APRENDIZAJE SENCILLO

Edición especial de Palo Alto Networks

Acceso Zero Trust (confianza cero) a la red

para dummies®

Descubra por qué ha muerto la VPN

Haga realidad el verdadero acceso de privilegio mínimo con ZTNA 2.0

Comprenda las limitaciones del ZTNA heredado

Presentado por

paloalto® NETWORKS

Lawrence Miller

Acerca de Palo Alto Networks

Palo Alto Networks es el líder mundial en ciberseguridad. Innovamos para adelantarnos a las amenazas cibernéticas y así permitir a las organizaciones adoptar la tecnología con confianza. Proporcionamos seguridad cibernética de última generación a miles de clientes de todo el mundo, en todos los sectores. Nuestras plataformas y servicios de ciberseguridad son los mejores de su clase, cuentan con el respaldo de unos conocimientos sobre amenazas líderes en el sector y se han consolidado con una automatización de vanguardia. Tanto si utiliza nuestros productos para implementar Zero Trust en su empresa como si responde a un incidente de seguridad o se asocia a nosotros para ofrecer mejores resultados de seguridad a través de un ecosistema de socios de primera clase, nos comprometemos a hacer lo posible para que cada día sea más seguro que el anterior. Es lo que nos convierte en el socio de ciberseguridad preferido.

En Palo Alto Networks, mostramos nuestro compromiso por reunir a las mejores personas al servicio de nuestra misión, así que también nos enorgullece ser la empresa de ciberseguridad preferida, con reconocimientos como uno de los lugares favoritos para trabajar (Most Loved Workplaces) de Newsweek en 2021, una de las mejores compañías en materia de diversidad (Comparably Best Companies for Diversity) en 2021 y uno de los mejores lugares para la igualdad LGBTQ (Best Places for LGBTQ Equality) de HCR en 2022. Para obtener más información, visite www.paloalonetworks.com.

Acceso Zero Trust (confianza cero) a la red

para dummies®

Acceso Zero Trust (confianza cero) a la red

Edición especial de Palo Alto Networks

por Lawrence Miller

para dummies®

Acceso Zero Trust (confianza cero) a la red para Dummies®, edición especial de Palo Alto Networks

Una publicación de
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-18376-0 (pbk); ISBN 978-1-394-18377-7 (ebk)

Para obtener información general sobre nuestros otros productos y servicios, o sobre cómo crear un libro *para Dummies* personalizado para su empresa u organización, póngase en contacto con el Departamento de Desarrollo Empresarial en EE. UU. en el teléfono +1 (877) 409 4177 o a través de info@dummies.biz, o visite www.wiley.com/go/custompub. Para obtener información sobre licencias de la marca *para Dummies* para productos o servicios, póngase en contacto con BrandedRights&Licenses@Wiley.com.

Agradecimientos del editor

Entre algunas de las personas que han ayudado a comercializar este libro figuran las siguientes:

Editora del proyecto: Elizabeth Kuball

Editora de adquisiciones: Ashley Coffey

Director editorial: Rev Mengle

Responsable de cuentas de clientes: Cynthia Tweed

Editor de producción: Magesh Elangovan

Colaboración especial: Don Meyer, Shannon Bonfiglio

Índice

INTRODUCCIÓN 1

Acerca de este libro 2
Algunas suposiciones obvias 2
Iconos utilizados en este libro 3
Más allá del libro 3

CAPÍTULO 1: **Cuáles son las implicaciones de la nueva normalidad en materia de seguridad** 5

El cambiante panorama actual 5
Aumento continuo de la sofisticación y frecuencia de las amenazas 6
Demasiadas herramientas y demasiada complejidad 6
Escasez de talento y habilidades en ciberseguridad 7
Comprender la necesidad de cambio 8
Evolución del trabajo: del lugar al que vamos a una actividad que realizamos 8
Usuarios por todas partes, aplicaciones por todas partes y datos por todas partes 10
La conectividad directa con la aplicación aumenta exponencialmente la superficie de ataque 10
Las VPN son demasiado rudimentarias 11
¿Qué es el acceso Zero Trust (confianza cero) a la red (ZTNA)? 12
Conceptos básicos de ZTNA 12
ZTNA 1.0 13
ZTNA 1.0 tiene limitaciones importantes en el entorno actual 14
Incumple el principio de privilegio mínimo 14
Incorpora un modelo de «permitir e ignorar» 15
No ofrece inspección de la seguridad 16
No protege los datos 17
No protege todas las aplicaciones 17

CAPÍTULO 2: **Introducción del acceso Zero Trust (confianza cero) a la red 2.0** 19

Acceso de privilegio mínimo garantizado 19
Verificación continua de la confianza 21
Inspección continua de la seguridad 22
Protección de todos los datos 22
Protección de todas las aplicaciones 23

CAPÍTULO 3: **Comprender las capacidades críticas para el éxito de ZTNA 2.0** 25
Una experiencia excepcional para el usuario 25
Una solución unificada 26

CAPÍTULO 4: **Cómo empezar a trabajar con ZTNA 2.0** 29
Sustitución de las VPN 29
Acceso seguro a Internet 34
Seguridad SaaS avanzada 37

CAPÍTULO 5: **Diez preguntas (más o menos) que debe hacer a su proveedor de ZTNA 2.0** 41
¿Ofrece visibilidad total de las aplicaciones en la capa 7? 41
¿Ofrece verificación continua de la confianza? 42
¿Protege sistemáticamente todas las aplicaciones en un solo producto? 43
¿Realiza una inspección completa de la seguridad? 43
¿Protege sistemáticamente todos los datos de la empresa? 43
¿Proporciona SLA de tiempo de actividad y rendimiento para todas las aplicaciones? 44
¿Tiene un único producto unificado para proteger toda la empresa? 44

Introducción

Cómo y dónde trabajamos es algo que ha cambiado de forma radical en relativamente poco tiempo. Las iniciativas de transformación digital que ya estaban en marcha antes de la pandemia de la COVID-19 (como el trabajo remoto y la informática en la nube) se aceleraron de una manera tan repentina como necesaria para hacer frente a las nuevas realidades del mundo moderno. Ahora vivimos en un mundo donde el trabajo ya no es un lugar al que vamos, sino que se ha convertido en una actividad que podemos realizar desde cualquier lugar.

Como resultado de este nuevo modelo laboral, la superficie de ataque ha aumentado exponencialmente y hay muchas arquitecturas que admiten ahora conexiones directas a la aplicación por Internet en lugar de enviar tráfico de retorno a centros de datos a través de redes privadas. La antigua conectividad VPN de acceso remoto ya no sirve de mucho en un mundo donde los usuarios y las aplicaciones están fuera de las redes y los centros de datos de las empresas. Las antiguas VPN de acceso remoto ofrecen demasiado acceso con poca o ninguna detección de amenazas o vulnerabilidades, lo que aumenta la vulnerabilidad de recursos privilegiados en cuentas de usuario que pueden verse comprometidas. Con el drástico aumento del volumen, la escala y la sofisticación de los ataques cibernéticos, las empresas habilitadas para la nube de hoy en día se esfuerzan por cerrar sus «brechas» de seguridad y han comenzado a recurrir a soluciones de acceso Zero Trust (confianza cero) a la red (ZTNA) para reducir la superficie de ataque y proteger a las empresas del *ransomware* y otras vulnerabilidades.

Sin embargo, las soluciones ZTNA existentes (o 1.0) no pueden satisfacer las necesidades de seguridad de las empresas actuales. Ofrecen demasiado acceso con muy poca protección, brindan una seguridad irregular e incompleta a través de aplicaciones tanto basadas en la web como no, y ofrecen un bajo rendimiento y unas experiencias de usuario deficientes. Como resultado, no pueden hacer frente a la avalancha de ataques nuevos y cada vez más sofisticados sobre unas superficies de ataque cada vez mayores.

Las soluciones ZTNA 2.0 parecen ser el mejor camino a seguir y han marcado el comienzo de una nueva era de acceso seguro en un mundo donde el trabajo es una actividad y no un lugar.

Acerca de este libro

Acceso Zero Trust (confianza cero) a la red para Dummies, edición especial de Palo Alto Networks, tiene cinco capítulos en los que se analiza lo siguiente:

- El cambiante panorama de la seguridad, los aspectos básicos de ZTNA y la necesidad de avanzar para dejar atrás ZTNA 1.0 (capítulo 1)
- Cómo ZTNA 2.0 aborda las limitaciones de las actuales soluciones de ZTNA (capítulo 2)
- Los factores de éxito críticos que hay que buscar en una solución ZTNA 2.0 (capítulo 3)
- Casos de uso clave de ZTNA 2.0 e historias de éxito de clientes (capítulo 4)
- Preguntas importantes que debe hacer a su proveedor de ZTNA (capítulo 5)

Cada capítulo se ha redactado de manera independiente, por lo que si ve un tema que despierta su interés, puede pasar a ese capítulo sin ningún problema. Este libro puede leerse en el orden que más le convenga (aunque no le recomendamos que lo lea boca abajo ni del revés).

También incluye un práctico glosario en caso de que se atasque con algún término o acrónimo.

Algunas suposiciones obvias

Se ha dicho que la mayoría de las suposiciones ha superado su utilidad, pero aun así doy por supuestas algunas cosas.

Principalmente, doy por supuesto que usted se ocupa de tomar decisiones tecnológicas o que su trabajo está relacionado con ellas, y que busca una solución innovadora para proporcionar un acceso seguro a sus trabajadores híbridos. Tanto si es director de seguridad de la información como responsable informático o ingeniero de redes o seguridad, en este libro descubrirá cómo ZTNA 2.0 puede ayudarle a abordar los retos de una superficie de ataque cada vez más amplia y de un panorama de amenazas cada vez más hostil.

Iconos utilizados en este libro

En todo este libro, utilizo unos iconos especiales para llamar la atención sobre información importante. Aquí se los muestro:

RECUERDE

Este icono señala información importante que debe registrar en su memoria no volátil, su materia gris o su coco.

CUESTIONES TÉCNICAS

Este icono explica la jerga que se esconde tras la jerga, y es el material del que están hechas las leyendas... o más bien los frikis legendarios.

CONSEJO

Los consejos se agradecen, pero nunca se deben dar por sentados, por eso de verdad espero que sepa apreciar la utilidad de esta información.

ADVERTENCIA

Le avisamos de cosas de las que ya le advirtió su madre. Bueno, probablemente no, pero sí ofrecemos algunos consejos prácticos.

Más allá del libro

En este libro tan breve no puedo abarcar todo lo que desearía, así que si termina el libro pensando «¿Dónde puedo seguir aprendiendo?», visite `www.paloaltonetworks.com/sase/ztna`.

EN ESTE CAPÍTULO

- Analizamos cómo ha evolucionado el panorama de la seguridad
- Vemos cómo ha cambiado la naturaleza del trabajo
- Comprendemos los aspectos básicos de Zero Trust
- Conocemos las limitaciones de ZTNA 1.0

Capítulo 1
Cuáles son las implicaciones de la nueva normalidad en materia de seguridad

En este capítulo, hablamos de los retos de seguridad modernos, como el aumento de las amenazas, la complejidad en el ecosistema de la seguridad y la escasez de talento en ciberseguridad. También explicamos los aspectos básicos del acceso Zero Trust (confianza cero) a la red (ZTNA) y por qué las organizaciones actuales necesitan adaptar sus estrategias de acceso remoto para estar en consonancia con los nuevos modelos de trabajo y evolucionar más allá de las soluciones de control de acceso tradicionales.

El cambiante panorama actual

El actual panorama de la seguridad continúa evolucionando porque las amenazas son cada vez más sofisticadas y frecuentes. En respuesta a estas amenazas, las organizaciones han puesto en marcha una enorme y creciente variedad de soluciones y herramientas de

seguridad puntuales. Sin embargo, para gestionar y utilizar estas herramientas inconexas, se necesitan a menudo habilidades y recursos especializados que no existen en la mayoría de los equipos de seguridad de las empresas.

Aumento continuo de la sofisticación y frecuencia de las amenazas

Las filtraciones de datos y los ataques de *ransomware* (secuestro de archivos) han pasado a ser tan frecuentes hoy en día que prácticamente se merecen su propia sección de noticias, como el tiempo, los deportes y el tráfico. Pero el hecho de que estos incidentes de seguridad sean tan habituales no hace que sean menos peligrosos. Las organizaciones que pasan a ser demasiado complacientes en su estrategia de seguridad se arriesgan a sufrir grandes daños cuando se produce un ataque.

ADVERTENCIA

Según el Ponemon Institute, el coste medio resultante de una filtración de datos aumentó en un 10 % hasta llegar a los 4,24 millones de USD entre 2020 y 2021. Este ha sido el mayor aumento anual de costes durante los últimos siete años.

Por desgracia, los equipos de seguridad de las empresas están librando una ardua batalla frente a las tácticas, técnicas y procedimientos (TTP) cada vez más avanzados que usan los ciberdelincuentes.

