appgate

Retorno de la Inversión Análisis del Acceso Universal a Redes de Zero Trust

Este white paper ofrece un análisis de la diferencia entre los enfoques arquitectónicos de enrutamiento directo y enrutamiento en la nube, las consideraciones clave y el posible retorno de la inversión (ROI) directo e indirecto para el Acceso universal a Redes de Zero Trust (ZTNA).

Análisis del ROI de ZTNA Universal

Índice de contenidos

INTRODUCCIÓN

Con los entornos de trabajo remotos e híbridos establecidos como el nuevo modelo de empresa, las soluciones de seguridad de red tradicionales han demostrado su ineficacia a la hora de proporcionar un acceso seguro a los usuarios. Este cambio está impulsando una creciente demanda de Zero Trust Network Access (ZTNA), desplegado inicialmente como el sustituto moderno y altamente seguro de acceso remoto para las tecnologías VPN, obsoletas y propensas al riesgo. El concepto de ZTNA universal va más allá del caso de uso principal de sustitución de VPN para ofrecer acceso seguro a través de entornos de TI híbridos complejos para cualquier usuario, desde cualquier dispositivo, ya sea local o remoto, con un modelo de política unificado.

ZTNA Universal facilita la aplicación coherente de los principios de seguridad de Zero Trust para garantizar el acceso de todas las identidades y a todos los recursos protegidos, independientemente de su ubicación. Adoptar el ZTNA Universal presenta una oportunidad para la consolidación de proveedores y herramientas, lo que permite a las organizaciones equilibrar la responsabilidad fiscal al tiempo que mantienen una postura de seguridad sólida. Este documento técnico ofrece un análisis de la diferencia entre los enfoques arquitectónicos de ZTNA de enrutamiento directo y enrutamiento en la nube, las consideraciones clave y el posible retorno de la inversión (ROI) directo e indirecto cuando se aplica sólo a la sustitución de VPN para acceso remoto o se extiende universalmente a todos los casos de uso de la empresa. El documento demuestra cómo las organizaciones pueden desbloquear casos de uso críticos para el negocio y lograr eficiencias de costes sustanciales a escala mediante la adopción de una solución ZTNA universal creada específicamente.

"Universal ZTNA" amplía las tecnologías ZTNA existentes a casos de uso que van más allá del acceso remoto, con el fin de dar soporte a la aplicación local en campus y sucursales locales. ('Universal ZTNA' es un término de marketing, ya que la definición original de ZTNA no se limitaba a casos de uso de acceso remoto). ZTNA Universal centraliza la política del acceso de Zero Trust del dispositivo y del usuario final para permitir una única definición de la política de acceso".

– Gartner 2023 Market Guide for ZTNA

Casos de uso que impulsan ZTNA universal

- **Sustitución completa de VPN:** Transición de las VPN tradicionales a ZTNA para todos los casos de uso
- **Acceso de terceros:** Garantizar que entidades externas puedan conectarse sin comprometer la integridad de la red
- **Transición del tráfico de MPLS a Internet:** Migrar el tráfico de red de las costosas conexiones MPLS a la Internet pública
- **Eliminar la red de área extensa definida por software (SD-WAN):** Proporcionar un acceso seguro a los recursos sin depender de las complejidades y posibles vulnerabilidades de la SD-WAN tradicional
- **Sustitución del control de acceso a la red (NAC):** Sustituya las costosas soluciones NAC por mecanismos de control de acceso coherentes para todos los usuarios, dispositivos y ubicaciones
- **Conectividad de sucursales de Zero Trust:** Garantizar la verificación y autorización continuas de todos los usuarios y dispositivos que acceden a los recursos corporativos desde las sucursales

