INFORMÁTICA FORENSE 2

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

Introducción

Muchos de los problemas de seguridad que aparecieron con la interconexión de redes en el surgimiento de Internet pueden ser remediados o atenuados mediante el uso de determinadas técnicas y controles. Con un firewall podemos implementar un nivel de seguridad apropiado permitiendo al mismo tiempo el acceso a los vitales servicios de Internet. Un firewall es un sistema o un grupo de sistemas que implementan una política de control de acceso entre dos o más redes.

Tabla de contenido

Estrategia de implementación de firewall

La administración del firewall sigue siendo la principal defensa de la red de una organización. Prácticamente, representa la actividad que más tiempo insume a los administradores de seguridad de redes en comparación con cualquier otra actividad. Y equivocarse es fácil, especialmente en el caso de los administradores de TI que desempeñan una doble función como personal de seguridad de TI de su organización.
Existen 5 áreas de enfoque para administrar un firewall:

1. Defina su plan de administración del cambio: Una autoridad de administración del firewall centralizada y un proceso documentado pueden ayudar a evitar cambios indeseados en la configuración actual de la red, al limitar los riesgos que perjudican la funcionalidad, dificultar los cambios futuros o abrir una brecha de seguridad en la red. Un plan de administración del cambio debe cumplir con lo siguiente:
2. Pruebe los cambios de firewall antes de implementarlos plenamente: De ser posible, cree un entorno de prueba que refleje los sistemas de producción. El hecho de no probar los cambios adecuadamente puede conllevar una interrupción del negocio, como problemas de latencia de red o cortes totales de suministro de red.
3. Tome una instantánea de la configuración antes de efectuar grandes cambios de firewall: Tenga implementado un sistema de revisión de cambios, con planes de recuperación y de conmutación por error, antes de que surja una necesidad imperiosa. Las instantáneas constantes del sistema pueden ahorrar tiempo y dinero si una migración se lleva a cabo incorrectamente o si falla un equipo de forma inesperada.
   Con el tiempo, estas instantáneas pueden generar un perfil de la actividad de la red. Este perfil puede ayudar a monitorear el uso de las características de la red, y a detectar los comportamientos irregulares, el exceso de suscripciones y los problemas de carga.
4. Monitoree el acceso de los usuarios a la configuración del firewall: Los registros de acceso de los usuarios pueden funcionar como un sistema de detección de intrusiones primario, que potencialmente puede revelar los intentos de acceso no autorizados desde dentro o fuera de la red. Los registros también pueden poner de manifiesto los cambios progresivos, incrementales e indeseados en la política de seguridad. Como bloqueo de una enorme brecha en la seguridad de su red, el firewall es un solo punto de entrada a la red y contiene elementos de prueba de conexiones no deseadas. El firewall puede exponer códigos malintencionados, troyanos y rootkits mediante alertas de conexiones denegadas o demasiadas conexiones permitidas.
5. Programe auditorías de políticas periódicas: Con el paso del tiempo, es posible que las reglas no coincidan con la política de seguridad, y que las reglas que no se usan bloqueen el tráfico y presenten una barrera a los cambios de red. La seguridad desfasada también puede presentar riesgos legales. Revise su política de firewall con regularidad, actualícela según sea necesario y verifique su cumplimiento mediante la revisión de la configuración y las reglas del firewall. Revise la política en los siguientes casos:
   a. Al introducir nuevas instancias de seguridad o firewall que alteren considerablemente las capacidades de la red.
   b. Al introducir a la red nuevas aplicaciones compatibles con IP.
   c. Al cambiar a un nuevo IPS (proveedor de servicios de Internet).
   d. Al comenzar a compartir tráfico de red en colaboración con un socio empresarial.
   e. Al atravesar un cambio empresarial u operativo importante.
   f. Al sostener una rotación de personal significativa.

Las reglas en un firewall

Las reglas definen qué tipo de tráfico de internet se permite o se bloquea, cada uno de los perfiles del firewall tiene un conjunto predefinido de reglas de cortafuegos, el cual no puede cambiar. Sólo puede agregar reglas nuevas a algunos de los perfiles. En algunos perfiles no podrá agregar sus propias reglas. También es posible que haya un perfil sin reglas predefinidas que le permita agregar sin restricciones su propio conjunto de reglas. El perfil de cortafuegos seleccionado también afecta la prioridad que reciben sus propias reglas en relación a las reglas predefinidas.

Una regla de cortafuegos se puede aplicar al tráfico procedente de Internet a su equipo (entrante) o desde su equipo a Internet (saliente). Una regla también se puede aplicar a ambas direcciones de forma simultánea.

Una regla de cortafuegos consta de servicios de cortafuegos, que especifican el tipo de tráfico y los puertos que este tipo de tráfico puede utilizar. Por ejemplo, una regla llamada Navegar por Internet tiene un servicio llamado HTTP, que utiliza TCP y el puerto número 80.

Las reglas de cortafuegos también definen si aparecen ventanas emergentes de la alerta de cortafuegos que muestran el tráfico que coincide con las reglas del cortafuegos.

