



FORTINET
NSE Training Institute

NSE 2 Web Filter Scripts—Spanish Version

¡Hola! En esta clase, veremos los filtros de contenido web y el desarrollo de esta tecnología.

En los orígenes de internet, existían pocas restricciones o ninguna con respecto a los sitios web que se podían visitar. Por desgracia, algunos de ellos tenían malware que infectaba la computadora desde la que se navegaba. O, a veces, un sitio web mostraba contenido que era objetable para algunas personas. Qué es objetable puede ser controvertido, pero estas dos razones, la seguridad y el contenido objetable, impulsaron el desarrollo de la tecnología de filtrado web.

Entonces, ¿qué es un filtro de contenido web? Es una aplicación que examina las páginas web entrantes para determinar si hay contenido que deba bloquearse en parte o en su totalidad. El filtro de contenido web toma estas decisiones según las reglas establecidas por la organización o la persona que instaló la aplicación. Por medio de la interfaz correspondiente, es posible configurar las reglas y determinar qué se bloquea y qué no. Un filtro de contenido web también permite establecer diferentes reglas para distintos tipos de usuarios. Por ejemplo, en un hogar, puede que los padres deseen aplicar reglas más estrictas para los niños que para los adolescentes y los adultos.

En los Estados Unidos, las bibliotecas fueron las primeras en instalar filtros de contenido web en las computadoras de acceso público, debido a la presión de la comunidad. En 2004, el Gobierno federal aprobó la Ley de Protección de la Infancia en Internet (CIPA), según la cual, si una biblioteca recibía fondos federales para computadoras con acceso a internet, todos los equipos debían contar con este tipo de filtros. No hubo una reacción uniforme a estas medidas. Cuando el filtrado de contenido web se extendió de las bibliotecas a las escuelas, hubo quienes argumentaron que censurar la información, por ofensiva que fuera, iba en contra de la misión de las bibliotecas y de la educación. Aún más, en ocasiones los filtros no tenían la complejidad suficiente para distinguir entre un contenido artístico y una fotografía obscena, o bien bloqueaban literatura debido a una grosería. A partir de las quejas legítimas sobre las limitaciones de la tecnología, los desarrolladores de estas aplicaciones diseñaron técnicas de filtrado más avanzadas e incorporaron una configuración de filtros más granular.

Si bien al principio, el objetivo era proteger a los niños, con el desarrollo de la tecnología su utilidad para otros fines se hizo evidente. La información podría censurarse por motivos religiosos, políticos o ideológicos. Además, las transgresiones pasadas de un determinado gobierno podrían borrarse del registro digital. No obstante, del otro lado de la balanza, la navegación se hizo más segura mediante el desarrollo de filtros que podían bloquear adware, correo basura, virus y spyware. Hoy en día, el filtro de contenido web es la primera línea de defensa contra los ataques en la web. Además de las estaciones de trabajo del cliente, los servidores web y los proveedores de servicios de internet (ISP), se agregaron filtros a otros dispositivos de red, como los firewalls, los servidores proxy, la tecnología sandbox y los puntos de acceso inalámbricos.

¿Cómo funciona un filtro de contenido web? Un filtro de contenido web puede consultar una base de datos de URL en la que figuran sitios web y dominios que utilizan malware, correos de suplantación de identidad y otras herramientas dañinas. Con más de mil millones de sitios web activos en internet, puede ser una tarea engorrosa. La lista negra en la que se encuentran estas URL también se conoce como lista de denegación. Asimismo, puede haber una lista de permitidos, que contiene las URL autorizadas. Otro método posible es un filtro que busca palabras clave o contenidos predefinidos. Como se señaló antes, el problema con este método es la cantidad de falsos positivos. En otras palabras, puede bloquear por error contenidos artísticos legítimos, por ejemplo. Con el tiempo, puede que el aprendizaje automático resuelva estos problemas. Otros tipos de filtros de contenido web, como el motor de búsqueda de Google, utilizan el aprendizaje automático para ayudar al usuario a encontrar lo que busca. Al igual que con otros dispositivos de seguridad de red, el aprendizaje automático es el siguiente paso en el diseño de filtros de contenido web más efectivos.

Fortinet ha incorporado estos filtros en varios de sus productos, como FortiClient®, FortiGate® y, para puntos de acceso inalámbricos, FortiAP™.

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