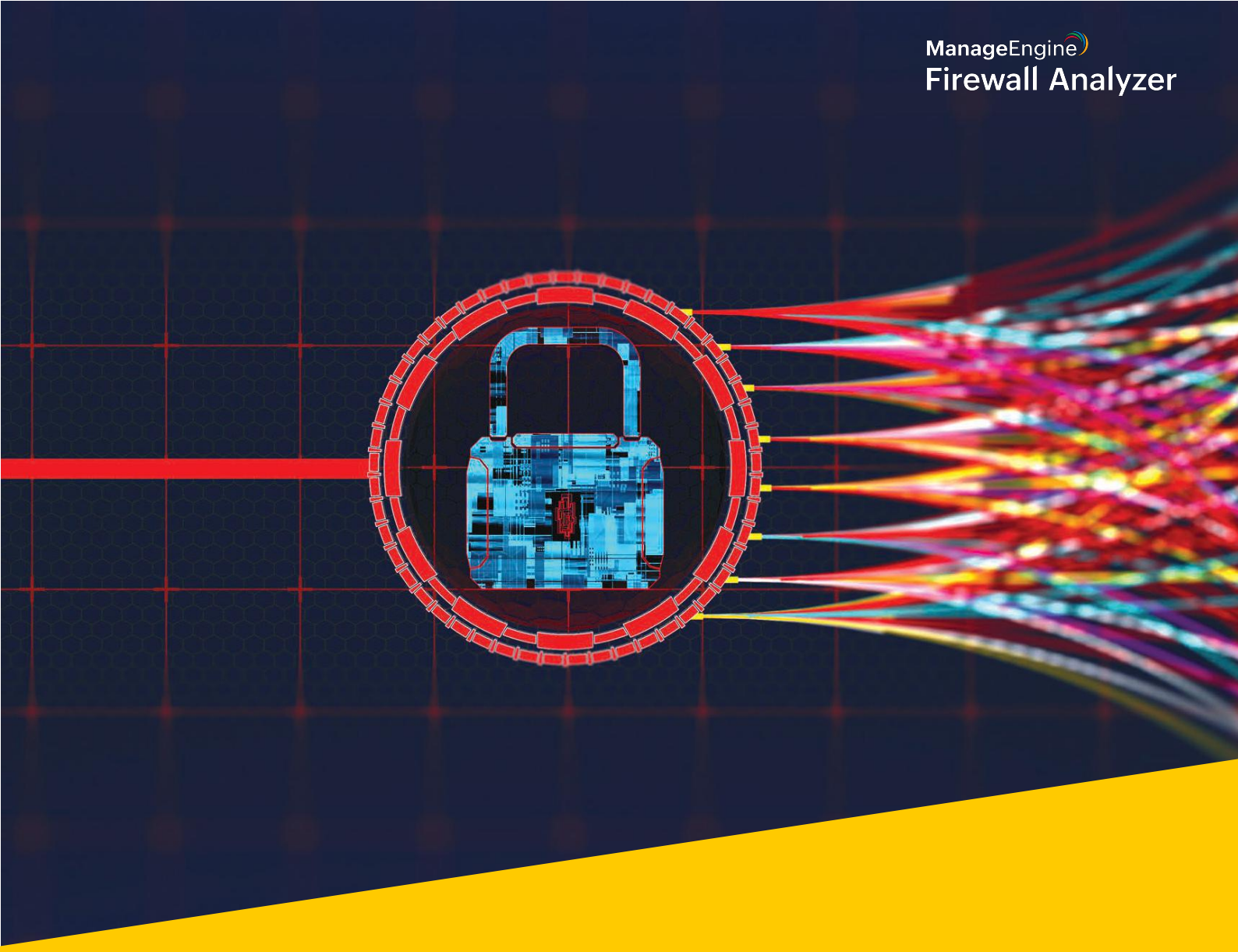
ManageEngine
Firewall Analyzer



E-BOOK GRATIS

10 MEJORES PRÁCTICAS DE FIREWALL PARA LOS ADMINISTRADORES DE SEGURIDAD DE RED

CONFIGURE EL FIREWALL PARA MAXIMIZAR LA EFICACIA

-Mouli Srinivasan

www.manageengine.com/latam/firewall/

Tabla de contenido

Introducción

¡No puede pasar!