Guía de mejores prácticas para implementar entornos de firewall

La guía de diseño de la tecnología ofrece detalles de implementación, información sobre software y productos validados, y mejores prácticas para la implementación del firewall. La seguridad del firewall es una parte integral de cada implementación de extremo de Internet, dado que protege la información mientras que satisface la necesidad de redes seguras y confiables, y aplica las políticas a fin de mantener la productividad de los empleados. Donde se aplican las regulaciones de la industria, los firewalls desempeñan una función crucial en la capacidad de las organizaciones para abordar los requisitos de cumplimiento regulatorio. Los requisitos regulatorios varían por país e industria; este documento no cubre requisitos de cumplimiento regulatorio específicos. Los servicios de Internet se han convertido en una parte clave de las operaciones diarias de muchas organizaciones hoy en día. Brindar un acceso seguro a Internet y evitar el ingreso de contenidos maliciosos a la organización es fundamental para mantener la productividad de los empleados. Además del acceso de los clientes a Internet, las organizaciones tienen la necesidad casi universal de contar con una presencia web disponible para que los partners y clientes accedan a la información sobre la organización. Colocar información corporativa en Internet acarrea el riesgo de exponer los datos a un ataque en los servicios públicos. Para que una organización use Internet eficazmente, se debe encontrar la solución de todos estos problemas.

La alta disponibilidad en la implementación de firewalls

En el escenario de disponibilidad, los firewalls se presentan de una manera en las arquitecturas de seguridad como un punto de estrangulamiento en la comunicación, donde todo el tráfico que entra y sale de Internet pasa, para ser evaluado, liberado o no. Esto quiere decir que si la solución de firewall no está disponible, el acceso a Internet será automáticamente cortado.

Muchas empresas invierten en enlaces de comunicación alternativos para, en caso de falla de uno de ellos, continuar teniendo acceso a Internet a través de otros proveedores de servicio. Esta es una estrategia válida, pero no sirve en caso de paralización del dispositivo de seguridad que conecta dichos vínculos. Si se detienen, todos los enlaces se detendrán automáticamente. Alternativas para hacer un bypass del dispositivo ponen en riesgo la seguridad del ambiente y no deben ser una opción para la empresa.

La buena noticia es que el costo con alta disponibilidad de firewalls ha sido reducido a lo largo del tiempo, tanto en términos de inversiones de hardware propiamente dicho, como en formatos de licenciamiento, que

flexibilizan especialmente en el modelo de activo-pasivo. Por lo tanto, la cuenta es simple y generalmente la inversión se devuelve rápidamente ya en la primera indisponibilidad.

Una estructura de firewall en alta disponibilidad presenta las siguientes ventajas:

- Continuidad de servicio frente a fallas de hardware.
- Posibilidad de usar hardware standard (PC clone) para funciones críticas.
- Permitir actualizaciones de software sin interrupción del servicio.
- Si además se puede contar con más de una conexión a internet, puede continuarse el servicio aún frente a una caída de uno de los enlaces.

Disponibilidad de firewalls en formato activo-pasivo

Existen básicamente dos formas de operar un firewall redundante, o un cluster de **alta disponibilidad de firewalls**. El primer modelo, activo-pasivo, significa que en un dado momento sólo un dispositivo responde por todas las requisiciones.

Otros dispositivos son accionados, de forma automática o manual, solamente en caso de caída del principal. Es un modelo interesante y ahorra algunos recursos, especialmente de licenciamiento, pero para muchos casos, donde hay mucho procesamiento, no es suficiente.

Disponibilidad de firewalls activo-activo

En este modelo, todos los nodos que componen el cluster de alta disponibilidad responden a las peticiones, y además de garantizar la continuidad del ambiente en caso de caída de algún dispositivo, distribuyen la carga de procesamiento.

En cuanto a la perspectiva de inversión son escenarios más caros pues es interesante que la capacidad de los equipos sea la misma, y además, el licenciamiento en la mayoría de los proveedores es duplicado.

Disponibilidad de firewalls cluster híbrido

Un cluster híbrido, generalmente operando en formato activo-pasivo, utiliza diferentes plataformas en la solución de firewall. Por ejemplo, el nodo activo es un appliance (dispositivo físico) mientras que el nodo backup es un virtual appliance, que se ejecuta dentro de algún hypervisor.

El modelo es interesante porque ahorra recursos o permite reutilizar equipos que serían descartados para una posición fuera de producción, siendo utilizados solamente en momentos de emergencia. Muchas empresas no se adhieren a este tipo de práctica, pero es una alternativa de viabilidad en muchos casos.

Independiente del modelo a ser utilizado, es interesante que las empresas estén debidamente preparadas para la continuidad de conectividad, y eso debe ser un ítem relevante a ser tratado en un Plan de Continuidad de Negocios.

El tamaño de la empresa ya no es justificativa para aprobar presupuestos para operar en modelos de redundancia con firewalls, cuanto más dependiente las empresas se vuelven de la disponibilidad, más fácil de justificar las inversiones asociadas a este tipo de proyecto.

Las redes DMZ (Zona DesMilitarizada)

El uso de éste termino es habitual para redes de empresas grandes donde podemos crear una zona segura de acceso a determinados equipos que se encuentran separados de otros, sirven sobre todo para evitar problemas existentes para ejecuta programas o acceder a determinados servicios desde el exterior que se encuentran en un dispositivo que esta bajo la regla DMZ lo que significa que al equipo que tiene esa dirección de equipo de la red LAN sobre la que el router de libres todos los puertos, salvo aquellos que se encuentran en reglas en la tabla NAT.

En muchos casos se utiliza para mejorar el rendimiento de las aplicaciones como videojuegos, programas, P2P, servicios web y así hasta completar una larga lista.

Conclusiones y recomendaciones

Como conclusión se puede decir que el firewall sirve para proteger una red privada contra intrusos dentro de un esquema de conectividad a Internet. También sirve para prevenir el acceso de usuarios no autorizados a los recursos computacionales en una red privada.

Referencias bibliográficas

- Carpentier, J. (2016). *La seguridad informática* en la PYME. Editorial ENI.
- Cañon, L. (2015). *Ataques Informáticos Ethical Hacking y conciencia de seguridad informática en niños. (Trabajo de Fin de Grado).* Universidad Piloto, Colombia.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica