Presentación del modelo Zero Trust Edge para servicios de seguridad y red

Secure Access Services Edge (SASE) es una solución Zero Trust Edge (ZTE)

Por David Holmes y Andre Kindness
28 de enero de 2021

Por qué debería leer este informe

Para respaldar la digitalización de una empresa mediante la cloud y el Internet de las cosas (IoT), muchos equipos de redes recurrieron a SD-WAN. Sin embargo, SD-WAN no aborda los nuevos requisitos de seguridad ni el factor impulsor de que los mundos de seguridad y redes deben fusionarse. Tanto los profesionales de infraestructuras y operaciones (I&O) como de riesgos y seguridad (S&R) deben leer este informe para comprender mejor la solución emergente Zero Trust que ayudará a unificar la infraestructura de redes y seguridad a fin de respaldar la estructura de red empresarial.

Conclusiones principales

Los casos de uso de seguridad llevarán a las empresas directamente a ZTE

El caso de uso inicial para la mayoría de las empresas que se encuentran en la transición a Zero Trust Edge (ZTE) será proteger y permitir el teletrabajo, al tiempo que se eliminan las complejas VPN de usuario que abundan actualmente en el sector.

La estructura de seguridad alojada en el perímetro de Internet es el Santo Grial, pero todavía está en sus inicios

El modelo ZTE aspira a ser una estructura de seguridad completa alojada en la cloud o en el perímetro, pero la tecnología no está disponible todavía, ya que hay otras dependencias. Mientras el ancho de banda sea un factor limitante en muchas partes del mundo, algunos elementos deberán localizarse.

No se olvide de la inteligencia perimetral de las instalaciones para lograr una mayor eficiencia

Aún se aplican casos de uso para tomar decisiones inteligentes a nivel de las instalaciones en el perímetro, especialmente para los entornos de uso intensivo de redes, IoT/OT y sanitario.

Presentación del modelo Zero Trust Edge para servicios de seguridad y red

Secure Access Services Edge (SASE) es una solución Zero Trust Edge (ZTE)

Por David Holmes y Andre Kindness
Con Glenn O'Donnell, Joseph Blankenship, Paul McKay, Renee Taylor y Peggy Dostie

28 de enero de 2021

Tabla de contenido

Documentos de investigación relacionados

Evaluate SDWAN Services Based On Branch Office Goals, Not Hardware Data Sheets

Now Tech: Software-Defined WAN Hardware/ Software, Q3 2020

Now Tech: Software-Defined WAN Services, Q3 2020

FORRESTER®

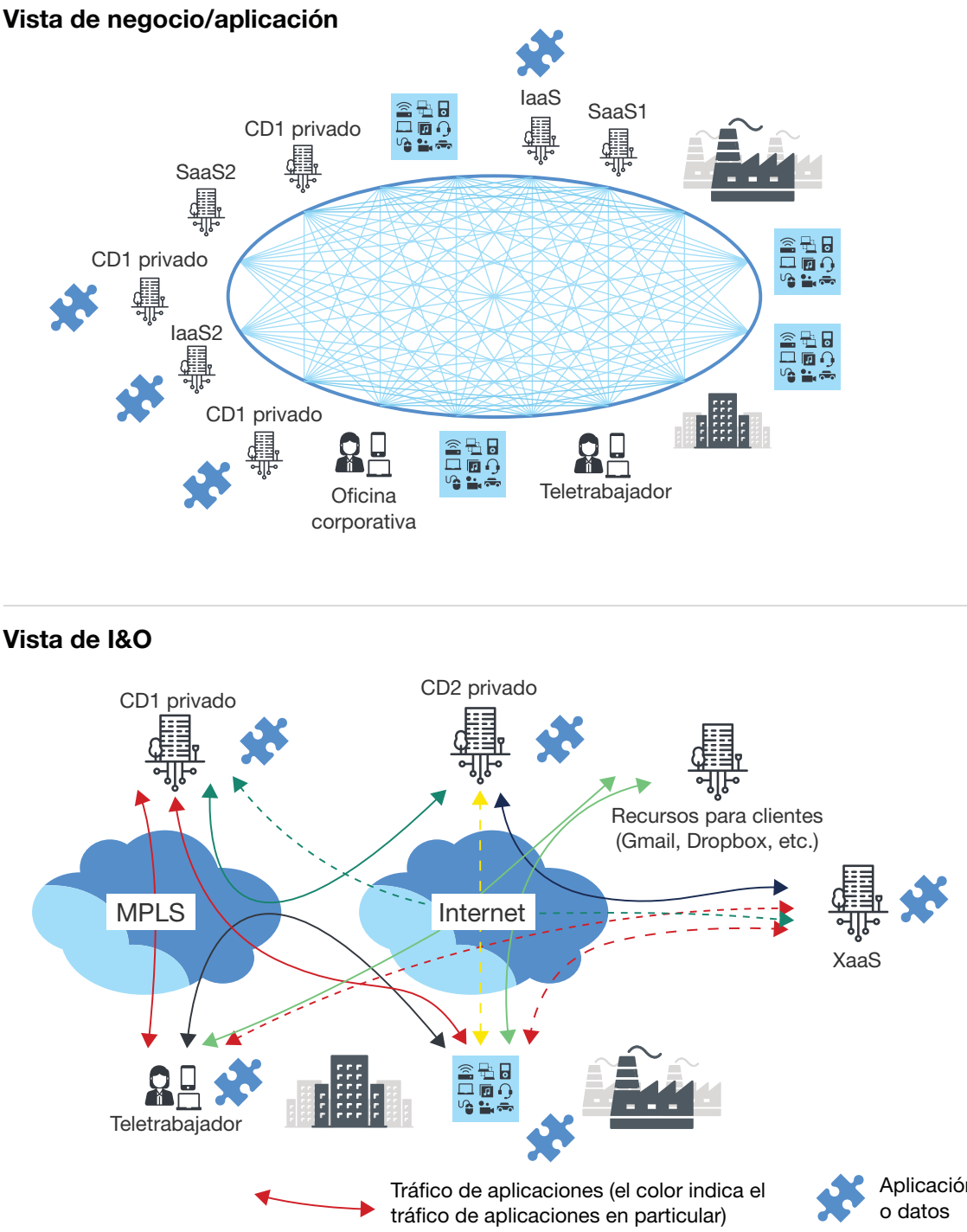
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140, EE. UU.
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Fusione seguridad y redes, o su empresa estará destinada al fracaso

Las redes y la seguridad tienen una larga y complicada historia conjunta; se podría describir como cordial, en el mejor de los casos, o totalmente hostil, en el peor de los casos. Sin embargo, este enfoque segregado no es una manera aceptable de operar y, a menudo, sabotea los beneficios de las iniciativas digitales. Las operaciones e infraestructuras de seguridad y redes aisladas están desapareciendo con rapidez debido a lo siguiente:

- **Las aplicaciones y los datos distribuidos en la cloud se encuentran fuera de la infraestructura del centro de datos.** La cloud, el perímetro y el IoT no solo están redefiniendo la ubicación de los datos y las aplicaciones, sino que estos componentes de la digitalización dejaron obsoleto el diseño de tipo hub-and-spoke de red tradicional[1]. Ahora, una estructura de red empresarial entrelaza activos empresariales, clientes, socios y activos digitales para conectar todas las partes del ecosistema empresarial (consulte la Figura 1)[2]. Como indica el informe de Forrester "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", esto solo puede ocurrir si la seguridad está integrada en el ADN de la red.
- **La COVID-19 obligó a los empleados a estar fuera de los controles del foso de la LAN corporativa.** Piense en esta sencilla realidad: hoy en día existen muchas aplicaciones empresariales en la cloud, y este número no deja de aumentar. Los usuarios también han abandonado ahora el perímetro empresarial tradicional; la encuesta sobre la experiencia durante la pandemia de Forrester reveló que el 53 % de los teletrabajadores nuevos deseaban continuar teletrabajando incluso después de que la crisis termine[3]. Puesto que las aplicaciones y los usuarios ya no están protegidos por las barreras del foso, la utilidad y el valor de la estructura de seguridad se han desplomado.

FIGURA 1 La dispersión de aplicaciones y datos entre los recursos empresariales



Los enfoques históricos de seguridad y redes no respaldan la empresa distribuida

La pandemia de 2020 hizo que millones de empleados pasaran de estar protegidos por un cómodo escudo dentro del perímetro empresarial a enfrentarse a las dificultades planteadas por el teletrabajo. El responsable de seguridad de la información (CISO) de una gran compañía de seguros con sede en Europa nos dijo que, antes de la pandemia de 2020, solo el 5 % de la plantilla de la empresa teletrabajaba. La pandemia cambió de golpe la situación y ahora los teletrabajadores conforman el 95 % de su base de empleados. Para empresas como la suya, la infraestructura de VPN, que ya era deficiente, no pudo hacer frente a la situación. La tecnología VPN es solo otra fisura más de las murallas erosionadas del castillo. Tanto los equipos de redes como de seguridad han tenido dificultades para cumplir los nuevos requisitos de uso de la cloud y respaldar a los teletrabajadores, puesto que los enfoques tradicionales se basaban en lo siguiente:

- **Dispositivos de software o hardware específico in situ.** La introducción de un tipo de solución específica para resolver un problema tecnológico concreto es cosa del pasado. Treinta años de conexión de dispositivos a la red, como optimizadores de WAN o firewalls, dieron lugar a más problemas de seguridad, mayores niveles de complejidad, menor flexibilidad y menor eficacia. Cada nuevo dispositivo aumenta exponencialmente la complejidad y los posibles problemas de seguridad.
- **Controles y repositorios de políticas en las instalaciones poco fiables.** El software de gestión in situ necesita hardware y personal específicos para mantener el software actualizado con las últimas funciones, correcciones de errores y mejoras de seguridad. El software de gestión que reside en una infraestructura privada no solo cuesta más a la empresa, sino que dificulta las capacidades de resiliencia. Por lo general, el software no se creó para reubicarse en plataformas de cloud, lo que limita la eficacia y las opciones para la recuperación ante desastres.
- **Limitación del enfoque centrado en el hardware.** Los aviones, los coches y los trenes tienen restricciones de forma y adaptación debido a restricciones de peso o tamaño. Incluso sin esas restricciones, los equipos tecnológicos no esperan introducir hardware en todas las partes de un centro de fabricación, tienda o estadio. Es poco factible suponer que el hardware se puede crear para satisfacer la adaptación, la forma y la función necesarias entre una extrusora de plástico y una cámara de calentamiento o sobrevivir a las temperaturas a las que un equipo debe operar en lugares como una subestación eléctrica de Dubái o una torre de comunicaciones del Valle de la Muerte.
- **Silos inconexos de seguridad y redes.** La práctica de relegar determinados tipos de hardware y operaciones a determinados grupos solo aumenta las ineficiencias operativas, disminuye la resiliencia de la infraestructura y da lugar a nuevos problemas de seguridad. Muchos dispositivos discretos, como firewalls y routers, se podrían combinar para reducir la latencia mediante el uso de una tabla para buscar reglas para paquetes y aplicar políticas de seguridad y redes en el puerto.

Aparición de Zero Trust Edge

Cuando la COVID-19 obligó a los empleados a trabajar desde casa, una minoría de profesionales de la seguridad con visión de futuro, que consideraba que la tecnología VPN no era la mejor vía, invirtió en soluciones de acceso de red Zero Trust (ZTNA) para evitar los problemas con las VPN; algunos de los que experimentaron la vía ZTNA preguntaron si podían adoptar otros enfoques ZT, ya que muchos profesionales de seguridad e I&O consideraban que Zero Trust era principalmente un concepto de centro de datos (consulte la Figura 2)[4]. Sin embargo, el marco de seguridad establecido en "The Zero Trust eXtended (ZTX) Ecosystem" de Forrester muestra cómo ZT es más que un concepto de centro de datos. ZT protege a las empresas de clientes, empleados, contratistas y dispositivos en sitios remotos que se conectan a través de redes WAN a un entorno más mordaz, abierto, peligroso y turbulento (consulte la Figura 3). Forrester considera este concepto como Zero Trust Edge (ZTE) y lo define de la siguiente manera:

> *Una solución Zero Trust Edge conecta y transporta de forma segura el tráfico, utilizando principios de acceso Zero Trust, dentro y fuera de sitios remotos, aprovechando la mayoría de los servicios de seguridad y redes basados en la cloud.*

FIGURA 2 Los primeros usuarios que adoptaron ZT asociaban los microperímetros de seguridad únicamente a máquinas virtuales (VM)

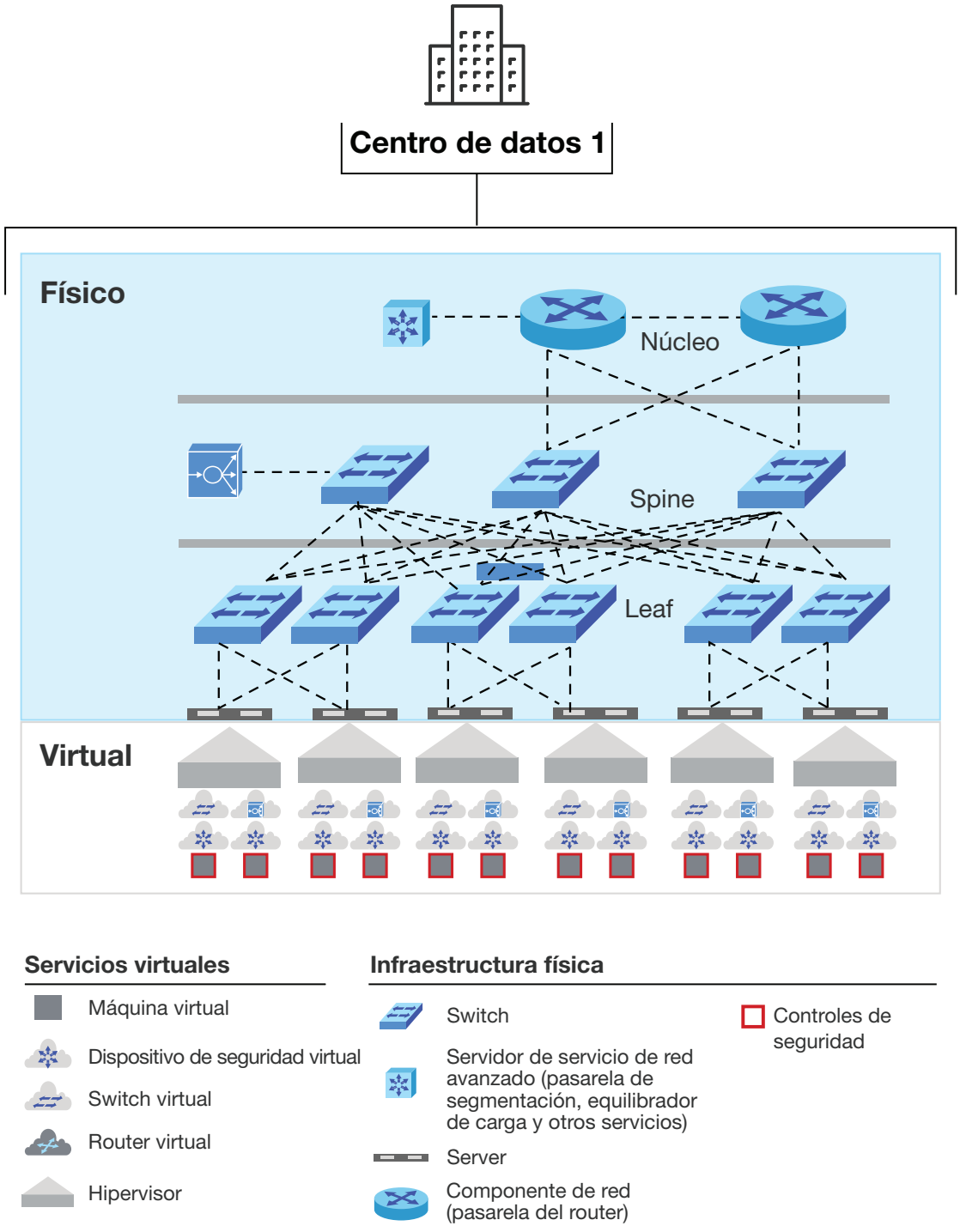
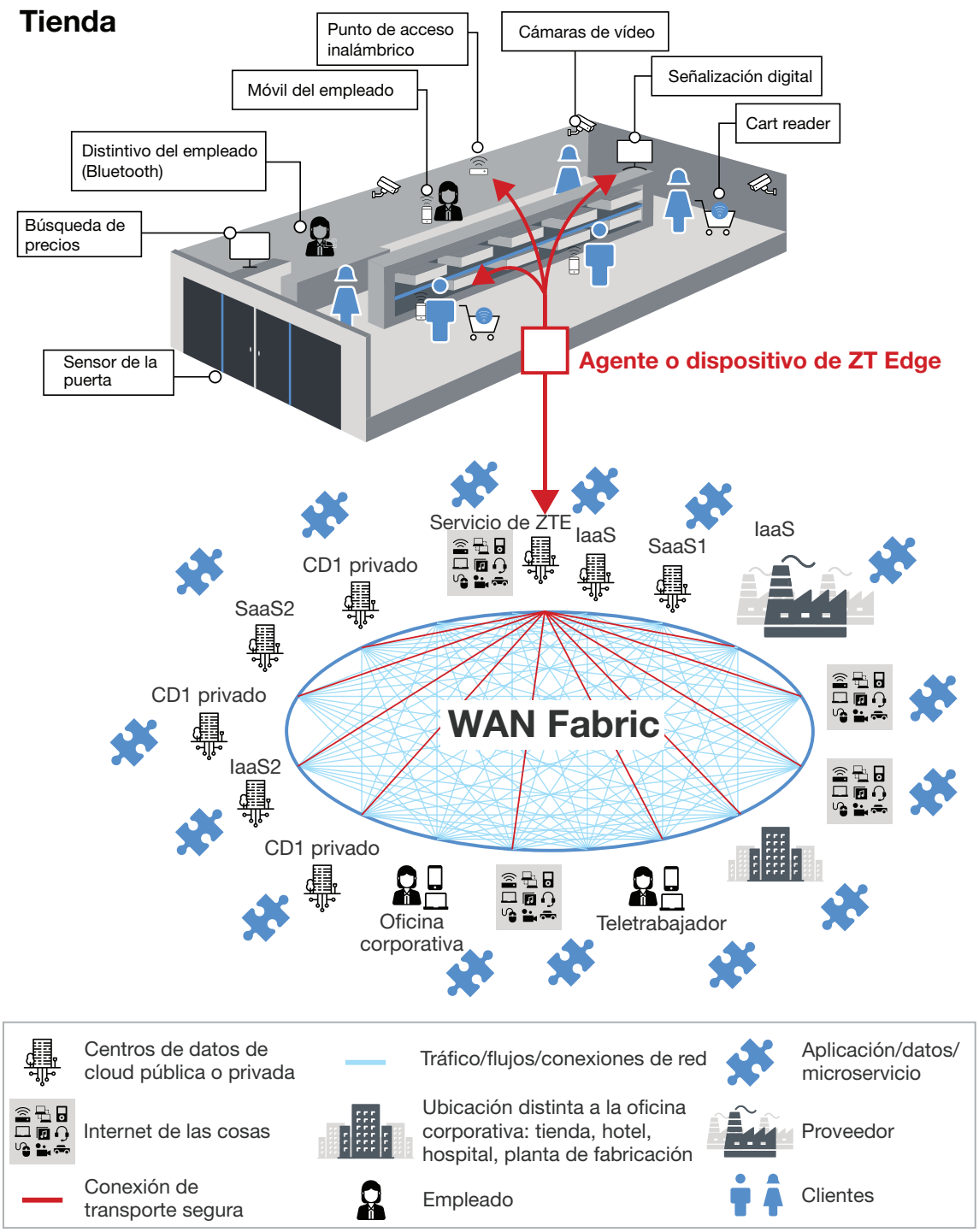


FIGURA 3 ZTE proporciona los controles de seguridad y las políticas de redes para proteger todas las conexiones in situ



¡Sorpresa! ZTE comienza en la cloud

ZTE configura el marco de seguridad y redes en torno al tráfico y los servicios que llegan a las empresas desde ubicaciones remotas, así como de los servicios que se dirigen hacia las ubicaciones o los usuarios. Aunque ZTE tiene como objetivo la empresa distribuida, las soluciones, que ofrecen un conjunto de servicios más rápido y ágil, deben estar basadas en dos elementos fundamentales:

- **Gestión de seguridad y redes basada en la cloud.** Tradicionalmente, las configuraciones de dispositivos y las políticas de seguridad existían en diferentes herramientas. Por ejemplo, los controles de acceso a la red tenían políticas de seguridad para los usuarios, mientras que las soluciones de gestión para firewalls y componentes de redes contenían las configuraciones de dispositivos. Esto aumenta la cantidad de errores de configuración y reduce la eficacia operativa a medida que el personal configura políticas similares en varios sistemas. La gestión de la cloud permite fusionar estos sistemas de back-end dispares y modificar, añadir o eliminar configuraciones en función de una única solución de gestión de configuraciones.
- **Análisis y supervisión basados en la cloud.** Las supervisiones de la seguridad y las redes suelen ser independientes entre sí, y son los requisitos fundamentales de la existencia de ZTE. Google es un buen ejemplo: utiliza su WAN definida por software para impulsar la utilización de enlaces hasta en un 100 %. La supervisión identifica irregularidades en el tráfico, a menudo problemas de seguridad, hasta las metrópolis interconectadas y fuera de los centros de datos de la empresa[5]. La cantidad de información que se debe recopilar y sintetizar obliga a que la supervisión de ZTE se base en la cloud. Necesita una plataforma informática amplia para aprovechar todas las funcionalidades de análisis.

Utilice ZTE para desplegar 18 servicios de seguridad y redes

Desde cualquier parte del mundo, las organizaciones pueden gestionar, supervisar y analizar de forma centralizada el conjunto de servicios de seguridad y redes que se encuentra en las soluciones ZTE (consulte la Figura 4). Algunos de los servicios permanecerán ubicados exclusivamente en la cloud (o en el perímetro de la cloud) y otros deberán alojarse en la ubicación remota.

FIGURA 4 Tipo de servicios disponibles en una solución ZTE

Red	
Garantía de ancho de banda	Determina una cantidad mínima de ancho de banda para un tráfico determinado.
Almacenamiento en caché de contenido	Proporciona copias localizadas de los datos.
Equilibrio y utilización de enlaces	Aprovecha varios enlaces simultáneamente para aumentar el ancho de banda del tráfico y el uso general de WAN.
Calidad del servicio	Prioriza el tráfico de red.
Resiliencia	Proporciona y mantiene un nivel de servicio aceptable ante fallos y retos de funcionamiento normal.
Enrutamiento/mejor ruta	Selecciona la ruta correcta para el transporte de nivel 3 incluso desde el teletrabajador hasta una aplicación alojada en la cloud.
WAN definida por software (SD-WAN)	Selecciona los mejores enlaces, rutas o conexiones en función de métricas de nivel superior, como la inestabilidad, la pérdida de paquetes y la afinidad con un perfil de aplicación.
Conexión WAN	Establece la conexión física con/desde una instalación.
Optimización de WAN	Proporciona la deduplicación, la fusión de paquetes y otras funciones de optimización de WAN.

FIGURA 4 Tipo de servicios disponibles en una solución ZTE (continuación)

Seguridad

Firewall básico	Ofrece capacidades sencillas de firewall de red (reglas de nivel 3 y 4) que se pueden dividir y mover localmente para reducir la cantidad de tráfico que sale del centro remoto.
Agente de seguridad de acceso a cloud (CASB)	Controla e informa sobre el acceso a aplicaciones en la cloud.
Firewall como servicio (FWaaS)	Proporciona funciones y características avanzadas de firewall basadas en la cloud.
Sistema de detección de intrusos/sistema de prevención de intrusos (IDS/IPS)	Analiza el tráfico de red basándose en firmas para detectar y desviar contenido malicioso específico.
Cifrado de enlaces	Cifra y descifra todo el tráfico de red en cada punto de enrutamiento de red.
Gestión de acceso e identidades (IAM)	Garantiza que las personas adecuadas de una empresa dispongan de acceso oportuno a los recursos tecnológicos.
Pasarela web segura (SWG)	Impide que el tráfico no seguro entre en una red interna de una organización. Los filtros de URL deben actualizarse constantemente y la tendencia ya era que se configuraran, alojaran y mantuvieran en la cloud.
Análisis avanzado de malware	Ejecuta programas en un entorno aislado (sandboxing) para detectar y contener malware de día cero.
Acceso de red Zero Trust (ZTNA)	Permite al teletrabajador conectarse a aplicaciones empresariales en función de su identidad, independientemente de dónde residan los trabajadores o las aplicaciones. Es el servicio de seguridad de autenticación de firmas que debe existir en ZTE.

Los casos de uso determinarán los tipos y ubicaciones de servicios de ZTE

Los arquitectos de red y seguridad deben garantizar la máxima utilidad a medida que progresan con Zero Trust Edge. Los tipos de servicios que se utilizan dependen de la ubicación, los dispositivos, las personas y otros elementos (consulte la Figura 5). Tres casos de uso muestran niveles cada vez mayores de factores impulsores (lo que significa una mayor cantidad de servicios de redes y seguridad que se activan en la solución ZTE):

- **Proteger a los teletrabajadores como caso de uso inicial.** La pandemia de 2020, y su consiguiente éxodo masivo, ha obligado a millones de trabajadores a pasar de trabajar en una oficina a trabajar en casa. Proporcionar un acceso seguro a las aplicaciones y los servicios corporativos para estos teletrabajadores es el caso de uso inicial que lleva a las organizaciones a usar Zero Trust Edge. Debido a muchos de los retos descritos en la investigación de Forrester, "Key Considerations For Network And Capacity Management When Operationalizing A Home-Based Workforce", la mayoría de las empresas se abstienen de proporcionar cualquier tipo de

hardware o software de redes en los hogares de los trabajadores. En su lugar, se despliegan agentes de software en los dispositivos de trabajo de los trabajadores, y sus conexiones se vinculan a servicios de seguridad del perímetro de la cloud (consulte la Figura 6).

- **Priorizar el tráfico de aplicaciones empresariales que domina la WAN de la sucursal.** El número de conexiones WAN se ha disparado debido al teletrabajo. Sin embargo, las conexiones de oficinas remotas representan la mayor parte del tráfico de WAN para una empresa, principalmente procedente de empleados, sus aplicaciones y dispositivos propiedad de la empresa. El tráfico de SaaS, como O365, se ha convertido recientemente en un factor importante y también puede contener tráfico de clientes. El tráfico de aplicaciones basado en SaaS necesita conexiones directas a Internet, y es posible que los clientes necesiten conectarse a las LAN de oficinas remotas. Para hacer frente a estos retos, los arquitectos empresariales dirigen cada vez más este tráfico a través del firewall como servicio (FWaaS). Esto se realiza a través de routers de oficinas remotas o soluciones SD-WAN destacadas en el informe de Forrester "Now Tech: Software-Defined WAN Hardware/Software, Q3 2020", o bien a través de un proveedor de servicios incluido en el informe de Forrester "Now Tech: Software-Defined WAN Services, Q3 2020" (consulte la Figura 7). Algunos proveedores, como Forcepoint, admiten la funcionalidad SD-WAN integrada con varios servicios de seguridad.
- **Por último, proteger el Internet de las cosas.** Además de los teletrabajadores y las sucursales genéricas, los dispositivos periféricos, el IoT y los socios empresariales tienen las riendas de la red. El arquitecto de sistemas de control industrial (ICS) tendrá que incorporar ubicaciones relacionadas que obligan a prestar mayor atención a las políticas de seguridad y red. Por ejemplo, un ingeniero de una planta de fabricación de automóviles tiene en cuenta el tráfico de empleados y contratistas, pero también debe tener en cuenta el tráfico de los controladores lógicos programables (PLC) de Siemens o los datos que describen los pesos de los estantes de control de inventario de Bosch. Debido a la ubicación y a la falta de ancho de banda disponible en el sitio, algunos elementos de seguridad básicos deben alojarse in situ, junto con todos los servicios de redes, para reducir la cantidad de tráfico dirigido a los servicios de seguridad en la cloud (consulte la Figura 8).

FIGURA 5 Cada caso tiene un conjunto diferente de factores de seguridad y redes a tener en cuenta

	Teletrabajo	Pequeña oficina	Sitio heterogéneo
Activos	Portátil	Escritorios, impresoras, salas de conferencias, cámaras web	Red física heterogénea
Pasarela a ZTE	Agente de punto de conexión	Dispositivo WAN con los servicios de red in situ necesarios o superposición mediante agente	Dispositivo WAN con los servicios de red in situ necesarios
IoT	No	Bajo	Alto
Edge computing	No	Bajo	Alto
Contratistas	No	No	Sí
Proveedores empresariales y tecnológicos	No	Bajo	Alto

FIGURA 6 Los teletrabajadores se benefician de los servicios de seguridad basados en la cloud de ZTE

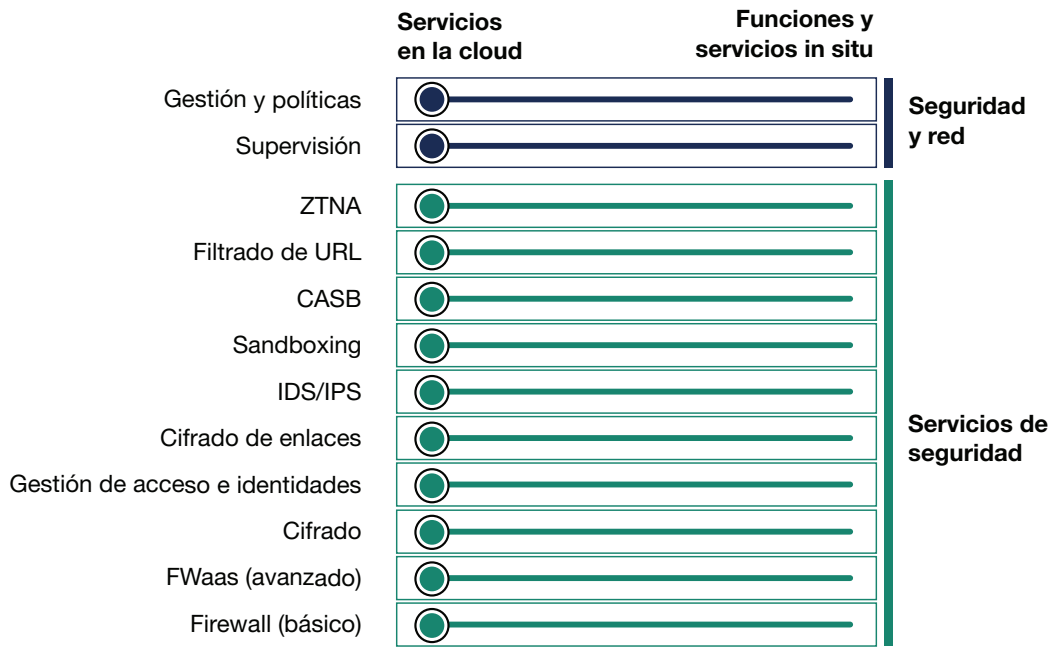


FIGURA 7 Las oficinas empresariales genéricas dirigen el tráfico a los servicios de seguridad basados en la cloud

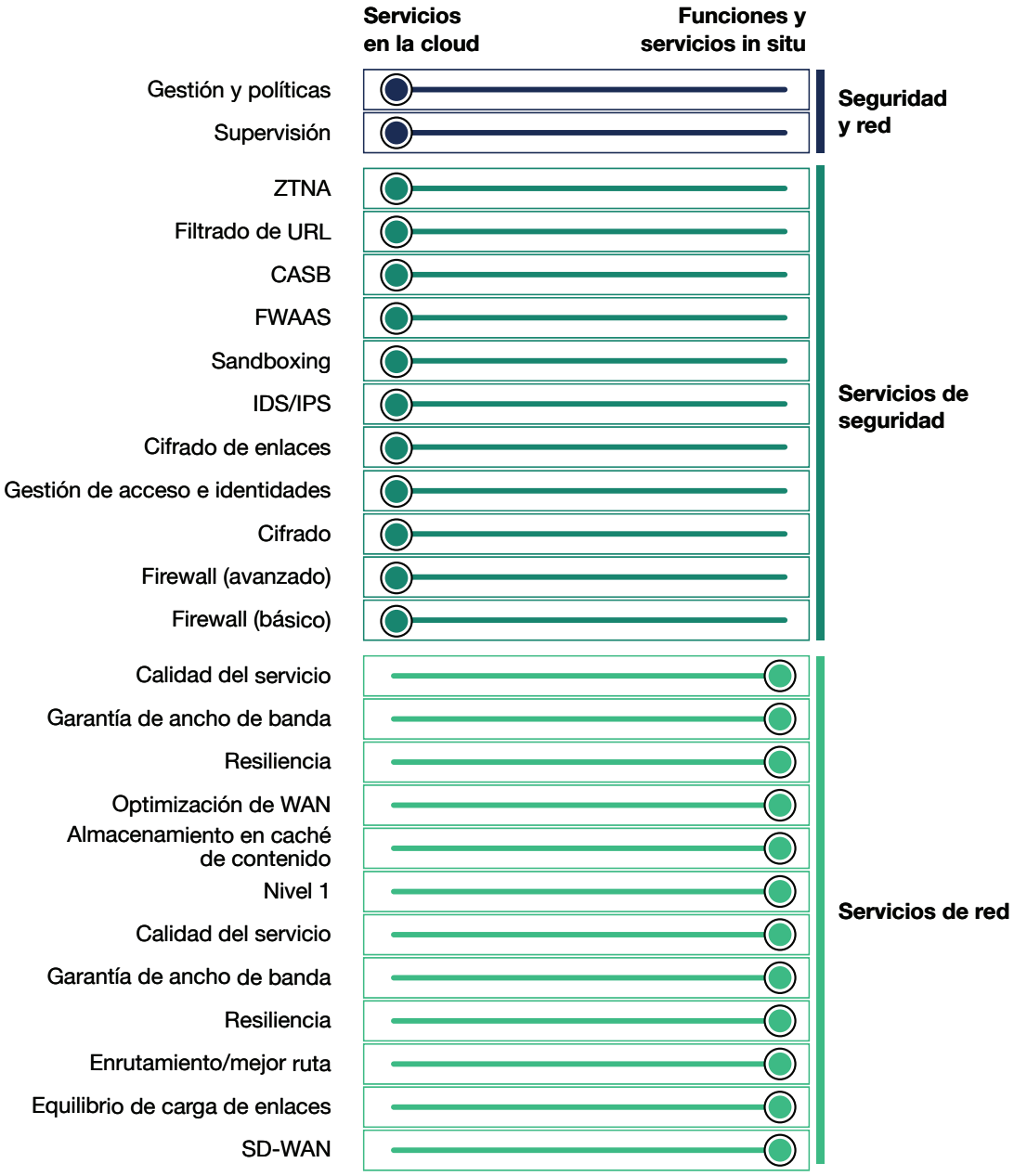
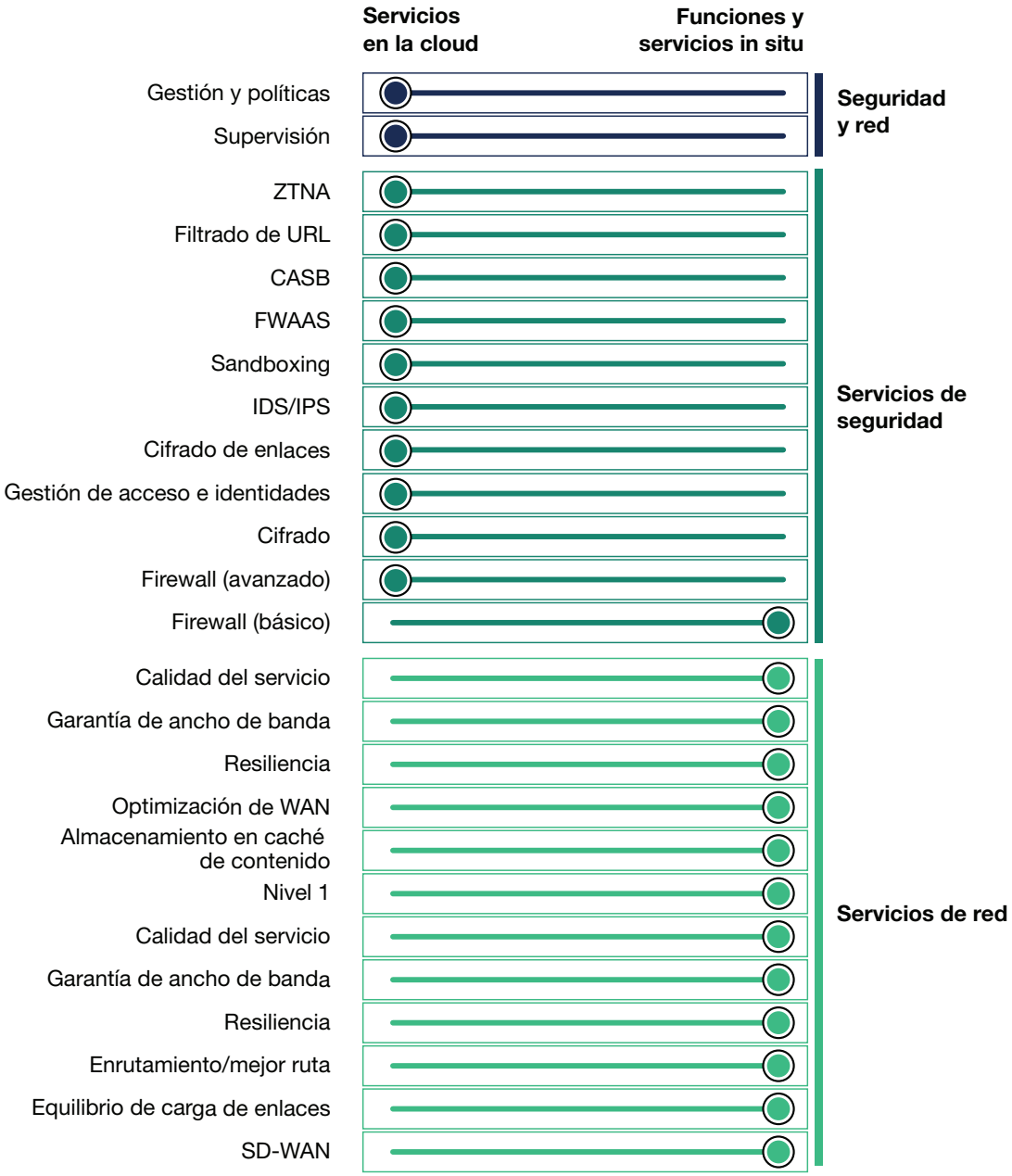


FIGURA 8 Los sitios complejos con ancho de banda de WAN limitado fuerzan algunas capacidades de seguridad localizadas



El mercado ofrece diferentes tipos de opciones de ZTE

Los profesionales de la tecnología pueden aprovechar ZTE a partir de tres métodos diferentes:

- **Un servicio ofrecido en la cloud.** Un conjunto relativamente nuevo de proveedores, servicios basados en la cloud de ZTE que provienen de un servicio gestionado por un proveedor como Cato Networks, que utiliza una red de terceros con decenas, o en algunos casos cientos, de puntos de presencia (POP) que ofrecen capacidades ZTE del perímetro de la cloud. Este enfoque ofrece todo el valor que las organizaciones pueden obtener de las soluciones de software como servicio. Sin embargo, ninguna empresa puede proporcionar todas las funciones que se encuentran en las mejores soluciones. Por supuesto, Forrester ha descubierto que las organizaciones no suelen utilizar todas las funciones de las soluciones en las instalaciones. A menudo, las soluciones de cloud se ajustarán a las necesidades de muchas organizaciones.
- **Servicios de ZTE en torno a un servicio de conexión WAN.** Otros incluirán un operador empresarial existente que conecta a sus clientes directamente a las redes de ZTE para obtener funciones de seguridad externas. Comcast Enterprise y Akamai ya llevan esto a cabo hoy en día. Muchos proveedores de hardware y software SD-WAN, como Versa Networks, se asociarán con Zscaler u otros proveedores de seguridad. Los equipos pueden elegir los mejores productos para asegurarse de que sacan el máximo partido de los servicios de redes y seguridad. Sin embargo, estos equipos no obtendrán la agilidad operativa ni la eficacia de los sistemas basados en la cloud. Un enfoque que envuelva SD-WAN y ZTE requiere pasos adicionales de los equipos tecnológicos, como la configuración de políticas para cada servicio independiente. No existe un único sistema de gestión y orquestación para una estrategia que envuelva SD-WAN y ZTE.
- **Un enfoque tipo “hágalo usted mismo” (DIY).** Una organización lo suficientemente grande y ágil podría crear su propia plataforma de ZTE mediante proveedores de servicios en la cloud como puntos de presencia y un servicio alojado en la cloud como el firewall empresarial de Barracuda como servicio de seguridad en la cloud de Azure de Microsoft. Esto garantiza que los servicios se ajusten mejor a las demandas de la empresa, pero requiere que los equipos gestionen bien los requisitos de la empresa y cuenten con las habilidades para crear la infraestructura y gestionarla. El informe “Evaluate SD-WAN Services Based On Branch Office Goals, Not Hardware Data Sheets” de Forrester muestra que a la mayoría de los equipos les falta uno de los dos aspectos.

Tanto las estructuras de varios proveedores como las de un único proveedor tienen su lugar

ZTE representa una amenaza existencial para muchas soluciones de seguridad de las instalaciones, por lo que la estrategia de ZTE ahora es fundamental para estos proveedores. Los proveedores más ambiciosos desean venderle todo el paquete completo (cuando lo tengan), y la idea de contar con un único proveedor para todas las soluciones de seguridad atendiendo únicamente a los gastos operativos será convincente para las PYMES y las empresas de mercado intermedio. Su propia elección depende del tamaño y la complejidad de su empresa, por ejemplo:

- **Las organizaciones más grandes optarán por un enfoque de varios proveedores a corto plazo.** Las empresas más grandes tienen requisitos más complicados y servicios más heterogéneos. Una carga mayor de aplicaciones heredadas hace que sea menos probable que adopten un enfoque de un único proveedor. Las personas entrevistadas para esta investigación estuvieron de acuerdo con este análisis. Para las organizaciones que ya han comenzado su

transición a Zero Trust Edge, un enfoque típico de varios proveedores puede utilizar sistemas de Silver Peak para la conexión SD-WAN a Zscaler para el filtrado de URL y ZTNA. Esto funcionará para el caso de uso inicial (protección de los teletrabajadores), pero la migración de otros elementos de la estructura de seguridad a una estructura de varios proveedores requerirá un encadenamiento importante de servicios, y las API entre los componentes deben funcionar de forma coherente y fiable.

- **Las organizaciones más pequeñas serán las pioneras en el enfoque de estructura de seguridad completa.** Forrester espera que las pequeñas empresas prueben con los proveedores de ZTE de estructura completa, como Netskope. Por lo general, tendrán un conjunto de requisitos más bajo y les será más fácil interactuar con un proveedor integral. Históricamente, la adopción de este tipo de soluciones requiere tiempo para los grupos tecnológicos empresariales más grandes. Por ejemplo, esto ha ocurrido en el mercado Wi-Fi con soluciones basadas en la cloud de Aerohive Networks, ahora parte de Extreme Networks, y Meraki, ahora parte de Cisco.

La complejidad también determina si se utiliza una superposición de agentes o una pasarela sin agentes

La conexión de todos los usuarios y aplicaciones es el objetivo de Zero Trust Edge, tanto si los sistemas se encuentran en las instalaciones, en la cloud o en una cloud privada, como funcionando de forma remota. Sin embargo, conectar una red compleja y heterogénea es claramente una tarea poco trivial. Por lo tanto, el mercado admite actualmente dos tipos de despliegues, uno para respaldar el objetivo estratégico y otro para respaldar una entrada táctica en Zero Trust Edge. Algunos proveedores, como Zscaler, pueden respaldar ambos modelos simultáneamente, y muchos otros proveedores están haciendo lo posible para hacer lo mismo.

- **Modelo uno: una pasarela es un único punto de seguridad.** Este modelo se convierte en su punto de entrada único a Internet. Piense en un controlador SD-WAN con un túnel GRE en una red perimetral alojada por un proveedor. A continuación, todo el tráfico saliente va a la red perimetral, que puede asignar inmediatamente políticas de seguridad al tráfico de ese inquilino en su red. La superficie de amenaza de la fuente original se reduce drásticamente, haciendo que los ataques como DDoS sean el problema de otro. Esta opción, aunque es más sencilla, es más probable que se adopte en el mercado de las medianas empresas; puede que no sea posible para entornos heterogéneos complicados a corto plazo.
- **Modelo dos: una superposición distribuye la seguridad, normalmente a través de agentes.** En este modelo, los puntos de conexión se conectan a la red perimetral mediante una superposición, normalmente facilitada por un agente de puntos de conexión que determina qué conexiones se redirigen a la red de ZTE. El modelo de superposición se puede implementar sin cambiar la red subyacente, pero un inconveniente importante es que la instalación de agentes puede no ser factible debido a políticas en entornos sensibles como el de la atención sanitaria, la fabricación e IT/OT. Axis Security tiene un enfoque innovador que, en última instancia, utiliza el modelo de superposición sin necesidad de agentes en dispositivos que quieren unirse a la red. Entrevistamos a un cliente importante que eligió la solución de Axis Security por exactamente este motivo.

Obstáculos en el camino hacia Zero Trust Edge

El modelo Zero Trust Edge es disruptivo, o más bien transformador, ya que revoluciona la forma en que se han utilizado tradicionalmente la seguridad y las redes. Las funciones de ciberseguridad, siempre en constante evolución, han sido más rápidas a la hora pasar a Zero Trust Edge. Las redes heredadas serán mucho más lentas. Las empresas están pasándose a Zero Trust Edge por el problema de seguridad de los teletrabajadores, pero aún quedan por delante importantes retos para hacer realidad la promesa del modelo, entre los que se incluyen:

- **Aplicaciones y servicios heredados.** Las aplicaciones web modernas comprenden la federación de identidades, lo que las hace (relativamente) fáciles de configurar en ZTE. Sin embargo, no será tan fácil con las aplicaciones basadas en protocolos no web, especialmente RDP/VDI y SIP/VoIP. Incluso estos dos tipos de aplicaciones muy comunes sufren la falta de un método estandarizado de consumo en el entorno de ZTE.
- **Dispositivos de red heredados.** Una vez que los portátiles, los servidores y las aplicaciones se unan a Zero Trust Edge, el arquitecto tendrá que tener en cuenta los miles, y en algunos casos cientos de miles, de dispositivos de OT e IoT en los que no se puede instalar ningún agente de software. Estos deben unirse en masa, utilizando protocolos de red aceptados, y es aquí donde los equipos de seguridad y redes tendrán que cooperar.
- **Capacidad y confianza.** Las organizaciones pueden utilizar ZTE para resolver tácticamente problemas como el acceso seguro para los teletrabajadores, pero aún no están preparadas para sustituir los servicios de red y seguridad de alta capacidad que tienen sus centros de datos existentes. Las organizaciones que han realizado grandes inversiones en sus propios centros de datos esperarán hasta un esfuerzo mayor, como la migración a la cloud de sus aplicaciones críticas, antes de que pasen esos servicios a la protección de Zero Trust Edge.

Lo que significa

La seguridad y las redes por fin se unen contra un enemigo común

Con la integración de la seguridad en la red para que forme parte de su ADN, Forrester observa que ocurre lo siguiente en las dos organizaciones:

1. **Organizaciones de seguridad que establecen las políticas de seguridad y las prueban.** El equipo de seguridad establecerá los tipos de tráfico y los servicios necesarios para cumplir los niveles de confianza aceptables. Con las herramientas de supervisión y análisis, los equipos se asegurarán de que se siguen las políticas, y probarán y auditarán de forma rutinaria el tráfico y las conexiones conjuntamente.
2. **Redes después de la seguridad.** Los profesionales de las redes realizarán su trabajo en función de las políticas de ZTE configuradas por el equipo de seguridad. Aunque este acuerdo avanza significativamente la ideología de Zero Trust, representa un giro de los últimos 25 años, en los que la seguridad se superponía a las redes.

3. **Por último, una vía de acceso a Internet más segura.** Cuando se les pregunta, los creadores de la red de Internet original admitirán que la seguridad nunca fue parte de su diseño. En los 30 años transcurridos desde su creación, la red de Internet mundial se ha convertido en algo muy peligroso. Zero Trust Edge por fin proporciona una ruta más segura.

Material complementario

Empresas entrevistadas para este informe

Queremos agradecer a las personas de las siguientes empresas que nos dedicaran tiempo de forma desinteresada durante los sondeos realizados para elaborar este informe.

419 Consulting
Akamai
AT&T
Axis Security
Barracuda
BlackBerry

Cato Networks
Cisco Systems
Citrix
Deutsche Telekom
Edelweiss Financial Services
Famous Supply
Fortinet
Infoblox
IronNet
Jefferies
Juniper
Lightstream
Marriott Vacations Worldwide
Menlo Security
Mentor Graphics
Netskope
Nuspire
Palo Alto Networks
Silver Peak
SKF
VMware
Windstream
Zentera Systems
Zscaler

Notas

[1] Un centro de datos privado es el núcleo de datos, aplicaciones y seguridad con ubicaciones remotas; restaurantes, centros de cuidados intensivos, centros de fabricación, por nombrar algunos, se conectan al centro de todos los recursos de la empresa.

[2] Consulte el informe de Forrester "Emerging Technology Spotlight: Businesswide Networking Fabric".

En un modelo de negocio en red, los miembros del ecosistema crean valor para el cliente de manera distribuida. Consulte el informe de Forrester "Customer-Obsessed Businesses Need Digital Ecosystems".

[3] En nuestras encuestas sobre la experiencia durante la pandemia (PandemicEX) se les preguntó lo siguiente a los entrevistados: "¿En qué medida está su empresa u organización adoptando estas medidas para gestionar el riesgo asociado al coronavirus?". Fuente: encuesta 1 de Forrester sobre PandemicEX para Estados Unidos del primer trimestre de 2020 (del 3 al 6 de marzo de 2020); encuesta 2 de Forrester sobre PandemicEX para Estados Unidos del primer trimestre de 2020 (del 17 al 19 de marzo de 2020); y encuesta 1 de Forrester sobre PandemicEX para Estados Unidos del segundo trimestre de 2020 (del 1 al 3 de abril de 2020).

Consulte el informe de Forrester "The State Of Remote Work, 2020".

[4] Los materiales de marketing de los proveedores en los primeros días de ZT solo destacaban las soluciones para el centro de datos privado. Por ejemplo, Palo Alto destacó en varios documentos técnicos cómo ZT puede proteger los activos del centro de datos. Fuente: "Best Practices - Data Center Security", Palo Alto Networks, 1 de junio de 2016 (https://www.paloaltonetworks.com/resources/whitepapers/best-practices-data-center-security).

[5] Fuente: Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jonathan Zolla, Urs Hölzle, Stephen Stuart y Amin Vahdat, "B4: Experience with a Globally-Deployed Software Defined WAN". Actas de la conferencia de la ACM SIGCOMM 2013, agosto de 2013 (https://storage.googleapis.com/pub-tools-public-publication-data/pdf/41761.pdf).

FORRESTER®

Trabajamos con los líderes empresariales y tecnológicos para desarrollar estrategias centradas en el cliente que impulsen el crecimiento.

PRODUCTOS Y SERVICIOS

- Investigación y herramientas básicas
- Datos y análisis
- Colaboración entre compañeros
- Ayuda de analistas
- Consultoría
- Eventos

Las investigaciones y los conocimientos de Forrester se adaptan a su función y a sus iniciativas empresariales esenciales.

FUNCIONES A LAS QUE PRESTAMOS SERVICIO

Profesionales de estrategia y marketing

Director de marketing
Marketing B2B
Marketing B2C
Experiencia del cliente
Conocimiento del cliente
Estrategia de canal e eBusiness

Profesionales de gestión de la tecnología

Director de informática (CIO)
Desarrollo y entrega de aplicaciones
Arquitectura empresarial
Infraestructuras y operaciones
- Seguridad y riesgos

Abastecimiento y gestión de proveedores

Profesionales del sector de la tecnología

Relaciones con analistas

ATENCIÓN AL CLIENTE

Para obtener información sobre las reimpresiones en papel o electrónicas, póngase en contacto con el servicio de atención al cliente en +1 866-367-7378, +1 617-613-5730, o a través del correo electrónico clientsupport@forrester.com. Ofrecemos descuentos por cantidad y precios especiales para instituciones académicas y sin ánimo de lucro.

161728