Capacidades críticas para un ZTNA Universal

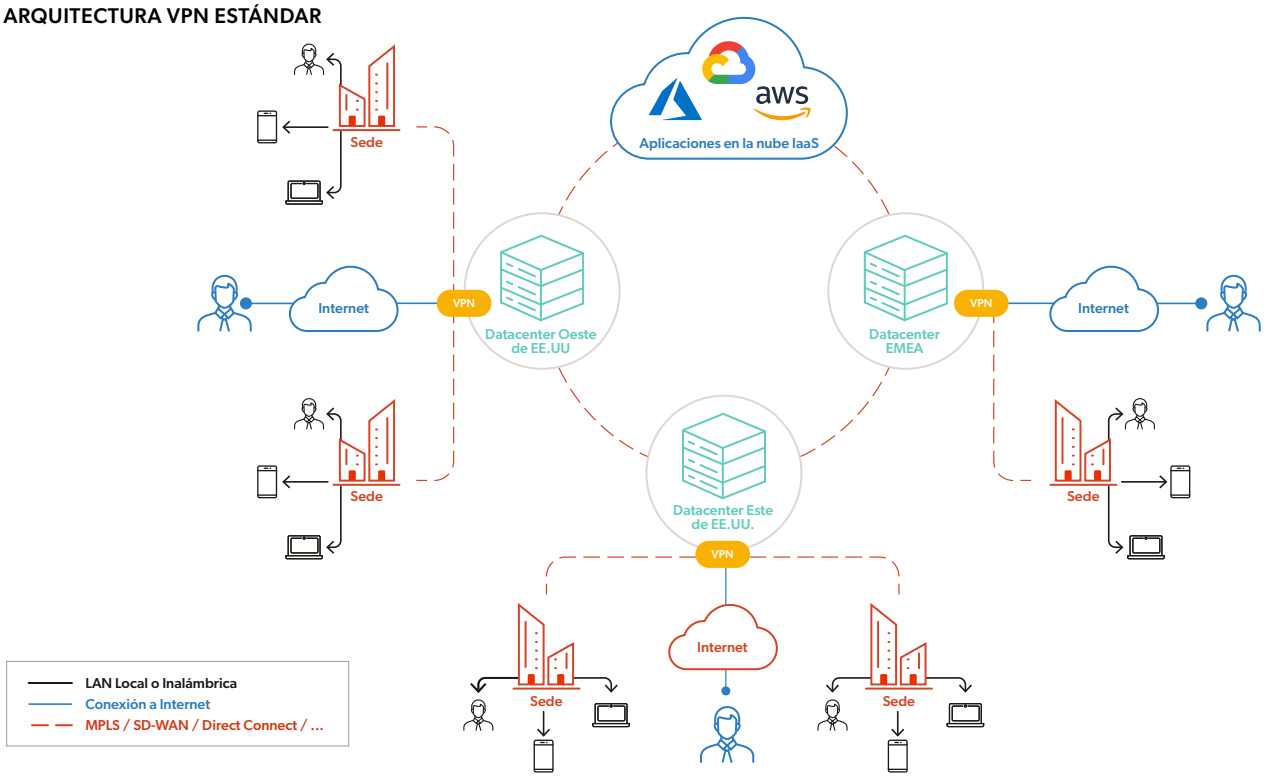
- **Seguridad centrada en la identidad:** Garantizando que sólo las entidades autorizadas y autenticadas puedan acceder a los recursos de red especificados
- **Control de acceso en la capa de aplicación:** Asegurando que los usuarios tengan el acceso mínimo necesario para realizar sus tareas
- **Políticas de acceso dinámicas:** Garantizando el acceso basado en el contexto específico del usuario y el dispositivo
- **Autenticación adaptativa:** Respondiendo a los cambios en el comportamiento del usuario o a factores contextuales para garantizar que los privilegios de acceso son adecuados para la situación de seguridad actual
- **Escalabilidad y alto rendimiento:** Ampliando la escalabilidad dinámica para dar cabida a usuarios y dispositivos adicionales, manteniendo al mismo tiempo un rendimiento óptimo sucursales

ZTNA: REEMPLAZO DE VPN PARA ACCESO REMOTO DE USUARIOS

La sustitución de las tecnologías VPN para dar soporte al acceso remoto de los usuarios suele ser un caso de uso inicial para la adopción de ZTNA. La tecnología VPN tradicional extiende el perímetro de la empresa hasta un dispositivo remoto. Sin embargo, si ese dispositivo se ve comprometido, un atacante puede violar el perímetro, establecer persistencia, realizar reconocimiento y moverse lateralmente por todo el entorno para llevar a cabo con éxito su ataque. Muchos ejemplos, ya sea a través de una VPN, una cuenta VPN o un exploit en el concentrador VPN, han demostrado que las VPN ya no cumplen con los estándares de seguridad modernos.

