opengear
A DIGI COMPANY

DOCUMENTO TÉCNICO

Por qué necesita la gestión fuera de banda

Las interrupciones del sistema pueden ser el resultado de ataques cibernéticos, errores humanos o cualquier cantidad de condiciones ambientales.

Una amplia gama de elementos de red también pueden causar interrupciones. Las interconexiones de cables, las fuentes de alimentación, los conmutadores, las carcasas de computación de alta densidad, las matrices de almacenamiento e incluso el aire acondicionado son posibles fuentes de problemas. Los dispositivos de red solo están aumentando en complejidad, con pilas de software que se actualizan con frecuencia y son susceptibles a errores, exploits y ataques cibernéticos.

ACCESO A SU RED DE CONEXIÓN PERMANENTE DISPOSITIVOS

Si su red principal no está disponible, ¿todas las partes de su red, desde los centros de datos y sucursales hasta las redes periféricas y dispositivos IoT, tienen flexibilidad de conexión? A medida que su negocio crece, su red se vuelve cada vez más compleja y las nuevas implementaciones o adquisiciones pueden carecer de la capacidad de conectarse sin problemas a través de Internet.

Considere estos ejemplos recientes de interrupciones y ataques importantes:

- **2015 y nuevamente en 2018 - Google :** Robo de información privada en los perfiles de Google+, incluido el nombre, el empleador y el cargo, la dirección de correo electrónico, la fecha de nacimiento, la edad y el estado de la relación. La violación provocó que Google cerrara permanentemente el servicio de Google+.
- **2018 - British Airways :** Un hackeo en el sitio web y la aplicación de BA permitió el robo de datos financieros y personales de más de 380.000 clientes.
- **2019 - Target :** Una interrupción de dos horas de los registros de la compañía les costó $ 50 millones en ventas.
- **2019 - Facebook:** Múltiples interrupciones de la red, que le cuestan a Facebook $ 6.3 millones por cada hora de inactividad. Esto no tiene en cuenta las pérdidas adicionales que sufrió la compañía cuando sus acciones sufrieron un golpe.

Ningún negocio puede permitirse interrupciones, pero cuanto más grande sea su red, más probable será que ocurran. Las interrupciones son costosas y pueden requerir que tenga técnicos en el sitio para que se encarguen de ellas en cualquier momento. Incluso las actualizaciones de firmware, los cambios de configuración y el ciclo de encendido para corregir los errores requieren ayuda práctica. Necesita acceso remoto a través de una conexión secundaria para tener acceso permanente a sus dispositivos de red.

¿QUÉ CAUSA LAS INTERRUPCIONES?

Las interrupciones del sistema pueden ser el resultado de ataques cibernéticos, errores humanos o cualquier cantidad de condiciones ambientales.

Las interrupciones también pueden ser causadas por fallas de hardware de red y vulnerabilidades en las pilas de software actualizadas con frecuencia.

> En junio de 2019, los proyectos de Google Cloud que ejecutan servicios en varias regiones de EE. UU. experimentaron una gran pérdida de paquetes como resultado de la congestión de la red durante varias horas. Al analizar la interrupción, informaron: "Los ingenieros de Google fueron alertados de la falla dos minutos después de que comenzó, y rápidamente se comprometieron con los protocolos de gestión de incidentes utilizados para los incidentes de producción más importantes. La depuración del problema se vio significativamente obstaculizada por el fracaso de las herramientas que compiten por el uso de la red ahora congestionada". Se dieron cuenta de que tenían un problema, pero carecían de una forma secundaria de abordarlo.

Una de las causas más comunes de interrupciones es la vulnerabilidad de la última milla de la red primaria. Mientras la conectividad ISP

ha mejorado en los últimos años, una debilidad que estos servicios no pueden superar es el problema de la última milla. Esto se refiere al segmento final de la red de producción que conecta su red con su ISP. Este es el enlace más débil en su conectividad.

