Firewall Implementation

Transcribed on July 31, 2025 at 10:01 AM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de cómo implementar un cortafuegos en una arquitectura basada en Cisco utilizando Packet Tracer.

Aunque nos enfoquemos en el Cisco Packet Tracer nos dará una visibilidad global de como también se realiza en otros tipos de cortafuegos, pero bueno, ya sabemos que Cisco es uno de los más utilizados, con lo cual es una buena práctica entender cómo funciona toda la parte de cortafuegos o de firewall en entorno Cisco.

Bien, vamos a crear un pequeño ejercicio, o mejor dicho una pequeña práctica en la cual vamos a configurar un cortafuegos utilizando Packet Tracer.

Para ello utilizaremos un pequeño escenario con al menos dos redes diferentes y un dispositivo que actúe como cortafuego entre ellos.

Usaremos un router Cisco para este propósito, aprovechando las funcionalidades de firewall básicas que ofrece iOS, pero lo que vamos a hacer, nos vamos a enfocar sobre todo en configurar las reglas de acceso para controlar el tráfico entre las dos redes.

Bien, pues tendremos dos redes, la primera le llamaremos red A, que será la lanza con la IP 192.168.10 con la máscara 24 y ésta se conectará al router por la interfaz, por ejemplo la Fast Ethernet.

Y después tenemos la red B que sería la DMZ que estaría ubicada en la IP 192.168.2.0 con máscara 24 y estará conectada al router en la interfaz de Fast Ethernet 0 1.

El objetivo es configurar el router para que actúe como cortafuegos permitiendo el tráfico de la red A hacia la red B, pero bloqueando todo el tráfico iniciado desde la red B hacia la red A.

Bien, este esquema tan simple intenta explicar un poco lo que acabo de contaros para implementar.

Fijaros, tenemos aquí la red A que es la LAN y la red B que es la DMZ, aquí tenemos un servidor y aquí tenemos un PC, una máquina.

El router que está en la LAN es el que hará de bloqueador, es el que va a intentar redirigir o no el tráfico entre ambas redes.

Por este motivo el objetivo es configurar que este router actúe como un firewall y que permita el tráfico desde la red A hasta la red B, pero que bloquee todo el tráfico que se ha iniciado desde la red B hacia la red A.

Quiere decir que bloqueará el tráfico desde aquí hacia la A, pero si dejará salir desde la A hacia la B, es el típico comportamiento de una DMZ, la cual no permite el tráfico en algún tipo de dirección normalmente hacia la red interna.

Bien, vamos a colocar dos switches y dos PC y finalmente un router que actuará como el cortafuegos entre las dos redes.

Un pequeño detalle antes de comenzar, comentaros que yo aquí he elegido unos tipos de de red o de elementos de red que ya tienen un modelo específico, si queréis evitar algún tipo de problema, porque hay diferencia entre los elementos que tienen un modelo específico y esto que podéis ver aquí que ponen ptrouter, son routers genéricos si queréis evitar problemas de algún tipo, aunque realmente lo que voy a hacer ahora vale igual tanto para un ptrouter de estos genéricos que para uno con una marca, pero os lo digo para el futuro, si queréis hacer de una forma más sencilla todas las instalaciones, os aconsejo ir hacia ptrouter, por ejemplo esto de aquí, o también podemos seguir hacia los switches igual aquí aparte aparecen aquí lo veis PTS, pero yo en este ejercicio quiero hacer lo contrario, quiero que veáis que utilizando cualquier tipo de router o modelo, bueno no cualquiera, con alguno es posible que tengamos que hacer algún tipo de configuración extra, pero que sepáis que también se puede hacer de forma que esté más cercana al dispositivo real, porque esto que veis aquí en pantalla son dispositivos genéricos a los cuales le faltan características, si queréis hacerlo más real tenemos que irnos al modelo concreto que aparece aquí abajo, que corresponde exactamente al modelo que existe en el mundo real.