Una red perimetral empresarial suele existir en uno o más centros de datos regionales o ubicaciones donde se alojan las aplicaciones principales y las pilas de seguridad. Esa ubicación puede ser una sala de servidores local, un centro de datos comercial o incluso en la nube a través de la infraestructura como servicio (IaaS). Estas ubicaciones suelen estar interconectadas mediante conexiones seguras y dedicadas (es decir, MPLS, SDWAN, conexión directa y fibra alquilada) proporcionadas por un servicio de telecomunicaciones. Estas conexiones son significativamente más caras que el ancho de banda de Internet tradicional. Sin embargo, la conexión es cifrada, dedicada e invisible para cualquier personaje nefasto en Internet.

ARQUITECTURA VPN ESTÁNDAR



Las últimas CVE hacen hincapié en las vulnerabilidades de las VPN

Junio 2023: Fortinet confirmó la existencia de una vulnerabilidad crítica de día cero que afecta a las VPN FortiGate SSL de Fortinet, rastreada como CVE-2023-27997 (CVSS: 9.2). Su explotación permitía a una amenaza remota y no autenticada ejecutar código en los dispositivos vulnerables. Como la vulnerabilidad era previa a la autenticación, los ataques eludían la autenticación multifactor (MFA).

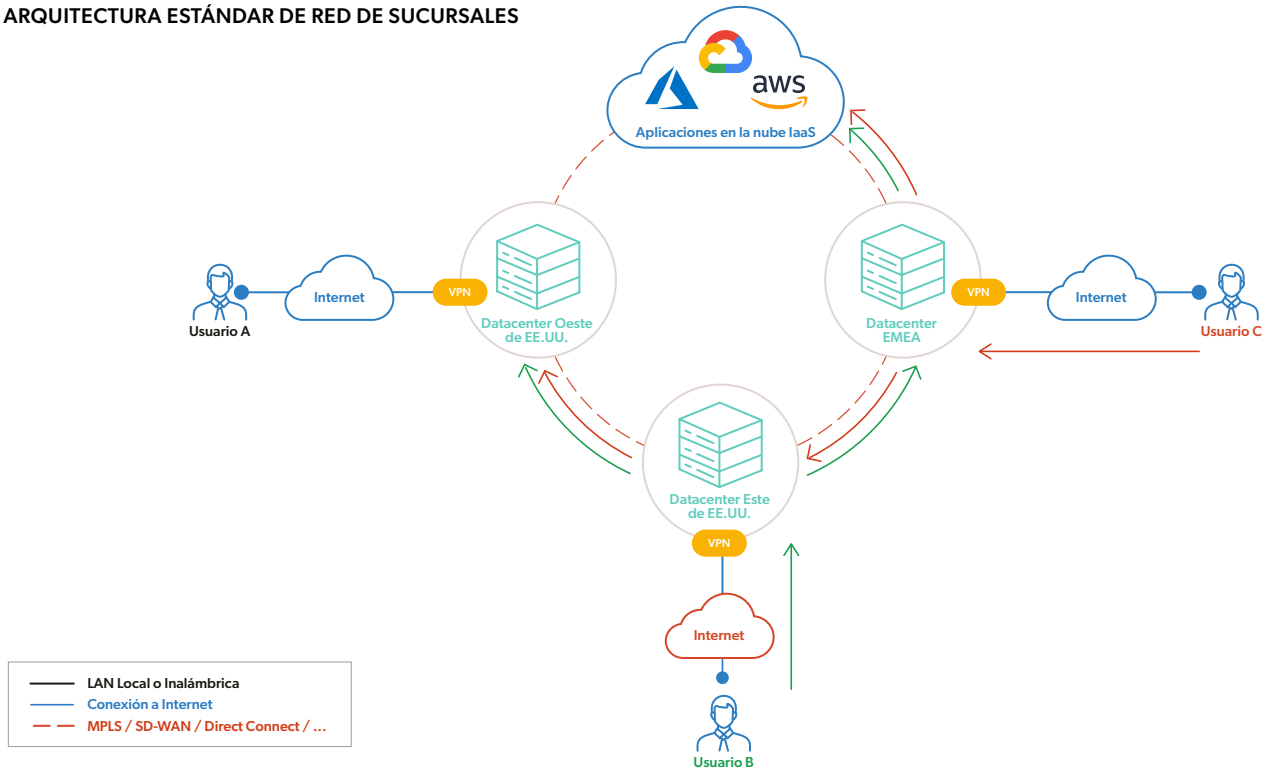
Septiembre 2023: Cisco confirmó una vulnerabilidad de día cero en la función VPN de acceso remoto de su software Adaptive Security Appliance y Firepower Threat Defense, rastreada como CVE-2023-20269. Su explotación permitía a un atacante identificar credenciales válidas que podían utilizarse para establecer una sesión VPN de acceso remoto no autorizada, así como una sesión VPN SSL sin cliente.