Todo el tráfico de red para una sola oficina, tienda, sucursal o centro de distribución se canaliza a través de enlaces únicos. El ancho de banda de estos enlaces limita efectivamente la cantidad de datos que se pueden transmitir a su ISP. Este cuello de botella lo deja expuesto a ataques DDoS y errores humanos básicos que conducen a interrupciones. Esta última milla puede ser víctima de una falla física. Un corte accidental de fibra puede dejar fuera de competencia toda su red y dejarlo desconectado de sus servicios de Internet durante períodos de tiempo significativos.

GESTIÓN EN BANDA Y FUERA DE BANDA

Su empresa tiene una conexión ISP de producción para el tráfico de red que incluye VPN, web, correo electrónico, aplicaciones en la nube y mucho más. A menudo, solo hay una tubería de red principal (T1, cable, SD-WAN o MPLS), que enruta este tráfico al Internet.

"Poder ingresar al equipo que necesita; ser capaz de manejarlo, independientemente de si tiene o no conectividad a través de medios normales. Así que, el 4G, el inalámbrico, toda esa conectividad es enorme".

Steve DiCicco
Ingeniero de redes sénior

La información de gestión fluye a través de las mismas interfaces que los datos del usuario. Cuando la gestión y los datos comparten este mismo plano, termina usando el plano de datos para acceder a su equipo de red. Esto se conoce como gestión en banda. Cuando administra su equipo utilizando una red dentro de la banda, los comandos de datos y control viajan a través de la misma ruta de red, por lo que su plano de gestión tiene las mismas vulnerabilidades de seguridad que su plano de datos. Y es posible que quede fuera del plano de gestión debido a la interrupción.

La ventaja de la gestión en banda es que es económica y simple, ya que solo necesita una red. Pero también es mucho menos segura porque combina el tráfico de usuarios con reglas de acceso y el tráfico de gestión generalmente menos estrictos. Las interrupciones y los ataques podrían poner en riesgo no solo los datos del usuario, sino también la gestión e integridad de su equipo de red. Además, cuando tiene una interrupción, no puede comunicarse con sus dispositivos.

Alternativamente, puede ejecutar el tráfico de gestión a través de una red independiente que solo maneja el tráfico de gestión. Esta es la gestión fuera de banda (OOB). La OOB le ofrece una forma alternativa de conectarse a su equipo remoto, como enrutadores, conmutadores y servidores a través del plano de gestión, sin acceder directamente a la dirección IP de producción del dispositivo en el plano de datos e independiente de la conexión ISP principal que utiliza su empresa. Esta ruta fuera de banda está completamente separada de la red de producción y permite a los administradores monitorear, acceder y administrar de manera segura todos los dispositivos sin interferir con las operaciones normales y, lo que es más importante, sin tener que permitir el acceso a nivel del plano de datos al plano de gestión.

Dado que la red fuera de banda separa el tráfico de usuarios y gestión, puede bloquear, restringir el acceso y asegurar completamente el plano de gestión. Además, puede configurar, administrar y solucionar problemas de sus dispositivos incluso cuando el plano de datos está inactivo. Una solución de OOB le ofrece una conexión secundaria, a menudo a través de 4G LTE, que le permite a su técnico de red resolver problemas desde cualquier lugar y, lo que es más importante, ahorrarle tiempo y dinero a su empresa.

La desventaja es el costo adicional de establecer una red solo para gestión, pero como verá más adelante en este documento, el ROI paga el gasto muy rápidamente.

TRES PLANOS SON MEJORES QUE UNO

Piense en una red que tiene tres planos 1:

El plano de datos consta de los componentes de la infraestructura que transportan los datos del usuario". Su propósito es permitir que los datos fluyan, por ejemplo, de un servidor web a la computadora de un cliente y viceversa.

El plano de control se encarga de mantener el flujo de datos. Contiene las reglas que permiten el enrutamiento de información de un lugar a otro. Por ejemplo, permite a los enrutadores de red crear una ruta para llevar datos desde un servidor web a la computadora de un cliente.

El plano de gestión se usa para la configuración y la gestión de conmutadores y enrutadores de red.

En muchas configuraciones, el plano de gestión se combina con el plano de datos, que puede ser problemático cuando ese plano de datos tiene problemas.

[1] Obtenga más información sobre los planos de red.