Mantenga su red a salvo de los hackers.

Su firewall es la primera línea de defensa contra las amenazas de seguridad, pero como ya sabrá, el simple hecho de añadir dispositivos de firewall y módulos de seguridad a su red no garantiza que su red sea más segura. Necesita observar y analizar regularmente los syslogs y las configuraciones de su firewall, y optimizar su rendimiento para proteger su red. El rendimiento de cualquier firewall depende en gran parte de las reglas y políticas. Si no se gestionan correctamente, podrían hacer que su red quede vulnerable ante los ataques.

Si no se gestionan correctamente, podrían hacer que su red quede vulnerable ante los ataques. Gartner predice que el 99 % de las vulnerabilidades explotadas seguirán siendo las conocidas por los profesionales de la seguridad y TI durante al menos un año. Gartner concluye que la mejor y más económica forma de mitigar los ciberataques causados por vulnerabilidades conocidas es eliminarlas por completo aplicando parches de manera periódica.

Gartner predice que el 99% de las vulnerabilidades explotadas seguirán siendo las conocidas por los profesionales de la seguridad y TI durante al menos un año.

Para muchos administradores de seguridad, mantener el rendimiento óptimo de las reglas es una tarea compleja. Las empresas exigen que las redes funcionen más rápido, lo que deja a los administradores de seguridad en la delgada línea que separa la velocidad de la seguridad. Teniendo en cuenta estos retos, a continuación se exponen algunas de las mejores prácticas de firewall que pueden ayudar a los administradores de seguridad a resolver el dilema de la velocidad frente a la seguridad.

Mejores prácticas de firewall

1. Documentar las reglas de firewall y añadir comentarios para explicar reglas especiales

Es fundamental que todos los miembros de un equipo de TI tengan visibilidad sobre todas las reglas que se han escrito. Además de la lista de reglas, es importante registrar:

- El propósito de una regla.
- El nombre del administrador de seguridad que escribió la regla, junto con la fecha de creación.
- Los usuarios y servicios afectados por la regla.
- Los dispositivos e interfaces afectados por la regla.
- La fecha de expiración de la regla.

Puede registrar esta información como comentarios cuando cree una nueva regla o modifique una existente. Lo primero que debe hacer, si aún no lo ha hecho, es revisar todas las reglas existentes y documentar esta información siempre que sea posible. Aunque esta tarea puede llevar mucho tiempo, sólo tendrá que hacerlo una vez y, eventualmente, ahorrará mucho tiempo a la hora de auditar y añadir nuevas reglas.

2. Reducir las reglas excesivamente permisivas e incluir "denegar todo o denegar el resto" siempre que sea necesario.

Es mejor prevenir que lamentar; es una buena práctica empezar a escribir reglas de firewall con una regla para "denegar todo". Esto ayuda a proteger su red de errores manuales. Después de probar e implementar las reglas, es una buena idea incluir una regla para "denegar el resto" al final.

Esto asegura que su firewall permita sólo el tráfico requerido y bloquee el resto. También querrá evitar el uso de reglas demasiado permisivas como "permitir cualquiera" ya que esto puede poner su red en riesgo.

Las reglas demasiado permisivas dan más libertad a los usuarios, lo que puede concederles acceso a más recursos de los que necesitan para realizar tareas relacionadas con la empresa. Esto conduce a dos tipos de problemas:

- Ancho de banda de red infrautilizado o sobreutilizado.
- Mayor exposición a sitios potencialmente maliciosos.

Restrinja las reglas demasiado permisivas y evite por completo estos problemas.

3. Revisar periódicamente las reglas del firewall. Organizar las reglas del firewall para maximizar la velocidad y el rendimiento.

A medida que pasan los años y diferentes administradores de seguridad definen nuevas políticas, el número de reglas tiende a acumularse. Cuando se definen nuevas reglas sin analizar las antiguas, éstas se vuelven redundantes y pueden contradecirse entre sí, provocando anomalías que afectan negativamente al rendimiento de su firewall. Limpiar las reglas no utilizadas de forma regular ayuda a evitar que colapse el procesador de su firewall, por lo que es importante auditar periódicamente las reglas, así como eliminar las reglas duplicadas, las anomalías y las políticas no deseadas.

Colocar las reglas más utilizadas en la parte superior y mover las menos utilizadas a la parte inferior ayuda a mejorar la capacidad de procesamiento de su firewall. Esta es una actividad que se debe realizar periódicamente, ya que los distintos tipos de reglas se utilizan en momentos diferentes.

4. Comprobar la salud de sus reglas con una prueba de penetración

Una prueba de penetración es un ciberataque simulado contra su sistema informático que comprueba si existen vulnerabilidades explotables. Al igual que los autos se someten a pruebas de choque para detectar fallas en el diseño de seguridad, las pruebas de penetración periódicas en su firewall le ayudarán a identificar las áreas vulnerables de la seguridad de su red.

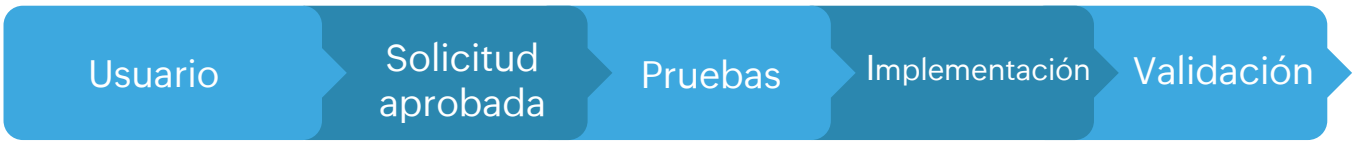
5. Automatizar las auditorías de seguridad.

Una auditoría de seguridad es una evaluación técnica manual o sistemática mensurable del firewall. Dado que consiste en una combinación de tareas manuales y automatizadas, es esencial auditar y registrar los resultados de estas tareas de forma regular. Necesita una herramienta que pueda automatizar tareas y registrar los resultados de las tareas manuales. Esto ayudará a supervisar cómo los cambios de configuración afectan al firewall.

6.Implementar una herramienta de gestión de cambios de extremo a extremo.

La clave para gestionar eficazmente las políticas es contar con una herramienta de gestión de cambios integral que pueda supervisar y registrar las solicitudes de principio a fin. Un procedimiento de cambio típico puede incluir los siguientes

Monitoreo de cambios en la configuración de extremo a extremo



- Un usuario solicita un cambio concreto.
- La solicitud es aprobada por el equipo de seguridad del firewall o de la red, y todos los detalles sobre quién aprueba la solicitud se registran para futuras consultas.
- Tras la aprobación, se prueba la configuración para confirmar si los cambios en el firewall tendrán el efecto deseado sin causar ninguna amenaza a la configuración existente.
- Una vez probados los cambios, la nueva regla se implementa en producción

- Se lleva a cabo un proceso de validación para garantizar que la nueva configuración del firewall funciona según lo previsto.
- Se registran todos los cambios, los motivos, las marcas de tiempo y el personal implicado.

7. Establecer un completo plan de gestión de alertas en tiempo real.

Es fundamental contar con un sistema de gestión de alertas en tiempo real para gestionar el firewall de manera eficiente. Es necesario:

- Monitorear la disponibilidad del firewall en tiempo real. Si un firewall falla, se debe activar un firewall alternativo inmediatamente para que todo el tráfico se pueda enrutar a través de este firewall provisionalmente.
- Activar alarmas cuando el sistema sufra un ataque para que el problema se pueda corregir rápidamente.
- Establecer notificaciones de alerta para todos los cambios que se realicen. Esto ayudará a los administradores de seguridad a vigilar de cerca cada cambio a medida que se produce.