Bien, dicho esto vamos a comenzar con el ejercicio o con el problema utilizando routers de un modelo específico.

Bien, pues buscamos switches aquí abajo en redes, y por ejemplo, pues este mismo switch, colocamos uno aquí y otro aquí, Bien, ahora colocamos dos PCs por aquí, PC número uno y PC número dos, aquí tenemos la red A y la red B, y ya sólo nos faltaría colocar el router, que lo pondremos aquí en medio.

Bien, voy a poner un poco mejor organizado esto para que después al hacer las conexiones todo tenga más sentido y se vea un poco mejor, lo pondremos así, Bien, conectaremos primero los PCs a los switches, pues utilizaremos un cable, este mismo por ejemplo este, y haremos de aquí fase ethernet al por ejemplo al primer puerto, y aquí haremos exactamente igual, fase de puerto primero, bien, Bien, ahora conectaremos cada switch al router.

Router firewall.

Entonces lo primero que vamos a hacer es colocar un cable como el mismo de cada switch, pondremos el 2, irá conectado aquí al 0, esta sería la red A y haríamos lo mismo con la otra aquí al siguiente libre gigabit y ya tendríamos las dos redes, red A y red B.

Bien ahora habrá que hacer una configuración básica de router, con lo cual tendremos que acceder a la interfaz de router, ya sabréis que hay varias formas de hacerlo.

Y una vez con doble clic ya nos aparece el router y nos vamos a la línea de comando.

Bien aquí le decimos que no y ya podemos empezar.

Primero hacemos un enable para conectar hasta la configuración y el famoso configure terminal que se pone siempre antes de empezar a configurar cualquier tipo de dispositivo iOS, Cisco iOS.

Bien pues vamos a configurar la interfaz Fast Ethernet, corresponde a la LED A, entonces haremos interface Fast Ethernet 0.0 bien este error os lo voy a dejar porque fijaros que he puesto de nombre fast ethernet, realmente router no tiene este nombre, esto es un error habitual porque tendemos siempre a asociar siempre los puertos a este tipo de nombres cuando ahora estamos trabajando con un router, Si vamos para atrás podemos ver que los puertos se llaman Gigabit Ethernet 0, Gigabit Ethernet 0, Gigabit ethernet 0, 1 y 2, con lo cual tenemos que utilizar el Gigabit Ethernet 0 y el Gigabit Ethernet 1.

De todas formas os diré un comando de Cisco BIOS que muestra el listado de tarjetas que tenemos o interfaces que tenemos disponibles, para eso tenemos que salir de la configuración y ahora sí hay que hacerlo antes de entrar, Show IP interface y aquí ya veremos los diferentes interface que tenemos.

Bien pues utilizaremos cualquiera de estos para hacer la conexión.

Pues de nuevo en la clinterface del router vamos a empezar a hacer la configuración, con lo cual volveremos a hacer enable configure terminal y ahora comenzaremos con la configuración, pondremos interface y ahora sí que veremos el número, con lo cual queremos coger la 0 que es la de la red A, pues podemos directamente aquí copiarlo y pegarlo.

Bien pues a esta interfaz le diremos que tiene la ip dress y le diremos la 192.

168.1 y 255.255.

255.0.

Le pondremos un no shutdown para que no se desconecte.

Tenemos un s.

Con esto hemos asignado la dirección ip 192.168.1.1 con una máscara de 24 gb a la interfaz que hemos marcado antes, que era la de Gigabit Ethernet y la activa, ya debe estar activa, de hecho podemos verlo si nos ponemos encima.

Esperamos un poco y aparece en verde, Fijaros.

Y ya pone up.

Y ya aparece en verde la conexión.

Bien, pues ahora haremos lo mismo con la conexión de la redbed de la otra red, con lo cual nos iremos otra vez al Cisco iOS y haremos lo mismo.

Esta vez haremos.

