Presentado por

Infoblox

Redes Empresariales Edge

para dummies®

Edición especial de Infoblox

- Visibilidad y control centralizados y escalables
- Defensa de red fortificada con DNS
- Alta disponibilidad con supervivencia local

Glenn Sullivan

Rod Dixon

Acerca de Infoblox

Infoblox es el líder reconocido en servicios críticos de red, que incluyen el sistema de nombres de dominio (DNS), el protocolo de configuración dinámica de host (DHCP) y la administración de direcciones IP (IPAM), conocidos colectivamente como DDI. Estas soluciones permiten una experiencia de red segura y basada en la nube, que es intrínsecamente simple, escalable y confiable, para todos. A través de amplias integraciones, Infoblox permite a las organizaciones aprovechar hoy todas las ventajas de las redes en la nube, mientras que maximizan sus inversiones en infraestructura existentes.

Los beneficios clave que las organizaciones obtienen de Infoblox incluyen:

- Simplicidad: automatizar y estandarizar la entrega de experiencias de redes y seguridad en diversas infraestructuras locales, virtuales y en la nube
- Confiabilidad: garantizar una alta disponibilidad para las redes que deben permanecer en funcionamiento en todo momento, utilizando la agilidad y la rentabilidad de la nube
- Escalabilidad: suministrar rápidamente servicios y aplicaciones a cualquier número de usuarios a través de una arquitectura de red construida sobre microservicios y diseño nativo de la nube
- Seguridad: extender fácilmente la seguridad a todos los usuarios y dispositivos en cualquier momento y en cualquier lugar, detener las amenazas desde el inicio del ciclo y reparar de manera más rápida a través de la integración generalizada del ecosistema de seguridad

Infoblox opera en más de 25 países, y brinda servicios de red seguros y administrados en la nube a más de 12 000 clientes, incluidos 356 de Fortune 500 y 66 % de Forbes 1000.

Redes empresariales edge

Edición especial de Infoblox

Por Glenn Sullivan y Rod Dixon

PRÓLOGO POR **Cricket Liu**

para dummies®

Redes empresariales edge para Dummies®, edición especial de Infoblox

Publicado por
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-83779-4 (pbk); ISBN 978-1-119-83763-3 (ebk)

Fabricado en Estados Unidos de América

10 9 8 7 6 5 4 3 2 1

Agradecimientos del editor

Algunas de las personas que ayudaron a publicar este libro se mencionan a continuación:

Editora de desarrollo: Amanda Cross
Editora de proyecto: Jennifer Bingham
Editor de adquisiciones: Steve Hayes
Director editorial: Rev Mengle
Representante de desarrollo de negocios: Matt Cox
Editor de producción: Mohammed Zafar

Prólogo

En estos días, todos estamos viviendo al límite. (Nota para el lector: definitivamente *no* es la mejor canción de Aerosmith). Eso es cierto en más de un sentido, pero en el contexto de este libro, me refiero específicamente al perímetro de la red.

No siempre fue así. Al comienzo de mi carrera, trabajé desde el punto más central de la que entonces era la red TCP/IP corporativa más grande del mundo: las oficinas corporativas de Hewlett-Packard, uno de los centros de Internet de HP. Pasé seis años trabajando desde esa ubicación privilegiada, disfrutando de una conexión de alta velocidad a Internet (una conexión de *10 megabits por segundo* a BARRNET, sí cariño, ¡y de allí a la red troncal de NSFNet!) y de la protección de nuestro firewall corporativo.

Pero después de seis años en el área corporativa, entré a la Organización de Servicios Profesionales de HP y me mudé a Colorado. De repente, mi acceso a Internet de HP fue a través de un módem de acceso telefónico y luego a través de una conexión DSL un poco más rápida. ¡Oh, cómo habían caído los valientes!

Cuando entré a Infoblox en 2003, volví a unirme a una nave nodriza (aunque una nave espacial mucho más pequeña), trabajando desde nuestra oficina corporativa en el Área de la Bahía de San Francisco. Por supuesto, en 2003, teníamos un acceso a Internet razonablemente rápido y firewalls bastante sofisticados y otros equipos de seguridad. ¡Estaba de vuelta en el ruedo! (Nota para el lector: una mejor canción de Aerosmith , aunque algo chirriante).

Eso cambió drásticamente a principios de 2020, y no solo para mí. La pandemia me envió a mí y a casi todos mis compañeros de trabajo a casa, a trabajar de forma remota durante muchos meses. Por supuesto que antes había trabajado ocasionalmente desde casa, pero ahora era la norma.

Eso significaba, y al momento de escribir este artículo todavía significa, acceder a los sistemas y servicios corporativos desde fuera del seno de nuestro firewall corporativo, desde una red doméstica poblada no solo por mi portátil del trabajo, sino por un termostato inteligente, detectores de humo, un coche, varias plataformas de juego, incluso un controlador de piscina.

Administrar y proteger un acceso como este desde mi hogar y desde muchos otros, así como desde oficinas más pequeñas en todo el mundo, no es una tarea fácil para nuestra organización de TI. Necesitan proteger la información y los recursos corporativos y, al mismo tiempo, brindar un acceso rápido, tanto desde los dispositivos de mi empresa como desde los míos personales. Deben asegurarse de que tenga acceso rápido y directo a los recursos y a las aplicaciones basados en la nube, así como a los que todavía ejecutamos en nuestra red corporativa. Y no pueden interferir con las comunicaciones entre los dispositivos "civiles" en la red e Internet: ¡los niños deben poder jugar a Overwatch! ¡Mi coche necesita sus actualizaciones!

Por supuesto, estos requisitos no son exclusivos. Muchas organizaciones en todo el mundo enfrentan desafíos similares y seguirán enfrentando incluso después de que la pandemia termine. (Crucemos los dedos sobre su terminación). Afortunadamente, pronto habrá una solución en forma de SASE o *Secure Access Service Edge*, Servicio de Acesso Seguro Edge. Los servicios SASE pueden brindar seguridad y acceso a una combinación de dispositivos corporativos y personales (bring your own device, BYOD) desde las pequeñas ubicaciones que componen la periferia de su red, sin la necesidad de un hardware costoso y engorroso, ni de agentes de software invasivos. Díganme por favor ¿cómo lo logra? Bueno, supongo que involucra DNS y DHCP de alguna manera. De lo contrario, ¿por qué pedirme que escriba el prólogo?

- Cricket Liu, arquitecto jefe de DNS y miembro principal de Infoblox

Introducción

Aunque no lo sepa, su organización ya está gravitando hacia el perímetro: el perímetro de la red. El perímetro se está convirtiendo rápidamente en el nuevo centro de atención de las redes empresariales. Proporciona el vínculo vital entre los dispositivos terminales como portátiles, teléfonos inteligentes y equipos de oficina con sensores, y las aplicaciones basadas en la nube y el almacenamiento que esos dispositivos requieren para funcionar correctamente.

Para prosperar en esta nueva era basada principalmente en la nube y centrada en el perímetro, su empresa necesita una red empresarial edge. En este libro, revelamos lo que se necesita para implementar una red de este tipo, que sea increíblemente rápida, resistente, elásticamente escalable, simple de administrar e intrínsecamente segura. También lo guiamos a través de los servicios de red fundamentales que requiere toda red perimetral empresarial.

Por eso escribimos este libro. Con los conocimientos que compartimos en estas páginas, aprenderá los conceptos básicos sobre el papel que juegan estos servicios vitales y los mecanismos de entrega más eficientes que le permiten aprovecharlos al máximo para cumplir con la promesa de las redes empresariales edge.

Acerca de este libro

Probablemente eligió este libro porque tiene suficiente autoestima para admitir que no sabe todo lo que desea sobre las redes empresariales edge, y es lo suficientemente inteligente como para buscar respuestas. Creemos que llegó al lugar correcto. En este breve volumen, analizamos cómo se están desarrollando las redes empresariales, los problemas que encontrará y las tecnologías que puede utilizar para optimizar su empresa.

Como todos los títulos de la serie para Dummies, este libro presenta una organización fácil de seguir. Al comienzo de cada capítulo, encontrará un resumen de los temas tratados, lo que le permitirá hojear fácilmente y encontrar la información que está buscando. No se pierda el capítulo 6, que describe las diez mejores prácticas para transformar la red perimetral en una de nivel empresarial.

Íconos utilizados en este libro

A lo largo de este libro, en ocasiones utilizamos íconos especiales para destacar información importante. Esto es lo que encontrará:

RECUERDE

Cuando vea el ícono Recuerde, tome nota de lo que está leyendo, porque esta información puede aparecer nuevamente en este libro.

INFORMACIÓN TÉCNICA

El ícono Información técnica indica lectura especialmente técnica. Puede omitir ese texto si quiere, o puede volver a él más tarde.

SUGERENCIA

El ícono Sugerencia señala información que es útil saber.

Más allá de este libro

Si alguno de estos temas en este libro lo deja pensando, continúe leyendo de todos modos, y luego envíe sus preguntas a `www.infoblox.com`. En Infoblox nos encantaría aclararle sus dudas.

EN ESTE CAPÍTULO

- **Explorar (las desventajas de) las arquitecturas tradicionales *hub-and-spoke***
- **Descubrir cómo las demandas de la red continúan cambiando**
- **Introducir un enfoque diferente del desarrollo de la red**

Capítulo 1
La red empresarial se desplaza desde el centro hacia el perímetro

Las redes empresariales se están volviendo más dispersas, impulsadas por la expansión del mercado y las tendencias comerciales de movilidad, Internet de las cosas (Internet of Things, IoT) y de la nube. Trabajar desde cualquier lugar que uno elija se convirtió en la norma para millones de personas en todo el mundo. Al mismo tiempo, se sigue expandiendo el crecimiento de la IoT en áreas como vigilancia, fabricación, atención sanitaria y oficinas inteligentes. Las aplicaciones y los servicios críticos para el negocio están cambiando rápidamente a alternativas de software como servicio (software as a service, SaaS) basadas en la nube como Salesforce, Microsoft Office 365 y Dropbox.

Como resultado, las redes se expandieron, principalmente en el perímetro, donde la cantidad de ubicaciones y los dispositivos aumentaron exponencialmente. Los usuarios, las partes interesadas, los clientes y los socios exigen un mayor acceso, tiempos de respuesta más rápidos y una conectividad más confiable. Esta evolución ha resultado en una mayor demanda de TI de soluciones perimetrales que simplifiquen y optimicen la implementación, la administración y el control a través de toda la organización.

Las redes tradicionales ya no pueden satisfacer las exigencias tecnológicas

Tradicionalmente, las empresas dependían principalmente de arquitecturas de red centralizadas locales en las que todo el tráfico fluía a través de los centros de datos corporativos o regionales en forma de estrella (hub – and-spoke arquitecture), como se puede ver en la figura. 1-1. Este modelo rígido es desafortunadamente inadecuado para las redes modernas. Hoy en día, todos quieren tener un acceso casi instantáneo a las aplicaciones y a los servicios basados en la nube en los dispositivos que elijan desde cualquier ubicación. Las arquitecturas de red en estrella existentes crean problemas inaceptables de latencia y rendimiento, especialmente para las aplicaciones SaaS potenciadas por la nube de las que dependemos muchos de nosotros.