¿POR QUÉ NECESITA LA OOB?

¿Realmente necesita agregar el costo y la complejidad de una forma secundaria de conectarse a su equipo?

Sí, es necesario. Hay varias razones por las cuales la OOB tiene sentido, incluso con un costo adicional.

Primero, habrá aumentado la seguridad. Sin ella, los puertos de la consola se conectarán a su banda red de producción, por lo que si un virus, bot o hacker invade su red, toda su red está en riesgo.

"Estábamos operando las pilas de nuestros conmutadores y la actualización falló, por lo que ya no pudimos llegar a las pilas. En lugar de conducir hasta la oficina y conectarnos a través de un puerto de consola, pudimos conectarnos mediante Opengear a través del módulo celular y volver a ponerlo en funcionamiento en 10 minutos. Nos ahorró mucho tiempo y angustia".

Evans Vogas
Analista de operaciones de red

En segundo lugar, podrá resistir una interrupción del servicio de Internet y mantener su organización en funcionamiento. Su conexión a Internet principal está sujeta a la vulnerabilidad de la "última milla". Algo tan simple como una retroexcavadora podría cortar su línea y su conexión principal, ya sea fibra o cable o cualquier otra cosa, está fuera de servicio. Con las consolas OOB avanzadas, la gestión de la interrupción se puede hacer de forma casi instantánea y remota.

Para las empresas con oficinas remotas, fuera de banda es una obviedad. En lugar de tener que enviar un técnico de red al sitio, la solución de problemas y la gestión de su equipo se pueden realizar en cualquier lugar, en cualquier momento, a través de un sistema de gestión centralizado.

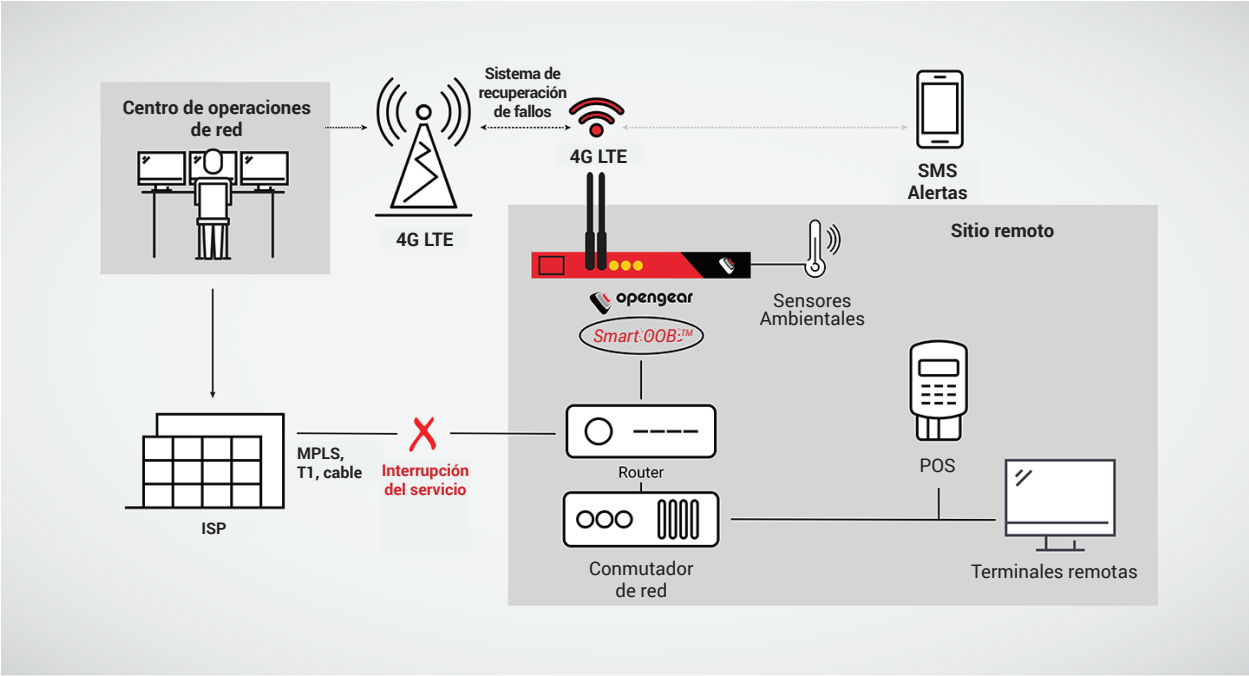
Tenga en cuenta que el ancho de banda LTE utilizado para realizar tareas administrativas es mínimo. Básicamente, los técnicos de red envían comandos de texto a través de un terminal y obtienen información de esos comandos. Alternativamente, pueden usar un software de gestión centralizada que, detrás de escena, todavía no usa un ancho de banda excesivo, manteniendo bajas las cargas LTE.

