

Configuración de Firewall

Transcribed on August 4, 2025 at 11:08 AM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión, en esta sesión vamos a solucionar el ejercicio planteado en el vídeo anterior, se pedía configurar una regla en el firewall que permitiera en el tráfico entrante la solicitud de eco, es decir la solicitud de PIN, de esta manera se podría hacer PIN a nuestro equipo, el firewall dejaría pasar esa petición que por defecto no está permitido y nuestro equipo respondería a este PIN, de tal forma que se podrían realizar con éxito pruebas de conexión hacia nuestro equipo en la máquina virtual.

Buscamos firewall y seleccionamos el firewall de Windows con seguridad avanzada, nos vamos a las reglas de entrada y aunque nosotros ya tenemos una serie de reglas que están creadas por defecto que tendríamos aquí disponibles, vamos a crear nosotros la regla para permitir la solicitud de eco, damos a nueva regla, seleccionamos personalizado, damos a siguiente a todos los programas y aquí seleccionamos el tipo de protocolo, vamos a seleccionar ICMP versión 4, pero dentro de ICMP no todo ICMP es solo solicitud de eco, entonces nos vamos a la parte de personalizar y vemos que dentro del protocolo ICMP y vemos que dentro del protocolo ICMP tenemos todos estos tipos disponibles, nosotros solo nos interesa la solicitud de eco, de hecho el protocolo ICMP viene cerrado por defecto porque hay ataques conocidos a puertos abiertos, en general hay ICMP, entonces cuando nosotros hacemos una regla de entrada en el firewall para permitir las solicitudes de eco, vamos específicamente a permitir las solicitudes de eco no vamos a permitir todo el protocolo de ICMP, incluso nosotros podríamos seleccionar que estas peticiones de solicitud de eco se hicieran solo desde una determinada red o se hicieran solo desde un determinado equipo, entonces nosotros aquí podríamos seleccionar que esas solicitudes de eco solo fueran desde una determinada red, pues por ejemplo la red que hay de los administradores IT, entonces seleccionaríamos, daríamos aquí a la parte de añadir y seleccionamos por ejemplo 192.168.1.0/24 que sería la red por ejemplo del departamento IT, daríamos a siguiente, en este caso lo que hacemos es una regla de permitir, pero el firewall de windows también nos permite hacer reglas para bloquear conexiones, si por ejemplo sabemos que hay un determinado malware que utiliza unos determinados puertos para establecer las conexiones, podemos denegarlo, incluso puede ser interesante denegar en la parte de reglas de salida aquellas conexiones que nosotros sabemos que son de malware y que ese malware utiliza esa conexión de salida por un determinado puerto, por un determinado protocolo para conectarse con una central o para hacer una conexión inversa para después que los equipos sean controlados o para descargar más malware.

Damos a siguiente y en este caso vamos a hacer una regla que sólo estaría disponible para el dominio o que estaría disponible para el perfil de dominio, para el perfil privado.

Una regla para permitir la solicitud de eco no tiene sentido que se aplique al perfil público.

Quiero que cuando mi dispositivo está en un hotel o está en un restaurante o estoy de viaje con el dispositivo, no se le pueda hacer una solicitud de eco al dispositivo.

Daríamos a siguiente y con esto yo ya tendría creada la regla.

De esta manera estoy permitiendo que se puedan hacer pruebas de conexión mediante ping a este dispositivo de una determinada red sólo cuando el dispositivo está en la red interna de mi organización y no permito cuando el dispositivo está utilizando una red pública que se haga ping y no lo habilitó para otras direcciones.

Con esto llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.