Firewalls vs. SBCs

Comprendiendo el modelo OSI y las implicaciones para RTC

White Paper

Introducción

Empresas de todos los tamaños están implementando soluciones de VoIP para apoyar los negocios globalizados y a las fuerzas de trabajo móviles . A pesar de una lenta adopción en los primeros días de VoIP, estudios indican que el mercado para servicios de VoIP alcanzará los $204,8 mil millones el año 2020. La adopción de VoIP no muestra indicios de ralentización, pero su implementación y gestión presentan algunos desafíos.

Las infraestructuras de telefonía tradicionales estaban sujetas al desvío de llamadas, re enrutamientos y a las escuchas a escondidas ya que hackers controlaban redes de telefonía corporativas de manera ilegal. Las redes PSTN están dando paso a soluciones de VoIP, pero eso no significa que las preocupaciones de seguridad tradicionales están desapareciendo. Los cibercriminales se aprovechan de la voluntad de empresas de abrir sus comunicaciones a la Internet con VoIP.

Muchas empresas creen que los firewall son suficientes medidas de seguridad para protegerse contra muchas amenazas diferentes. La realidad es que la mejor seguridad para servicios de VoIP son los controladores de frontera de sesión (SBC por sus siglas en inglés).

A pesar de que los firewall y SBC parecen cumplir con las mismas metas de seguridad, al examinar sus diferencias en el manejo de comunicaciones en tiempo real podemos ver la necesidad de ambos para una seguridad adecuada.

La evolución de los firewall

Tradicionalmente, los firewalls operan en la Capa 2 (capa de enlace de datos), Capa 3 (capa de red) y Capa 4 (capa de transporte) del modelo OSI y bloquean el tráfico en base a puertos en toda su red. A pesar de que esto aún es parte de la ecuación, los firewalls de última generación tienen una funcionalidad elevada con conciencia de aplicación.

Ahora no importa qué tipo de tráfico está circulando por la red. Si este es en base a IP, el firewall de última generación puede identificar las firmas de la aplicación, comprender el contexto de los paquetes de datos y bloquear malware de manera inteligente. En lugar de implementar políticas generales en base a puertos, los firewall de última generación pueden rápidamente actualizar las listas de malware conocidos y permanecer delante de atacantes. Y si un malware es detectado, estos nuevos firewall pueden enviar paquetes de datos a un entorno de pruebas para examinar archivos y códigos potencialmente maliciosos. Mejor aún, cuando firewalls de última generación trabajan en conjunto con protección del End Point, se puede contar con una solución de seguridad flexible capaz de adaptar a prácticamente cualquier tráfico de datos.

Dejando atrás a antivirus basados en firmas y firewalls basados en puertos por estas soluciones de última generación y flexibles puede parecer la manera perfecta de cubrir toda necesidad de seguridad. Sin embargo, estas soluciones no están optimizadas para abordar las vulnerabilidades emergentes en comunicaciones de voz y video en tiempo real.

OSI Model

	Datos	Capas
Host Layers	**Datos**	**Aplicación** Proceso de la red a la Aplicación
	Datos	**Presentación** Representación y codificación de Datos
	Datos	**Sesión** Interhost Comunicación
	Segmentos	**Transporte** Conexiones y Contabilidad de Extremos a Extremo
Media Layers	**Paquetes**	**Red** Determinación de IP de Ruta (Direccionamiento Lógico)
	Marcos	**Enlace de Datos** MAC y LLC (Direcionamiento Físico)
	Bits	Medios, Señal y Transmisión Binaria Física

Firewalls vs. SBCs: Implicaciones para soluciones de comunicaciones en tiempo real:

Los sistemas de comunicaciones de negocios son críticos y deben estar disponibles 24/7. Profesionales de InfoSec no pueden simplemente activar y desactivar tráfico en puertos específicos y aun esperar poder conducir una empresa. De hecho, los firewall pueden ser desplegados como servidor proxy SIP que puede retransmitir y controlar información de señales SIP. Sin embargo, ya que el servidor no está activamente involucrado en la ruta de medios del protocolo de transporte (RTP por sus siglas en inglés) en tiempo real, este no puede controlar las comunicaciones en tiempo real de manera de asegurar conexiones de voz y video de calidad y seguras.

Los SBC, por otra parte, están específicamente diseñados para la gestión y seguridad de comunicaciones IP, y proporcionar ventajas claves para la calidad y seguridad del RTP:

- Transcodificación de protocolo
- Visibilidad de KPIs de voz y video tales como inestabilidad, latencia, rendimiento y más
- Control de política dinámico para aplicaciones de comunicaciones

El principal problema con los firewall de última generación para la protección del tráfico de comunicaciones es que están construidos especialmente para ignorar flujos en tiempo real. Sus gateway de capa de aplicación (ALGs por sus siglas en inglés) integrados no están optimizados para el tráfico de comunicaciones, lo que significa que muchas veces cortan el flujo de datos para cualquier cosa superior a llamadas básicas. Incluso peor, no están diseñados para manejar la encriptación RTP por lo que, si usted está usando encriptación en su tráfico de voz y video, los firewall no podrán ofrecer ninguna protección contra intrusiones, sin importar qué tan avanzada es la aplicación.