Estamos ya en config, pues haremos un interface y cogeremos la que es esta de aquí, La cogeremos aquí, Copiamos para no equivocarnos y la colocamos.

La seleccionamos y ahora hacemos lo mismo pero esta vez ponemos una dirección diferente.

192768.

Y esta vez ponemos 2 en vez de 1 como hicimos antes.

255-255-2550.

Hacemos el no shutdown para activarla y hacemos un s.

Bien, pues ya deberíamos de ver las dos redes en verde y ahí está correcto.

Y en up.

Bien, ya hemos configurado las redes A y la DED B.

El siguiente paso será configurar el file airwall y para eso crearemos una lista de control de acceso, una ACL.

Bien, pues como hemos hecho antes, doble clic y nos conectamos para crear la access list.

Hay un comando directo que es access list y ya empezaremos a poner los diferentes parámetros.

Lo primero que aquí haremos será permitir todo el tráfico IP desde la red A a la red B.

Para eso haremos esto y pondremos permit.

Bien, access list y ponerle el 100 indica que estamos configurando una lista de acceso con el número 100 es el número de la lista de acceso.

Permit lo que está diciendo es que permite el tráfico que cumple con los criterios que vamos a especificar o que están especificados.

Y ip indica la lista de acceso que se aplica en este caso a paquetes IP.

Bien, pues pondremos la dirección IP de la primera red.

Eso lo hacemos con 192.

168.1 0, porque aplicaremos la máscara 0.0.0255 y después veremos la otra red, que es la 192.168.20.

Y podemos bien, la primera, la 192.

168.10 es la dirección de origen y la otra, la 2.0, la que acaba en 192.

168.2.0 es la dirección de destino.

Y esa máscara lo que hace que en ambos sitios implica que se aplica a cualquier dirección IP dentro de ese rango.

Y bien, este comando lo que va a hacer es emitir el tráfico IP que tiene como origen cualquier dirección en la red 192.168.10 y como destino cualquier dirección a la red 192.16820.

Pues ahora haremos la segunda línea, que lo que va a hacer es justo lo contrario, que es denegarlo.

Con lo cual, ¿Qué es lo que dijimos que iba a denegar?

Pues en este caso el tráfico de la red B a la red A, Es decir, negar todo el tráfico IP que tiene como origen cualquier dirección de red en la 192.168.20 y como destino cualquier punto de la red de la 192.168.10.

Ambas con la máscara baja 24.

¿Y para aplicarlo?

Pues directamente ponemos access como antes, access list lista 100.

Y ahora ponemos deny.

Y ahora de IP.

Y hacemos lo que hemos comentado antes.

¿Qué direcciones de red queremos bloquear?

Las que están en la 2.0.

Cualquier rango relacionado con la 2.0, con esta máscara.

¿Y hacia donde?

A las 192.

168.10 con la máscara 0.0.0 2 5 5.

Bien, con esto tenemos la parte de denegación, ya hay que añadir una lista más, que lo que hace es permitir todo el tráfico IP que no esté dentro de esta regla.

Pues haremos un access list 100.

Permit IP.

Ya hemos creado nuestra access list, ahora tenemos que aplicarla.

¿Y dónde la vamos a aplicar?

Pues en la conexión de red que está asociada a la red B, pues para eso sabemos que la red B está asociada aquí al Gigabit Ethernet, con lo cual copiaremos que nos hará falta ahora.

Y ahora haremos pues una conexión al interfaz, lo pegamos aquí, de Gigabit Ethernet, que es la que está en la red B como hemos dicho.

Y ahora una vez dentro le aplicamos la ACL, que es IP Access Group, este comando lo que hace es que aplica esa ACL al Gigabit Ethernet.

Ya sólo nos quedará hacer algunas pruebas.

Bien, pues bien, ya sólo nos quedará hacer algunas pruebas.