RECUERDE

Para que una organización pueda estar al día en el actual panorama de amenazas, necesita herramientas eficaces y un equipo formado por analistas de seguridad capacitados. Lamentablemente, lograr el equilibrio perfecto entre tecnología y expertos capacitados suele ser la excepción y no la regla en la mayoría de las organizaciones.

Demasiadas herramientas y demasiada complejidad

Durante muchos años, los equipos de seguridad de las empresas han estado implementando soluciones de seguridad puntuales y aisladas para abordar problemas de seguridad concretos y casos de uso limitados. A menudo, esto se ha racionalizado erróneamente como una «defensa en profundidad». El desafortunado resultado es que el ecosistema de la seguridad está repleto de demasiadas herramientas que generan un entorno operativo complejo, caro e ineficiente. Según un estudio de IBM de 2020, la empresa media utiliza 45 herramientas de seguridad, y el 30 % de las organizaciones utiliza más de 50 herramientas. Según el informe *Panaseer 2022 Security Leaders Peer Report*, citado en la revista *InfoSecurity Magazine*, «el cambio al

trabajo remoto y en la nube ha generado en los dos últimos años un aumento del 19 % en el número de herramientas de seguridad que deben gestionar las organizaciones, de 64 a 76».

Normalmente, estas herramientas de seguridad generan miles de alertas diarias, lo que supera el volumen que los equipos de seguridad de las empresas pueden gestionar de manera eficaz. Estas alertas proceden de muchas herramientas inconexas, lo que hace que sean los analistas de seguridad los que tengan que montar el puzle (consulte la figura 1-1).

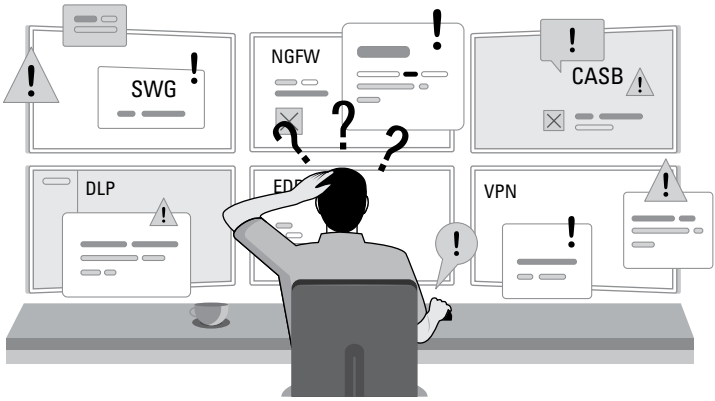

FIGURA 1-1: demasiadas herramientas de seguridad generan complejidad y fatiga ante tantas alertas.

Escasez de talento y habilidades en ciberseguridad

Más allá de la frecuencia y sofisticación crecientes de las amenazas y de la mayor complejidad y número de herramientas de seguridad en las empresas, los retos del panorama de seguridad actual se complican aún más por la escasez global de talento y habilidades en ciberseguridad. La Asociación de Auditoría y Control de Sistemas de Información (ISACA) calcula que casi dos terceras partes de los equipos de seguridad de las empresas necesitan más personal, y más de la mitad tienen puestos vacantes. El Consorcio Internacional de Certificación de Seguridad de Sistemas de Información (ISC)[2] calculó que la escasez mundial de profesionales de la ciberseguridad era de 2,72 millones en 2021.

Comprender la necesidad de cambio

Además de un panorama de seguridad y amenazas en continua evolución, los cambios en la naturaleza del trabajo y en cómo y dónde se accede a los datos y las aplicaciones están generando la necesidad de ejecutar unos cambios esenciales en la noción de confianza y en la manera de ofrecer a los usuarios y los dispositivos acceso a nuestros datos y aplicaciones.

Evolución del trabajo: del lugar al que vamos a una actividad que realizamos

La naturaleza del trabajo ha cambiado: ha pasado de ser un lugar al que íbamos a convertirse en una actividad que realizamos. Ya no «vamos al trabajo»; ahora simplemente «trabajamos». Para muchas empresas, la ubicación de sus trabajadores y el lugar donde llevan a cabo sus tareas laborales individuales han pasado a ser algo irrelevante. Ahora podemos realizar nuestras actividades en el lugar y el momento necesarios. Este cambio se ha producido por dos tendencias importantes:

- **Las aplicaciones están en todos los sitios.** La mayoría de las empresas han pasado a un modelo en el que ya no se consumen aplicaciones que se ejecutan en un centro de datos empresarial. El modelo de entrega de aplicaciones, incluido el *software* como servicio (SaaS), la web y la nube, es ahora híbrido. La mayoría de las empresas actuales utilizan alguna combinación de nube privada, nube pública, Internet y SaaS.

  
  CONSEJO

  Según el informe *2021 State of the Cloud Report* de Flexera, el 80 % de las organizaciones sigue una estrategia de nube híbrida. Según Statista, la organización media utiliza 110 aplicaciones SaaS.

- **Los usuarios están en todas partes.** Muchas organizaciones hoy en día han adoptado un modelo de trabajo híbrido, es decir, un trabajo *parcialmente remoto* (trabajo en casa dos o tres días a la semana), completamente remoto o una combinación de ambos. Esta tendencia se ha visto acelerada en gran medida por la pandemia mundial y, a medida que las empresas se han dado cuenta de las ventajas para la productividad y el estado de ánimo de los empleados, se ha convertido en la nueva normalidad laboral.

CONSEJO

» Según el informe *The State of Hybrid Workforce Security 2021* de Palo Alto Networks, el 76 % de los empleados desea un modelo híbrido, incluso después de la pandemia.

Sin embargo, este cambio tiene consecuencias importantes para la informática y la seguridad.

Anteriormente, las organizaciones conectaban a sus trabajadores remotos con los centros de datos y protegían el acceso a las aplicaciones de dicho centro de datos y a las aplicaciones web y SaaS. Para ello, se implementaban varias herramientas de seguridad puntuales en el perímetro del centro de datos, como cortafuegos, *proxies*, sistemas de prevención de intrusiones (IPS), agentes de seguridad para el acceso a la nube (CASB), protección contra el *malware* y seguridad en el sistema de nombres de dominio (DNS), entre otras.

En este modelo, las organizaciones construían sus redes de área extensa (WAN) con conmutación por etiquetas multiprotocolo (MPLS) y otros enlaces específicos que conectaban las sucursales al centro de datos. Todo el tráfico de Internet se enviaba a través del centro de datos, lo que significaba que esta enorme pila de seguridad podía centralizarse y que todo el tráfico se enviaba a través de ella (consulte la figura 1-2).

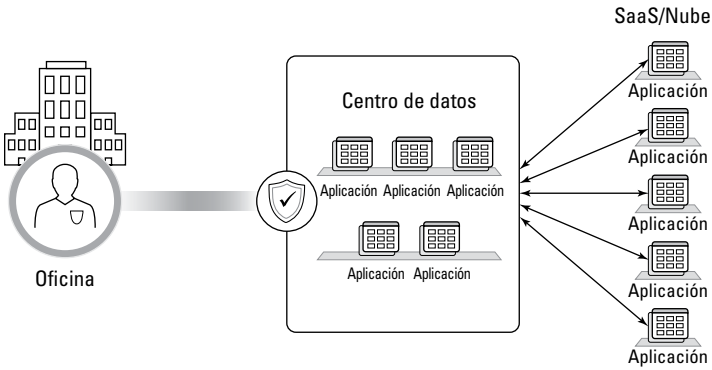

FIGURA 1-2: la seguridad era relativamente sencilla cuando el trabajo era un lugar al que se iba todos los días.

Pero lo que vemos ahora es un modelo totalmente diferente.

Usuarios por todas partes, aplicaciones por todas partes y datos por todas partes

Las organizaciones han cambiado su arquitectura WAN, que ha pasado de conectar trabajadores remotos a los centros de datos a ir directamente a Internet. Como resultado, ahora deben centrarse en ofrecer un acceso seguro y fiable a los usuarios, que trabajan desde cualquier lugar —en oficinas centrales o sucursales, desde sus casas o con dispositivos móviles—, y en proporcionar una conexión a aplicaciones y datos diseminados por todas partes (en centros de datos, nubes privadas, nubes públicas y aplicaciones SaaS).

Ahora, los usuarios se conectan directamente a todas las aplicaciones que necesitan para trabajar (consulte la figura 1-3). La ubicación de la aplicación no importa tanto; lo que importa ahora es proporcionar una experiencia uniforme, optimizada y segura para acceder a todas esas aplicaciones.

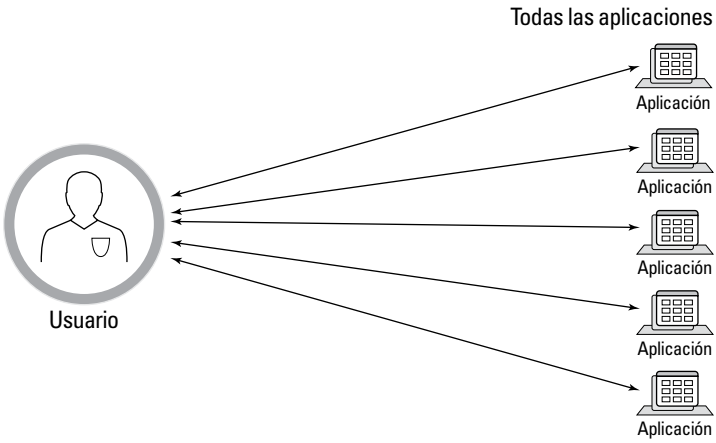

FIGURA 1-3: los usuarios se conectan ahora directamente a sus aplicaciones.

La conectividad directa con la aplicación aumenta exponencialmente la superficie de ataque

Esta conectividad directa con la aplicación es un cambio drástico con respecto al modelo tradicional, y aumenta exponencialmente la superficie de ataque de la empresa. Cuanto más se amplíe la superficie de ataque, más controles de seguridad y

acceso se necesitarán para proteger las aplicaciones y los datos de la empresa (consulte la figura 1-4).

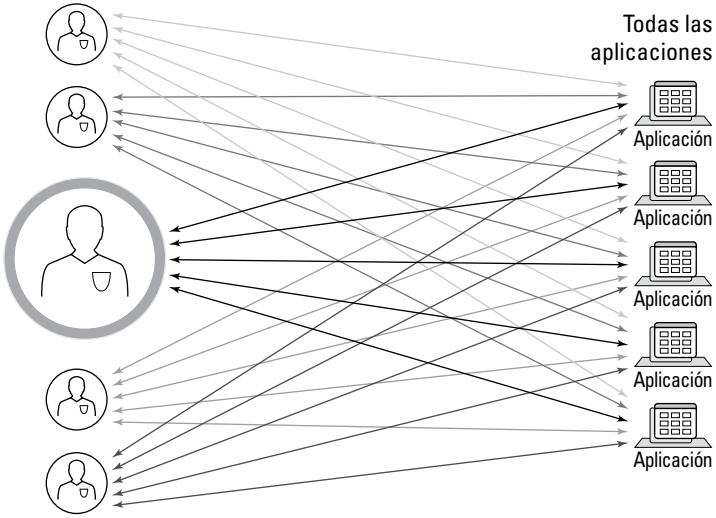

FIGURA 1-4: la superficie de ataque se ha ampliado.

Las VPN son demasiado rudimentarias

Las redes privadas virtuales (VPN) se diseñaron para poder acceder a una red de área local (LAN) o subred dentro de la LAN mediante un túnel privado y cifrado que permite a los empleados remotos conectarse a la red de la empresa. Aunque esta pueda parecer una solución práctica, por desgracia las VPN carecen de la flexibilidad y granularidad necesarias para controlar y ver exactamente lo que pueden hacer los usuarios y a qué aplicaciones tienen acceso. Después de que se conceda acceso a un usuario, este puede acceder a cualquier cosa en la red o subred, lo que ocasiona brechas de seguridad y problemas con el cumplimiento de las políticas.

En cambio, ZTNA ofrece un acceso remoto seguro a las aplicaciones basado en políticas de control de acceso granular. Solamente permite el acceso a las aplicaciones autorizadas para cada usuario en lugar de seguir el método de las VPN, que consiste en «una vez verificado, se tiene acceso a todo». Por tanto, ZTNA ofrece un enfoque de privilegio mínimo para reducir considerablemente la superficie de ataque y mejorar la estrategia de seguridad general.

¿Qué es el acceso Zero Trust (confianza cero) a la red (ZTNA)?

ZTNA es una categoría de productos que ofrece acceso remoto seguro a aplicaciones y servicios conforme a unas políticas de control de acceso definidas. Las soluciones ZTNA niegan el acceso de forma predeterminada y solo lo permiten a aquellas aplicaciones o servicios que hayan sido explícitamente autorizados para cada usuario. Es importante comprender las brechas de seguridad y los beneficios que las soluciones ZTNA pueden reportar a las organizaciones a medida que crece el número de usuarios que se unen a la red.

RECUERDE

ZTNA es una parte clave de la filosofía Zero Trust, consistente en «no confiar nunca, verificar siempre», desarrollada por Forrester para identificar la necesidad de proteger los datos. ZTNA exige a los usuarios que desean acceder a las aplicaciones una autenticación a través de un agente de puerta de enlace antes de que puedan acceder a las aplicaciones que necesitan. Este requisito ofrece la capacidad de identificar a los usuarios y crear políticas para restringir el acceso, minimizar la pérdida de datos y mitigar rápidamente cualquier problema o amenaza que pueda surgir.

Conceptos básicos de ZTNA

Con ZTNA, el acceso se establece después de que el usuario se haya autenticado a través de un agente de acceso. A continuación, el servicio ZTNA ofrece acceso a la aplicación en nombre del usuario mediante un túnel cifrado y seguro. Esto proporciona una capa de protección adicional para las aplicaciones y servicios empresariales al proteger direcciones de protocolo de Internet (IP) que serían públicamente visibles de otro modo.

Al igual que ocurre con los perímetros definidos por *software* (SDP), ZTNA hace uso del concepto de «nube oscura», que evita que los usuarios vean las aplicaciones y servicios para los que no tienen permiso de acceso. Esto protege frente al movimiento lateral, donde un *endpoint* o credenciales en peligro permitirían de otro modo la exploración o acceso a otros servicios por parte de un atacante.

ZTNA 1.0

Las primeras soluciones ZTNA, o ZTNA 1.0, llegaron en un momento en el que el panorama de las amenazas, las redes de empresa y la forma y el lugar de trabajo de las personas eran muy diferentes a como son hoy en día. Por ello, las soluciones ZTNA 1.0 ya no están a la altura del nuevo mundo laboral, y los ciberdelincuentes están encontrando nuevas maneras de vulnerar las limitaciones de estos enfoques de ZTNA 1.0.

ZTNA 1.0 se diseñó para proteger a las organizaciones limitando su exposición y reduciendo su superficie de ataque. Hace uso de un agente de acceso para facilitar la conectividad a una aplicación. Cuando un usuario solicita acceso a una aplicación, el agente de acceso determina si ese usuario debe tener permiso para acceder a ella. Una vez verificado el permiso, el agente de acceso concede el acceso y se establece la conexión (consulte la figura 1-5).

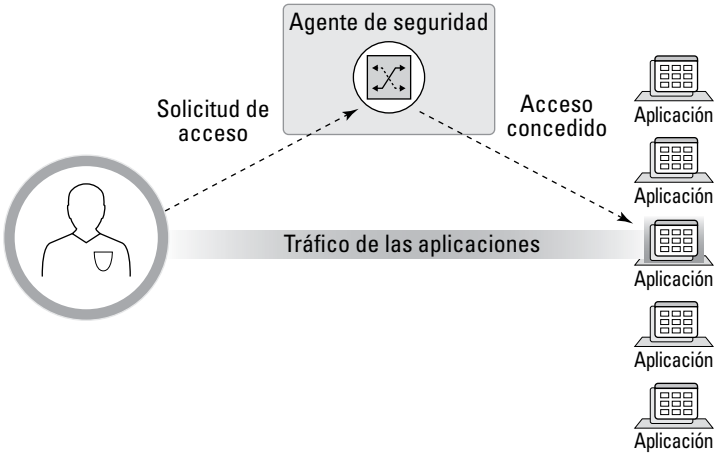

FIGURA 1-5: el sector trató de solucionar el acceso seguro con ZTNA 1.0.

Y ya está. El agente desaparece de escena, y el usuario tiene ahora acceso completo a la aplicación sin ninguna supervisión más por parte del sistema de seguridad.

Este enfoque de «permitir e ignorar» es el modelo de arquitectura de ZTNA 1.0. Pero en el contexto del panorama de amenazas actual, este modelo no solo es problemático, sino también peligroso.

ZTNA 1.0 tiene limitaciones importantes en el entorno actual

Muchas soluciones ZTNA 1.0 se basan en arquitecturas SDP, que no inspeccionan el contenido y crean por tanto una discrepancia en los tipos de protección disponibles para cada aplicación. En lo que respecta a una protección homogénea, la organización es responsable de incorporar controles adicionales, además del modelo ZTNA, e inspeccionar todo el tráfico de todas las aplicaciones. Más allá de estos retos, hay cinco problemas importantes relacionados con las soluciones ZTNA 1.0 que limitan su eficacia en el panorama de la seguridad y el entorno laboral actuales, que tan rápidamente evolucionan.

Incumple el principio de privilegio mínimo

El principio de privilegio mínimo requiere que a un usuario se le conceda solamente el mínimo nivel de acceso a una aplicación o recurso que sea necesario para llevar a cabo una tarea autorizada, y nada más. Una estrategia Zero Trust implica una desconfianza intrínseca ante cualquier intento de conectarse a una aplicación o recurso en la red, incluidos usuarios, aplicaciones y dispositivos.

Las soluciones ZTNA 1.0 existentes gestionan el acceso a las aplicaciones en las capas 3 (red) y 4 (transporte) del modelo de interconexión de sistema abierto (OSI) usando solamente los puertos de direcciones IP, el protocolo de control de transmisión (TCP) y el protocolo de datagramas de usuario (UDP).

Una red no es lo mismo que una aplicación, pero las soluciones ZTNA 1.0 dependen de los controles de acceso a nivel de red para ofrecer a los usuarios acceso a nivel de aplicaciones. Por desgracia, depender de políticas definidas en las capas 3 y 4 genera una serie de problemas. Por ejemplo, si una aplicación usa puertos o direcciones IP de tipo dinámico, es necesario conceder acceso a distintas direcciones IP y puertos, lo que deja expuesta más superficie de la necesaria. El acceso no puede restringirse a nivel de subaplicación ni a nivel de función de la aplicación; el acceso solo puede concederse a aplicaciones en su conjunto. El resultado inevitable es que los usuarios acaban con un acceso mucho mayor de lo que se desea o pretende (consulte la figura 1-6).

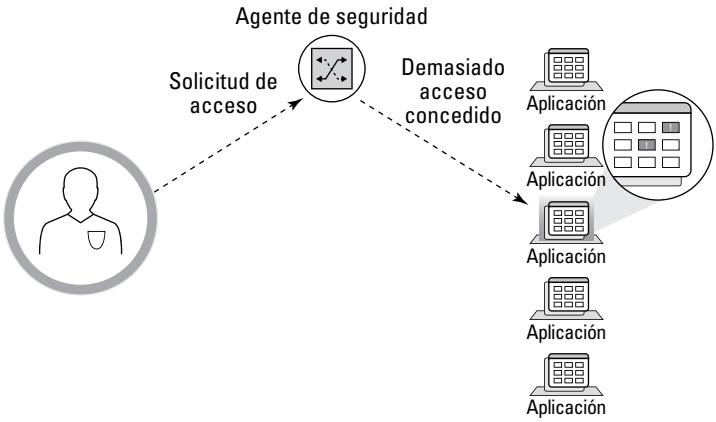

FIGURA 1-6: ZTNA 1.0 incumple el principio de privilegio mínimo.

ADVERTENCIA

Cualquier *malware* que esté a la escucha en las mismas direcciones IP y números de puerto que las aplicaciones con permisos podrá comunicarse libremente con la infraestructura de comando y control (C2) y propagarse lateralmente.

Incorpora un modelo de «permitir e ignorar»

Otra limitación de las soluciones ZTNA 1.0 es que dependen de un arriesgado modelo de «permitir e ignorar» (consulte la figura 1-7). Cuando el agente de acceso establece la conexión entre el usuario y la aplicación, se confía en ese usuario y en el tráfico del dispositivo y ya no se lleva a cabo ninguna otra verificación durante toda la sesión.

Asumir que la confianza solo debe verificarse una vez y no volver a comprobarse de nuevo es una invitación al desastre. Pueden ocurrir muchas cosas después de que se haya establecido una confianza inicial. El comportamiento del usuario y de la aplicación puede cambiar, y las aplicaciones pueden verse comprometidas.

ADVERTENCIA

Muchas amenazas modernas se aprovechan de una actividad permitida para evitar activar las alarmas.

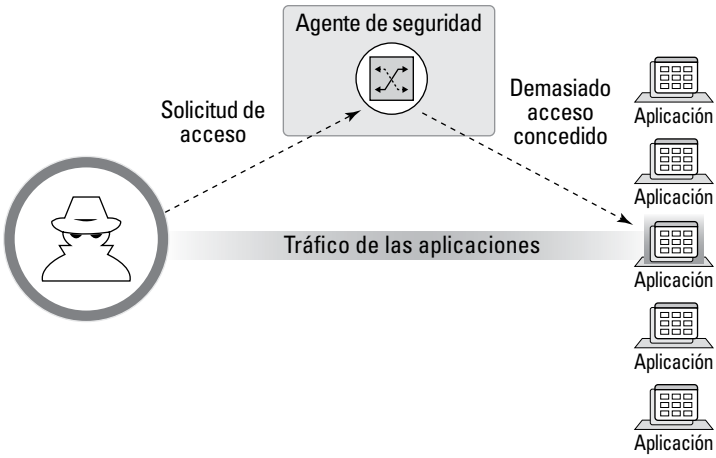

FIGURA 1-7: ZTNA 1.0 permite e ignora.

No ofrece inspección de la seguridad

Las soluciones ZTNA 1.0 tampoco inspeccionan el tráfico de la aplicación (consulte la figura 1-8). Cuando se establece una conexión, ZTNA 1.0 confía en la sesión activa implícitamente y, por tanto, no vuelve a inspeccionar el tráfico. Si el dispositivo sufre un ataque y se introduce *malware* en la sesión, no hay forma de que la solución ZTNA 1.0 detecte el tráfico malicioso ni ningún otro tipo de tráfico atacado, por lo que no responderá como corresponde.

FIGURA 1-8: ZTNA 1.0 no ofrece inspección de seguridad.

No protege los datos

Las soluciones ZTNA 1.0 no ofrecen protección de datos, sobre todo si estos se encuentran en aplicaciones privadas (consulte la figura 1-9). Esto deja una buena parte del tráfico de la organización vulnerable a la exfiltración de datos por parte de personas internas malintencionadas o atacantes externos. Además, este enfoque necesita soluciones adicionales de prevención de pérdida de datos (DLP) para proteger datos confidenciales en las aplicaciones privadas frente a las aplicaciones SaaS. ZTNA 1.0 introduce más complejidad y riesgo porque exige a las organizaciones el uso de productos en múltiples puntos para proteger los datos en cualquier lugar.

FIGURA 1-9: ZTNA 1.0 no ofrece protección de datos.

No protege todas las aplicaciones

Por último, las soluciones ZTNA 1.0 no abarcan todas las aplicaciones (consulte la figura 1-10). No funcionan con aplicaciones en la nube ni con otras aplicaciones que usan puertos dinámicos ni con aplicaciones iniciadas en el servidor, como las aplicaciones de asistencia al usuario que utilizan conexiones iniciadas en el servidor a dispositivos remotos. Las soluciones ZTNA 1.0 tampoco funcionan con las aplicaciones SaaS.

Las pilas de aplicaciones modernas nativas de la nube están formadas por numerosos contenedores y microservicios, que usan a menudo direcciones IP y números de puerto de tipo dinámico. El control de acceso de ZTNA 1.0 es completamente ineficaz en estos

entornos porque necesita que el acceso esté abierto a distintos tipos de direcciones IP y puertos, lo que anula la finalidad de Zero Trust.

FIGURA 1-10: ZTNA 1.0 no puede proteger todas las aplicaciones.

A medida que aumenta el número de organizaciones que adoptan la nube y utilizan aplicaciones nativas de la nube, ZTNA 1.0 se queda cada vez más obsoleto.

CONSEJO

ZTNA 1.0 tiene tantas limitaciones que se estará preguntando cómo es posible que se haya comercializado. Recuerde que ZTNA 1.0 se introdujo hace aproximadamente 10 años; en aquella época, el mundo era muy diferente. Antes de ZTNAs 1.0, el acceso a través de una VPN era en realidad todo lo que se necesitaba, porque todas las aplicaciones se encontraban en el centro de datos y la mayoría de los usuarios trabajaban en una oficina. ZTNA 1.0 se introdujo para solucionar algunos de los problemas relacionados con las VPN, ya que tanto los usuarios como las aplicaciones comenzaban a salir de la oficina y el centro de datos. Hoy en día, en un mundo de entornos de red híbridos y trabajadores híbridos, donde el trabajo es una actividad y no un lugar, y las aplicaciones y los usuarios están en todas partes, existe claramente la necesidad de adoptar un nuevo enfoque. En el capítulo 2 explicamos cómo ZTNA 2.0 aborda los retos de seguridad modernos y va más allá de las limitaciones de ZTNA 1.0.

EN ESTE CAPÍTULO

- Implementación del acceso de privilegio mínimo
- Verificación continua de la confianza
- Inspección continua de la seguridad
- Protección de todos los datos
- Control y protección del acceso a las aplicaciones

Capítulo 2
Introducción del acceso Zero Trust (confianza cero) a la red 2.0

Los enfoques antiguos para el acceso remoto seguro y las arquitecturas desfasadas —como las redes privadas virtuales (VPN) y la iteración inicial del acceso Zero Trust (confianza cero) a la red (ZTNA)— no pueden gestionar la avalancha de los nuevos y cada vez más sofisticados ciberataques dirigidos a superficies de ataque cada vez mayores. Está claro que se necesita un nuevo enfoque. En este capítulo, presentamos ZTNA 2.0 y explicamos cómo aborda los retos de seguridad modernos a la vez que supera las limitaciones de los enfoques anteriores para ofrecer acceso remoto seguro a los trabajadores híbridos de hoy en día.

Acceso de privilegio mínimo garantizado

ZTNA 2.0 utiliza capacidades con control de estado para identificar aplicaciones, usuarios y dispositivos con el fin de implementar un acceso de privilegio mínimo (consulte la figura 2-1).

Esto significa entender las aplicaciones desde un punto de vista fundamental en la capa 7 (aplicación) del modelo de interconexión de sistemas abiertos (OSI), más allá de las construcciones de redes de bajo nivel como la capa 3 (red [dirección IP]) y la capa 4 (transporte [puerto o protocolo]), mediante una recopilación continua de información sobre la sesión del protocolo de control de transmisión (TCP), protocolos de enlace de la aplicación, comportamiento de la aplicación y protocolos con control de estado, entre otras cosas.

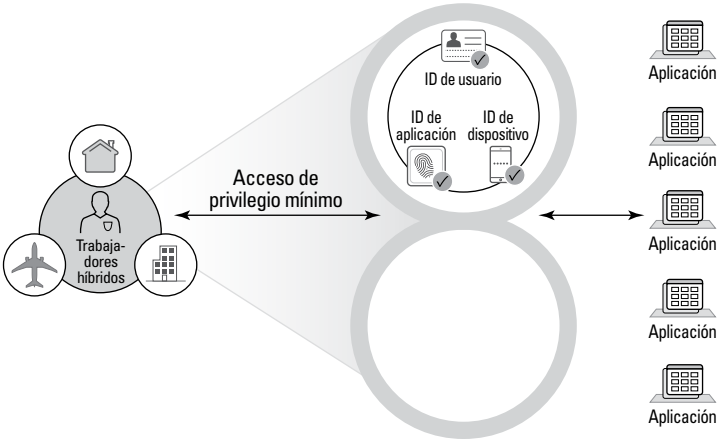

FIGURA 2-1: ZTNA 2.0 utiliza la identificación de aplicaciones, usuarios y dispositivos para garantizar un acceso de privilegio mínimo.

Al conseguir este nivel de visibilidad de las aplicaciones, sobre todo de las modernas aplicaciones de microservicios, ZTNA 2.0 puede ofrecer controles precisos para evitar exponer las funciones de las subaplicaciones u otros esquemas de comunicación a los que los usuarios no necesitan tener acceso. Al mismo tiempo, los controles de identificación de usuarios y dispositivos recopilan información continuamente sobre los usuarios y sus dispositivos. La combinación de la identificación de aplicaciones, usuarios y dispositivos llega más allá que una simple protección en un momento dado (como ocurría con ZTNA 1.0) con un entorno que ofrece información contextual enriquecida para tomar mejores decisiones sobre el control del acceso. Con ZTNA 2.0, las organizaciones pueden permitir a cualquier usuario con cualquier dispositivo el acceso a la aplicación específica que solicite y recopilar continuamente más contexto para reaccionar

ante los cambios en tiempo real, con lo que se reduce drásticamente la superficie de ataque y se garantiza, al mismo tiempo, un verdadero acceso de privilegio mínimo.

Verificación continua de la confianza

El principio fundamental de Zero Trust es eliminar la confianza implícita, es decir, se basa en «no confiar nunca, verificar siempre». Sin embargo, sin una función de verificación continua de la confianza, el sistema debe asumir que el usuario, el dispositivo y la aplicación siempre se comportan de forma fiable indefinidamente después de establecerse la conexión. Pero pueden ocurrir muchas cosas que perjudiquen a la confianza después de conceder acceso, como cambios en la conducta del usuario, dispositivo o aplicación, o que la seguridad corra algún peligro.

La verificación continua de la confianza en ZTNA 2.0 supervisa y comprueba de manera ininterrumpida la posición del dispositivo y cualquier cambio que se produzca en él, además de los comportamientos del usuario y de la aplicación, para responder en tiempo real cuando sea necesario (consulte la figura 2-2).

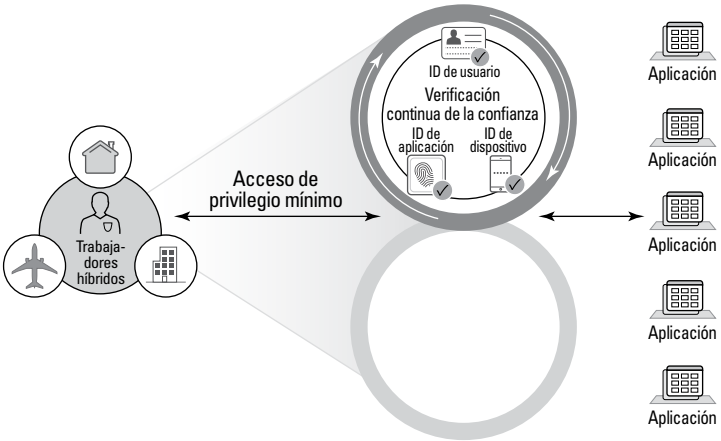

FIGURA 2-2: la verificación continua de la confianza supervisa de manera ininterrumpida la posición del dispositivo y los comportamientos tanto de la aplicación como del usuario, incluso después de que los usuarios hayan obtenido el acceso

Inspección continua de la seguridad

ZTNA 2.0 ofrece una inspección continua de la seguridad con información sobre amenazas, filtrado avanzado de localizador uniforme de recursos (URL), prevención de amenazas, seguridad de *software* como servicio (SaaS), seguridad de sistema de nombres de dominio (DNS) y mucho más. Las capacidades de inspección de paquetes en profundidad (DPI) y de inspección continua de la seguridad también hacen uso de tecnologías de prevención de amenazas mediante inteligencia artificial (IA) y aprendizaje automático (AA), para evitar amenazas de día cero en línea (consulte la figura 2-3).

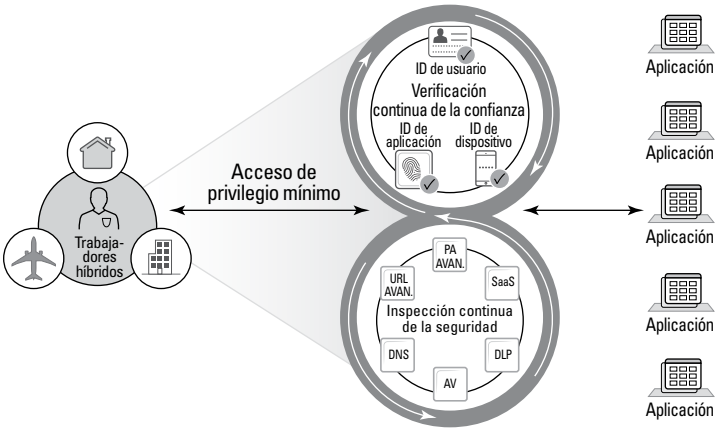

FIGURA 2-3: la inspección continua de la seguridad supervisa su entorno para protegerlo de las amenazas.

Protección de todos los datos

ZTNA 2.0 aplica funciones avanzadas de prevención de pérdida de datos (DLP) de modo uniforme a todos los datos de las aplicaciones. Estas mismas políticas DLP se aplican independientemente de si los datos residen en una aplicación personalizada, una aplicación SaaS, una aplicación web, un repositorio público o una base de datos, lo que elimina la necesidad de adivinar qué aplicaciones están protegidas y qué datos están seguros. Las organizaciones pueden obtener una sólida protección de los datos y políticas de seguridad en todas sus aplicaciones con una única solución (consulte la figura 2-4).

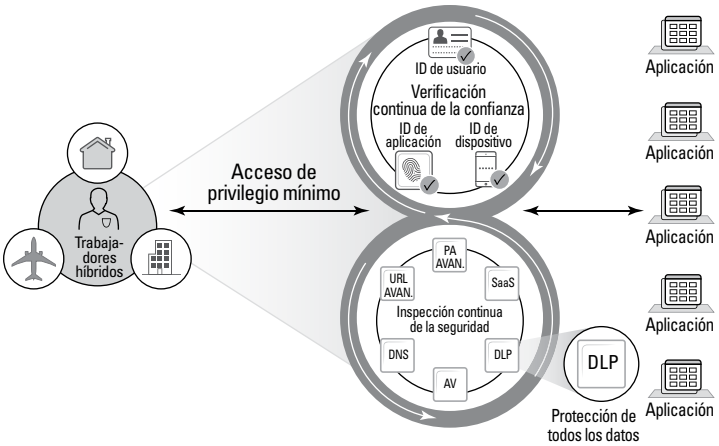

FIGURA 2-4: la protección de datos uniforme aplica una protección de datos y políticas de seguridad sólidas a todo el entorno.

Protección de todas las aplicaciones

ZTNA 2.0 ofrece una seguridad uniforme a todas las aplicaciones de la organización. Puede ser una moderna aplicación en la nube basada en microservicios que no está restringida por direcciones IP y puertos, una aplicación SaaS, una aplicación personalizada o una aplicación antigua (consulte la figura 2-5).

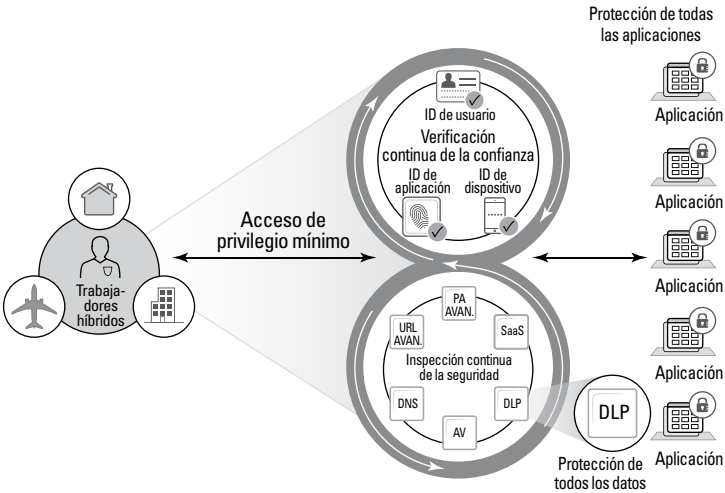

FIGURA 2-5: ZTNA 2.0 ofrece una seguridad uniforme a todas sus aplicaciones, ya sean nativas de la nube, SaaS, personalizadas o antiguas.

RECUERDE

ZTNA 2.0 supera las limitaciones de las soluciones ZTNA 1.0 a las que actualmente se enfrentan las organizaciones, además de ofrecer mejores resultados de seguridad para satisfacer las necesidades de la transformación digital y de los trabajadores híbridos. Los cinco principios clave de ZTNA son los siguientes:

- **Privilegio mínimo:** utiliza el mecanismo más riguroso para el cumplimiento del principio de privilegio mínimo, ofreciendo control de acceso desde la capa 3 (red) hasta la capa 7 (aplicación) para reducir drásticamente la superficie de ataque.
- **Verificación continua de la confianza:** cuando cambia el comportamiento de un usuario, el comportamiento de una aplicación o la posición de un dispositivo, debe existir una evaluación continua del nivel de confianza otorgado y la capacidad de responder de forma adecuada, en tiempo real, a cualquier cambio que se presente.
- **Inspección continua de la seguridad:** todo el tráfico se supervisa constantemente para protegerlo de todas las amenazas, incluidas las amenazas persistentes avanzadas (APT) y las amenazas de día cero, así como de todos los vectores de amenazas.
- **Protección de datos:** todos los datos están protegidos con políticas aplicadas de modo uniforme a todos los datos de las aplicaciones, desde los datos que residen en aplicaciones que se ejecutan en procesadores centrales antiguos hasta datos almacenados en modernas aplicaciones de colaboración nativas de la nube.
- **Seguridad uniforme para todas las aplicaciones:** todas las aplicaciones a lo largo y ancho de la organización, incluidas las aplicaciones personalizadas, las nativas de la nube y las aplicaciones SaaS, están protegidas y seguras.

EN ESTE CAPÍTULO

- La importancia de una experiencia de usuario excepcional
- Una solución simple y unificada

Capítulo 3
Comprender las capacidades críticas para el éxito de ZTNA 2.0

En este capítulo hablamos de por qué ofrecer una experiencia de usuario excepcional y una solución unificada es fundamental para adoptar con éxito una solución ZTNA 2.0.

Una experiencia excepcional para el usuario

Si pregunta a los usuarios qué piensan de las herramientas de seguridad de su organización, es probable que ninguna de las respuestas sea «¡Me encanta la experiencia de usuario!». En realidad, a los usuarios siempre les ha resultado difícil comprender y utilizar las herramientas de seguridad, que normalmente ralentizan su trabajo. Los análisis para detectar *malware* roban a los usuarios una gran cantidad de valiosa memoria y hacen que sus ordenadores vayan más lentos. La conexión a la red privada virtual (VPN) ralentiza el acceso a Internet y aumenta la latencia en sus aplicaciones. Como resultado, muchos usuarios buscan formas creativas de saltarse los controles de seguridad creados para protegerlos de ellos mismos.

Con las soluciones ZTNA 1.0 actuales pasa lo mismo. Dependen de equipos físicos instalados en distintos centros que funcionan de forma conjunta, pero dispersa, aprovechando la Internet pública como eje principal. Este método limita enormemente el alcance, la escala y el rendimiento de la solución, a la vez que supone una dependencia no deseada de centros de datos de terceros y conexiones deficientes. Estas soluciones también carecen de una verdadera capacidad para el uso de inquilinos múltiples a fin de mitigar los problemas que suponen los «vecinos ruidosos» y el «destino compartido», por lo que los clientes deben sacrificar la seguridad en aras de la experiencia.

Para garantizar un alto rendimiento constante, las soluciones ZTNA 2.0 deben proporcionar un plano de datos específico para cada cliente, evitando así el problema del «vecino ruidoso» de los enfoques de ZTNA 1.0.

Las soluciones ZTNA 2.0 también deben diseñarse con capacidades de supervisión de la experiencia digital (DEM) nativas, que ofrezcan una identificación proactiva de los problemas y ayuden a resolverlos automáticamente con el fin de reducir la cantidad de formularios de incidencias que gestionan los administradores de TI, ofreciendo así mayor información y visibilidad para conseguir la mejor experiencia posible.

CUESTIONES TÉCNICAS

Según Gartner, «la supervisión de la experiencia digital (DEM) es una disciplina de análisis del rendimiento que respalda la optimización de la experiencia operativa y el comportamiento de un agente digital, humano o máquina, con la cartera de aplicaciones y servicios de las empresas. Estos usuarios, humanos o digitales, pueden ser una combinación de usuarios externos fuera y dentro del cortafuegos. Esta disciplina también busca observar y modelar el comportamiento de los usuarios como un flujo de interacciones en forma de recorrido de cliente».

Una solución unificada

Las soluciones ZTNA 1.0 le exigen gestionar políticas independientes en diferentes consolas de administración para proteger completamente a todos los usuarios y aplicaciones. Con ZTNA 1.0, es imposible evitar incidentes de manera eficaz o detectar incidentes y responder a ellos cuando la gestión, las políticas y los datos están dispersos en la infraestructura.

Las soluciones ZTNA 2.0 brindan una seguridad superior al tiempo que ofrecen un rendimiento sin concesiones y experiencias de usuario excepcionales, todo con un solo enfoque unificado. ZTNA 2.0 proporciona una arquitectura verdaderamente nativa de la nube creada para proteger a las empresas digitales de hoy en día a escala de la nube, con un rendimiento sin concesiones respaldado por acuerdos de nivel de servicio (SLA) de rendimiento y tiempo de actividad que garantizan experiencias de usuario excepcionales.

Al estar completamente basado en *software* y ser independiente del *hardware*, ZTNA 2.0 garantiza un escalado automático para mantenerse al día con los cambios del personal híbrido y la evolución de las exigencias comerciales, sin necesidad de interacciones ni procesos manuales.

RECUERDE

Las soluciones ZTNA 2.0 ofrecen un producto unificado en todas las capacidades, incluidas ZTNA, SWG, CASB de próxima generación, FWaaS, DLP y más.

ZTNA Y SASE

El servidor perimetral de acceso seguro (SASE) es la convergencia de redes de área extensa (WAN) y servicios de seguridad en un «perímetro» de servicios entregados en la nube, diseñado para ayudar a las organizaciones a modernizar sus infraestructuras de redes y seguridad y adaptarse así a las necesidades de los entornos y trabajadores híbridos.

Las soluciones SASE consolidan múltiples productos puntuales, incluidos ZTNA, SWG en la nube, CASB, FWaaS y redes de área extensa definidas por *software* (SD-WAN), en un único servicio integrado, lo que reduce la complejidad de la seguridad y la red al tiempo que aumenta la agilidad de la organización.

EN ESTE CAPÍTULO

- Cómo librarse de las redes privadas virtuales antiguas
- Cómo proteger las aplicaciones web y el tráfico de Internet
- Cómo habilitar la protección avanzada de aplicaciones SaaS y prevenir la pérdida de datos

Capítulo 4
Cómo empezar a trabajar con ZTNA 2.0

Empezar a utilizar el acceso Zero Trust (confianza cero) a la red (ZTNA) 2.0 no debería ser una tarea difícil ni abrumadora, ni debería exigir hacer ningún tipo de concesiones. Todo se reduce a la alineación: relacionar las necesidades de su organización con las preocupaciones o desafíos clave a los que se enfrenta y resolver estos desafíos sin necesidad de un cambio o trastorno masivo. Este capítulo analiza tres casos de uso habituales que representan algunos de los mayores desafíos a los que se enfrentan las organizaciones en la actualidad.

Sustitución de las VPN

Durante años, la herramienta estándar para conectar a los usuarios remotos con una red corporativa fue la red privada virtual (VPN). Las VPN se crearon con un objetivo principal: permitir a los usuarios remotos acceder de forma segura a los recursos que estaban dentro de la red empresarial. Sin embargo, a medida que las aplicaciones y las cargas de trabajo migran cada vez más hacia la nube, las organizaciones necesitan algo más que simple acceso remoto: también necesitan un acceso seguro a las aplicaciones en la nube y a Internet.

Las VPN antiguas usan una arquitectura radial (consulte la figura 4-1) para conectar ubicaciones remotas (los radios) con una oficina o centro de datos central (el concentrador). Esta conectividad de ubicación a ubicación es la mejor arquitectura para las aplicaciones de centro de datos porque el objetivo es llegar al «concentrador» donde están alojadas las aplicaciones y los datos internos.

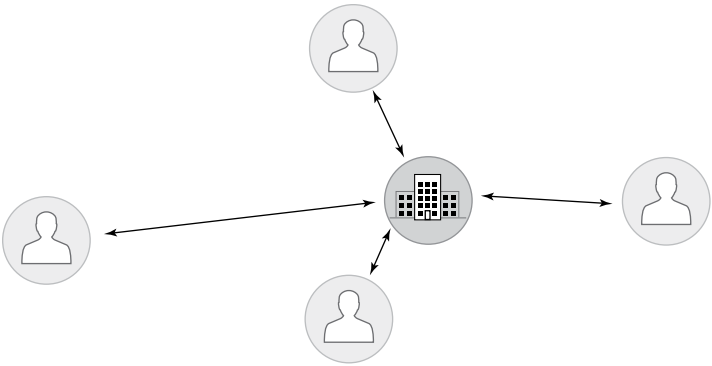

FIGURA 4-1: arquitectura de VPN radial tradicional.

El modelo deja de funcionar cuando entra en juego una combinación de aplicaciones en la nube y en Internet. Con las VPN tradicionales, el tráfico siempre va primero al concentrador o puerta de enlace de la VPN, aunque la aplicación esté alojada en la nube (consulte la figura 4-2). Como resultado, el tráfico se dirige a la puerta de enlace de la VPN ubicada en la oficina central o el centro de datos y, a continuación, sale del cortafuegos perimetral a Internet, mientras que la respuesta de la aplicación tiene que pasar por la oficina central o el centro de datos antes de llegar al usuario. Con las aplicaciones en la nube, este tráfico básicamente hace un rodeo, es decir, sigue una ruta larga y lenta hasta llegar a una ubicación con acceso a Internet. Aunque esto tenga sentido desde el punto de vista de la seguridad, no es lo más lógico si se desea optimizar la red.

CUESTIONES TÉCNICAS

El término *tromboning* hace referencia a la práctica de enrutar el tráfico de la red a través de un punto de control (como un cortafuegos). Esto a menudo supone un tráfico de retorno, por ejemplo, destinado a Internet, a través de una red de conmutación por etiquetas multiprotocolo (MPLS) y a través de un cortafuegos central en lugar de seguir una ruta más directa. El tromboning aumenta la latencia y complejidad de la red, entre otros efectos negativos.

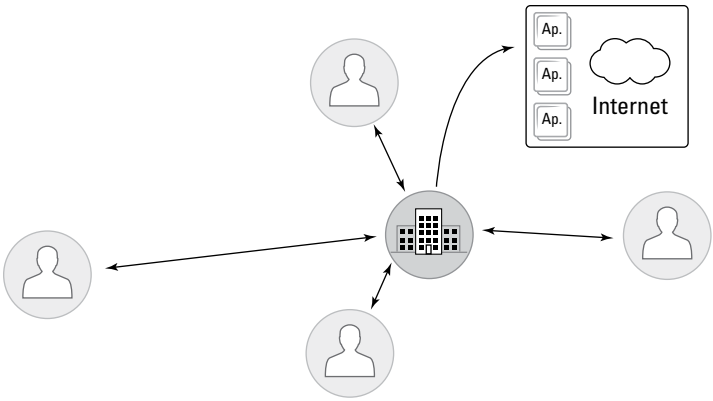

FIGURA 4-2: tráfico de retorno de una VPN tradicional para llegar a la nube.

El uso de aplicaciones en la nube a través de VPN antiguas empeora la experiencia del usuario y, como resultado, los usuarios finales optarán por evitar utilizar las VPN siempre que puedan. En su lugar, optarán por conectarse cuando necesiten acceso al centro de datos interno y desconectarse cuando ya no lo necesiten, lo que da lugar a muchos problemas. Cuando los usuarios se desconectan, las organizaciones pierden la visibilidad del uso de las aplicaciones, el control del acceso a aplicaciones no autorizadas y la capacidad de hacer cumplir sus políticas de seguridad.

En la actualidad, un área clave de trabajo para muchas organizaciones es reemplazar las tecnologías VPN obsoletas que ofrecen una granularidad insuficiente en los controles, un rendimiento deficiente y una experiencia de usuario insatisfactoria. Las iniciativas de reemplazo de VPN suelen estar impulsadas por varios factores, entre los que figuran los siguientes:

- **Aplicaciones que pasan a un verdadero modelo híbrido, aprovechando los entornos locales, en la nube y de múltiples nubes:** la tecnología VPN antigua que retorna o devuelve el tráfico a un «concentrador» local no puede ampliarse ni ofrece la mejor experiencia de usuario posible.
- **Cambios en los requisitos de acceso a las aplicaciones empresariales:** tradicionalmente, los empleados usaban dispositivos gestionados para llevar a cabo tareas relacionadas con el trabajo. Sin embargo, cada vez más dispositivos no gestionados, como teléfonos y tabletas personales, se han abierto camino en las redes corporativas y pueden acceder a las aplicaciones de la empresa.

- **Organizaciones que buscan un modelo unificado de protección y seguridad para todas las aplicaciones en general, no solo para las aplicaciones web o antiguas.**

Las tecnologías VPN no se diseñaron para la entrega constante, de alto rendimiento y a rápida escala de los servicios de seguridad avanzados necesarios para conectar a los trabajadores híbridos de manera segura con la variedad de aplicaciones que necesitan para realizar su trabajo. Así, las organizaciones han comenzado a sustituir las implementaciones de VPN obsoletas por soluciones ZTNA.

Son varias las soluciones que pueden satisfacer algunas de estas necesidades, pero solo ZTNA 2.0 transforma las redes y la seguridad para trabajar con dispositivos gestionados y no gestionados, a la vez que ofrece una protección de seguridad uniforme a todas las aplicaciones de toda la organización.

Reemplazar su VPN con una solución ZTNA 2.0 facilita al personal que trabaja en sucursales, en casa y con dispositivos móviles un acceso remoto seguro a las aplicaciones en la nube pública, la nube privada y el centro de datos (consulte la figura 4-3). Entre las capacidades clave se encuentran la verificación continua de la confianza y la inspección continua de la seguridad, lo que permite lo siguiente:

- Un modelo Zero Trust para acceder a las aplicaciones privadas
- Compatibilidad con el acceso de clientes gestionados y no gestionados
- Protección unificada en toda la empresa

FIGURA 4-3: sustitución de una VPN por ZTNA 2.0

Algunos de los beneficios clave de la sustitución de las VPN por ZTNA 2.0 son los siguientes:

- Experiencia óptima para el usuario
- Producto unificado
- Red de área extensa definida por *software* (SD-WAN) integrada

CONSEJO

Reemplace las tecnologías VPN antiguas con una solución moderna ZTNA 2.0 que permita a los trabajadores remotos e híbridos un acceso seguro a la red, que supere los cuellos de botella del rendimiento y que simplifique la gestión.

PROTECCIÓN DEL ACCESO PRIVADO PARA UNA EMPRESA DE CONSULTORÍA DE LA LISTA FORTUNE 100

Una empresa de servicios de consultoría de la lista Fortune 100 estaba buscando una solución moderna de acceso remoto para poder eliminar su implementación de VPN obsoleta y no ampliable de distintos proveedores.

Debido a la mezcolanza por la que se caracterizaba la solución VPN, a la empresa le resultaba difícil conseguir visibilidad y seguridad uniformes para su gran número de empleados y ubicaciones en todo el mundo.

Además, el nivel de satisfacción de los empleados con la combinación de soluciones existente era muy bajo, pues sufrían a menudo conexiones lentas, un rendimiento irregular y experiencias de usuario deficientes en los distintos sitios y ubicaciones.

Impulsores del proyecto

- Retirar la solución VPN de acceso remoto no ampliable.
- Conseguir uniformidad en la visibilidad y seguridad de los empleados, independientemente de su ubicación.
- Mejorar la experiencia de los usuarios.

Este cliente necesitaba una sustitución moderna de su VPN y eligió la solución ZTNA 2.0 de Palo Alto Networks. Con ZTNA 2.0, ahora puede conectar a sus 350 000 usuarios repartidos por 158 países sin interrupciones, además de ofrecer una conectividad segura directa a Internet a sus cientos de sucursales de todo el mundo. Es más, ZTNA 2.0 garantiza un acceso uniforme y seguro a todas las aplicaciones, incluidas las ya

(continuación)

(continuación)

existentes, a través de más de 30 centros de datos y ubicaciones en la nube.

Resultados

- Seguridad para 350 000 usuarios en 158 países
- Internet local con seguridad en la nube para proteger cientos de oficinas en todo el mundo
- ZTNA para miles de aplicaciones en más de 30 centros de datos y ubicaciones en la nube

Acceso seguro a Internet

Las organizaciones usan muchas aplicaciones, algunas a nivel local y otras en la nube. A medida que las empresas crecen y aumenta el número de sus trabajadores móviles e híbridos, cada vez resulta más difícil proteger a los usuarios remotos de las amenazas que surgen con el acceso a todas estas aplicaciones distintas.

A las aplicaciones locales se accede normalmente a través de una VPN de acceso remoto. Sin embargo, cuando los usuarios acceden a aplicaciones y servicios de Internet, se desconectan de la VPN y quedan expuestos al riesgo. Las organizaciones usan puertas de enlace seguras (SWG) para ofrecer un acceso a Internet seguro cuando los usuarios remotos se desconectan de la VPN.

Las SWG actúan normalmente como un *proxy* (intermediario) entre los usuarios y los recursos de Internet para proteger a los usuarios de las amenazas en la web, además de para aplicar y hacer cumplir las políticas de uso aceptable de la empresa. En lugar de conectar al usuario a un sitio web directamente, se le dirige a la SWG, que se encarga de conectar al usuario al sitio web deseado y de llevar a cabo otras funciones, como el filtrado del localizador uniforme de recursos (URL), la visibilidad de la web, la inspección de contenidos maliciosos, los controles de acceso a la web y otras medidas de seguridad.

RECUERDE

Las SWG permiten a las empresas:

- Bloquear el acceso a sitios web o contenidos no adecuados según unas políticas de uso aceptable

- Hacer cumplir las políticas de seguridad para que el acceso a Internet sea más seguro
- Proteger los datos de transferencias no autorizadas

Sin embargo, las SWG antiguas se implementan normalmente como dispositivos en las redes empresariales, lo que hace necesario que el tráfico de usuario retorne a la SWG, que suele estar situada en un centro de datos corporativo. Este enrutamiento ineficaz del tráfico aumenta la latencia y afecta de forma negativa a la experiencia del usuario.

Otro problema de las SWG antiguas es que son normalmente soluciones independientes que no tienen capacidad para coordinar flujos de trabajo, generar informes ni crear registros con otra infraestructura de seguridad en la organización. Esto puede aumentar la complejidad con el paso del tiempo, porque las organizaciones a menudo tienen varios productos de seguridad puntuales, lo que disminuye la eficiencia y eficacia de sus operaciones de seguridad.

Las organizaciones buscan formas de mejorar la experiencia de sus empleados cuando acceden a Internet y a las aplicaciones web, y las funciones de SWG en la nube de ZTNA 2.0 ofrecen una solución eficaz que elimina la latencia y mejora la estrategia de seguridad general (consulte la figura 4-4).

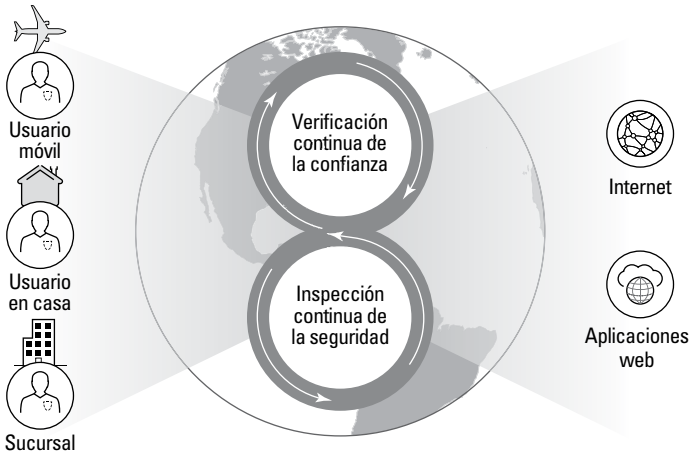

FIGURA 4-4: ZTNA 2.0 para sustitución de SWG/SWG en la nube.

(continuación)

CONSEJO

Estos son algunos de los requisitos clave que deben tenerse en cuenta a la hora de evaluar ZTNA 2.0 como sustituto de los productos de SWG antiguos:

- **No debe exigir cambios importantes en la red:** las organizaciones desean poder mantener simplemente los métodos basados en *proxy* para minimizar las interrupciones y grandes reformas de la red.
- **Debe ofrecer un enfoque opcional basado en agentes:** tener la opción de instalar un agente en el *endpoint* del usuario es deseable, pero no debe ser el único modelo de implementación disponible.
- **Debe permitir el cumplimiento constante de las políticas:** la solución debe permitir que todos los trabajadores híbridos, tanto desde sus casas como desde las sucursales o a través de dispositivos móviles, puedan cumplir constantemente todas las políticas.

PROTECCIÓN DEL ACCESO A INTERNET DE UN LABORATORIO FARMACÉUTICO DE LA LISTA FORTUNE 100

Un laboratorio farmacéutico de la lista Fortune 100 quería reducir sus instalaciones de *hardware* locales de varios proveedores y modernizar su infraestructura con una solución de seguridad en la nube.

Puesto que un número cada vez mayor de las herramientas y aplicaciones que los empleados necesitaban para hacer su trabajo estaban migrando a la nube, las soluciones existentes no podían ofrecer una experiencia ininterrumpida ni cumplir con las expectativas, lo que provocó un bajo nivel general de satisfacción de los usuarios con las soluciones existentes.

Este cliente necesitaba un enfoque de seguridad moderna en la nube y eligió la solución ZTNA 2.0 de Palo Alto Networks. Con ella, pudo migrar fácilmente a sus 100 000 usuarios en menos de tres meses sin tener que modificar su arquitectura de red, aprovechando las capacidades *proxy* explícitas de ZTNA 2.0.

Su nueva solución nativa en la nube consolidó y eliminó el *hardware* de *proxy* local y le permitió lograr una mejor estrategia de seguridad para todos sus usuarios y ubicaciones. También implementó las funciones

nativas de gestión autónoma de la experiencia digital (ADEM) de Prisma Access para facilitar una experiencia de usuario excepcional a todos los trabajadores híbridos.

Impulsores del proyecto

- Migrar a la nube
- Reducir el hardware local
- Mejorar la experiencia de usuario

Resultados

- Migración de 100 000 usuarios en menos de tres meses
- Eliminación del hardware SWG local con una solución nativa en la nube
- Mejora drástica de la estrategia de seguridad
- Experiencia de usuario excepcional con ADEM

Seguridad SaaS avanzada

Hace años, las empresas almacenaban todas sus aplicaciones y datos en un centro de datos local. En este entorno, tenían una visibilidad completa y un control granular sobre quién accedía a sus aplicaciones y datos, y cuándo lo hacía, así como qué dispositivos (generalmente ordenadores de sobremesa o portátiles) se usaban para acceder a ellos.

Con el tiempo, a medida que las empresas trasladaron sus datos a la nube y comenzaron a usar servicios en la nube como las aplicaciones SaaS, descubrieron que ya no tenían información sobre quiénes accedían y usaban sus aplicaciones y datos en la nube ni qué dispositivos se utilizaban para acceder a estos servicios en la nube, debido a la llegada de tecnologías móviles como los ordenadores portátiles y los teléfonos inteligentes. Además, la ubicuidad y la facilidad de adopción de las aplicaciones SaaS a menudo generan una «TI en la sombra», en la que los usuarios aprovechan las aplicaciones no autorizadas o no aprobadas con fines comerciales sin darse cuenta de que exponen los datos confidenciales a un mayor riesgo.

Esta falta de visibilidad hace que a las empresas les resulte difícil proteger sus datos y las expone a una gran cantidad de riesgos de seguridad empresarial, como brechas de datos, incumplimiento normativo, *malware* y *ransomware*, entre otros.

Para hacer frente a estos desafíos, los proveedores de seguridad desarrollaron las soluciones de agente de seguridad para el acceso a la nube (CASB). Las soluciones CASB ayudan a las organizaciones a descubrir dónde se encuentran sus datos en las aplicaciones SaaS y cuándo están en movimiento en entornos de servicios en la nube, centros de datos locales y trabajadores móviles. Una solución CASB también hace cumplir las políticas de seguridad, gobernanza y cumplimiento normativo de una organización, lo que permite que los usuarios autorizados accedan a aplicaciones en la nube y las utilicen, al tiempo que las organizaciones protegen sus datos confidenciales de manera eficaz y uniforme en múltiples ubicaciones.

Sin embargo, las soluciones CASB convencionales no pueden incorporar rápidamente nuevas aplicaciones en la nube porque dependen de bibliotecas de aplicaciones estáticas que se van completando manualmente. Las aplicaciones de colaboración modernas, como Slack, Zoom, Confluence, Jira y otras, donde los usuarios pasan la mayor parte del tiempo en la actualidad, generalmente no están protegidas por la interfaz de programación de aplicaciones (API) que ofrecen estas soluciones CASB.

Una solución CASB convencional ofrece unas funciones básicas de seguridad en la nube con un alcance y profundidad limitados, por lo que solo proporciona una seguridad fragmentada. Por ejemplo, sus funciones de prevención de pérdida de datos (DLP) son bastante básicas e imprecisas, ya que solo cubren los datos de ciertas aplicaciones SaaS y son completamente independientes de cualquier DLP que proteja al resto de la empresa. También carecen de los mecanismos esenciales de protección contra amenazas que detectan las infinitas variaciones de amenazas que los ciberdelincuentes utilizan constantemente para atacar las aplicaciones SaaS.

CUESTIONES TÉCNICAS

Cuando las soluciones CASB se desarrollaron por primera vez, se diseñaron como una solución puntual basada en un *proxy* independiente. El problema de las soluciones CASB basadas en *proxy* es que requieren un redireccionamiento del tráfico complejo desde el cortafuegos de la red con agentes de configuración automática de *proxy* (PAC) y recopiladores de registros; esto provoca una complejidad arquitectónica y operativa significativa, además de un alto coste de propiedad.

Las empresas que utilizan soluciones CASB antiguas en la actualidad no pueden seguir el ritmo del rápido crecimiento de las aplicaciones SaaS y la TI en la sombra, el crecimiento generalizado de los datos y el número cada vez mayor de trabajadores híbridos y remotos. Reemplazar una solución CASB antigua con funciones CASB de próxima

generación entregadas en una arquitectura de servidor perimetral de acceso seguro (SASE) que incluya ZTNA 2.0 permite a las empresas adoptar servicios en la nube de manera segura con una verificación de la confianza e inspección de la seguridad continuas, además de funciones que incluyen lo siguiente (consulte la figura 4-5):

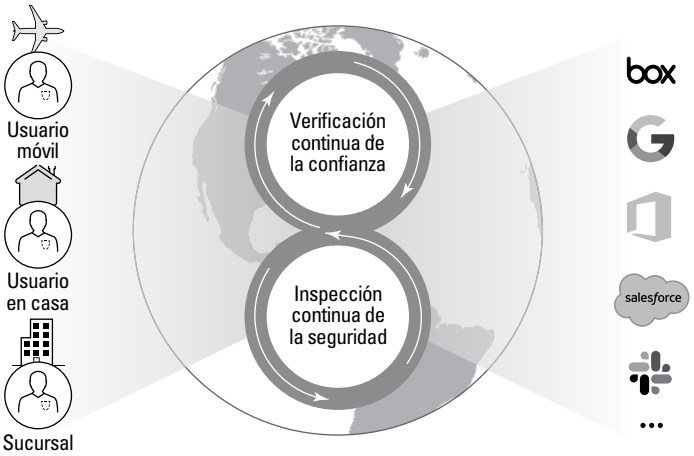

FIGURA 4-5: ZTNA 2.0 para una seguridad avanzada de las aplicaciones SaaS/CASB de próxima generación

- Visibilidad y control de las aplicaciones SaaS
- Protección de las aplicaciones SaaS autorizadas
- DLP avanzado

SEGURIDAD AVANZADA EN APLICACIONES SAAS PARA UN IMPORTANTE PROVEEDOR DE AUTOMOCIÓN

Un líder mundial en tecnología de automoción, con más de 190 000 empleados en cientos de plantas de fabricación, docenas de importantes centros técnicos en todo el mundo y presencia en más de 40 países,

(continuación)

(continuación)

dependía de varias aplicaciones en la nube. Necesitaba una mejor visibilidad y un control granular de las aplicaciones SaaS conocidas y desconocidas, una gestión consolidada de productos de varios proveedores e inspección de amenazas en línea.

La empresa también buscaba una manera de crear y ejecutar políticas con sencillez sin utilizar un *proxy* ni agentes, y quería eliminar la necesidad de sincronizar riesgos, políticas y objetivos en una capa independiente de la pila.

La solución ZTNA 2.0 de Palo Alto Networks con funciones CASB de próxima generación permitió a la empresa eliminar la necesidad de actualizar y configurar agentes para la inspección en línea y proteger *endpoints* no gestionados.

Impulsores del proyecto

- Adoptar de forma masiva la nube/SaaS
- Obtener visibilidad y control de aplicaciones conocidas y desconocidas
- Reducir la complejidad y consolidar la seguridad

Resultados

- La seguridad en la nube simplificó la implementación y la creación de políticas
- Aumentó considerablemente la visibilidad y el control de todas las aplicaciones
- Se ofreció una protección uniforme a 190 000 usuarios en todo el mundo

EN ESTE CAPÍTULO

- Garantía de visibilidad y control totales
- Verificación continua de la confianza
- Seguridad en todas las aplicaciones con una solución unificada
- Inspección completa de la seguridad
- Prevención de la pérdida de datos en todos los entornos
- Garantía de rendimiento y tiempo de actividad de las aplicaciones
- Reducción de la complejidad y los costes en una única solución

Capítulo 5
Diez preguntas (más o menos) que debe hacer a su proveedor de ZTNA 2.0

Aquí tiene algunas preguntas importantes que le ayudarán a evaluar a los posibles proveedores de acceso Zero Trust (confianza cero) a la red (ZTNA) 2.0 y sus soluciones.

¿Ofrece visibilidad total de las aplicaciones en la capa 7?

Los usuarios utilizan cada vez más una gran variedad de aplicaciones, incluidas aplicaciones de *software* como servicio (SaaS) desde multitud de dispositivos y ubicaciones, para fines tanto laborales como personales. Muchas aplicaciones, como la mensajería instantánea (MI), el intercambio de archivos punto a punto (P2P) y el protocolo de voz sobre Internet (VoIP, por sus siglas en inglés), pueden funcionar en puertos y direcciones IP no estándar o de tipo dinámico.

Además, los usuarios están cada vez más preparados para poder ejecutar aplicaciones en puertos no estándar a través de protocolos como el protocolo de escritorio remoto (RDP) y Secure Shell (SSH), independientemente de la política de la organización con respecto a diversas aplicaciones (autorizadas, toleradas, no autorizadas). Por lo tanto, una solución ZTNA que identifique aplicaciones en función de asignaciones arbitrarias de puertos de capa 3 y esté limitada al control de acceso de capa 3 o 4 ya no es suficiente para proteger su empresa.

CONSEJO

Busque una solución ZTNA 2.0 que pueda clasificar el tráfico por aplicación en todos los puertos constantemente y de forma predeterminada, sin generar más trabajo administrativo con la exigencia de averiguar los puertos que utiliza cada aplicación para configurar unas políticas y normas adecuadas. Una solución ZTNA 2.0 completa proporciona una visibilidad total a nivel de capa 7 (aplicación) sobre el uso de la aplicación, además de funciones para comprender y controlar dicho uso.

¿Ofrece verificación continua de la confianza?

El principio básico de Zero Trust es «no confiar nunca, verificar siempre», no «no confiar nunca, verificar una vez» ni «no confiar nunca, verificar de vez en cuando». Confiar en una entidad basada en credenciales de cuenta estáticas examinadas una vez en un dispositivo que parece legítimo en un momento dado es una invitación al desastre. Los ciberdelincuentes aprovechan este modelo defectuoso de confianza intrínseca para moverse libremente dentro de un entorno de red después de haber vulnerado las defensas perimetrales.

CONSEJO

Una solución ZTNA 2.0 sólida proporciona una verificación continua de la confianza basada en el comportamiento individual del usuario, que aprovecha el aprendizaje automático (AA) para determinar el riesgo e identificar posibles amenazas. El acceso a la red o a una aplicación debe permitirse solo después de una investigación exhaustiva de los usuarios y dispositivos que incluya la autenticación multifactor (MFA). Pero la cosa no acaba aquí. La verificación continua de la confianza debe producirse de forma constante y sin interrupciones durante la sesión para garantizar que la posición de seguridad del usuario o del dispositivo no haya cambiado ni se haya visto comprometida.

¿Protege sistemáticamente todas las aplicaciones en un solo producto?

Como hemos visto en el capítulo 1, las soluciones de seguridad puntuales que solo protegen aplicaciones específicas o admiten casos de uso limitados generan complejidad, ineficacia y, en última instancia, una estrategia de seguridad más débil. Los usuarios encontrarán nuevas formas creativas de eludir los controles de seguridad que sean confusos e incómodos de usar. Los equipos de seguridad son más propensos a cometer errores al configurar y utilizar herramientas que tienen diferentes sistemas operativos, interfaces y sintaxis, y se verán abrumados con alertas que no pueden relacionarse fácilmente con amenazas específicas en una solución integrada.

CONSEJO

Su solución ZTNA 2.0 debe proteger de manera uniforme todas sus aplicaciones, incluidas las aplicaciones personalizadas heredadas, las modernas aplicaciones nativas de la nube basadas en microservicios, las aplicaciones SaaS y mucho más en un solo producto unificado.

¿Realiza una inspección completa de la seguridad?

Una solución ZTNA 2.0 debe hacer algo más que limitarse a permitir o bloquear el tráfico en función de una inspección limitada de los encabezados de los paquetes y la aplicación de reglas de cortafuegos estáticas. También debe prevenir el *malware* avanzado, incluido el *ransomware*, e inspeccionar las amenazas conocidas y desconocidas en el tráfico de datos y aplicaciones con o sin cifrado; y una vez más, en todo el tráfico de las aplicaciones, no solo en el de las aplicaciones privadas.

CONSEJO

Una solución ZTNA 2.0 completa debe proporcionar inspección y control totales de la seguridad, con prevención de *malware* y amenazas.

¿Protege sistemáticamente todos los datos de la empresa?

Una protección de datos uniforme exige la consolidación de las políticas de protección de datos en todos los entornos y vectores de comunicación de datos. Unas políticas y configuraciones de protección de datos inconexas para las diferentes aplicaciones SaaS, los repositorios locales, las comunicaciones por correo electrónico, el

almacenamiento local, etc. provocan puntos ciegos de seguridad, complejidad de gestión, controles irregulares y TI en la sombra.

CONSEJO

Elija una solución ZTNA 2.0 que facilite una política de prevención de pérdida de datos (DLP) uniforme en todos los entornos donde se alojan y trasmiten datos, independientemente de su ubicación.

¿Proporciona SLA de tiempo de actividad y rendimiento para todas las aplicaciones?

Las herramientas de seguridad que perjudican el tiempo de actividad y el rendimiento de las aplicaciones crearán una experiencia de usuario deficiente que, en última instancia, provocará más TI en la sombra a medida que los usuarios buscan nuevas formas de eludir las herramientas que se han creado para su protección.

CONSEJO

Las soluciones ZTNA 2.0 modernas se entregan en la nube y, por lo tanto, proporcionan unas garantías de fiabilidad y rendimiento que aseguran que los usuarios de su organización puedan usar las aplicaciones que necesitan, incluidas las internas y basadas en SaaS, de manera segura y eficaz, cuando las necesitan. Asegúrese de que su proveedor de ZTNA 2.0 proporcione acuerdos de nivel de servicio (SLA) de rendimiento y tiempo de actividad que satisfagan las necesidades de su organización.

¿Tiene un único producto unificado para proteger toda la empresa?

Las herramientas de seguridad inconexas que no se pueden integrar fácilmente con otras soluciones añaden costes y complejidad a su entorno y pueden retrasar la detección, correlación e identificación de amenazas críticas, así como la respuesta a ellas. Esta complejidad añadida conduce en última instancia a un aumento de los gastos generales de gestión y aumenta significativamente los riesgos y la exposición.

CONSEJO

Un proveedor de ZTNA 2.0 debe ofrecer una única solución unificada, como un servidor perimetral de acceso seguro (SASE), que proteja toda su empresa, incluidos los usuarios, las aplicaciones, los dispositivos y los datos (independientemente de su ubicación) para reducir el riesgo y conseguir mejores resultados en materia de seguridad.

Glosario

AA: *consulte* aprendizaje automático (AA).

acceso *Zero Trust* (confianza cero) a la red (ZTNA): un método de seguridad que se basa en el principio de «no confiar nunca, verificar siempre», que garantiza el contexto adecuado de usuario mediante la autenticación y verificación de atributos antes de permitir el acceso a aplicaciones y datos en la nube o un centro de datos.

acuerdo de nivel de servicio (SLA): normas formales de rendimiento mínimo para sistemas, aplicaciones, redes o servicios.

ADEM: *consulte* gestión autónoma de la experiencia digital (ADEM).

análisis de comportamiento de entidades y usuarios (UEBA): un tipo de solución o característica de ciberseguridad que descubre amenazas mediante la identificación de actividad que se desvía de un comportamiento normal de referencia. Aunque UEBA puede utilizarse por distintos motivos, se utiliza normalmente para supervisar y detectar patrones de tráfico inusuales, movimientos y accesos no autorizados a los datos, o actividad sospechosa o maliciosa en una red informática o *endpoint*.

análisis del tráfico de red (NTA): una categoría de herramientas que se utilizan para interceptar, registrar y analizar patrones del tráfico de la red con el fin de detectar y responder a anomalías y actividades sospechosas mediante una combinación de aprendizaje automático, modelado de comportamiento y detección basada en reglas. *Consulte también* aprendizaje automático.

antivirus (AV): *software* diseñado para detectar y evitar virus informáticos y otro tipo de *malware* que pueda infectar un sistema. *Consulte también malware*.

API: *consulte* interfaz de programación de aplicaciones (API).

aprendizaje automático (AA): un método de análisis de datos que permite a los ordenadores analizar un conjunto de datos y llevar a cabo automáticamente acciones basadas en los resultados sin necesidad de una programación explícita.

archivo de configuración automática de *proxy* (PAC): un conjunto de reglas basado en web y escrito en JavaScript que indica al *endpoint* cómo dirigir el tráfico en relación con una URL determinada: mediante un *proxy* web o directamente a Internet. Puede incluir información como la dirección IP del sitio web, la dirección IP del usuario, y el *host* que solicitó el sitio web. *Consulte también* localizador uniforme de recursos (URL).

autenticación multifactor (MFA): un mecanismo de autenticación que necesita dos o más de los factores siguientes: algo que sabe, algo que tiene o algo que es. Por ejemplo, un usuario puede autenticarse con su nombre de usuario y contraseña (algo que sabe) y con un código de acceso de un solo uso que se envíe a un teléfono móvil que se ha registrado anteriormente con la organización (algo que tiene).

AV: *consulte* antivirus (AV).

C2: *consulte* comando y control.

centro de operaciones de seguridad (SOC): una instalación que ofrece control, evaluación, defensa y corrección de ciberseguridad a los recursos informáticos y de red de la empresa, incluidos los entornos locales y en la nube.

comando y control: tráfico de comunicaciones entre *malware* o sistemas en peligro y la infraestructura de servidor remoto de un atacante utilizada para enviar y recibir comandos maliciosos o exfiltrar datos.

conmutación de etiquetas multiprotocolo (MPLS): un método para reenviar paquetes a través de una red mediante el uso de etiquetas introducidas entre los encabezados de las capas 2 y 3 del paquete.

cortafuegos como servicio (FWaaS): una plataforma de cortafuegos ofrecida como servicio en un entorno de nube.

detección y respuesta en el *endpoint* (EDR): una categoría de herramientas que se utilizan para detectar e investigar amenazas en los *endpoints*. Las herramientas de EDR ofrecen por lo general capacidades de detección, investigación, búsqueda de amenazas y respuesta.

DLP: *consulte* prevención de pérdida de datos (DLP).

DNS: *consulte* sistema de nombres de dominio (DNS).

DPI: *consulte* inspección de paquetes en profundidad (DPI).

EDR: *consulte* detección y respuesta en el *endpoint* (EDR).

EPP: *consulte* plataforma de protección de *endpoint* (EPP).

***exploit*:** *software* o código que aprovecha una vulnerabilidad en un sistema operativo o aplicación y provoca un comportamiento no deseado en dicho sistema operativo o aplicación, como mayores privilegios, control remoto o un ataque de denegación de servicio.

FWaaS: *consulte* cortafuegos como servicio (FWaaS).

gestión autónoma de la experiencia digital (ADEM): una función de Prisma Access de Palo Alto Networks que ofrece una monitorización de la experiencia digital nativa de SASE y total visibilidad para solucionar de forma autónoma los problemas de conectividad del usuario antes de que se produzcan o cuando surjan. *Consulte también* servidor perimetral de acceso seguro (SASE).

IA: *consulte* inteligencia artificial (IA).

información de seguridad y gestión de eventos (SIEM): un sistema que ofrece recopilación, análisis, correlación y presentación en tiempo real de registros y alertas de seguridad. Los analistas del centro de operaciones de seguridad (SOC) utilizan herramientas SIEM para gestionar los incidentes de seguridad y para detectar con rapidez posibles amenazas y responder a ellas. *Consulte también* centro de operaciones de seguridad (SOC).

inspección de paquetes en profundidad (DPI): un método avanzado para examinar y gestionar el tráfico de la red que llega más allá de los encabezados de los paquetes iniciales.

inteligencia artificial (IA): la capacidad de un ordenador para interactuar con su entorno y aprender de él para llevar a cabo acciones automáticamente sin necesidad de una programación explícita.

interfaz de programación de aplicaciones (API): un conjunto de protocolos, rutinas y herramientas utilizados para desarrollar e integrar aplicaciones.

IP: *consulte* protocolo de Internet (IP).

IPS: *consulte* sistema de prevención de intrusiones (IPS).

LAN: *consulte* red de área local (LAN).

localizador uniforme de recursos (URL): lo que normalmente se conoce como «dirección web». Es el identificador único para todos los recursos conectados a la web.

***malware*:** *software* o código malicioso que normalmente daña o deshabilita un sistema informático, asume el control de este o le roba información.

mensajería instantánea (MI): un tipo de *chat* en línea en tiempo real a través de Internet.

MFA: *consulte* autenticación multifactor (MFA).

MI: *consulte* mensajería instantánea (MI).

modelo de interconexión de sistemas abiertos (OSI): el modelo de referencia de siete capas para las redes. Las capas son las siguientes: física, enlace de datos, red, transporte, sesión, presentación y aplicación.

modelo OSI: *consulte* modelo de interconexión de sistemas abiertos (OSI).

MPLS: *consulte* conmutación de etiquetas multiprotocolo (MPLS).

NTA: *consulte* análisis del tráfico de red (NTA).

nube híbrida: un entorno que consta de recursos de varias nubes públicas y privadas que ofrecen portabilidad de aplicaciones y datos entre nubes. *Consulte también* nube privada *y* nube pública.

nube privada: un modelo de servicios informáticos en la nube que consta de una infraestructura basada en la nube utilizada exclusivamente por una sola organización.

nube pública: un modelo de servicios informáticos en la nube que consta de una infraestructura basada en la nube de uso público.

P2P: *consulte* punto a punto (P2P).

PAC: *consulte* archivo de configuración automática de *proxy* (PAC).

perímetro definido por *software* (SDP): un perímetro definido por *software* protege todas las conexiones a los servicios que se ejecutan en todas las capas de una infraestructura de red, según el nivel de seguridad que se defina y establezca.

plataforma de protección del *endpoint* (EPP): un conjunto integrado de tecnologías de seguridad de *endpoint*, como antivirus, cifrado de datos, prevención de pérdida de datos, cortafuegos personal, y control de puertos y dispositivos.

prevención de pérdida de datos (DLP): una aplicación o dispositivo que se utiliza para detectar el almacenamiento o la transmisión no autorizados de datos confidenciales.

protocolo de control de transmisión (TCP): un protocolo orientado a la conexión que se encarga de establecer una conexión entre dos *hosts* y garantizar la entrega de datos y paquetes en el orden correcto.

protocolo de datagramas de usuario (UDP): un protocolo de red que no garantiza la entrega de paquetes ni el orden de entrega de paquetes a través de una red.

protocolo de escritorio remoto (RDP): un protocolo patentado de Microsoft que ofrece acceso remoto a un ordenador. RDP utiliza el puerto TCP 3389 y el puerto UDP 3389 de manera predeterminada. *Consulte también* protocolo de control de transmisión (TCP) y protocolo de datagramas de usuario (UDP).

protocolo de Internet (IP): el protocolo de capa 3 de OSI que forma la base de la Internet moderna. *Consulte también* modelo de interconexión de sistemas abiertos (OSI).

puerta de enlace web segura (SWG): una plataforma o servicio de seguridad que se ha diseñado para mantener la visibilidad de todo tipo de tráfico a la vez que impide las evasiones que pueden ocultar amenazas. Puede ofrecer más funciones, como filtrado de contenido web y prevención de robo de credenciales.

punto a punto (P2P): una arquitectura de aplicación distribuida que permite compartir entre nodos.

RDP: *consulte* protocolo de escritorio remoto (RDP).

red de área extensa (WAN): una red informática que abarca un área geográfica amplia y puede conectar varis redes de área local. *Consulte también* red de área local (LAN).

red de área extensa definida por *software* (SD-WAN): un nuevo enfoque para las redes de área extensa que separa los procesos de control y gestión de la red del *hardware* subyacente, dejándolos disponibles como *software*. *Consulte también* red de área extensa (WAN).

red de área local (LAN): una red informática que conecta ordenadores en un área relativamente pequeña, como un edificio de oficinas, un almacén o un domicilio.

red privada virtual (VPN): una VPN crea una conexión privada, conocida como «túnel», a Internet. Toda la información que viaja de un dispositivo conectado a una VPN se cifra y pasa a través de este túnel. Cuando un dispositivo se conecta a una VPN, se comporta como si estuviera en la misma red local que la VPN. La VPN dirige el tráfico del dispositivo hacia y desde el sitio web o red previstos a través de una conexión segura.

SaaS: *consulte software* como servicio (SaaS).

SDP: *consulte* perímetro definido por *software* (SDP).

SD-WAN: *consulte* red de área extensa definida por *software* (SD-WAN).

***Secure Shell* (SSH):** un protocolo de red criptográfico que proporciona acceso seguro a un ordenador remoto.

SIEM: *consulte* información de seguridad y gestión de eventos (SIEM).

sistema de nombres de dominio (DNS): una base de datos jerárquica y descentralizada de servicios de directorio que convierte los nombres de dominio en direcciones IP para ordenadores, servicios y otros recursos informáticos conectados a una red o a Internet. *Consulte también* protocolo de Internet (IP).

sistema de prevención de intrusiones (IPS): una aplicación de *software* o *hardware* que detecta y bloquea intrusiones sospechosas en la red o en el *host*.

SLA: *consulte* acuerdo de nivel de servicio (SLA).

SOC: *consulte* centro de operaciones de seguridad (SOC).

***software* como servicio (SaaS):** un modelo de distribución de *software* basado en la nube en el que un proveedor externo hospeda aplicaciones que pone a disposición de los clientes a través de Internet. El proveedor de *software* se encarga de hospedar y mantener los servidores, bases de datos y código que forman la aplicación.

SSH: c*onsulte Secure Shell* (SSH).

SWG: *consulte* puerta de enlace web segura (SWG).

tácticas, técnicas y procedimientos (TTPs): los comportamientos, métodos, estrategias y herramientas utilizados por los ciberdelincuentes para atacar a su objetivo.

TCP: *consulte* protocolo de control de transmisión (TCP).

TI en la sombra: aplicaciones y servicios informáticos que adquieren y operan los usuarios finales sin la autorización explícita de la organización y, a menudo, sin el conocimiento ni el respaldo del departamento de TI de la organización.

***tromboning*:** la práctica de enrutar el tráfico de la red a través de un punto de control (como un cortafuegos).

TTP: *consulte* tácticas, técnicas y procedimientos (TTPs).

UDP: *consulte* protocolo de datagramas de usuario (UDP).

UEBA: *consulte* análisis del comportamiento de entidades y usuarios (UEBA).

URL: *consulte* localizador uniforme de recursos (URL).

***varias nubes*:** un entorno que consta de recursos de varias nubes públicas o privadas, pero que no ofrece necesariamente portabilidad de aplicaciones y datos entre nubes (es decir, los distintos entornos de nube pueden funcionar como nubes inconexas). Cabe destacar que, aunque todos los entornos de nube híbrida son también entornos de varias nubes, no todos los entornos de varias nubes son entornos de nube híbrida. *Consulte también* nube híbrida, nube privada *y* nube pública.

VoIP: *consulte* voz sobre protocolo de Internet (VoIP).

voz sobre protocolo de Internet (VoIP): protocolos de telefonía diseñados para transportar comunicaciones de voz a través de redes TCP/IP. *Consulte también* protocolo de control de transmisión (TCP) *y* protocolo de Internet (IP).

VPN: *consulte* red privada virtual (VPN).

WAN: *consulte* red de área extensa (WAN).

Zero Trust: *Zero Trust* (confianza cero) es una iniciativa estratégica que ayuda a frustrar las brechas de datos eliminando el concepto de confianza de la organización. Basada en el principio de «no confiar nunca, verificar siempre», Zero Trust se ha diseñado para evitar el movimiento lateral.

ZTNA: *consulte* acceso *Zero Trust* (confianza cero) a la red (ZTNA).

Zero Trust with Zero Exceptions

ZTNA 1.0 is over. Secure the future of hybrid work with ZTNA 2.0. Only available with Prisma® Access.

Palo Alto Networks Prisma® Access protects the hybrid workforce with the superior security of ZTNA 2.0 while providing exceptional user experiences from a simple, unified security product. Purpose-built in the cloud to secure at cloud scale, only Prisma Access protects all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach.

Learn how Prisma Access secures today's hybrid workforce without compromising performance, backed by industry-leading SLAs to ensure exceptional user experiences.

https://www.paloaltonetworks.com/sase/ztna

PRISMA® ACCESS
BY PALO ALTO NETWORKS

Conozca ZTNA hoy mismo

Los trabajadores híbridos y las arquitecturas directas a la aplicación han hecho que las soluciones de seguridad tradicionales se hayan quedado obsoletas y que haya aumentado exponencialmente la superficie de ataque. Al mismo tiempo, aumentan la frecuencia y la sofisticación de las amenazas, mientras que la proliferación de herramientas de seguridad dispares genera complejidad operativa. Las soluciones de seguridad en la nube existentes permiten demasiado acceso con muy poca protección, proporcionan seguridad de forma irregular e incompleta a través de las aplicaciones y ofrecen un bajo rendimiento y unas experiencias de usuario deficientes. El acceso Zero Trust (confianza cero) a la red 2.0 ofrece una mejor opción de cara al futuro.

En el interior...

- Descubrirá casos de uso para empezar su camino hacia la adopción de ZTNA 2.0
- Comprenderá las diferencias entre ZTNA 2.0 y las soluciones ZTNA antiguas
- Conocerá los cinco principios clave de ZTNA 2.0
- Sabrá cuáles son las preguntas que debe hacer a su proveedor de ZTNA
- Verá cómo una solución unificada ofrece experiencias de usuario excepcionales

paloalto® NETWORKS

Lawrence Miller fue contramaestre en la Marina estadounidense y ha trabajado en distintos sectores de la tecnología de la información durante más de 25 años. Es coautor del libro *CISSP para Dummies* y ha escrito más de 200 guías *para Dummies* sobre muchos temas relacionados con la tecnología y la seguridad.

Visite Dummies.com®
para ver vídeos, fotografías paso a paso y artículos con instrucciones o para comprar productos.

ISBN: 978-1-394-18376-0

para dummies®

WILEY END USER LICENSE AGREEMENT

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