En última instancia, estas ventajas le ahorrarán una enorme cantidad de dinero, más que compensar la inversión en OOB.

CONSOLAS AVANZADAS ACTUALES DE GESTIÓN FUERA DE BANDA

Una consola de gestión fuera de banda ofrece características que minimizan sustancialmente el tiempo de inactividad y reducen sus costos operativos:

- Operar independientemente desde la red en banda, lo que significa diversidad de enlaces para una verdadera capacidad de recuperación de la red.
- Sistema de recuperación de fallos automática a celular. Cuando el enlace principal no está disponible, se proporciona conectividad a Internet para redes LAN remotas y equipos 4G LTE.
- Ofrecer aprovisionamiento sin intervención (ZTP). El ZTP permite a los administradores automatizar el proceso de implementación. A su vez, esto le permite automatizar tareas repetitivas, reducir puntos de contacto humanos, reducir errores y escalar el proceso de implementación a cualquier tamaño.
- Enviar alertas automáticas por correo electrónico o SMS para notificar cualquier problema de red.
- Identificar cualquier inconsistencia o actividad inusual con las condiciones de temperatura, las posiciones de las puertas de la jaula y la disponibilidad de la red.
- Permitirle volver a poner en funcionamiento la red de forma remota sin una visita in situ desde un solo panel de vidrio.



"Debería poder volver a conectarse sin problemas después de una interrupción. Así es como diseñamos nuestras ubicaciones, para que cualquiera pueda entrar y reiniciarlo. Opengear nos ha salvado muchas, muchas veces".

Landon Orr
Ingeniero de redes de producción

RETORNO DE SU INVERSIÓN EN OOB

Las consolas OOB pueden pagarse rápidamente por sí mismas al reducir los costos operativos y las pérdidas por tiempos de inactividad potencialmente catastróficas. En términos de costos operativos, considere el costo de una ubicación de posición periférica única que baja.

Una visita del servicio técnico podría costar $ 500. Una consola OOB avanzada puede costar $ 1500. Solo 3 interrupciones han compensado el costo. Un viaje en avión para solucionar el problema podría ser aún más costoso, alcanzando un costo rentable en un incidente. Y esta es solo una posición periférica.

Las pérdidas operativas también se reducen, ya que según

Gartner, el costo promedio de 1 minuto de tiempo de inactividad es de $ 5,600 . Considere una red con 10 ubicaciones físicas.

Ahora, equipar su red con una implementación de gestión fuera de banda típica con 10 ubicaciones y un sistema de gestión centralizado costará aproximadamente $ 25k. En promedio, alcanza la rentabilidad después de solo cinco minutos de tiempo de inactividad.

CONCLUSIÓN

La gestión fuera de banda elimina la necesidad de que le servicio técnico y los ingenieros de redes visiten centros de datos, sucursales, quioscos, oficinas dispersas o puntos de venta POS. Puede cargar de forma remota configuraciones e imágenes del sistema operativo, simplificar las funciones de copia de seguridad y restauración, reiniciar los enrutadores para reiniciar el equipo y reducir los tiempos de reparación. OOB es un gran impulso de tiempo y productividad para su empresa. Para sus clientes, la gestión fuera de banda puede significar la diferencia entre operaciones sin problemas y fallas catastróficas. Si sus clientes no pueden acceder a su negocio, la confianza básica y la lealtad sufren y usted obtiene una gran rotación de clientes.