8. Conservar logs conforme a la normativa.

Debe conservar los registros durante el periodo de tiempo estipulado por la normativa que debe cumplir. A continuación se muestran algunas de las principales normas de cumplimiento junto con el periodo de conservación exigido para cada normativa.

Regulación	Requisito de retención
PCI DSS	1 año
ISO 27001	3 años
NIST	3 años
NERC CIP	3 años
HIPAA	7 años
FISMA	3 años
GLBA	6 años
SOX	7 años

Cada país tiene una normativa diferente sobre el tiempo que se deben conservar los registros a efectos legales y de auditoría. Consulte con su equipo jurídico para saber qué normativas debe cumplir su empresa.

9. Comprobar periódicamente el cumplimiento de las normas de seguridad.

Las auditorías internas periódicas, combinadas con las comprobaciones del cumplimiento de las distintas normas de seguridad, son aspectos importantes para mantener una red en buen estado. Cada empresa seguirá unas normas de cumplimiento diferentes en función del sector al que pertenezca. Puede automatizar las comprobaciones y auditorías de cumplimiento para que se realicen de forma periódica y garantizar que cumple las normas del sector.

10. Actualizar el software y firmware de su firewall.

Ninguna red o firewall es perfecto, y los hackers trabajan día y noche para encontrar cualquier brecha de seguridad que puedan. Las actualizaciones periódicas del software y firmware de su firewall ayudan a eliminar las vulnerabilidades conocidas de su sistema. Ni siquiera el mejor conjunto de reglas de firewall puede detener un ataque si no se ha parcheado una vulnerabilidad conocida.

¿Cómo puede ayudar Firewall Analyzer a cumplir estas buenas prácticas de firewall?

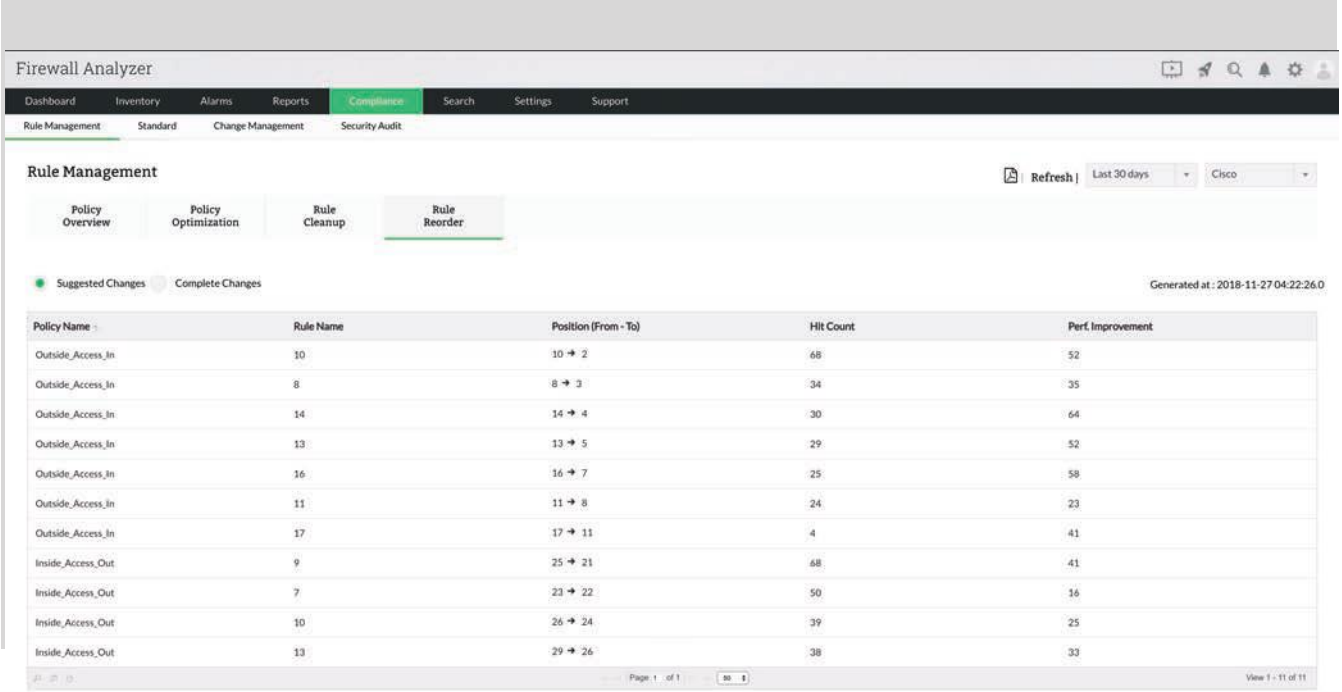
1. Gestión de reglas:

Resumen de la política: Documentar manualmente todas las reglas del firewall y revisarlas regularmente es una tarea ardua y que requiere mucho tiempo. Para resolver este problema, puede utilizar Firewall Analyzer para obtener el conjunto completo de reglas escritas para su firewall. Para simplificar la revisión, también puede filtrar las reglas según los siguientes criterios:

- Reglas permitidas y denegadas.
- Reglas entrantes y salientes.
- Reglas inactivas.
- Reglas con el registro desactivado.
- Reglas excesivamente permisivas, de cualquiera para cualquiera.

Optimización de la política: La función de optimización de políticas de Firewall Analyzer identifica las reglas ocultas, la redundancia, la generalización, la correlación y las anomalías de agrupación. Estas anomalías afectan negativamente al rendimiento del firewall y eliminarlas le ayudará a optimizar la eficiencia de las reglas.

Reordenamiento de las reglas: Firewall Analyzer ofrece sugerencias para el orden de las reglas correlacionando el número de aciertos de las reglas con la complejidad y las anomalías de las reglas. Puede estimar cómo mejora el rendimiento con un cambio sugerido.

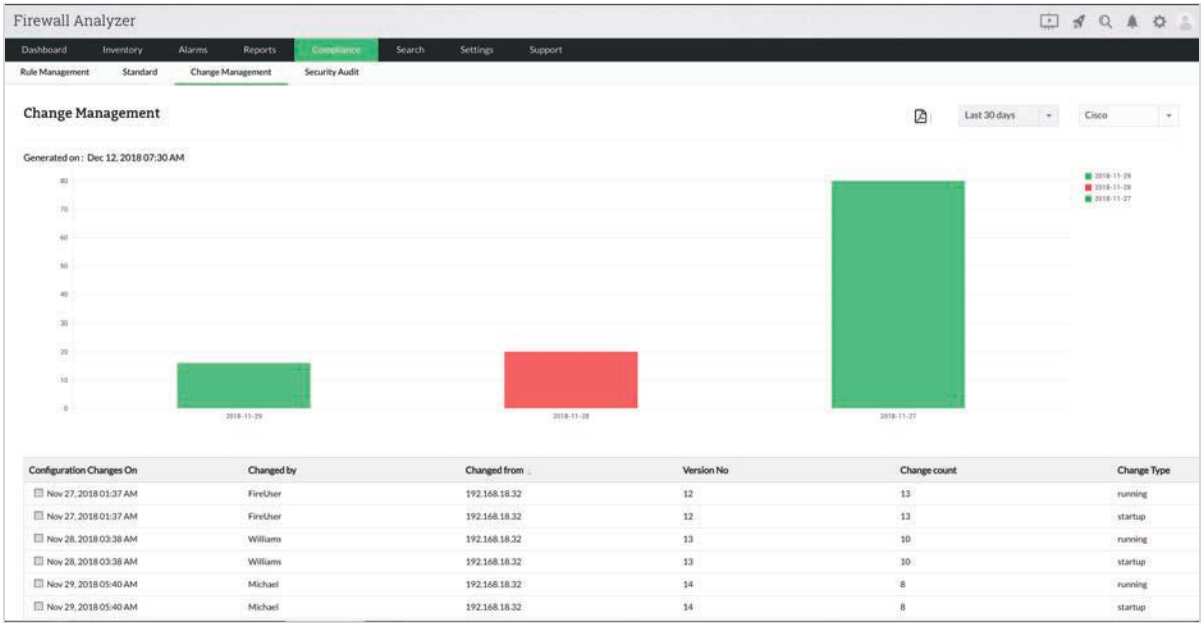


Limpieza de las reglas: Firewall Analyzer proporciona una lista detallada de todas las reglas, objetos e interfaces de firewall no utilizados. La función de limpieza de las reglas le proporciona un resumen general de alto nivel de cuáles reglas, objetos e interfaces se pueden eliminar o desactivar.

Como puede ver, Firewall Analyzer no sólo proporciona visibilidad de las reglas del firewall; sus informes detallados de "Optimización de reglas" y "Reordenamiento de reglas" ayudan a eliminar anomalías e ineficiencias en el rendimiento de las reglas. Juntos, estos informes ayudan a:

- Documentar las reglas del firewall.
- Revisar las reglas del firewall.
- Optimizar el rendimiento del firewall.
- Organizar las reglas del firewall para maximizar la velocidad.

2. Gestión de cambios en la configuración: Firewall Analyzer busca los cambios en la configuración de los dispositivos de firewall y genera el siguiente informe de gestión de cambios.