En momentos en que los atacantes se han dado cuenta que un malware sencillo puede pasar directamente a través de una red si es enviado vía un puerto de video, las empresas no pueden confiar en firewalls de última generación para proteger su tráfico de comunicaciones críticas. Es ahí donde los SBCs entran en escena.

Cómo los SBC garantizan la seguridad de VoIP

Los SBCs van más allá de una terminación SIP y traducción de dirección de red. Están profundamente involucrados en las señales del tráfico de comunicaciones y están construidos para trabajar con todas las características avanzadas de voz/video. A diferencia de los firewall, los SBCs actúan como puntos de delimitación de borde, lo cual significa que pueden decodificar tráfico para analizar la presencia de actividad maliciosa sin interrumpir los flujos en tiempo real.

Contar con SBCs es esencial para la seguridad y calidad del tráfico de comunicaciones único. A diferencia de la mayoría del tráfico de datos, los flujos de voz y video están divididos en una capa de señales y una capa de medios. Los firewall están diseñados para tráfico de un flujo, mientras que los SBCs pueden comprender el contexto de las capas de señales y medios para asegurar el flujo en tiempo real.

Como resultado, los SBCs cubren cinco preocupaciones de seguridad claves que los firewall no pueden abordar:

- **Protección contra ataques maliciosos:** Al ocurrir ataques de denegación de servicio (DoS) y DDoS distribuido (DDoS), estos inundan las redes con tráfico malicioso intentando desactivar los sistemas e investigar la presencia de debilidades. Los SBCs pueden fácilmente separar el tráfico de VoIP de la actividad maliciosa, permitiendo que sólo tráfico de voz pase y eliminando el resto. Los SBCs pueden dinámicamente ajustar la asignación de recursos para aislar de degradación en la QoS a los sistemas de comunicación que ocurren con picos de tráfico DoS y DDoS.

• **Protección contra fraude de tarifas:** Un número en aumento de hackers está entrando en los sistemas de VoIP para encaminar onerosas llamadas internacionales lo que puede resultar en decenas de miles de dólares en cargos. Con un SBC instalado, las organizaciones pueden programar la solución de VoIP para denegar tonos de marcación secundarios.
• **Encriptación:** Mensajes de comunicación en tiempo real son relativamente fáciles de interceptar. Sin embargo, Zeus Kerravala, Analista Principal en ZK Research, indica que "los SBCs usan Seguridad de Capa de Transporte para asegurar el tráfico de señales y que este sea invisible para hackers. Los SBCs usan el Protocolo de Tiempo Real Seguro para asegurar los media packets y agregar otra capa de protección."
• **Ocultamiento de topología:** Comunicar entre dos redes le puede entregar acceso a la topología de red corporativa a usuarios autorizados. Los SBCs eliminan el riesgo al ocultar la topología en todas las comunicaciones.
• **Gestión de tráfico IP:** Básicamente, los SBCs limitan la cantidad de sesiones que pueden ocurrir al mismo tiempo. De manera similar a la protección contra DDoS, la gestión de tráfico IP garantiza la calidad del servicio al mitigar los efectos que grandes volúmenes de llamadas tienen en el sistema como un todo.

Conclusión: Tanto los SBC y los Firewall son necesarios para la seguridad

Garantizar la seguridad y la calidad debe ser una prioridad a medida que organizaciones de todos los tamaños implementan soluciones de VoIP. Si bien los firewall y SBCs parecen cumplir con similares metas de seguridad de manera superficial, sus diferencias en el manejo de comunicaciones en tiempo real prueban que existen diferencias significativas. Las soluciones de comunicaciones en tiempo real tienen requerimientos únicos, e incluso las interrupciones más mínimas a nivel de red pueden resultar en discursos incomprensibles, llamadas de conferencia llenas de estático, pixelado del video y problemas de sonido.

Comprender cómo los firewall y SBC controlan el tráfico e implementan políticas de seguridad es el primer paso para crear un diseño de red que protega los sistemas de comunicación vitales al proporcionar a los usuarios con los niveles de QoS que necesitan para hacer sus trabajo diariamente. Sin un SBC trabajando con firewalls, los grupos de TI estarán constantemente respondiendo reclamos de usuarios y solucionando problemas que pueden ser extremadamente difíciles de resolver en el largo plazo.

Sobre Ribbon Communications

Ribbon es una empresa con dos décadas de liderazgo en comunicaciones en tiempo real. Construida sobre tecnología de clase mundial y propiedad intelectual, Ribbon entrega comunicaciones en tiempo real inteligentes, seguras e integradas para el mundo de hoy. La empresa transforma redes fijas, móviles y corporativas desde ambientes de legado a arquitecturas IP seguras y basadas en la nube, habilitando comunicaciones altamente productivas para consumidores y empresas. Con ubicaciones en 28 países alrededor del mundo, la cartera innovadora y líder del mercado de Ribbon empodera a proveedores de servicios y empresas con la rápida creación de servicios en un ambiente completamente virtualizado. La Plataforma de Comunicaciones
como un Servicio (CPaaS) Kandy de la empresa entrega un conjunto integral de capacidades avanzadas de comunicaciones
integradas que permiten esta transformación.

Para saber más, por favor visite rbbn.com