Network Security

Transcribed on July 27, 2025 at 8:45 AM by Minutes AI

Speaker 1 (00:06)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la importancia desde el punto de vista de la seguridad, de la selección de una correcta topología de red, así como dividirla de forma eficiente y segura usando lo que llamamos subnetting o segmentación de la red.

En función del tamaño de la organización o empresa sobre la cual vamos a diseñar o auditar una arquitectura segura será necesario en principio una visión global de su topología.

Es importante que la base de diseño siempre esté respaldada por alguna topología eficiente de base para el tipo de negocio o funcionalidad que se está ofreciendo.

Por tanto este sería el punto principal para revisar dentro de un diseño de una arquitectura segura de red.

La topología de red más conocida es la tipo anillo o ring, debido a su diseño ésta nos permite cierta facilidad a la hora de escalar o redirigir el tráfico de red en caso de incidente.

El problema de este tipo de topología aparece a medida que la red se va haciendo más grande, donde comenzamos a perder un poco el control de ésta.

También podemos ver las tipologías tipo bus que son muy sencillas porque básicamente transmiten la información en una sola dirección.

Otro tipo de topología de red son los tipo estrella o star, cada nodo cliente se conecta con un dispositivo central, por ejemplo un switch.

Esta configuración reduce el impacto que puede tener el fallo de algún nodo, pero centraliza y focaliza, osea quiere decir crea un punto de fallo centralizado de toda la comunicación central, es decir todo el peso recae sobre el dispositivo, si éste deja de funcionar la red también cae.

Las redes LAN o redes locales son el ejemplo más claro de esta topología.

Después tenemos la topología también llamada árbol o de tree que funciona como una extensión de la topología de estrella, ya que ésta consta básicamente en ir añadiendo configuraciones de estrella de forma anidada en diferentes capas.

También tenemos las redes con topología tipo mes, las cuales son una especie de mezcla de topología estrella con anillo, de esta forma llegamos a la interconexión total lo cual nos permite una infraestructura más robusta.

Las redes tipo wifi o wireless suelen implementarse utilizando este tipo de topología.

El método más utilizado de direccionamiento es utilizar la dirección IP y este es clave para una infraestructura y su securización.

Si tenemos que crear una infraestructura desde cero es importante tener un plan de direccionamiento IP bastante detallado el cual nos permite fácilmente identificar y gestionar mejor los dispositivos.

Por ejemplo una práctica habitual es usar el formato X X X para el gateway, aunque también se utiliza mucho el que acaba en.

Bien, vamos a ver ahora por qué el direccionamiento IP es algo básico e importantísimo a la hora de securizar nuestra red.

Desde el principio ya sabemos que el método utilizado de direccionamiento es utilizar direcciones IP.

Pues bien, si tenemos que crear una infraestructura desde cero, es importante tener un plan de direccionamiento IP bastante detallado, el cual nos va a permitir fácilmente identificar y gestionar mejor los dispositivos.

Por ejemplo, una práctica habitual es usar la terminación con punto 1 para los gateway o los, pero incluso podemos asignar el tipo de dispositivo según el rango.

De esta forma también tendremos fácilmente identificados todos los dispositivos críticos de la arquitectura.

La reserva de direcciones IP para dispositivos de red y sobre todo aquellos críticos, debe ser una de las tareas principales a la hora de un diseño de una arquitectura de redes sociales.

Existen básicamente dos tipos de direccionamiento, la dirección pública y la dirección privada.

La dirección pública son las direcciones globales asignadas por la IANA, que es la Internet Assigned Numbers Authority.

En el caso de redes empresariales es habitual y necesario obtener un rango de este tipo de direcciones, ya que son imprescindibles para ofrecer acceso a Internet a las diferentes redes sociales.

Estas redes se suelen utilizar, además del acceso a Internet, para configurar otro tipo de redes como una DMZ, la cual veremos más adelante, o routers, etc.

Después tenemos la red privada, que son direcciones reservadas para su uso interno para construir una red de comunicaciones.

Basándonos en el protocolo TCP IP, cualquier empresa podría utilizar estas direcciones IP de forma privada para configurar su propia red empresarial.

Bien, esta tabla muestra algunos ejemplos generales de subnetting.

La primera columna, que se llama notación de longitud de prefijo o también llamada CIDR, muestra la anotación de Classes Interdomine Routing.

Ese es el significado de CIDR, que es una forma de representar la dirección IP y su máscara de subred asociada.

Esta anotación utiliza un prefijo seguido por una barra diagonal y un número que indica cuántos bits de la dirección constituyen el prefijo de red.

Por ejemplo, barra 24 indica que los primeros 24 bits de la dirección son el prefijo de red.

La segunda columna lo que muestra son las direcciones máximas totales.

Esta columna indica el número máximo de direcciones IP que se pueden asignar dentro de la red o subred especificada por la anotación CIDR.

Este número es una potencia de dos basada en la cantidad de bits que no se utilizan para el prefijo de red, es decir 32 menos la longitud del prefijo.

La columna número 3 lo que nos muestra son los hosts disponibles, indica el número de direcciones IP dentro de la subred que realmente pueden ser asignadas a dispositivos.

Este número es generalmente el número máximo de direcciones menos 2, debido a que una dirección se usa para identificar la subred misma y la otra se usa como dirección de broadcast.

Longitud de subred esta muestra el número de bits que se utilizan para la dirección de la subred en la máscara de subred, es el mismo número que aparece después de la barra diagonal en la no notación CIDR que antes hemos visto.

Y finalmente tenemos la máscara de subred y esta representa la máscara de subred asociada a la notación CIDR y determina qué porción de la dirección IP representa la red y qué porción representa los host dentro de esa red.

Es una serie de unos seguidos de cero en la representación binaria, donde los unos representan los bits de la red y los ceros los bits del host, representan los bits de la red y los ceros los bits del hosting.

Bien, ahora veremos algunas direcciones IP que son un poco especiales dentro de todo este subnetting.

La primera que vemos son las direcciones IPV especiales que son la tabla primera que veis arriba a la izquierda.

Aquí se indica que el rango de dirección del host local es de 127.000 a la 127.255 255 255 y además se utiliza para pruebas en bucles, de ahí el loopback.

Usamos muchas veces dentro de la máquina, por ejemplo la 127001 o localhost que tanto hemos utilizado.

Después tenemos las direcciones APIPA o APIPA que van desde la 169.

254 hasta la 169.254.

255.255 y se asignan de forma automática a máquinas cliente cuando no hay servidores DHCP presentes.

El siguiente bloque son las direcciones IP BOGO, se denominan así por la palabra BOGUS que significa falso.

En redes una IP bogon es un paquete con una dirección IP que nunca debería de aparecer en un Internet público.

Comúnmente son direcciones que no han sido asignadas a un host o están reservadas para redes privadas, no son legítimas cuando se ven en Internet público y son indicativas de redes mal configuradas o actividad maliciosa.

Dado que estas direcciones no provienen de una fuente válida, a menudo se utilizan en filtrado para evitar el tráfico no deseado o para la suplantación o también para ataques de denegación de servicio.

A continuación podéis ver algunos ejemplos, por ejemplo el que se llama disk network o esta red que es se utiliza para denotar un host de origen en la red actual, que se usa típicamente en tablas de enrutamiento por ejemplo.

Pues bien, a la derecha tenemos otra tabla que podéis ver que están las diferentes clases clase a, b, c, d, e y bueno como os de paso que sepáis que las direcciones de clase A va desde la hasta la 127.255.255.255 y están diseñadas para las redes grandes con una máscara de subred de 255.000.

Las direcciones de clase B van desde la 128.000 hasta la 191.255.255.255 y son adecuadas para redes medianas con una máscara de Schulter de doscientos cincuenta y cinco millones doscientos cincuenta Y cinco.

Las direcciones de clase C van desde la uno noveve dos punto cero hasta doscientos veintitrés millones doscientos cincUenta y cinco millones veinte y cinco mil doscientos cincuenta York cinco y están destinadas para redes pequeñas con una máscara de survival de 255.000 255.000 250 50.

Las direcciones de clase D están reservadas para grupos de multidifusión y van desde la 224.000 hasta la 239.255.255.255 y no utilizan una máscara de subred estándar.

Y por último tenemos las direcciones de clase e que van desde la 240.000 hasta la 255.255.255.255 y están reservadas para propósitos experimentales y no se utilizan en la subred estándar.

Para acabar podéis ver ahí también una tabla abajo a la derecha que habla de direcciones IP privadas, por ejemplo la primera se utilizan dentro de una red local y no son enrutables en Internet, como por ejemplo puede ser la uno cero punto cero cero 1.

La siguiente que es la o 172 16 estas direcciones son privadas y se utilizan dentro de redes locales, no en el Internet público.

La siguiente que tiene un rango 192.

168 hasta la 192.168.255.255 se usa ampliamente para redes locales, domésticas y de pequeñas empresas.

Otro de los grandes servicios a tener en cuenta dentro de una red es el DHCP o Dynamic Host Configuration Protocol, que es un elemento vital dentro de la fase de direccionamiento por direcciones IP dentro de una red privada.

Cada dispositivo que se encargue de suministrar direcciones IP debe estar perfectamente sincronizado con el plan de direccionamiento inicial que antes hemos visto.

Es decir, si hemos asignado rangos específicos, lo que se llama el DHCP pool para dispositivos usuarios, éste debe de aplicar esos filtros.