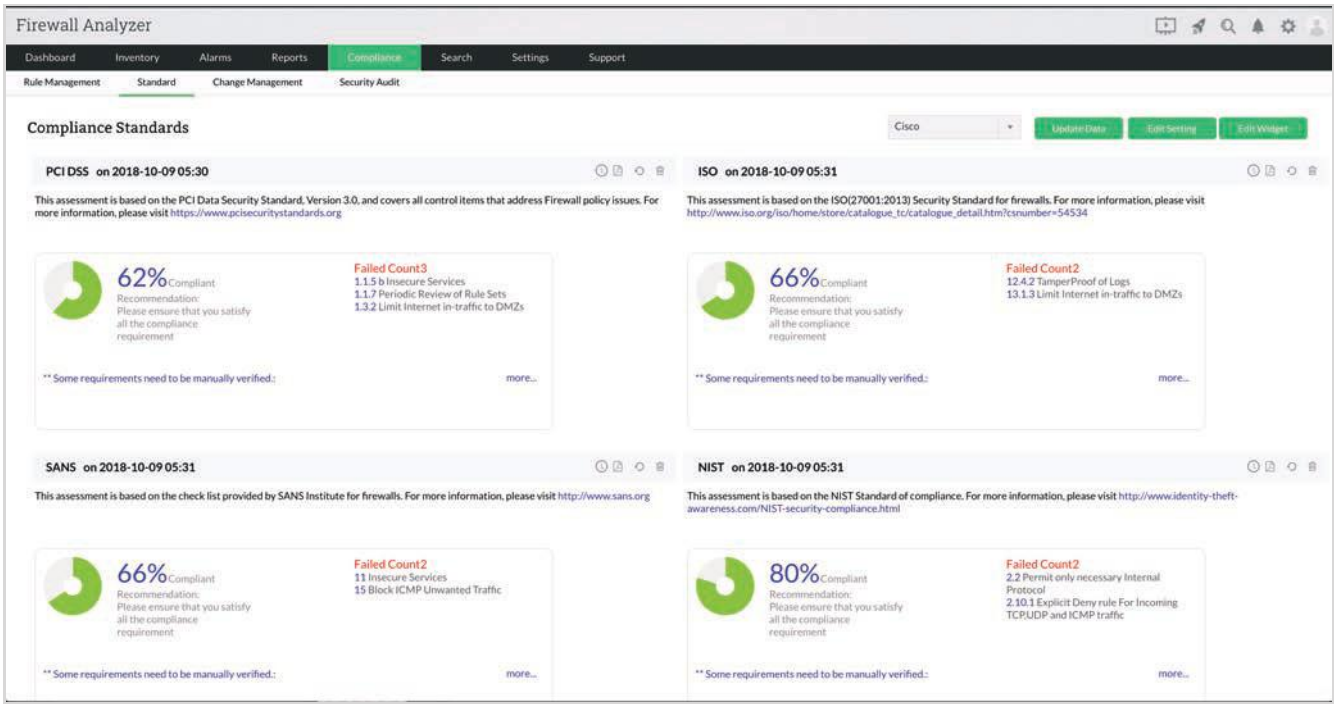


Este informe le ayuda a encontrar quién hizo qué cambios, cuándo y por qué. Firewall Analyzer también envía alertas en tiempo real a su teléfono cuando se producen cambios. Este informe garantiza que todas las configuraciones y los cambios posteriores realizados en el firewall se registren periódicamente y se almacenen en una base de datos.

Al combinar ManageEngine ServiceDesk Plus para gestionar tickets y Firewall Analyzer para monitorear los cambios de configuración, los administradores de seguridad obtienen un monitoreo de cambios de extremo a extremo. Este tipo de sistema de monitoreo de cambios de extremo a extremo es crítico para evitar eventos de seguridad causados por errores humanos.

3. Informes de cumplimiento: Firewall Analyzer genera informes out-of-the-box sobre el cumplimiento de las siguientes normas del sector:

- Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS)
- ISO 27001:2013
- Publicación especial del NIST 800-53
- Norma de Protección de Infraestructura Crítica de la NERC
- Lista de verificación de firewall del instituto SANS



Con estos informes, puede supervisar el estado de cumplimiento de sus dispositivos de flrewall en tárminos de configuraciones.

4. **Auditorías de configuración de seguridad:** Firewall Analyzer puede realizar auditorías de seguridad en el entorno de configuración de su firewall y proporcionar informes detallados sobre las brechas de seguridad. Firewall Analyzer también proporciona la gravedad de las brechas de seguridad, la posibilidad de sufrir un ataque debido a estas brechas, y una recomendación sobre cómo solucionar los problemas reportados.