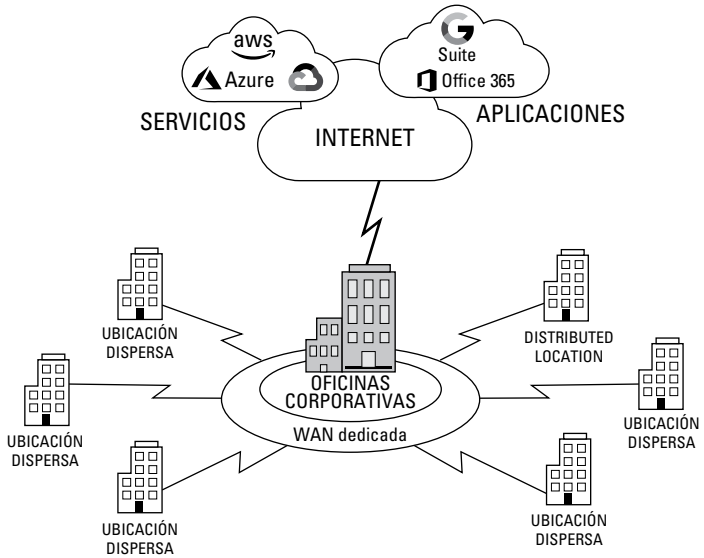


FIGURA 1-1: las arquitecturas tradicionales de red en estrella crean latencia y son difíciles de administrar ante el crecimiento de las redes distribuidas.

Además, el crecimiento de las redes distribuidas (dispersas) también está exponiendo puntos únicos de error, lo que crea inconsistencias de administración generalizadas y provoca interrupciones del servicio.

La necesidad del equipo de TI de configurar y actualizar los sistemas en los centros de datos e individualmente en cada ubicación solo aumenta

los desafíos. La recopilación de datos para la evaluación, el diagnóstico y el cumplimiento es a menudo un proceso manual complejo. Las organizaciones de TI enfrentan desafíos crecientes para planificar, implementar, administrar y resolver problemas de manera efectiva en ubicaciones remotas en expansión, lo que limita la escalabilidad y aumenta los costos.

Las organizaciones que se expandieron rápidamente a través de centros de datos distribuidos, así como aquellas que dependen de una infraestructura en la nube pública, privada o híbrida, también enfrentan grandes desafíos. Estos entornos descentralizados carecen de visibilidad y de administración consolidadas necesarias para manejar los requisitos que están evolucionando rápidamente en el perímetro.

Mayor complejidad y menos recursos

En respuesta a las consecuencias de la red distribuida, las organizaciones de TI luchan por reinventar modelos de implementación que puedan proveer una red más simple y rápida en el perímetro. Sin embargo, muchos departamentos de TI carecen del tiempo, capacidad o personal para administrar el trabajo que ya tienen, y mucho menos explorar nuevas soluciones perimetrales.

RECUERDE

Se debe responsabilizar en parte a la nube por el cambio generalizado. Cada vez más infraestructuras han migrado a la nube en los últimos años, pero con poco o ningún aumento correspondiente en los recursos de TI. En consecuencia, muchas organizaciones hoy en día no disponen de personal suficiente a la hora de abordar las complicaciones no solo de las redes, sino también de las complejidades involucradas en la totalidad de la transformación digital. La escasez de personal es especialmente grave en las ubicaciones distribuidas, lo que supone un doble revés para las organizaciones ya que el número de estas ubicaciones sigue aumentando.

Entonces, ¿cuáles son las opciones disponibles para administrar las interacciones perimetrales? La parte negativa es que los equipos de redes han tenido muy pocas opciones que elegir, aparte de ciertas innovaciones de redes de área amplia definidas por software (software-defined networking in a wide area network, SD-WAN) y sucursal definida por software (software-defined branch, SD-branch). La parte positiva es que esta escasez está cambiando drásticamente; el resto de este libro contiene más información al respecto.

La opción de trabajar desde cualquier lugar está aquí para quedarse

En solo unos pocos años, los eventos globales y la innovación tecnológica transformaron profundamente el lugar de trabajo. Antes, se daba por hecho que los empleados en muchos ámbitos trabajaban en oficinas centralizadas, instalaciones regionales o sucursales. Este ya no es el caso. El trabajo se volvió mucho más descentralizado. La ubicación de la sucursal de hoy bien puede ser el lugar desde donde se inicie sesión: el campus corporativo, la oficina en casa, una terminal de aeropuerto, el avión, el coche o algún punto intermedio.

La adopción de la nube, la tecnología móvil y el acceso de banda ancha generalizado hicieron posible que seamos tan productivos fuera de los entornos laborales convencionales como dentro de ellos. La opción de trabajar desde cualquier lugar se está expandiendo gracias a una creciente variedad de dispositivos no tradicionales (y a menudo no administrados), como los teléfonos inteligentes, que son convenientes y fáciles de usar. De hecho, esta nueva forma dispersa de trabajar se convirtió en un elemento permanente del panorama empresarial.

RECUERDE

Todo esto implica que, para brindar un servicio efectivo a las legiones crecientes de usuarios que trabajan desde cualquier lugar, las organizaciones de TI ahora tienen la responsabilidad de ampliar la velocidad, confiabilidad, seguridad y facilidad de acceso de nivel empresarial a todas y cada una de las ubicaciones, sin importar el tamaño ni la distancia, y en los dispositivos que prefieran sus usuarios. Por si esto no fuera suficiente, deben lograrlo con menos recursos y en un contexto de complejidad y expectativas crecientes provenientes de todas las direcciones.

El punto de inicio de ese esfuerzo es, obviamente, el perímetro empresarial: consulte el capítulo 2 para obtener más información.

EN ESTE CAPÍTULO

- Diferenciar las redes edge de las redes tipo *hub-and-spoke*
- Comprender los matices del perímetro en comparación con la nube
- Identificar una red empresarial edge resistente

Capítulo 2
¿Qué son las redes empresariales edge?

Las redes edge evolucionaron en respuesta a las fuerzas del mercado y al desarrollo creciente de las redes (para más información, consulte el capítulo 1). Una red perimetral funciona junto con una red empresarial tradicional. Mientras que la red tradicional se ejecuta principalmente a través de centros de datos centralizados, una red perimetral mueve la potencia informática clave, el almacenamiento y el acceso a las aplicaciones lejos del centro de datos hacia el perímetro de la red, cerca de las terminales. Muchas organizaciones seguirán necesitando ambos durante un tiempo indefinido.

Sin embargo, la comparación del perímetro con la red tradicional no es la única diferencia que deben comprender las organizaciones. También es importante entender la diferencia entre las *redes en la nube* y las redes edge. Algunos creen que se refieren a lo mismo, pero no es así.

INFORMACIÓN TÉCNICA

Por supuesto, los dos conceptos son muy interdependientes. Las *redes en la nube* consisten en el alojamiento de aplicaciones, datos, infraestructura y recursos informáticos, generalmente en grandes almacenes de datos o *data warehouses* administrados por proveedores de servicios en la nube como Amazon, Google y Microsoft. Por el contrario, las *redes edge* se refieren a la *última milla* (o *last mile*) entre el lugar donde residen los recursos en la nube y las terminales donde las personas los usan. En verdad, la última milla es figurativa, no literal. Lo que

distingue a una red perimetral es que los procesos ocurren cerca de las terminales para reducir la latencia y mejorar el rendimiento.

El desafío para las empresas es que las redes edge requieren tanto cuidado y atención como las redes en la nube. Pero debido a que las redes edge son un fenómeno mucho más nuevo, las soluciones de administración del perímetro efectivas solo están surgiendo ahora.

Entonces, ¿qué es una red empresarial edge y por qué es importante esta distinción? Una red empresarial edge aporta resistencia, velocidad y agilidad de nivel empresarial al perímetro (como se muestra en la figura 2-1). Cuando se implementan correctamente, las redes empresariales edge permiten a las organizaciones aprovisionar, implementar, administrar y controlar de manera centralizada la infraestructura de red, mientras suministra de manera eficiente y segura aplicaciones y servicios a las partes interesadas, socios comerciales, usuarios y clientes, donde sea que estos se encuentren dentro de sus entornos dispersos.

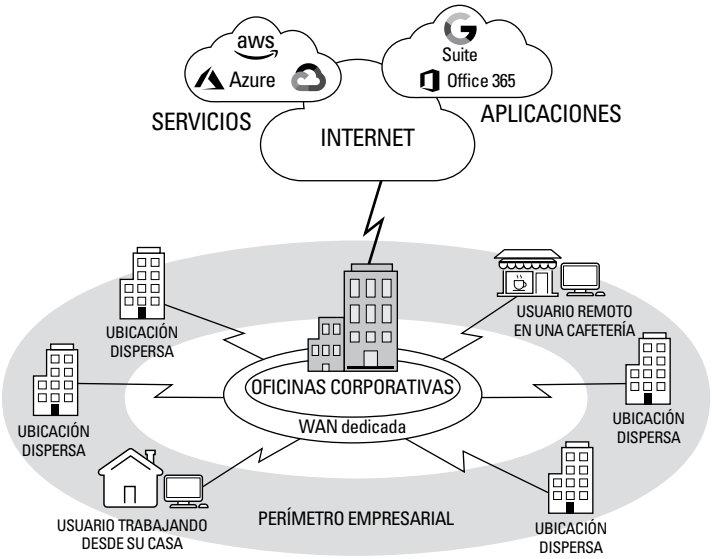


FIGURA 2-1: el crecimiento de las redes dispersas dio lugar al perímetro empresarial, un desafío para la arquitectura de red tipo hub-and-spoke tradicional.

Características de una red empresarial edge resistente

Una red edge típica alcanza el nivel empresarial cuando puede:

- Proporcionar una vía de acceso inteligente a la nube optimizando el acceso a las aplicaciones de software como servicio (software as a service, SaaS) según la ubicación del usuario
- Servir ubicaciones dispersas con un modelo mejor que una única solución, con la capacidad de escalar elásticamente según los requisitos de capacidad y rendimiento de los usuarios locales
- Mejorar la capacidad de respuesta y la disponibilidad de la red mediante la automatización
- Proteger los datos y la privacidad del usuario procesando los datos lo más cerca posible del usuario
- Asegurar que cada ubicación pueda operar de forma autónoma y funcionar con sus propios recursos en caso de que pierda la conectividad con las oficinas corporativas

El papel fundamental de los servicios críticos de red

En una era cada vez más dependiente de la nube, mucho depende de la capacidad de una organización para suministrar redes empresariales edge. Sin embargo, aún con las soluciones disponibles centradas en el perímetro, los equipos de TI necesitan todas las ventajas que puedan obtener. Da la casualidad de que ya hay disponible una gran ventaja. De hecho, es algo que todas las organizaciones ya tienen: servicios críticos de red. Estos incluyen la administración de direcciones DNS, DHCP e IP (comúnmente conocida con las siglas DDI).

RECUERDE

Los servicios DDI juegan un papel fundamental en cada conexión de red, interacción y flujo de trabajo digital en todo el entorno. Facilitan los intercambios entre aplicaciones, servicios, terminales y usuarios, independientemente de la ubicación. Los principales componentes de DDI son:

- **Sistema de nombres de dominio (Domain Name System, DNS):** traduce los nombres de dominio en direcciones IP numéricas (a veces denominado "la guía telefónica de Internet")

- **Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol, DHCP):** asigna direcciones IP a dispositivos conectados a la red con previa solicitud
- **Administración de direcciones de protocolo de Internet (Internet Protocol Address Management, IPAM):** permite a los administradores de red planificar, realizar un seguimiento y administrar la asignación y la recuperación de direcciones IP dentro de una organización

Los servicios DDI son ideales para optimizar las redes empresariales edge. Para empezar, DNS, DHCP e IPAM son omnipresente en las redes y están ubicados cerca de las terminales. Además, debido a los datos que contienen y su ubicación única dentro de las redes, los servicios DDI brindan a las organizaciones capacidades sin precedentes en términos de visibilidad, control, automatización y seguridad de la red en ubicaciones dispersas.

RECUERDE

Aunque los servicios DDI son fundamentales para las redes empresariales edge, muchas organizaciones ignoran o no comprenden su función, y mucho menos los importantes beneficios que pueden ofrecer estos servicios. Esos beneficios de DDI se extienden a las tecnologías que afectan y habilitan el perímetro de la red, como verá en el capítulo 3.

EN ESTE CAPÍTULO

- Descubrir los desafíos que presentan las tecnologías clave en el perímetro
- Volver a descubrir las tecnologías DDI comprobadas
- Usar servicios básicos y tecnologías recientes para superar desafíos

Capítulo 3
Tendencias y facilitadores clave de la tecnología edge

Una red empresarial edge no es algo que pueda comprar en la tienda. En lugar de pensar en una red perimetral como algo físico (como una colección de cajas negras y software), piense en ella como un lugar dentro de una red extensa cerca de las terminales donde ocurren las interacciones perimetrales.

El perímetro de la red converge con una serie de tendencias tecnológicas crecientes, y ambos están configurando los requisitos en el perímetro e impulsando su adopción. Estas tendencias también presentan sus propios desafíos que pueden afectar negativamente la confiabilidad del perímetro, las experiencias del usuario, la capacidad de administración y la seguridad.

Los servicios críticos de red en forma de DNS, DHCP e IPAM (DDI) (consulte la figura 3-1) pueden ayudarlo a superar estos desafíos y simplificar la complejidad de la visibilidad, el control y la seguridad del perímetro. En este capítulo, resumimos las tendencias más importantes y las formas en que los servicios DDI pueden contribuir a optimizar cada una.

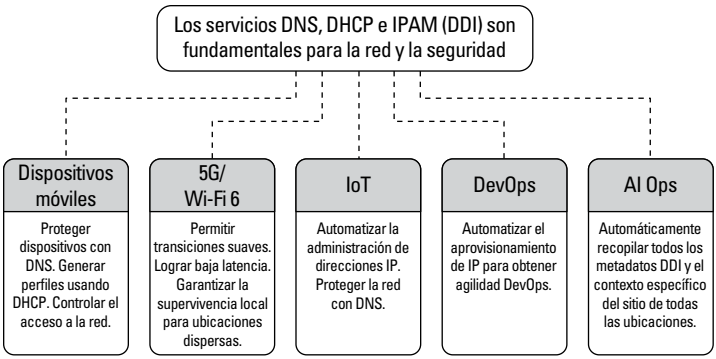


FIGURA 3-1: los servicios DDI fundamentales mejoran la visibilidad, el control y la seguridad de las tecnologías edge.

Tecnología clave que afecta al perímetro

En esta sección, analizamos varios factores que afectan las soluciones de las redes empresariales edge:

Dispositivos móviles

El cambio a los dispositivos móviles se ha estado llevando a cabo durante décadas y solo se está acelerando. De hecho, la penetración de las tecnologías móviles y el cambio generalizado a escenarios de trabajo desde cualquier lugar se encuentran entre los principales impulsores de la demanda de soluciones viables de las redes edge.

RECUERDE

Los dispositivos móviles se están multiplicando a velocidades astronómicas y también se están volviendo más inteligentes. Los teléfonos inteligentes de hoy son capaces de realizar muchas de las tareas que antes estaban reservadas para computadoras de escritorio, portátiles y tabletas. En muchos casos, los teléfonos inteligentes son estaciones de trabajo de nivel empresarial por sí solos. Los dispositivos móviles también continúan evolucionando hacia una variedad de formas más pequeñas y poderosas, como relojes inteligentes y otros dispositivos móviles.

Los empleados, clientes y socios están pegados a sus dispositivos móviles, y ahora todos también esperan un acceso instantáneo a la red desde los dispositivos que prefieran.

Qué tan bien pueda administrar y proteger esas interacciones móviles depende de la medida en que pueda administrar y proteger el perímetro de la red (consulte la figura 3-2). No es una tarea sencilla. Tenga en cuenta que sigue sin haber pautas claras entre los dispositivos que se

utilizan para acceder a las aplicaciones y a los datos corporativos, y los que se utilizan para tareas personales y entretenimiento. La masificación del consumo de TI ya se completó y no hay vuelta atrás.

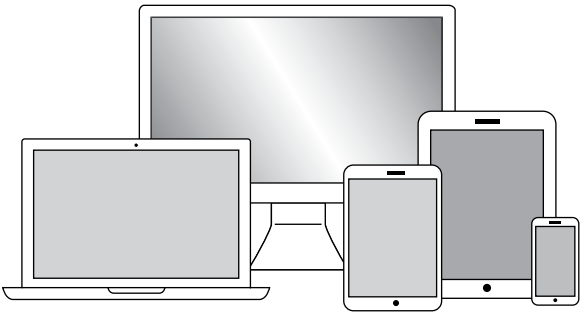


FIGURA 3-2: los dispositivos móviles requieren un acceso seguro a la red que se pueda administrar y controlar fácilmente.

Desafíos de los dispositivos móviles en el perímetro

Los principales desafíos de las redes y la seguridad para los dispositivos móviles incluyen:

- **Los dispositivos administrados versus no administrados:** ¿debería permitir solo dispositivos móviles autorizados en la red? Si es así, podría muy bien reducir la productividad de los empleados para mantener el control. A menos que proporcione a cada usuario un dispositivo móvil administrado por la empresa (una perspectiva costosa) y prohíba específicamente la práctica de dispositivos personales (bring your own device, BYOD), los usuarios usarán sus propios dispositivos móviles en la red perimetral de su empresa. Si impide el acceso, es muy probable que sus usuarios simplemente opten por eludir su red y hacer negocios de la empresa fuera del firewall a través de la red telefónica 5G.

  Las empresas astutas saben que deben adoptar plenamente la tendencia BYOD en lugar de luchar contra ella. El problema subsiguiente es cómo proteger su red y sus usuarios al mismo tiempo que permite el acceso a dispositivos no administrados.

SUGERENCIA

- **El carácter transitorio de las conexiones móviles:** los usuarios de dispositivos móviles no son predecibles en lo que respecta a la cantidad de dispositivos móviles que utilizan, la frecuencia con la que los llevan "in situ", si técnicamente son "sus" dispositivos o cuándo deciden utilizarlos. Piense en los casos en los que un empleado pide prestado un teléfono a su cónyuge o inicia sesión

desde casa con uno de los dispositivos de sus hijos porque el suyo no tiene batería. No puede saber de antemano cuándo van a aparecer los dispositivos móviles en la red, y nunca puede estar seguro de la asociación de esos dispositivos con sus usuarios. Esa incertidumbre hace que la protección de los dispositivos móviles sea como mínimo una tarea complicada.

- **El propietario del dispositivo:** en la actualidad, es mucho más rentable para las empresas permitir que los empleados utilicen su propia tecnología móvil en lugar de asumir ellas mismas los gastos. La compensación, por supuesto, es que el dispositivo pertenece al empleado, no a la empresa, por lo que la responsabilidad de cualquier seguridad en el dispositivo recae en el empleado. Sin la capacidad de instalar agentes de usuario y perfiles de red privada virtual (virtual private network, VPN) personalizados, los administradores deben confiar en la creación de perfiles de dispositivos, la autenticación de usuarios y la segmentación para proteger las redes empresariales edge.

Cómo ayudan los servicios críticos de red

Los datos que residen en DNS, DHCP e IPAM contienen un tesoro de información que los administradores pueden utilizar para realizar tareas como las siguientes:

- Proteger todos los dispositivos, tanto administrados como no administrados, a través de DNS. Todos los dispositivos dependen de DNS para conectarse a las redes, y esas conexiones iniciales ocurren en el perímetro. Con el comando de los servicios DNS, puede convertir este protocolo de Internet más básico en uno de los puntos de cumplimiento más eficaces de la red. Al hacerlo, motivará al personal para que utilice las herramientas móviles que mejor les resulten, desde donde quieran conectarse.
- Generar perfiles de los dispositivos que se unen a su red mediante metadatos DHCP. Los metadatos de las concesiones DHCP pueden proporcionar visibilidad del uso de los dispositivos móviles, incluido el tipo de dispositivo, el fabricante del hardware, el modelo, el sistema operativo instalado y otros detalles útiles. Esta información es de gran ventaja tanto para los equipos de redes como para los de seguridad, ya que proporciona información detallada sobre el uso de los dispositivos, el contexto de la red y los eventos de seguridad emergentes en su red.
- Controlar el acceso a los recursos de red desde dispositivos móviles no administrados mediante el uso de portales cautivos a través de redireccionamientos de inicio de sesión único (single sign-on, SSO) a través de DNS y DHCP. Este paso garantiza que el tráfico

procedente de los dispositivos móviles que se topa con recursos empresariales se autentique y se asocie con un usuario autorizado.

- Registrar todo con la ayuda de datos DDI. No se puede desestimar este punto. Sin control directo de un dispositivo, las empresas deben recopilar toda la información forense que pueda ser necesaria en caso de una fuga de información u otro incidente de seguridad. Las concesiones DHCP, las consultas de DNS y cualquier otro metadato sobre los dispositivos que se unen a su red perimetral deben registrarse y almacenarse durante un mínimo de 30 días (más si su directiva de cumplimiento lo exige).

Hay muchos otros aspectos a considerar al planificar su estrategia BYOD, pero estos están más allá del alcance de esta guía. Sin embargo, es importante recordar que aprovechar los servicios DDI y los datos que brindan puede contribuir en gran medida a implementar una red edge que pueda acomodar de manera segura todos los dispositivos móviles que sus usuarios desean conectar a su red.

5G y Wi-Fi 6

Con la combinación de redes móviles 5G y estándares Wi-Fi 6 de próxima generación, es casi obsoleto conectar un cable de red físico. Ambas tecnologías inalámbricas complementarias se centran en ofrecer conectividad de velocidad extremadamente alta dondequiera que vayan los usuarios. Ambas aumentan la dependencia de las redes empresariales edge y tienen implicaciones para quienes tienen la tarea de operarlas de manera segura.

En la mayoría de los casos, las personas se conectan con Wi-Fi 6 cuando están en interiores, como cuando se encuentran en un entorno corporativo. Las redes Wi-Fi 6 generalmente son controladas y administradas por la empresa. Por otro lado, las personas usan celulares 5G principalmente en exteriores, a través del roaming. La tecnología también se está implementando en casas, apartamentos y empresas. Tenga en cuenta que los operadores de terceros, no la empresa, administran y controlan las redes 5G (consulte la figura 3-3).

Las redes empresariales edge deben admitir a los usuarios conectarse ó desconectarse desde cualquiera de las tecnologías de conexión, según su ubicación en un momento dado y los recursos a los que acceden. Los dispositivos móviles están diseñados para mantener simultáneamente las conexiones Wi-Fi y móvil, y en la mayoría de los casos, si ambas señales son fuertes, los usuarios tendrán la opción de unirse a cualquiera de ellas. En otros casos, el dispositivo o la aplicación toma esta decisión por ellos, en función de la intensidad de la señal y otros factores.

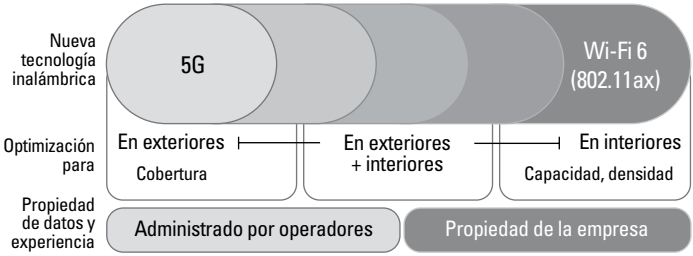


FIGURA 3-3: las Edge empresariales deben proporcionar transiciones suaves, baja latencia y capacidad de supervivencia local para dispositivos que aprovechan 5G y Wi-Fi 6 en el perímetro.

Desafíos 5G y Wi-Fi 6 en el perímetro

Los desafíos que se plantean a las redes empresariales edge incluyen los siguientes:

- **Problemas de transición:** los estándares actuales de Wi-Fi y los estándares móviles correspondientes no son tan compatibles con respecto a la información de transición entre tecnologías. Por ejemplo, si inicia una sesión de videoconferencia mientras está conectado a la red Wi-Fi y sale a caminar donde se conecta al 5G, ninguna de las tecnologías se responsabiliza de mantener la sesión durante la transición. (La aplicación de videoconferencia debe hacerlo, y probablemente no tenga la capacidad). Básicamente, esto crea una transición "fría" entre la Wi-Fi y las redes móviles, lo que puede resultar en conexiones interrumpidas. En un mundo perfecto, las redes comunicarían la información de la sesión mediante una transición "suave" y crearían una experiencia de red ininterrumpida.
- **Latencia inaceptable:** las aplicaciones 5G requieren una latencia extremadamente baja. Para lograr eso, el 5G y el tráfico que transporta deben residir cerca del usuario final. Sin embargo, como señalamos anteriormente, las arquitecturas de red tipo *hub-and-spoke* tradicionales, del tipo que todavía se usa ampliamente en las organizaciones, aumentan la latencia.
- **Complicaciones de seguridad:** al ofrecer velocidades de descarga 100 veces más rápidas que 4G, el rendimiento de las redes móviles 5G puede tentar a los usuarios a elegir 5G sobre la Wi-Fi empresarial.

  Sin embargo, debe alentar a los usuarios a que se queden con la red Wi-Fi administrada por la empresa cuando estén "in situ" y que usen la red 5G durante el roaming. ¿Por qué? Porque 5G es otro punto de entrada a su red que debe protegerse. Puede fomentar este comportamiento manteniendo las redes Wi-Fi y los sitios

SUGERENCIA

remotos en funcionamiento en todo momento, para que los usuarios no se sientan tentados de usar el roaming.

Cómo ayudan los servicios críticos de red

INFORMACIÓN TÉCNICA

Los servicios críticos de red pueden ayudar a superar estos desafíos de las siguientes maneras:

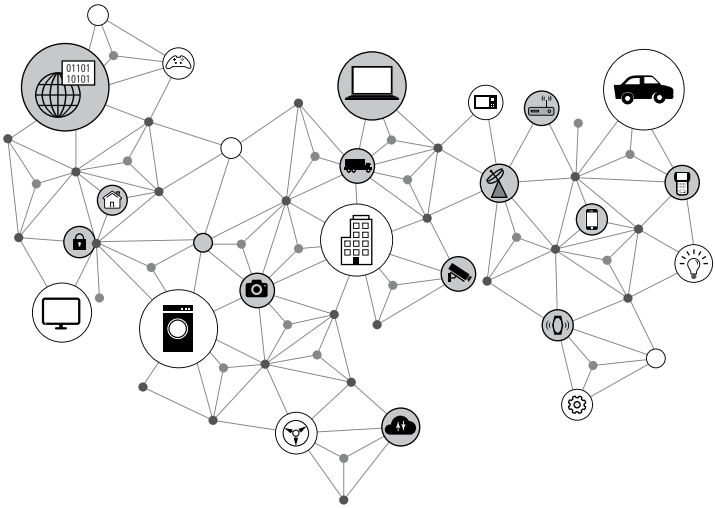
- **Habilitar las transiciones suaves a través de DHCP.** Los datos a nivel de dispositivo en DHCP lo convierten en un candidato ideal para mantener la información de la sesión durante las transiciones entre las redes Wi-Fi administradas por la empresa y su equivalente 5G. Además, si mantiene la integridad de la sesión durante las transiciones, es más probable que los usuarios resistan el impulso de desconectar la Wi-Fi en favor del 5G permanente.
- **Lograr una baja latencia moviendo el procesamiento de DNS al perímetro.** El DNS es fundamental para las redes 5G, por lo que su infraestructura de almacenamiento en caché de DNS debe ser lo más sólida posible. La latencia de DNS de las soluciones convencionales es demasiado alta para admitir muchas aplicaciones 5G. Por ejemplo, la telecirugía, los coches conectados, la realidad aumentada/realidad virtual (augmented reality/virtual reality, AR/VR) y los juegos requieren una latencia integral extremadamente baja. Para garantizar un flujo de tráfico sin obstáculos en el perímetro, también debe colocar los servicios DNS en el perímetro.
- **Garantizar la supervivencia local para ubicaciones dispersas.** Los servicios críticos de red, como el DNS, proporcionan un medio para mantener la conectividad de las oficinas corporativas e Internet para ubicaciones dispersas que usan Wi-Fi. Conocida como, *supervivencia local*, estas conexiones siempre activas fomentan el uso de la Wi-Fi corporativa como la opción principal para los empleados.

IoT

El Internet de las cosas (Internet of Things, IoT) está en todas partes y está creciendo rápidamente. Es posible que haya leído sobre IoT asociado con dispositivos de consumo, como cafeteras "inteligentes", asistentes digitales activados por voz, heladeras, termostatos y sistemas de seguridad para el hogar que se conectan a Internet. Pero, en realidad, IoT es mucho más grande. Abarca todo, desde equipos de fabricación, robots industriales y coches conectados hasta máquinas de resonancia magnética.

En el ámbito empresarial, IoT comprende dispositivos móviles, como teléfonos y relojes inteligentes, así como un número cada vez mayor de

impresoras conectadas a la nube, lectores de credenciales, escáneres de huellas digitales, electrónica para salas de conferencias, soluciones de videovigilancia y sistemas de climatización. La figura 3-4 ilustra cómo IoT afecta múltiples aspectos de nuestras vidas.



Dispositivos de IoT empresariales comunes

- Impresoras
- Lectores de credenciales
- Cámaras de seguridad
- Alarmas de edificios/sensores de movimiento
- Sistemas de iluminación
- Sistemas de climatización
- Autenticación digital

FIGURA 3-4: IoT no es solo productos de consumo. Abarca cualquier dispositivo conectado.

La mayoría de las "cosas" conectadas de IoT son dispositivos, gadgets y sensores integrados que necesitan acceso a la red (generalmente a la nube) pero, a diferencia de un teléfono inteligente, carecen de un sistema operativo. Piense en un oleoducto que está monitoreado por una serie de sensores de presión inalámbricos no más grandes que una moneda implementados a intervalos regulares a lo largo de su recorrido. No puede ejecutar Windows, Linux o MacOS en dichos dispositivos, por lo que no puede administrarlos como un servidor o un host de usuario final.

RECUERDE

Los dispositivos de IoT, por naturaleza, operan en el perímetro de la red. También se comunican a través de tecnologías inalámbricas, que incluyen infrarrojos, Bluetooth, Wi-Fi y móvil, según la ubicación, el tipo de dispositivo y la tarea que realiza. La cantidad está creciendo

estratosféricamente. Su minihorno inteligente puede tener un sensor conectado integrado. Un avión de pasajeros tiene miles. Según las estimaciones, habrá entre 50 mil millones y 200 mil millones de dispositivos IoT interconectados en todo el mundo para el 2030.

Desafíos de IoT en el perímetro

Para las redes empresariales edge, IoT presenta dos desafíos principales. Cada uno es abrumador a su manera:

- **Administración de direcciones IP:** cada dispositivo de IoT, desde esos pequeños sensores de presión de oleoductos hasta las legiones de dispositivos integrados en un avión de pasajeros, tiene su propia dirección IP. Para su empresa, eso significa que alguien dentro de su organización (o quizás todo un equipo) debe asignar, aprovisionar y administrar esas direcciones IP para cientos, tal vez miles, de dispositivos IoT implementados en sus operaciones extendidas.

  Muchas empresas tienen muchos más dispositivos IoT operando en sus instalaciones de los que creen. Gracias a la innovación tecnológica en curso y las mejoras de la banda ancha, puede estar seguro de que habrá más en camino.

  Si su organización se basa en implementaciones tradicionales para administrar direcciones IP con sus procesos manuales y montañas de hojas de cálculo, es un gran desafío mantener todo conectado sin problemas en el perímetro.

- **Seguridad del dispositivo IoT:** la *inseguridad* del dispositivo es una frase más precisa. La pura verdad es que la gran mayoría de los dispositivos de IoT carecen de controles de seguridad. Dado que también carecen de sistemas operativos o interfaces de seguridad estándar, no es fácil instalar medidas de seguridad en ellos.

  En consecuencia, los dispositivos de IoT aumentan considerablemente la superficie de ataque de su red. Una vulnerabilidad de seguridad en un dispositivo de iluminación inteligente conectado a su red es una entrada a la red para un ataque. Proteger la infraestructura de red de las amenazas de seguridad expuestas a través de IoT es una tarea ardua cuando sus equipos de seguridad ya están al límite con la administración de recursos y dispositivos de red tradicionales.

Cómo ayudan los servicios críticos de red

Los servicios críticos de red pueden ayudar a superar estos desafíos de las siguientes maneras:

- **Automatizar la administración de direcciones IP.** Las mejores soluciones DDI permiten a los equipos de redes automatizar la gran cantidad de partes móviles involucradas en la administración de direcciones IP y eliminan la necesidad de rastrear direcciones en hojas de cálculo. Los mejores sistemas también se escalan dinámicamente a medida que se amplían los requisitos de las direcciones IP.
- **Utilizar DNS para proteger la red de los dispositivos IoT.** Como mencionamos, no se pueden instalar medidas de seguridad en la mayoría de los dispositivos de IoT. Los equipos de seguridad deben usar estos dispositivos como están. Afortunadamente, la misma estrategia de seguridad DNS que funciona para dispositivos móviles también funciona para sus parientes de IoT. En ambos casos, el DNS es la primera línea de defensa ideal, debido a que ya se utiliza en cada interacción de dispositivo y se encuentra en el perímetro de la red, cerca de las terminales.
- **Adoptar un enfoque centrado en los datos para la seguridad del dispositivo.** La seguridad DNS ofrece una protección sustancial para las redes, pero no es completa. Muchas amenazas no dependen de las rutas de DNS. Una forma de aumentar la seguridad DNS es mediante estrategias defensivas que utilizan los datos transmitidos en los dispositivos de IoT.

  Un enfoque centrado en los datos le permite considerar las características de los datos generados por estos dispositivos. Todos los dispositivos de IoT producen datos DDI, como la identificación digital DHCP, que se puede aprovechar a efectos de seguridad.

  Pero DDI es solo un tipo de datos que transportan los dispositivos de IoT. Después de todo, el trabajo principal de estos dispositivos es compartir datos (como datos de telemetría de sensores de temperatura). Esos datos, cómo están protegidos, dónde se almacenan y cómo se accede a ellos (con qué frecuencia, quién lo hace y bajo qué restricciones), pueden formar la base para establecer parámetros de seguridad basados en el contexto, que cubren un amplio espectro de escenarios de IoT.

RECUERDE

Cuando se combinan, las medidas de seguridad que puede tomar con los servicios DDI le permiten maximizar su estrategia de IoT de forma segura y con confianza.

DevOps

Desde que el término se acuñó por primera vez en 2008, *DevOps* (Development and Operations) se utiliza para describir todos los aspectos de la infraestructura que se benefician de una estrategia de entrega continua.

En el desarrollo de TI tradicional, los productos se crean, se prueban y se suministran a las operaciones. El desarrollo luego se detiene cuando los equipos recopilan los comentarios y los requisitos de los clientes. Pasan semanas y, a veces, meses antes de que comience el trabajo en la siguiente iteración (repetición).

En DevOps, no hay fechas de lanzamiento de productos porque los procesos de desarrollo e implementación nunca terminan. El objetivo de DevOps es hacer llegar las innovaciones a los usuarios, ya sea software o nuevas capacidades de infraestructura, con la mayor frecuencia posible, realizar ajustes esencialmente sobre la marcha y repetirlos. La figura 3-5 muestra el flujo conceptual del proceso DevOps. Así se obtienen resultados mejores y más rápidos a menor costo.

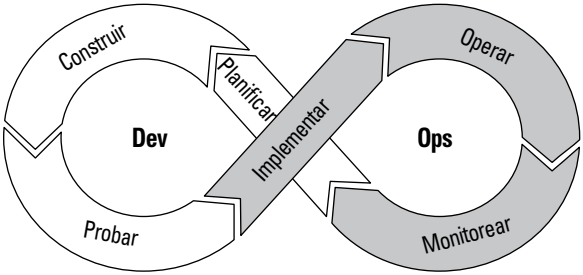


FIGURA 3-5: DevOps es un ciclo continuo que permite la innovación continua.

La fusión de los ámbitos del desarrollo y las operaciones produce entornos que son más ágiles y adaptables a las necesidades en constante cambio de las aplicaciones y sus usuarios. Gran parte del trabajo de desarrollo que surge de DevOps está orientado a mejorar las experiencias de red en el perímetro, buscando formas de hacer que las redes tengan más capacidad de respuesta y sean más eficientes para los usuarios de todo tipo.

Para lograr sus objetivos, DevOps requiere una infraestructura de red que sea muy ágil y flexible. De hecho, la estrategia de DevOps prefiere, siempre que sea posible, implementar "infraestructura como código". En otras palabras, la infraestructura se desacopla del hardware subyacente para que los equipos puedan tratar esa infraestructura como si fuera un software utilizado en un trabajo de desarrollo ágil. DevOps quiere tener la capacidad de lanzar esa infraestructura en un instante según sea necesario, como si fuera software.

Desde la perspectiva de DevOps, uno de los elementos más cruciales de la infraestructura de red es DDI. Sus servicios están estrechamente

involucrados en cada etapa de los ciclos de desarrollo y operaciones. DDI permite a DevOps ejecutar sus procesos al garantizar que los componentes en desarrollo puedan conectarse a la red y a todos los recursos de red involucrados en los procesos de desarrollo e implementación.

Desafíos de DevOps en el perímetro

Varios desafíos de DevOps afectan los ciclos de desarrollo en el perímetro de la red, pero uno se destaca por sobre los demás. No es sorprendente que tenga que ver con DDI. La mayoría de las implementaciones de DDI son demasiado lentas y rígidas para DevOps.

Muchas empresas implementan servicios críticos de red utilizando hardware físico en todas las ubicaciones. Estas implementaciones dependen de herramientas de administración separadas e inconexas para la administración de direcciones IP, DHCP y DNS.

RECUERDE

Las implementaciones convencionales de DDI como estas requieren una gran cantidad de procesamiento manual para realizar tareas básicas (como realizar un seguimiento de direcciones IP a través de hojas de cálculo), junto con la configuración manual de servidores y routers en cada sitio. El resultado es que la DDI tradicional es simplemente demasiado lenta e inflexible para moverse a la par del ritmo vertiginoso de DevOps.

Cómo ayudan los servicios críticos de red

Los servicios críticos de red pueden ayudar a superar estos desafíos de las siguientes maneras:

- **Se puede integrar DDI en una única plataforma automatizada:** para satisfacer las demandas de agilidad de DevOps, los servicios de administración de direcciones IP, DNS y DHCP deben automatizarse, organizarse y administrarse desde un solo punto.

  La automatización es clave. Moverse a la velocidad de DevOps significa que no hay tiempo para el aprovisionamiento manual de direcciones IP durante el desarrollo y prueba de la solución. El aprovisionamiento de IP automatizado y las capacidades de DDI escalables dinámicamente ayudan a las organizaciones de TI a alcanzar sus objetivos de desarrollo rápido.

  Mejor aún, desde el punto de vista de DevOps, una plataforma que proporciona servicios DDI puede moverse de forma nativa a la nube con la destreza del software. Describimos más en detalle lo que eso implica en el capítulo 4.

» **Los datos DDI pueden acelerar los procesos de DevOps:** los servicios críticos de red hacen mucho más que permitir que los equipos de DevOps mantengan sus procesos de desarrollo e implementación conectados de manera confiable. Los datos que producen estos servicios también proporcionan información valiosa sobre las interacciones entre los objetivos de desarrollo, y cómo esos objetivos interactúan con otros recursos y componentes de la red. Con estos datos, los equipos de DevOps pueden resolver problemas técnicos más rápidamente.

AIOps

Si una misión principal de DevOps es automatizar procesos para acelerar las tareas de desarrollo e implementación, la Inteligencia Artificial para Operaciones de TI (Artificial Intelligence for IT Operations, AIOps) es paralela, y se enfoca exclusivamente en la analítica. Un subconjunto de DevOps, el término AIOps fue establecido por Gartner en 2016 para referirse al uso de *big data*, aprendizaje automático (machine learning, ML), inteligencia artificial (AI) y una amplia automatización para identificar y solucionar problemas de TI más rápido mientras se impulsa la innovación. Puede ver los detalles del modelo AIOps en la figura 3-6.

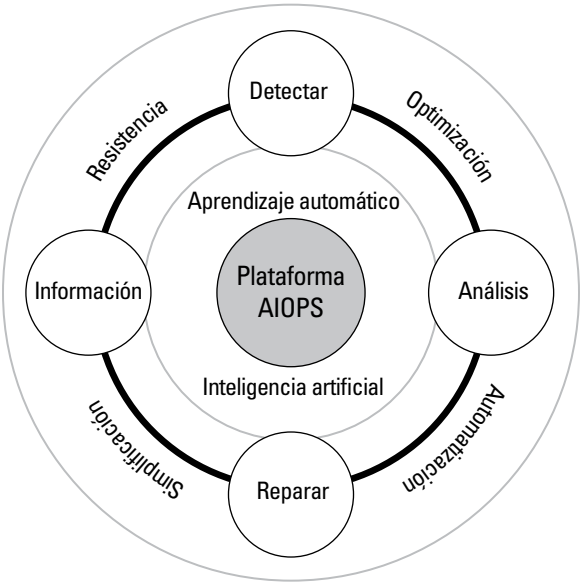


FIGURA 3-6: AIOps utiliza big data, aprendizaje automático (ML) e inteligencia artificial (AI) con automatización para solucionar problemas de TI más rápido e impulsar la innovación.

AIOps es una disciplina emergente que es especialmente útil en organizaciones con una infraestructura compleja que se extiende a través de ubicaciones dispersas. La eficacia de AIOps depende de la arquitectura del perímetro de la red.

Al analizar conjuntos de datos masivos de toda una empresa, AIOps revela patrones, tendencias y anomalías en los sistemas de TI que las soluciones de monitoreo individuales no pueden ver. Para producir los resultados más precisos, AIOps requiere metadatos de todos los recursos de la red, aplicaciones y elementos de infraestructura, ya sean locales o basados en la nube.

Para obtener mayor velocidad y facilidad de administración, los datos empresariales para AIOps generalmente se agrupan en un repositorio centralizado y se analizan en la nube. Con los hallazgos de AIOps, los equipos de TI pueden abordar rápidamente los problemas que necesitan atención, idealmente de forma automática siempre que sea posible. Por ejemplo, la detección de un aumento en el uso de una aplicación en particular basada en la nube podría desencadenar un aumento automatizado en la capacidad del servidor para esa aplicación.

Entonces, ¿qué tiene que ver todo esto con el perímetro de la red? Todo. Algunos de los metadatos más útiles para el análisis en AIOps se pueden encontrar en los servicios críticos de red. La cantidad disponible de esos datos con fines de AIOps se reduce a la arquitectura del perímetro de la red.

Desafíos de AIOps en el perímetro

Los metadatos DDI que causan la mayoría de los desafíos son los asociados con las ubicaciones dispersas, en otras palabras, los datos de las interacciones de la red en sucursales y oficinas remotas, y durante el roaming. Para muchas empresas, los metadatos DDI de estas ubicaciones son difíciles de incluir en los repositorios centralizados que requiere AIOps. En otros casos, simplemente no están disponibles. Existen dos motivos principales para ello:

- **Complicaciones de implementación de DDI tradicional:** en las implementaciones tradicionales de DDI, los metadatos de DDI residen en decenas a miles de dispositivos individuales en ubicaciones dispersas; cada dispositivo se administra y mantiene localmente, lo que hace que la transferencia de los metadatos a un lago de datos (o *data lake*) central sea un proceso manual y que requiere mucho tiempo. Este proceso es especialmente inadecuado para los objetivos de agilidad y automatización de TI que AIOps se esfuerza por alcanzar.

- **Limitaciones de DDI solo en la nube:** otras implementaciones de DDI renuncian completamente al uso de dispositivos DDI en el sitio y enrutan todo el tráfico de red a servidores proxy en la nube. Con estas soluciones solo en la nube, se pierden valiosos datos contextuales de los dispositivos "in situ" y sus interacciones con la red.

Cómo ayudan los servicios críticos de red

El papel de las ubicaciones dispersas en las redes empresariales se está expandiendo, una tendencia que no muestra signos de desaceleración. En consecuencia, los metadatos DDI que atraviesan estos sitios dispersos tienen un valor cada vez mayor para los objetivos de AIOps. La forma más simple y efectiva de capturar esos metadatos es a través de implementaciones híbridas de DDI que fusionan la presencia local de la implementación on-premises con la eficiencia y elasticidad de la administración de la nube.

Con esta arquitectura híbrida para DDI, las organizaciones de TI pueden agregar automáticamente metadatos DDI y contexto específico del sitio de todas las ubicaciones. Como resultado, la salida de AIOps es más precisa y completa porque tiene en cuenta el alcance completo de los datos de todos los dispositivos, aplicaciones e infraestructura en toda la empresa.

SASE: un habilitador emergente de las redes empresariales edge

Las tecnologías que acabamos de describir no solo operan en el perímetro de la red, sino que también imponen cargas sustanciales en ese perímetro. En esta sección, echamos un vistazo a un enfoque emergente que está diseñado específicamente para reducir esas cargas (el perímetro de servicio de acceso seguro [secure access service edge, SASE]) y cómo los servicios críticos de red contribuyen a sus objetivos.

INFORMACIÓN TÉCNICA

Identificado por primera vez por Gartner en 2019, SASE es un nuevo modelo de redes y seguridad diseñado para satisfacer la creciente demanda de arquitecturas de red que sean más fluidas, seguras y fáciles de administrar.

El concepto SASE aborda las complejidades de la red asociadas con las empresas dispersas. Es una respuesta a las limitaciones de las arquitecturas de tipo *hub-and-spoke*, la proliferación de herramientas, las soluciones en silos y los procesos manuales que impiden que las organizaciones se muevan a la velocidad de la nube. Una red SASE fusiona las capacidades de red y seguridad, se construye utilizando principios

nativos de la nube, se entrega en la nube bajo demanda, se basa en SaaS y se apoya en DDI como una capa fundamental y unificadora (consulte la figura 3-7).

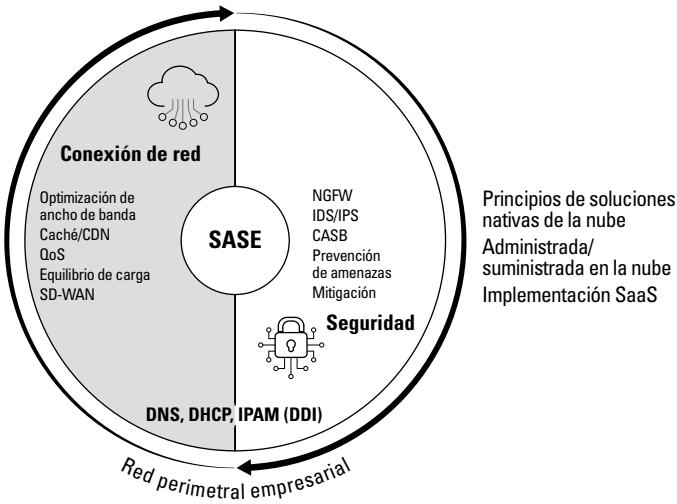


FIGURA 3-7: una red SASE.

SASE: simplificando el perímetro de la red

Utilizando arquitecturas nativas de la nube, SASE unifica las redes y la seguridad en una sola plataforma, con la información del contexto de la red del usuario. Las organizaciones implementan y administran una red SASE desde la nube como capacidades basadas en SaaS.

En un marco SASE, la carga de administrar y proteger una red se traslada de las aplicaciones basadas en el servidor que demandan mucho trabajo en el centro de datos a las aplicaciones virtuales y en contenedores en la nube. Como resultado, las redes SASE permiten a las organizaciones:

- Simplificar la administración
- Escalar elásticamente
- Implementar dinámicamente capacidades de red y seguridad según sea necesario
- Consumir capacidades de seguridad y de red versátiles como aplicaciones basadas en la nube

Capacidades de integración clave que faltan en las implementaciones de SASE

Es posible que se le perdone por suponer que si implementa una plataforma SASE unificada, su red sería, en consecuencia, de nivel empresarial en el perímetro. Si sólo fuera así de simple. Desafortunadamente, las implementaciones de SASE carecen actualmente de la integración fundamental necesaria para las redes empresariales edge. Eso no debería sorprenderlo. Después de todo, la integración vital a la que nos referimos aquí involucra los mismos servicios críticos de red que la mayoría de las organizaciones de TI, redes y seguridad subestiman constantemente.

Cómo los servicios críticos de red habilitan las redes SASE

En un modelo SASE, las capacidades de red y seguridad están diseñadas para estar estrechamente integradas y ser interoperables. Y, sin embargo, para lograr todo el potencial de integración, una plataforma basada en SASE debe poder aprovechar los servicios de red que son comunes a todas las funciones de red y seguridad: DNS, DHCP y administración de direcciones IP. La mayoría de las implementaciones de SASE, tal como se ofrecen actualmente, no integran adecuadamente estos servicios en sus plataformas.

Cuando se incorporan como una capa fundamental en las redes basadas en SASE, los servicios críticos de red brindan las siguientes ventajas:

- **Visibilidad centralizada.** Los datos que residen en los servicios críticos de red brindan una visibilidad de red mejorada para las implementaciones de SASE, lo que permite a los equipos de redes y seguridad monitorear y administrar el uso de dispositivos y aplicaciones de manera centralizada en la infraestructura física, virtual y en la nube.
- **Contexto del usuario de la red.** De manera similar, los servicios críticos de red, como DNS, permiten a las implementaciones de SASE optimizar las implentaciones de red y proteger automáticamente el acceso a las aplicaciones en el perímetro.
- **Capacidad de supervivencia local para ubicaciones dispersas.** La resistencia es la máxima prioridad para una red SASE. Aplicados de manera eficaz, los servicios críticos de red pueden garantizar el acceso continuo a Internet para ubicaciones dispersas en cualquier momento que pierdan la conectividad con las oficinas corporativas.

Entrega nativa de la nube para servicios críticos de red

El marco SASE enfatiza el uso del diseño nativo de la nube en los componentes de red. A medida que evalúa sus opciones para incorporar servicios críticos de red en el diseño de su red edge, busque soluciones creadas con microservicios y contenedores nativos de la nube.

INFORMACIÓN TÉCNICA

Las instancias en contenedores de servicios DDI son más rápidas y fáciles de administrar que las alternativas virtualizadas. También consumen muchos menos recursos y ofrecen una latencia extremadamente baja, lo que le proporciona la agilidad y la resistencia que necesita en el perímetro de la red.

EN ESTE CAPÍTULO

- Explorar las implementaciones de DDI tradicionales y en la nube
- Encontrar la plataforma que esté lista para la red edge
- Comprender por qué los servicios críticos de red son importantes en el perímetro

Capítulo 4
Servicios modernos para la red empresarial edge

Este capítulo analiza cómo puede aprovechar DNS y otros servicios DDI para brindar mejor conexión de red y seguridad en el perímetro. Para propiciar el marco idóneo, es útil tener un poco más de información sobre los servicios DDI, sus métodos de entrega tradicionales y cómo esa entrega debe cambiar para satisfacer los requisitos de las redes edge. Muchas organizaciones no aprovechan el tremendo potencial de las conexiones de red que contienen los servicios DDI debido a la falta de conocimiento.

RECUERDE

Por ejemplo, la gente suele suponer que las plataformas en la nube pública, como las de Amazon, Microsoft y Google, ofrecen una administración y un control integral de DDI. No lo hacen. En el mejor de los casos, proporcionan capacidades DDI limitadas, y en detrimento de la eficiencia y seguridad de la red edge. Pero ese no es el mayor problema.

Las implementaciones tradicionales de DDI no están preparadas para las redes edge

Llevar DDI al perímetro requiere reflexionar cómo la mayoría de las organizaciones implementan actualmente estos servicios cruciales. Irónicamente, aunque cada interacción en el perímetro de la red invoca DDI, muchas empresas confían en implementaciones de DDI que no son para nada favorables para el perímetro. Por lo general, DDI implica el uso de dispositivos y routers basados en servidor en ubicaciones dispersas (para obtener más información, consulte el capítulo 3). Con estos y otros sistemas similares, las organizaciones deben administrar individualmente y aprovisionar DDI manualmente en cada ubicación de la empresa. Si consideramos que una empresa puede tener desde varias docenas hasta miles de sitios, esto nos da una idea de lo complejo que puede ser este proceso.

Además, cuando un usuario se conecta a las aplicaciones y a los datos en la nube, muchas organizaciones transfieren el tráfico DNS y DHCP desde la ubicación del usuario a un centro de datos centralizado, a menudo a miles de kilómetros de distancia. La figura 4-1 ilustra la gran distancia que pueden viajar los datos. La combinación de aplicaciones administradas localmente y redes de retorno (*backhauling*) es costosa de administrar y no proporciona la baja latencia y la alta disponibilidad que exigen las redes edge.

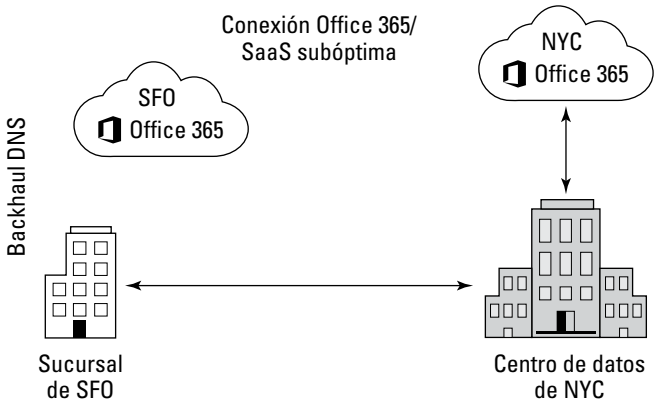


FIGURA 4-1: acceso y rendimiento subóptimos de SaaS a través del centro de datos.

Administrar DDI desde la nube

Un enfoque mucho más eficaz es trasladar la administración y el control de los servicios DDI de la infraestructura de hardware subyacente a la nube. La DDI administrada en la nube proporciona un complemento más flexible, ágil y rentable para las soluciones de DDI locales basadas en servidor (consulte la figura 4-2).

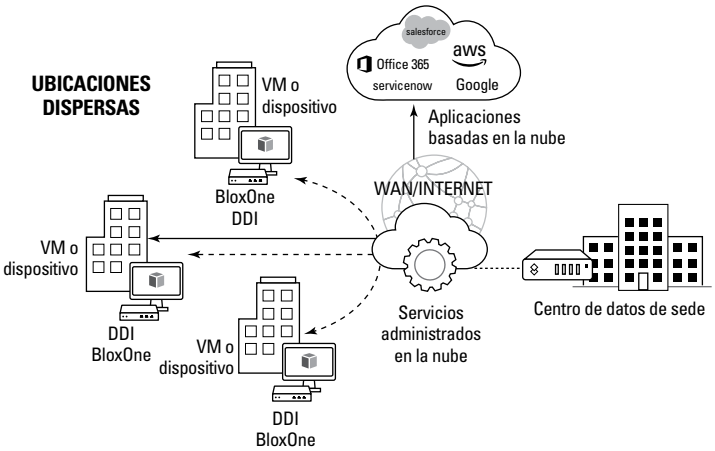


FIGURA 4-2: administrar DDI desde la nube.

RECUERDE

Las soluciones basadas en la nube reemplazan los servidores de gran tamaño con dispositivos virtuales o físicos más ágiles en cada ubicación. Eliminan la necesidad de realizar una configuración local de dispositivos o de un complejo suministro de servicios "in situ". Además, estas soluciones simplifican enormemente las redes y la seguridad mediante la centralización, la visibilidad mejorada y la automatización.

La plataforma es clave

Los servicios críticos de red administrados en la nube son un verdadero punto de inflexión en la era del perímetro de la red. Entonces, ¿cómo puede acceder a estos servicios? La manera más eficiente es a través de una plataforma que proporciona capacidades de red y de seguridad que utilizan DDI como base. Las mejores plataformas de este tipo comparten mucho en común con un marco SASE. De hecho, son facilitadores vitales de la implementación de SASE.

SUGERENCIA

La siguiente lista contiene algunas características que se deben buscar en una plataforma de servicios de red diseñada para el perímetro empresarial:

- **Arquitecturas nativas de la nube:** estas arquitecturas brindan capacidades de red y de seguridad a través de microservicios extensibles y diseño basado en contenedores (por ejemplo, servicios críticos de red que pueden ejecutarse en contenedores y organizarse a través de Kubernetes).
- **Compatibilidad con DevOps y AIOps:** esta característica garantiza que tenga los servicios de red siempre activos y sumamente ágiles que requieren los ciclos continuos de desarrollo/implementación de DevOps, AIOps y las operaciones de red y seguridad.
- **Escalabilidad horizontal:** estos servicios se pueden escalar rápida y elásticamente para satisfacer las necesidades de redes dinámicas en el perímetro.
- **Entrega como servicio:** esta característica hace que los servicios críticos de red estén disponibles mediante un modelo de suscripción basado en SaaS modular y sumamente flexible, lo que garantiza que las organizaciones paguen solo por el nivel de servicios que necesitan y nunca corran el riesgo de exceder el aprovisionamiento de la infraestructura.

Con la plataforma que ofrece la combinación adecuada de servicios, puede lograr un control y una seguridad sin precedentes para su red perimetral.

Controlar el perímetro a través de los servicios críticos de red

Confiar en la DDI basada y administrada en la nube genera beneficios significativos a través de toda una organización. Las siguientes secciones amplían algunos de esos beneficios.

Administración, automatización y visibilidad centralizadas

Casi todas las organizaciones valoran la capacidad de administrar de forma centralizada la infraestructura de red desde un único punto de control. Es aún más crítico a medida que las redes se vuelven cada vez más dispersas y complejas y deben adaptarse a los requisitos en constante evolución para la migración a la nube, SD-WAN, dispositivos móviles, IoT, DevOps, SASE y otros impulsores de tecnología. Una solución administrada en la nube unifica la administración y automatización de los servicios DDI en todas las ubicaciones, independientemente de la dispersión geográfica. La administración centralizada basada en la nube también automatiza el aprovisionamiento, la configuración y el control de políticas a gran escala, lo que simplifica mucho la administración de la red.

INFORMACIÓN TÉCNICA

Además, con información disponible solo a través de datos DDI, las soluciones más efectivas brindan detección automatizada, lo que permite una visibilidad y control centralizados en toda la red. Los administradores de red pueden acceder a los detalles clave de los servicios de red en cada dispositivo de la red, incluida la identificación del dispositivo y los atributos de las terminales y pueden visualizar todo en un solo lugar.

Optimización de aplicaciones y servicios

El tráfico de red de *backhauling* a través del centro de datos crea una latencia grave y cuellos de botella para los usuarios finales. Este problema afecta particularmente a sitios dispersos, como sucursales y oficinas remotas donde los usuarios necesitan acceder a aplicaciones sensibles a la latencia.

Las mejores ofertas de DDI administradas en la nube mejoran la confiabilidad de la red y reducen la latencia al permitir el acceso directo a Internet a las aplicaciones basadas en la nube para todos los usuarios, independientemente del dispositivo o la ubicación. Estos sistemas aseguran que los usuarios se conecten al punto de presencia local (point of presence, PoP) más cercano en la nube, lo que brinda a los usuarios en ubicaciones dispersas una experiencia de red más ágil y productiva con acceso de reconocimiento de la ubicación a aplicaciones y datos clave. La figura 4-3 muestra cómo la optimización de aplicaciones y servicios mejora el rendimiento en comparación con los datos de *backhauling*.

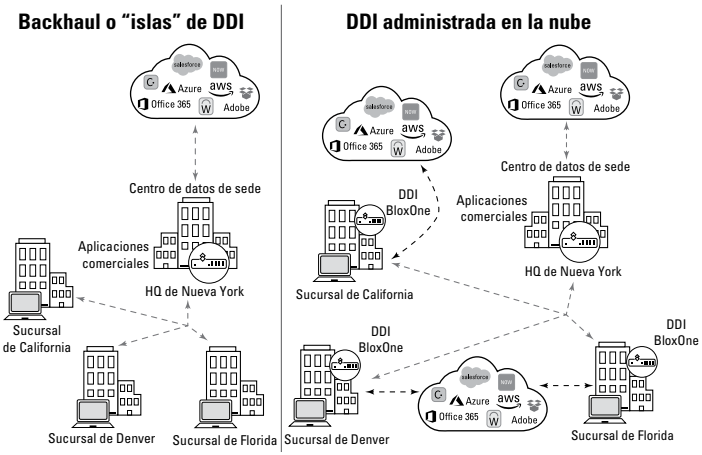


FIGURA 4-3: la DDI administrada en la nube mejora la confiabilidad y reduce la latencia al permitir el acceso directo a Internet a las aplicaciones basadas en la nube para los usuarios del perímetro empresarial.

Capacidad de supervivencia local para ubicaciones dispersas

El *backhauling* tradicional de DNS y DHCP a un centro de datos central afecta más que solo la latencia de la aplicación. Depender de las oficinas corporativas para estos servicios críticos de red también pone en riesgo la continuidad del negocio en sucursales y sitios remotos. Si la conexión a las oficinas corporativas se interrumpe por cualquier motivo, las ubicaciones dispersas se desconectan del centro de datos para la resolución de DNS y DHCP. Esto resulta en la pérdida de acceso a Internet y a las aplicaciones SaaS basadas en la nube.

Si bien muchas interrupciones de la red son simplemente inoportunas, otras pueden tener graves consecuencias. Una cosa es que los cajeros de una sucursal bancaria pierdan temporalmente la conexión con una aplicación financiera. Otra muy distinta es que un médico de una clínica de salud rural pierda el acceso a una aplicación de telemedicina en un momento crítico. A través de dispositivos ligeros virtuales y en contenedores implementados en todos los sitios, la DDI administrada en la nube brinda capacidad de supervivencia local para ubicaciones dispersas en caso de interrupciones con las conexiones de las oficinas corporativas, lo que garantiza un acceso siempre activo para todos los usuarios (consulte la figura 4-4).

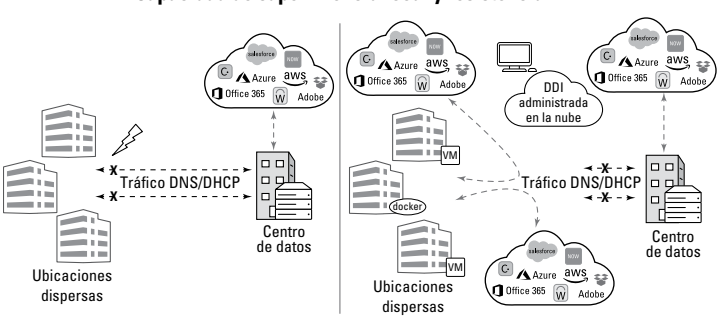


FIGURA 4-4: la DDI administrada en la nube proporciona capacidad de supervivencia local y resistencia.

Una plataforma que habilita los servicios de red administrados en la nube también ofrece beneficios sustanciales para la seguridad de la red. Ese tema se trata en el capítulo 5.

EN ESTE CAPÍTULO

- Explorar la seguridad en el perímetro
- Comprender cómo el DNS a menudo se infrautiliza
- Descubrir capacidades clave de una buena solución de seguridad

Capítulo 5
Proteger el perímetro empresarial

La seguridad es una preocupación para todas las organizaciones. Se convierte en una prioridad aún mayor a medida que su empresa se vuelve más distribuida y dispersa, y el perímetro de seguridad tradicional en el que antes podía confiar prácticamente desaparece. Analice estos datos:

- Las aplicaciones críticas para el negocio ahora se encuentran en la nube.
- La gente espera un acceso rápido y sin problemas a estas aplicaciones utilizando las tecnologías que les resulten más convenientes.
- El teletrabajo presenta una superficie de ataque mucho más amplia, porque los empleados utilizan dispositivos que comparten redes domésticas, Wi-Fi públicas y 5G, a menudo cuentan con una variedad mucho mayor de dispositivos IoT que los que se encuentran en el entorno laboral.

Cada vez más, la tarea de proteger la empresa ocurre en el perímetro de la red.

Desafortunadamente, cuando se trata de proteger el perímetro, las organizaciones de seguridad enfrentan muchos desafíos. Por ejemplo, la mayoría de las soluciones de seguridad empresarial todavía se centran en proteger los entornos y la infraestructura de las oficinas corporativas

tradicionales. Todavía no están optimizadas para una fuerza de trabajo dispersa.

Como si esos problemas no fueran suficientes, las operaciones de seguridad en muchas organizaciones ya están abrumadas, no cuentan con los fondos suficientes y cada vez están más limitadas. Hay demasiados equipos y demasiadas alertas, y nunca se tiene suficiente tiempo ni personal capacitado.

RECUERDE

En nuestro entorno donde las tareas se realizan principalmente en la nube, la misión de implementar un perímetro de red que brinde seguridad de nivel empresarial exige una arquitectura que sea flexible, automatizada, altamente adaptable y administrada en la nube. Integrales a esa arquitectura se encuentran los mismos servicios críticos de red (DNS, DHCP y administración de direcciones IP, [DDI]) que permiten el control de la red más eficiente que analizamos en el capítulo anterior.

El medio más simple y rentable para implementar una arquitectura de este tipo es a través de una plataforma nativa de la nube diseñada expresamente para brindar servicios de seguridad versátiles basados en DDI para el perímetro de la red.

Permitir la seguridad básica en el perímetro con servicios críticos de red

Los servicios DDI, particularmente DNS, tienen propiedades de seguridad únicas que muchas organizaciones no conocen, propiedades que son especialmente valiosas en el perímetro de la red.

DNS resuelve varios problemas de seguridad complejos directamente relacionados con las redes edge. Para empezar, cada transacción entre dispositivos, aplicaciones y recursos de la red invocan al DNS. Sin embargo, la mayoría de las organizaciones protegen mal su DNS, y los ciberdelincuentes lo saben. Aprovecharon la naturaleza abierta del DNS hasta el punto en que se convirtió en la ruta principal para el malware.

Sin embargo, como parte de una implementación de una red empresarial edge, el DNS puede servir como una señal para el despliegue de eventos de seguridad y como un punto de cumplimiento incesante para una reparación rápida.

SUGERENCIA

Los metadatos DDI, principalmente en forma de consultas DNS e identificación digital DHCP, revelan asociaciones entre dispositivos y usuarios, los destinos que visitan los usuarios en un periodo específico y los recursos de su red que necesitan más protección.

Capacidades clave de la seguridad una edge administrada en la nube

Una plataforma basada en la nube puede permitir a las organizaciones elevar sustancialmente la seguridad en el perímetro de la red, hacer que los recursos sobrecargados sean más efectivos y obtener más valor de las inversiones en infraestructura existentes. Las siguientes secciones ofrecen una breve descripción de las principales capacidades de seguridad que puede encontrar en las plataformas de seguridad centradas en el perímetro.

Detección y respuesta automatizadas

La seguridad innovadora basada en DNS y otros servicios críticos de red permite que las operaciones de seguridad (Security Operations, SecOps) realicen las siguientes tareas:

- Proteger todas las conexiones, independientemente del dispositivo o la ubicación, ya sea local o en la nube
- Detectar, bloquear y reparar automáticamente el mayor número de amenazas de seguridad basadas en DNS, incluidas las familias de DGA, la filtración de datos, el uso de dominios look alike, *fast flux* y muchas otras
- Detectar automáticamente dispositivos nuevos y fraudulentos que se conectan a la red, incluidos dispositivos móviles y de IoT no autorizados
- Remediar más rápido y con mayor certeza aprovechando el conocimiento de la situación y el contexto de red proporcionado a través de metadatos DDI

Administración y eficiencia simplificadas

La plataforma ideal para la seguridad administrada en la nube simplifica las complejas actividades de seguridad perimetral al:

- Proporcionar un punto centralizado de control y visibilidad a través de toda la organización.
- Implementar fácilmente los beneficios de seguridad a nivel de las oficinas corporativas a todos los usuarios de todo el mundo sin tener que depender de las VPN.
- Aliviar parte de la carga de las herramientas de seguridad, como los firewalls y los sistemas de detección/prevención de intrusiones. Las mejores soluciones garantizan que las amenazas basadas en DNS se detecten y mitiguen automáticamente antes de

que lleguen a otras herramientas de seguridad de las terminales en su ecosistema. Esto resulta en una priorización de amenazas más efectiva y menos alertas que deben manejar sus equipos y sistemas.

- Implementar rápidamente sin la necesidad de infraestructura adicional. Las principales soluciones administradas en la nube se pueden ejecutar como aplicaciones en el hardware existente.

Automatización e integración de ecosistemas

RECUERDE

Con un diseño e implementación adecuados, la seguridad perimetral administrada en la nube puede aprovechar una amplia automatización e integración. Puede habilitar todo el ecosistema de ciberseguridad y que funcione al unísono para acelerar la respuesta a las amenazas. Las capacidades clave que debe identificar incluyen:

- Una amplia gama de integraciones de API con herramientas y sistemas de ciberseguridad de terceros, como NGFW, IPS/IDS, SIEM, SOAR, DevOps, AIOps y SASE. La figura 5-1 muestra amplias integraciones de ecosistemas habilitadas con una plataforma de seguridad administrada en la nube de alto rendimiento.
- La organización de la seguridad que puede compartir automáticamente eventos de red e indicadores de compromiso (derivados de metadatos DDI) a nivel de dispositivo en tiempo real en todo el ecosistema de defensa.
- Integración con analítica e inteligencia de amenazas consolidada y protegida basada en inteligencia artificial y aprendizaje automático que permite a los equipos de seguridad anticipar las amenazas y detener los ataques de día cero.

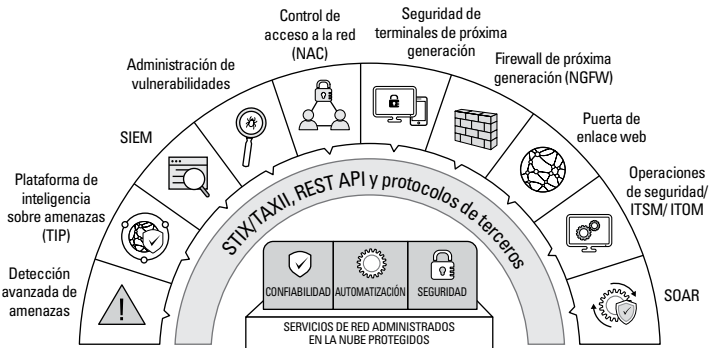


FIGURA 5-1: la amplia integración del ecosistema a través de API es una característica principal de una plataforma de seguridad administrada en la nube de alto rendimiento.

Arquitecturas híbridas

Las redes edge son el punto donde la infraestructura local y la infraestructura de la nube convergen e interoperan. Eso explica por qué las opciones de seguridad perimetral administradas en la nube más efectivas se basan en una arquitectura híbrida que abarca la infraestructura local y los recursos basados en la nube. La figura 5-2 ilustra los beneficios clave de una arquitectura híbrida. Con una plataforma de este tipo, las organizaciones pueden lograr los siguientes resultados:

- Proteger a los usuarios y los datos sin importar dónde se encuentren: en la infraestructura de red tradicional o en la nube.
- Aprovechar los valiosos metadatos locales que no están disponibles para las medidas de seguridad solo en la nube. Estos datos proporcionan información que resulta en una solución de respuesta a incidentes más rápida y priorizada en todo el perímetro de la empresa.

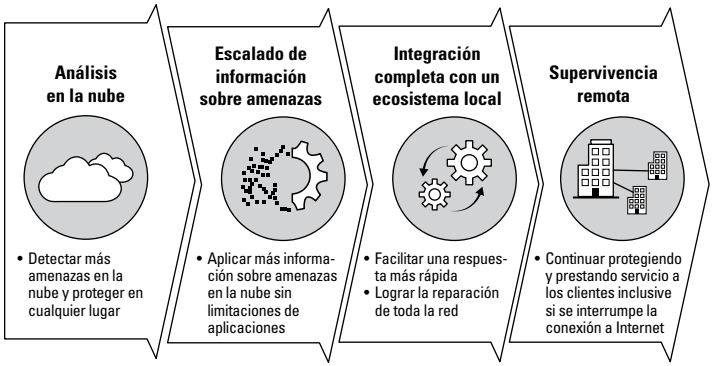


FIGURA 5-2: el enfoque híbrido protege donde sea que esté implementado.

Seguridad discreta

Una desventaja de las medidas de seguridad, como las VPN, es que ralentizan el rendimiento de la red. Lo hacen desviando todo el tráfico de la red a servidores centrales donde se lleva a cabo el cifrado de seguridad.

RECUERDE

Por el contrario, la seguridad DNS administrada en la nube, cuando se implementa correctamente, bloquea solo las solicitudes de DNS sospechosas o malignas, y deja que todas las solicitudes legítimas fluyan sin trabas. El resultado es una protección de red avanzada sin impacto adverso en la velocidad o el rendimiento. Dichas soluciones:

- Son ideales para proteger a todos los usuarios y datos sin afectar las experiencias del usuario final, un beneficio con la ventaja adicional de alentar a los usuarios a permanecer en la infraestructura de red controlada por la empresa
- No crean latencia: un requisito fundamental para las aplicaciones 5G y en la nube basadas en SaaS
- Pueden usar DNS para el filtrado de contenido, lo que garantiza automáticamente que el contenido al que acceden los empleados desde los dispositivos corporativos siga cumpliendo con las políticas corporativas, a la vez que elimina el costo y la latencia asociados con la implementación de cientos de puertas de enlace web seguras

Capítulo 6
Mejores prácticas para una red empresarial edge

Este capítulo resume las conclusiones más importantes de este libro. Piense en estas diez mejores prácticas como un punto de partida en su viaje hacia las redes empresariales edge.

- **Aprovechar el poder de los servicios críticos de red:** las propiedades únicas de los servicios críticos de red, DNS, DHCP e IPAM (DDI), pueden ayudarlo a optimizar el perímetro para dispositivos móviles, implementaciones de IoT, 5G y Wi-Fi 6, así como para las necesidades de DevOps, AIOps y SASE.
- **Mover los servicios básicos cerca de los usuarios:** los servicios DDI funcionan mejor cuando están ubicados lo más cerca posible del usuario, de modo que se pueda acceder a los servicios basados en la nube desde el PoP más cercano. Busque opciones de entrega de DDI que pueda implementar fácilmente "in situ" a través de las ubicaciones dispersas.
- **Centralizar la administración:** los servicios críticos de red suministrados y administrados en la nube le permiten implementar estos servicios críticos en cualquier lugar, pero administrarlos desde un solo lugar e incluso desde una sola pantalla.

- **Insistir en la entrega como servicio:** los servicios de infraestructura más versátiles y flexibles de la actualidad, incluidas las principales soluciones de seguridad y DDI, son aquellos que se pueden consumir como servicio.
- **Elegir soluciones basadas en la nube:** los detalles son importantes. Las plataformas heredadas se crean mediante la virtualización, lo que dificulta la administración de las integraciones y la funcionalidad entre aplicaciones. Elija soluciones creadas con microservicios en contenedores modernos, basados en la nube o habilitados para la nube.
- **Incorporar la supervivencia local:** protéjase contra la interrupción del servicio asegurándose de que los servicios de su red principal sean resistentes, es decir, que permanecen en línea incluso si hay una pérdida de conectividad desde el sitio a las oficinas corporativas.
- **Aprovechar DDI para una seguridad fundamental:** el mejor lugar para tomar decisiones informadas sobre la postura de seguridad en el perímetro es al inicio de la sesión de red. DHCP y DNS se encuentran entre los primeros protocolos que utilizan los dispositivos cuando se conectan a una red. Elija soluciones que maximicen las capacidades de seguridad integradas en estos servicios.
- **Utilizar un modelo de implementación híbrido:** controle las interacciones perimetrales en cualquier lugar y protéjase en todas partes con servicios de red que unifican su infraestructura local y en la nube, y le permiten aprovechar los datos que residen en ambos ámbitos.
- **Elegir un escalado elástico:** tradicionalmente, las organizaciones han construido en exceso o minimizado drásticamente su infraestructura de DDI, especialmente en las ubicaciones dispersas. Busque opciones que se ajusten dinámicamente a sus necesidades cambiantes para que sus implementaciones y costos tengan siempre el tamaño adecuado.
- **Siempre tener en cuenta al usuario:** si lo construye, es posible que vengan, pero ¿se quedarán? Sus usuarios tienen más opciones que nunca para conectarse a lo que necesitan. Para proteger a las personas y los datos, seleccione soluciones de infraestructura que sean sencillas y discretas para los usuarios finales.

Aproveche el poder de una experiencia de red segura basada principalmente en la nube

La base para las redes
Empresariales edge

Ya sea que su organización nació con centros de datos o completamente en la nube, el éxito depende de su capacidad para aprovechar todo el poder de la nube y las redes edge para desenvolverse ágilmente en un panorama empresarial en constante cambio, con una fuerza laboral que trabaja desde cualquier lugar. Eso comienza con los servicios críticos de red: DNS, DHCP e IPAM (conocidos colectivamente como DDI). La plataforma BloxOne® de Infoblox permite una experiencia de red segura basada principalmente en la nube para empresas dispersas a través de BloxOne® DDI y BloxOne® Threat Defense.

BloxOne DDI es la primera solución basada en SaaS de la industria que simplifica, automatiza y controla el DNS y otros servicios críticos de red desde la nube. BloxOne DDI permite la implementación rápida de servicios de red a escala, contribuye con el rendimiento de las aplicaciones basadas en la nube e independiza la actividad de la red para ubicaciones dispersas.
Más información en: https://www.infoblox.com/products/bloxone-ddi/

BloxOne Threat Defense maximiza la protección de la marca al proteger las redes existentes, así como los elementos digitales: SD-WAN, IoT y la nube. Impulsa las soluciones de organización, automatización y respuesta de la seguridad (Security orchestration, automation and response, SOAR), y reduce drásticamente el tiempo para investigar y reparar las amenazas cibernéticas. Funciona con sus soluciones actuales para optimizar el rendimiento de todo el ecosistema de seguridad, no requiere infraestructura adicional y reduce el costo total de defender a la empresa contra amenazas.
Más información en: https://www.infoblox.com/products/bloxone-threat-defense/

Infoblox®

Simplificar y proteger un perímetro de la red de nivel empresarial

Las redes empresariales se están volviendo más dispersas, impulsadas por las tendencias clave del mercado y comerciales de movilidad, Internet de las cosas (IoT) y de la nube. Para prosperar en esta nueva era centrada en la nube y en el perímetro, su empresa necesita una red empresarial edge de nivel empresarial. En este libro electrónico, le brindamos toda la información que se necesita para implementar una red de este tipo, una que sea increíblemente rápida, resistente, con escalabilidad elástica, simple de administrar e intrínsecamente segura. También lo guiamos a través de los servicios fundamentales de red y de seguridad que requiere toda red empresarial edge.

Adentro...

- Redes empresariales del centro al perímetro
- Tecnologías y tendencias que afectan el perímetro
- SASE: habilitador de las redes Empresariales edge
- Administrar DDI desde la nube
- Proteger el perímetro empresarial
- Implementar una red empresarial edge

Infoblox

Glenn Sullivan es Jefe encargado de productos en Infoblox. **Rod Dixon** es Director senior de marketing de productos en Infoblox.

Vaya a Dummies.com®
para ver videos, fotos instructivas, artículos ¡o para comprar!

ISBN: 978-1-119-83779-4

para dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.