seguridad a una gran variedad de puntos de acceso a nuestra arquitectura.

Entonces, ¿Es vital aquí la segmentación?

Algunas técnicas de segmentación son las comunes a las que ya hemos visto, como por ejemplo las VLANs, pero en cambio ese tipo de redes requieren una atención especial tanto en su diseño, lo que es la segmentación, como en seguridad, tal y como veremos ahora.

Y aquí quiero puntualizar que la seguridad de las redes wifi tienen un impacto directo y realmente grande e importante sobre instalaciones o infraestructuras que están relacionadas con el mundo del iot o el Internet of Things.

Estos dispositivos suelen usar tecnologías inalámbricas como wifi, Bluetooth, etc.

Bien, pues para hacer una correcta segmentación y seguridad de una red wifi, el primer paso es hacer una buena elección de su nombre o SSID, que significa Service Set Identified.

Es importantísimo porque una buena elección del nombre SSID bien elegido sería o buscando siempre que no ofrezca información a un posible atacante.

En algunos casos, aunque no es muy efectivo, estas redes también se suelen ocultar.

También es importante no dejar los nombres por defecto que se suelen ser asignados por los dispositivos que la gestionan, ya que esta información es pública y se podría sacar información, por ejemplo el tipo de cifrado utilizado o el modelo del dispositivo de red y de esta forma pues por ejemplo mirar contraseñas por defecto, buscar algún tipo de vulnerabilidad asociada a ese dispositivo, etc.

También podemos utilizar diferentes dispositivos que se llaman los AP o Access Point, que nos permiten segmentar de forma física también la red y también nos sirven para ampliar el rango de utilización de dichas redes wifi.

También es importante respetar el estándar o la normativa que rige las conexiones que es el IEE 802.11.

Es importante ir viendo las diferentes versiones que van apareciendo sobre este estándar o normativa.

Pues bien, el último punto que es RADIUS nos sirve para la autenticación de acceso a nuestra red, pues justamente este es el protocolo que se utiliza para esa operación, que significa Remote Authentication Dial in User Service.

Estos servidores RADIUS o que tienen el servicio de RADIUS se conectan con el directorio de servicios de la empresa, por ejemplo con un LRAP, con un directorio activo, etc.

Y de esta forma autenticar los accesos de los usuarios.

Para comprobar la autenticación se utilizan cifrados como PAP, CHAP o CHAP o EAP.

Es posible configurar este tipo de servicios RADIUS directamente contra un servidor, por ejemplo en Windows o Linux, es decir, no hace falta un dispositivo específico, aunque la mayoría de los routers empresariales lo llevan ya por defecto.

Bien, aquí quiero destacar que en las redes empresariales tenemos que evitar a toda costa conectar dispositivos sin autenticación, es decir, no sólo aquellos que tienen usuarios que se validan, sino también los dispositivos con cuentas que están asociadas al directorio de la infraestructura, es decir, que tienen un nombre de usuario y una contraseña.

Veremos ahora lo que se llama el etiquetado VLAN o VLAN Tagging, que es una técnica que se utiliza en redes sociales para implementar lo que se llama una VLAN.

Centrándonos en las VLAN o las VLAN que después veremos más en profundidad, hay que saber que nao VLAN lo que hace es segmentar una red física en diferentes redes lógicas independiente, de manera que los dispositivos en diferentes VLAN no pueden comunicarse entre sí si no hay en medio un anotador o una configuración especial en esos dispositivos de red.

Esto mejora muchísimo la seguridad al limitar el tráfico a un grupo de dispositivos y puede reducir la congestión al limitar los dominios del broadcast.

Y una de las técnicas para implementar estas VLAN es el VLAN Tagging, que es el gráfico que veis en pantalla.

Vamos a ver ahora paso a paso cómo funciona el etiquetado VLAN.

Nos centramos en el device, que es el dispositivo emisor, y no es más que un dispositivo en una red que necesita enviar datos a otro dispositivo.

Este otro dispositivo está conectado a un switch que conoce las VLANs.

Nos centramos ahora en el switch número 1.

Cuando el switch recibe la trama de datos del dispositivo, asigna una etiqueta, le hace un VLAN a esa trama y esta etiqueta identifica qué VLAN pertenece la trama.

Esto es parte de un protocolo llamado IEQ, que es el estándar para el etiquetado de VLAN.

Bien, pues ahora si nos fijamos en la trama que pone etiqueta VLAN o Frame with VLAN Tag, ahora ésta contiene información adicional en su encabezado que incluye el identificador de la VLAN, que es el VLAN ID, y este identificador es crucial para que otros dispositivos de la red puedan manejar la trama correctamente de acuerdo con las reglas de la VLAN.

Bien, nos centramos ahora en el switch número 2.

Aquí la trama etiquetada se envía a través de la red al siguiente switch.

Este switch lee la etiqueta VLAN para determinar a qué VLAN pertenece esa trama.

Finalmente se produce un reenvío de la trama.

Aquí, basándose en la etiqueta VLAN, el Switch 2 sabe qué puerto o puertos debe reenviar dicha trama.

Solamente los puertos que pertenecen a la misma VLAN recibirán esa trama y esto nos asegura que los dispositivos en diferentes VLAN no puedan acceder a los datos destinados a otra VLAN.

Y ya finalmente tenemos el dispositivo destino o el Destination Device, en el que finalmente la trama llega al dispositivo en esta misma VLAN que el dispositivo emisor.

El dispositivo recibe los datos como si estuviera en una red física separada, aunque comparte la misma infraestructura de red con otros dispositivos en otras VLAN.

Es decir, veremos diferentes tramas con diferentes etiquetados que van circulando por la misma ubicación pero se van entregando en las diferentes VLAN.

Pues bien, la segmentación física de la red lo que hace es reforzar muchísimo la seguridad mediante el aislamiento de sistemas críticos, además de optimizar su rendimiento.

La segmentación lógica que se implementa a través de las VLANs o las VLANs ofrece una mayor flexibilidad y control sobre el tráfico de red, lo que permite una asignación eficiente de recursos y una seguridad reforzada sin la necesidad de hardware adicional.

Además, la segmentación y la seguridad de las redes wifi es vital para proteger contra accesos no autorizados y amenazas, asegurando un acceso segmentado y seguro para diferentes grupos de usuarios, lo que también mantiene una integridad y una confidencialidad de los datos que se han enviado de forma inalámbrica.

Llegamos.