5. **Gestión de alarmas:** Con Firewall Analyzer, puede establecer notificaciones de alarma tanto para incidentes de seguridad como de tráfico. Firewall Analyzer monitorea los syslogs y envía una notificación cada vez que se supera un umbral de alarma. Las notificaciones de alerta pueden enviarse por correo electrónico o SMS. Las alarmas de Firewall Analyzer le ayudan a identificar los incidentes de seguridad y tráfico en cuanto se producen.

6. **Retención de logs:** Con Firewall Analyzer, puede conservar logs en la base de datos o en el archivo. También puede establecer un periodo de tiempo para la retención de logs con el fin de ahorrar espacio en disco y mejorar el rendimiento; después de todo, los requisitos de espacio en disco pueden superar los 10TB si es necesario conservar los datos de log durante todo un año.

Resumen

Monitorear y revisar continuamente las reglas, la configuración y logs de su firewall es importante para garantizar la seguridad de su red.

Con ManageEngine Firewall Analyzer, puede:

- Documentar y revisar las reglas del firewall.
- Organizar las reglas del flrewall para maximizar la velocidad.
- Monitorear todos los cambios en la configuración del firewall.
- Realizar análisis forenses de los logs del firewall.
- Establecer notificaciones de alarma para anomalías de tráfico y seguridad.
- Generar informes de cumplimiento y realizar auditorías de seguridad.

Con Firewall Analyzer, puede gestionar eficazmente las reglas de su firewall y adherirse a las mejores prácticas.

Acerca de Firewall Analyzer

Firewall Analyzer es un software de análisis de reglas, configuración y logs que ayuda a los administradores de seguridad a detectar y prevenir proactivamente las amenazas a la seguridad de la red. Firewall Analyzer es compatible con los principales firewalls comerciales y dispositivos de seguridad de código abierto.

Con Firewall Analyzer, puede gestionar eficazmente las reglas de su firewall y adherirse a las mejores prácticas.

DESCARGAR PRUEBA GRATIS **SOLICITAR DEMOSTRACIÓN**