Bien, pues como hemos dicho, esta de la izquierda es la red A y esta es la red B, con lo cual todo el tráfico de la red a la red B tiene que estar habilitado, pero de la red B a la red A no.

¿Este es un poco el principio de la DMZ, verdad?

Que no se pueda, que yo pueda comunicarme con ella, pero ella conmigo no, para evitar ese tipo de acceso desde fuera hacia nuestra DMZ.

Bueno, os he puesto ahí un par de notas, aquí la podéis ver, para que se pueda distinguir mejor cuál es cuál.

Eso lo he hecho con el comando que veis aquí, que es para colocar notas en cualquier ubicación.

Bien, pues ya sólo nos quedaría probar si el PC es capaz de hacer un ping, por ejemplo, al PC, y si el PC es incapaz de hacer un ping al PC, veremos que no tiene asignada una dirección IP, pues tenemos que asignar a nosotros, por ejemplo, le daremos a este equipo una IP, una IP cualquiera.

Bien, antes de asignar la IP tenemos que saber que, vamos a verlo aquí, aquí lo vemos, Tenemos que saber que está conectado al Gigabyte Ethernet, que tiene las 192.168.1.1 con lo cual le podemos dar a este PC la dirección IP 192.168.12 por ejemplo.

Así que iremos a Config, como hicimos la otra vez en Static, pues iremos a Fast Ethernet y pondremos la dirección estática 192.168.1255.255.2550 bien, perfecto, ya lo tenemos.

Bien, es importante además de la IP de la máquina o de la tarjeta, también poner la dirección del gateway.

Se ve aquí en Settings, y pinchando aquí en el Default Gateway pondremos la dirección IP que corresponde a cada uno de ellos, Por ejemplo, al PC que está en la LAN, en la red interior sería 192.168 en cambio para el que está fuera, el PC que está en la DMZ, hay que poner lo mismo, buscamos el PC en settings 192.168.2.1 así cada uno tendrá su gateway para poder enrutar la información correctamente.

Y ahora le pondremos una dirección IP al otro PC, ya la vemos que aquí que está asignada, pues este que está conectado a Gigabit Ethernet 0, tiene la dirección 192.16821.

En este caso pues iremos al PC como antes, iremos a config, iremos a fase Ethernet y la dirección IP estática que sería 192.

168.

255.

Pues igual que antes, salimos a ver si ya está correcto, vemos la IP conectado en su fase, el arnet 0 está conectado al Gigabit del router, con lo cual ya hay conectividad.

Están conectados, con lo cual ya podríamos hacer la primera prueba.

Veremos la prueba de la red A hacia la red B, veremos si hay conectividad, debería de haber conectividad.

Vamos a verlo.

Desktop y nos vamos al Command Prompt y aquí haremos un ping hacia la otra máquina.

Si ahora hacemos un pin desde el PC al PC debería dar fallo, no debería de llegar, así que bueno, vamos a hacer la prueba, vamos a hacer un ping hacia 192 168, sería desde el PC al PC 0, o sea el PC que está en la red P, que es la DMZ.

Queremos hacerle pin al que está en la red interna, en la LAN, pues sería el 1,2.

Nos dice que no puede llegar, no está permitido acceder a esa ubicación.

Packet Tracer es una herramienta invaluable para probar y configurar cortafuegos o firewall de Cisco y de otros fabricantes, porque proporciona un entorno muy fluido para la simulación y para la experimentación que mejora la competencia y la preparación en seguridad de redes.

Además tiene la capacidad de emular dispositivos de seguridad bastante complejos y difíciles de configurar y que de otra forma sería imposible porque son dispositivos bastante caros y complicados de conseguir.

Así que Packet Tracer lo que tiene es que nos fomenta el aprendizaje práctico y con este ejemplo que acabamos de ver, aunque sea en un entorno controlado, tiene una base que se podría hacer exactamente igual en un entorno directamente en producción.

Los comandos son exactamente igual, los mismos.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.