Opinión profesional

Proteger el Internet de las Cosas

El desafío de las nuevas tecnologías

El Internet de las Cosas está en constante crecimiento. Este avance trae aparejada una cantidad de datos muy grande que demandará, a su vez, una mayor capacidad de procesamiento en la red y mayor seguridad para enfrentar los ataques informáticos a los que estará expuesto.

Aaron Goldberg
IDG Contributing Editor

A medida que crece Internet de las Cosas (IdC), la atención se centra en los miles de millones de dispositivos que podrán conectarse a través de la red. Sin embargo, lo que a menudo se pasa por alto es el problema más importante: ¿cuánto tráfico de red se creará como el resultado del IdC? Según un informe elaborado por la compañía Bell Labs, el IdC cambiará la manera en la que se administran las redes, mientras que IDC pronostica que las cargas de trabajo en esquemas IdC crecerán a tasas de 750 % entre el 2014 y 2019.

Muchos dispositivos primitivos para IdC en la actualidad pueden mover una pequeña cantidad de datos por conexión, aunque eso irá cambiando a medida que las aplicaciones de monitoreo constante (como vehículos autónomos, análisis de tiempo real y aplicaciones basadas en localización) creen flujos mucho más grandes, que deberán ser manejados en tiempo real.

Otra consideración importante es que muchos de estos dispositivos también requerirán un control de monitoreo de seguridad que pueda asegurar que no se convertirán en un conducto de malware y otros atentados. Ya se ha visto que los hackers son capaces de entrar a un Jeep y desactivar al automóvil de manera remota. Aunque esto fue una demostración y no se trató de un ataque real, dejó en evidencia lo grave que puede ser una amenaza puesta en práctica.

USO DE IDC Y SU IMPACTO EN LA RED

Sobre la base de lo que se conoce en la actualidad, hay dos tipos específicos de IdC, masivo y crítico, que serán la base de su crecimiento. Cada uno de ellos tiene su propio impacto, tanto en el tráfico de la red como en su seguridad.

- IdC masivo: es el más común, en el que se piensa cuando se nombra IdC. Consiste en un gran número de dispositivos que se comunican con otros dispositivos o servidores. El impacto en el tráfico de la red se dará de dos maneras distintas: la primera, la más obvia, es un rápido crecimiento en la cantidad del tráfico de la red. La segunda es que habrá varios tipos de dispositivos, cada uno con su tráfico propio, que requerirán visibilidad y monitoreo.
- IdC crítico: este se refiere a las aplicaciones como conducción autónoma, cuidado de la salud, internet táctil y cargas de trabajo similares, que demandarán mínimos retrasos en los retornos en "U" de estos dispositivos en relación con su comunicación con la red. Este tipo de tráfico añadirá un gran número de nuevas cargas de trabajo críticas que deberán ser consideradas QoS de primerísimo nivel. Como resultado, la visibilidad de tráfico y las herramientas de monitoreo deberán ser capaces de soportar grandes cargas de trabajo de distintas aplicaciones, donde la latencia y los retrasos no serán aceptables.

VISIBILIDAD DE TRÁFICO Y HERRAMIENTAS DE MONITOREO

Los retos actuales de la seguridad tradicional en IdC han convertido al monitoreo del tráfico integral y la visibilidad en elementos esenciales para proteger a las organizaciones de una manera eficiente y efectiva.

Una de las prácticas posibles es la de optimizar los elementos del sistema de seguridad: a medida que el tráfico crece rápidamente, es fundamental asegurar que los dispositivos de seguridad no sean abrumados con el tráfico de datos; sobre todo por el que no es relevante. La capa de visibilidad entrega inteligentemente solo el tráfico apropiado para que estos dispositivos puedan priorizarlo y así permanecer dentro de los parámetros de funcionamiento. Las aplicaciones críticas no serán impactadas por la necesidad de implementar nuevas instancias para estas herramientas.

La habilidad de proteger rápidamente los dispositivos o sistemas contra nuevos tipos de amenazas será también muy valorada. La única certeza cuando hablamos de amenazas en el Internet de las Cosas es que veremos nuevas versiones de ellas, desconocidas actualmente. La capacidad de usar soluciones integrales de visibilidad de tráfico para identificar lo nuevo o inusual es determinante.

Un excelente soporte para múltiples niveles de QoS para cargas de trabajo en IdC es indispensable. Como se señaló anteriormente, con una amplia gama de cargas de trabajo y el tráfico, la capacidad de identificar el nivel apropiado de servicio para los diferentes tipos de tráfico es esencial. La visibilidad del tráfico hace que, dentro de la red, se pueda equilibrar de manera más simple. Esto no solo mejora la capacidad de entrega de QoS, sino que esta misma capacidad de priorización puede ser llevada a soportar el tráfico que se reenvía a diferentes soluciones de seguridad.

A medida que el Internet de las Cosas se vuelva más común, habrá un mayor impacto en las herramientas necesarias para asegurar el tráfico. Apoyar la seguridad del IdC requerirá dos enfoques principales: la visibilidad del tráfico integral de la red y el monitoreo en conjunto con una plataforma de seguridad. Esto proporcionará un proceso para que las soluciones de seguridad estén seguras del tráfico que están analizado, protegiendo y evaluando, manteniendo un nivel apropiado en los servicios y en la capacidad de respuesta. ■