FORTINET
NSE Training Institute

NSE 2 Firewall Scripts—Spanish Version

En esta clase, veremos cómo se diseñaron los firewalls o cortafuegos para brindar una seguridad rudimentaria a la red y cómo evolucionaron hacia una nueva generación para seguir el ritmo del dinámico mundo de las amenazas.

Cuando las redes comenzaron a crecer y a interconectarse y, finalmente, a conectarse a internet, controlar el flujo de tráfico de la red se tornó indispensable. Al principio, dicho control consistía en un firewall de filtrado de paquetes, que examinaba las capas inferiores de los protocolos, como las direcciones de red de origen y de destino, los protocolos y los números de los puertos. Las reglas del firewall utilizaban estos atributos para definir qué paquetes podían atravesar el filtro. Si las direcciones de red, el protocolo y los números de los puertos del paquete se ajustaban a la regla de filtrado de paquetes del firewall, se habilitaba su acceso. En caso contrario, se bloqueaba o se descartaba de manera silenciosa.

La desventaja del firewall de filtrado de paquetes era que adoptaba un enfoque único para decidir si habilitaba el tráfico o no, y los agentes maliciosos podían burlar sus reglas. ¿Qué podía evitar que los agentes maliciosos inyectaran paquetes falsos mediante puertos y protocolos aceptables o que aprovecharan un error en un programa informático de red? Para compensar ese punto débil, en los firewalls de segunda generación se diseñaron criterios adicionales para bloquear o habilitar el tráfico.

Los firewalls de segunda generación, conocidos como firewalls *stateful* o con inspección de estado, se crearon para observar las conexiones de red continuamente. Controlaban las nuevas conexiones de red y analizaban sin pausa la conversación entre los endpoints. Si una conexión actuaba de modo extraño, el firewall la bloqueaba. Cualquier paquete que no perteneciera a una conversación conocida quedaba descartado.

Si bien constituían una mejora, los firewalls de segunda generación aún no podían bloquear los paquetes falsos que utilizaban un protocolo aceptable, como el HTTP. La explosión de la red informática mundial o *World Wide Web* promovió el HTTP, que se convirtió en uno de los protocolos de red más utilizados. El problema es que se utiliza de diversas maneras, como en el contenido de texto estático, el comercio electrónico, el alojamiento de archivos y en muchas otras aplicaciones web. Puesto que todos usan el mismo número de puerto, el firewall no puede distinguirlos. Los administradores de red necesitaban diferenciar las aplicaciones web para bloquear las maliciosas y habilitar las que no lo eran. Para determinar el modo en el que los protocolos como el HTTP se utilizan, el firewall debe analizar los datos en profundidad.

Eso es, precisamente, lo que hacía el firewall de tercera generación. Si bien seguía siendo de tipo *stateful*, interpretaba los protocolos de alto nivel y las aplicaciones que había en ellos, y controlaba los diferentes usos del mismo protocolo básico. Eso se conoce como filtrado en la capa de aplicación (*application layer filtering*). Los firewalls que implementan este filtrado pueden interpretar protocolos del tipo HTTP, FTP y DNS, entre otros. En el caso del HTTP, pueden diferenciar el tráfico del navegador en blogs, sitios para compartir archivos o de comercio electrónico, voz por internet, correos electrónicos y muchos más.

El crecimiento de las conexiones a internet generó además profundos cambios en el trabajo, los juegos, el entretenimiento y el comercio. Las empresas evolucionaron y aprovecharon los servicios multinube más económicos, y la conveniencia de los dispositivos móviles y de internet de las cosas expandió drásticamente los límites de la red. Como consecuencia, se amplió la superficie de ataque. Los agentes de amenaza se transforman sin cesar en cuanto a la complejidad y los métodos de ataque. Hoy en día, los ataques provienen de usuarios, dispositivos y aplicaciones de confianza que esparcen malware, ya sea involuntariamente o con fines maliciosos.

Los ciberataques están en constante evolución. Un firewall debe prevenirlos en todos los extremos de la red y, al mismo tiempo, debe brindar seguridad, fiabilidad y un buen rendimiento de la red. Esto nos lleva a las capacidades avanzadas de seguridad que se

encuentran en los firewalls de última generación (*next-generation firewall*, NGFW). Al igual que un aeropuerto, un firewall de última generación tiene múltiples controles de seguridad. Así como los agentes de seguridad verifican las tarjetas de embarque como primera línea de defensa, un firewall de última generación verifica los paquetes y toma decisiones basadas en reglas para habilitar o descartar el tráfico. A continuación, el equipaje se controla para ver si hay elementos maliciosos. Algo parecido sucede cuando un firewall de última generación lleva a cabo una inspección profunda de paquetes (IPS o sistema de prevención de intrusiones). Si en el equipaje se hallan elementos dudosos, el sistema de control mejorado del aeropuerto lo aparta para examinarlo con más detalle. De modo semejante, un firewall de última generación envía los elementos maliciosos a un entorno de pruebas o *sandbox* para analizarlos en detalle.

A medida que las redes continúan evolucionando y presentando nuevos retos, los firewalls de última generación evolucionan a la par. Por ejemplo, tienen la capacidad de controlar aplicaciones, ya sea mediante la clasificación o según el usuario. La seguridad en la capa de aplicación ayuda a los clientes que navegan por la web a protegerse frente a ataques y amenazas.

Los firewalls de última generación también adoptaron varias estrategias de segmentación para discriminar usuarios, dispositivos y aplicaciones que se ajustan a las necesidades de la empresa. Al segmentar las redes en lugar de utilizar una red plana, el firewall ayuda a que no exista un único punto de entrada, que facilitaba a los ciberdelincuentes el acceso a la red para esparcir amenazas en ella.

Los firewalls de última generación también llevan a cabo una inspección de alto rendimiento y brindan una mayor visibilidad de la red, con una degradación tendiente a cero, para admitir y proteger los modernos centros de datos distribuidos que son parte de una infraestructura de TI híbrida y compleja. Los centros de datos híbridos ofrecen a las empresas una mayor agilidad y flexibilidad, y una escala a demanda. Asimismo, tienen una amplia superficie de ataque que requiere una estrategia de seguridad igualmente evolucionada. La inspección de alto rendimiento incluye aplicaciones, recursos informáticos, análisis y datos cifrados que circulan

en toda la infraestructura, además del almacenamiento de datos a través de diversas nubes públicas y privadas.

FortiGate® es el firewall de última generación de Fortinet. El dispositivo FortiGate® está integrado por completo a otros productos de seguridad que comparten información y que se administran centralmente en el denominado Fortinet Security Fabric.

Gracias por su tiempo, y no olvide responder las preguntas a continuación.