Enero 2024: Ivanti ha confirmado la existencia de dos vulnerabilidades de día cero que están siendo explotadas en la naturaleza, rastreadas como CVE-2023-46805 y CVE-2024-21887. La primera era una vulnerabilidad de autenticación que permitía el acceso remoto a materiales restringidos. La segunda era una vulnerabilidad de inyección de comandos que permite a los administradores autenticados enviar peticiones únicas y ejecutar comandos arbitrarios. En febrero de 2024 se publicaron más CVE.

Las sedes o las redes locales suelen estar conectadas a uno o varios centros de datos regionales o ubicaciones en la nube mediante conexiones dedicadas similares. Es una práctica común que los centros de datos regionales sean los puntos de entrada y salida de Internet para la empresa. Los concentradores VPN a menudo se alojan aquí y suelen proporcionar acceso regional a los usuarios remotos y, a continuación, enrutan el tráfico de la aplicación a través de la red interna a las diferentes ubicaciones si es necesario.

Visualizando el tráfico VPN de usuarios remotos, todo el tráfico de un usuario ingresa a la red de la empresa en una ubicación, normalmente el concentrador VPN regional. Por ejemplo, el usuario C conecta su VPN al centro de datos regional de EMEA y todo el tráfico VPN llega a esa ubicación. También podrían conectarse a aplicaciones locales en el centro de datos del este de EE.UU. o aplicaciones en otros centros de datos regionales. En este caso, el usuario remoto consume ancho de banda de las distintas conexiones privadas entre esos centros de datos. El ancho de banda consumido a través de una conexión privada es significativamente más caro que el ancho de banda de Internet. Además, si el usuario debe pasar por varios enlaces para llegar a una aplicación, el coste asociado, así como la latencia, serían aún mayores.

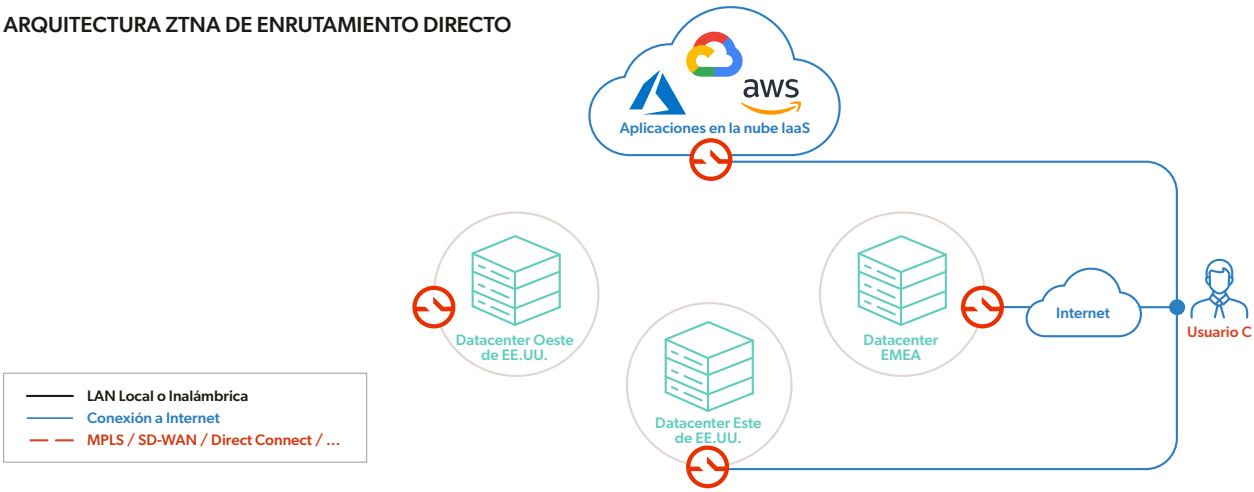
ARQUITECTURA ESTÁNDAR DE RED DE SUCURSALES



REEMPLAZO DE VPN POR ARQUITECTURA ZTNA DE ENRUTAMIENTO DIRECTO

Tomemos este mismo ejemplo pero sustituyamos la solución VPN por ZTNA de enrutamiento directo. En lugar de un único punto de entrada a la red de la empresa, ahora tenemos una pasarela en cada ubicación. El usuario creará un túnel TLS mutuo (mTLS) para cada ubicación para la que tenga derechos de aplicación o red. Las pasarelas son invisibles en Internet mediante el uso de Single Packet Authorization (SPA), que requiere que el cliente envíe un paquete especial antes de que el socket de red pueda conectarse desde ese cliente a la pasarela. Esta técnica mitiga el riesgo de ataques distribuidos de denegación de servicio (DDoS) y de día cero, que no pueden soportarse con las tecnologías VPN. El usuario C de este ejemplo ha establecido túneles mTLS directos entre los tres centros de datos, aprovechando el ancho de banda estándar de Internet. Como se muestra en la siguiente imagen, el usuario remoto C está completamente liberado de toda conectividad MPLS/SD-WAN, de la que no son capaces las tecnologías VPN.

ARQUITECTURA ZTNA DE ENRUTAMIENTO DIRECTO



ROI directo: Reemplazo de VPN por ZTNA de enrutamiento directo

Reducción de los costos de conectividad MPLS/SD-WAN:

La cantidad de ancho de banda MPLS/SD-WAN que consumen los usuarios de VPN depende de dónde estén ubicados los concentradores de VPN y de lo distribuidas que estén las aplicaciones en la red de la empresa. Si la organización está muy centrada en la nube, pero sigue utilizando una VPN local para conectarse a los entornos de nube, se producirá un ahorro inmediato para todos los usuarios remotos al pasar del costoso ancho de banda MPLS/SD-WAN a la conectividad estándar a Internet. Al cambiar los usuarios de VPN a ZTNA de enrutamiento directo para el acceso remoto, las organizaciones deberían esperar ver un descenso general del 10% al 20% en los costos de conectividad MPLS/SDWAN.

Reducción de los costos de hardware:

ZTNA de enrutamiento directo sustituye a los concentradores VPN por una solución puramente de software, lo que facilita la adición de más puntos de entrada sin necesidad de comprar o mantener costosos dispositivos hardware de VPN adicionales. Además, facilita el escalado automatizado de la nube, permitiendo el aprovisionamiento y desaprovisionamiento de recursos en respuesta a la fluctuación de la demanda. Por otra parte, durante acontecimientos significativos como una pandemia mundial o condiciones meteorológicas adversas que afecten a regiones específicas, se puede apoyar un cambio repentino al trabajo remoto para todos los usuarios sin ninguna interrupción. Es importante tener en cuenta que los paquetes VPN basados en hardware pueden oscilar entre 4.700 dólares por 75 usuarios a 300.000 dólares para 10.000 usuarios, como muestra esta estructura de precios de Cisco. Para las empresas más centradas en la red, con consideraciones de equilibrio de carga y redundancia, el gasto de capital en hardware podría ser incluso mayor, con costos añadidos de mantenimiento de los dispositivos.

¿Qué es ZTNA de enrutamiento directo?

Las arquitecturas ZTNA de enrutamiento directo ofrecen un enfoque flexible y específico para adaptarse al conjunto único de aplicaciones privadas e infraestructuras de red dentro de una empresa. Este modelo garantiza un control total sobre la forma en que los datos atraviesan la red, proporcionando un acceso seguro a todas las conexiones de usuario a recurso y de recurso a recurso desde cualquier lugar a través de infraestructuras híbridas ubicadas en cualquier lugar. Una ventaja clave es la escalabilidad y el rendimiento de las arquitecturas de enrutamiento directo, que permiten a las empresas ampliar su negocio manteniendo un rendimiento óptimo de la red. El modelo de precios asociado a la ZTNA de enrutamiento directo es transparente, fácilmente comprensible y carente de cargos ocultos, lo que proporciona a las empresas una estructura de costes predecible y gestionable.