Pero no sólo se suministra una dirección IP, también se encarga de enviar la dirección IP del gateway o de las DNS primaria y secundaria.

También es posible configurar el tiempo de préstamo de la dirección IP, lo que se llama el list time.

DHCP identifica a los clientes por su dirección Mac.

Por lo tanto es posible asignar una dirección IP específica a un dispositivo o rango de dispositivos IP.

Y una de las tareas más usuales y que también tenemos que evitar o al menos tener muy controladas, es la reserva de direcciones IP.

Una dirección IP reservada no es una dirección IP estática, ya que la primera se suministra por el servidor DHCP, mientras que la otra, la estática, se configura directamente en el dispositivo y su tarjeta de red.

Las direcciones estáticas se suelen configurar para servicios y servidores donde un cambio de la dirección IP o un fallo del DHCP a la hora de hacer la reserva de IP puede tener consecuencias en la infraestructura.

Por ejemplo, se suele asignar a routers, switches, servidores de VPN, etc.

En la diapositiva podéis ver algunas ventajas y desventajas que se aplican a los servicios de IP dinámica y IP estática.

Bien, ahora vamos a ver un pequeño ejemplo de lo que sería un ataque que va dirigido hacia los DHCP.

Pues bien, un ataque muy común a este tipo de servidores DHCP es el que se llama Ataque de agotamiento de direcciones o DHCP Starvation Attack.

Este ataque tiene diferentes fases.

Viendo el diagrama de izquierda a derecha, lo primero que vemos es el inicio del ataque.

Aquí es donde el atacante comienza a enviar peticiones de DHCP Discovery desde una máquina que tiene bajo su control con una dirección Mac falsa.

Después lo que hace es enviar muchas solicitudes.

Entonces genera y envía una gran cantidad de peticiones DHCP Discover, cada una con una dirección Mac diferente, simulando así múltiples dispositivos intentando unirse a la red.

En este punto es cuando vienen las respuestas del servidor DHCP, porque claro, éste empezará a responder a cada solicitud con un mensaje de DHCP ofreciendo una dirección IP del pool de direcciones disponibles.

Después podemos ver que viene el agotamiento del pool de direcciones.

En este punto el servidor agota su pool de direcciones IP disponibles debido a las respuestas a las peticiones falsas y esto lo que hace es provocar directamente una denegación de servicios para clientes nuevos.

Los clientes legítimos que intentan unirse a la red y obtener una IP a través del DHCP no pueden hacerlo porque no hay direcciones IP disponibles y esto provoca una denegación de servicio.

Ya finalmente incluso se puede aplicar un ataque llamado Man in the middle o hombre en medio.

Con la red ya agotada de direcciones IP, el atacante podría establecer su propio servidor DHCP malicioso para ofrecer direcciones IP y parámetros de configuración, permitiéndole potencialmente interceptar o redirigir todo el tráfico de red.

Otras funciones que podemos hacer relacionadas con el subnetting son el NAT, SNAT y DNAT que veremos a continuación.

El NAT o Network Address Translation básicamente es un procedimiento que se utiliza de forma habitual en router y firewall que lo que hace es cambiar la dirección IP de origen y de destino además de los puertos.

Por otro lado, además de reducir el número de IP públicas, también ofrece un sistema de protección ya que oculta las direcciones privadas reales.

Después tenemos el S NAT o Static Address Translation que es un tipo de NAT el cual permite asignar la misma dirección IP pública a un host.

De esta forma cada vez que este host conecte a Internet siempre tendrá la misma IP pública.

Y finalmente vemos el DNAT o Destination NAT, el cual permite que un elemento fuera de la red corporativa sea capaz de acceder a un equipo concreto para redireccionar el tráfico enviado a la IP pública.

Un ejemplo podría ser una red corporativa que tiene configurado en su router un S NAT para hacer que todos los elementos de la red privada tengan acceso a Internet y ésta también pueda dar un servicio, como por ejemplo una página web.

También hay configurado en este router, por ejemplo, un DNAT para que se active en caso de fallo de la red principal.

De esta forma todo el tráfico entrante se puede redireccionar a otra red interna.

Para acabar, seleccionar una topología de red adecuada es fundamental para garantizar la eficiencia en la transmisión de datos y la utilización de recursos.

La subdivisión correcta de redes o subnetting potencia esta eficiencia al optimizar la asignación de direcciones y reducir los dominios de difusión, lo que resulta una mejora de la seguridad y la escalabilidad de la red.

En resumen, una topología bien diseñada junto a un subnetting efectivo, asegura que una infraestructura de red sea confiable, adaptable y capaz de satisfacer las demandas empresariales en constante evolución de nuestra empresa u organización.

Llegamos al final de la sesión.

Os esperamos.