ROI Indirecto: Reemplazo de VPN por ZTNA de enrutamiento directo

Reducción del riesgo de infracciones y preservación de la continuidad empresarial:

Con el Single Packet Authorization (SPA), se puede aprovechar la Internet estándar para el tráfico de red empresarial crítico. SPA hace invisibles los puntos de borde, por lo que se eliminan las posibilidades de ataques DDoS, parches de vulnerabilidad VPN y ataques de día cero. Según informa SecurityWeek, el tiempo de inactividad debido a un ataque DDoS a una aplicación con éxito cuesta a las organizaciones una media de 6.000 dólares por minuto. En consecuencia, con una solución ZTNA de enrutamiento directo se puede ahorrar en costos y riesgos operativos y de gestión de DDoS y mantener la continuidad del negocio.

Superficie de ataque minimizada:

Las políticas detalladas de ZTNA Universal garantizan que no se conceda a los usuarios un acceso amplio a la red, lo que reduce significativamente la superficie de ataque, especialmente si un usuario o dispositivo malintencionado intenta conectarse desde una ubicación remota. Además, las políticas detalladas permiten adaptar los privilegios de acceso en función de factores contextuales, lo que mejora la capacidad de una organización para proporcionar un acceso seguro a los usuarios y evitar al mismo tiempo los intentos de acceso no autorizado por parte de agentes malintencionados.

Aumento de la productividad:

ZTNA universal agiliza el proceso para que los usuarios autorizados accedan a los recursos necesarios, lo que permite a los propietarios de empresas acelerar el despliegue de aplicaciones en producción. También permite a los equipos de seguridad informática proporcionar a terceras entidades un acceso preciso a los sistemas críticos, como los sistemas HVAC o los robots de fabricación, reduciendo eficazmente el riesgo de ataques de terceros. El retorno de la inversión se refleja en la mejora de la productividad y la eficiencia de los empleados o contratistas que necesitan un acceso seguro a los recursos de la empresa.

Cumplimiento simplificado:

ZTNA de enrutamiento directo puede ayudar a las organizaciones a cumplir diversas normativas y estándares, y proporciona políticas basadas en la identidad, que son más fáciles de auditar en comparación con las reglas y registros tradicionales de los cortafuegos de red. El retorno de la inversión puede medirse mediante la automatización de la recopilación de datos y la elaboración de informes, que a menudo requieren un enfoque manual con las soluciones tradicionales de acceso seguro. ZTNA puede ayudar a reducir el alcance de los informes de cumplimiento y evitar el incumplimiento de las normativas del sector.

ROI Comprobado de Appgate SDP para la Transición del Tráfico de MPLS a Internet:

Un proveedor global de servicios de TI de la lista Fortune 500 implantó ZTNA Universal en su base de 130.000 usuarios. La adopción de una arquitectura de enrutamiento directo permitió a cada usuario establecer túneles de Internet cifrados individuales que conectaban con los seis centros de datos principales de la organización, sustituyendo la conectividad MPLS privada compartida utilizada anteriormente. Antes de esto, se requería una conectividad MPLS de 10 Gbit como interconexión entre los seis centros de datos principales de todo el mundo. La empresa eliminó MPLS de más de 600 sitios, reduciendo los costos totales de conectividad en un 67%, lo que les permitió contratar compromisos de ancho de banda más bajos. Esto supuso un ahorro anual de decenas de millones, 10 veces lo que la empresa paga anualmente por la solución universal ZTNA.

ROI Comprobado de Appgate SDP o Conectividad de Sedes Zero Trust:

Una empresa mundial de alimentación y salud adoptó ZTNA Universal para proporcionar acceso seguro a todos los usuarios de su extensa red. Una vez instalado, los usuarios de las sedes podían operar desde la red Wifi para invitados, lo que permitió a la empresa eliminar la mayoría de los equipos de seguridad de red tradicionales. La empresa ahorró 750.000 dólares en costos de renovación de equipos para sus 14 sedes en todo el mundo. Esto racionalizó sus gastos operativos y eliminó la necesidad de mantener y actualizar soluciones de seguridad dispares en cada ubicación. La implantación de ZTNA Universal garantizó una experiencia de usuario coherente y uniforme para los empleados, independientemente de si trabajaban local o remoto.

REEMPLAZO DE VPN CON ARQUITECTURA ZTNA DE ENRUTAMIENTO EN LA NUBE

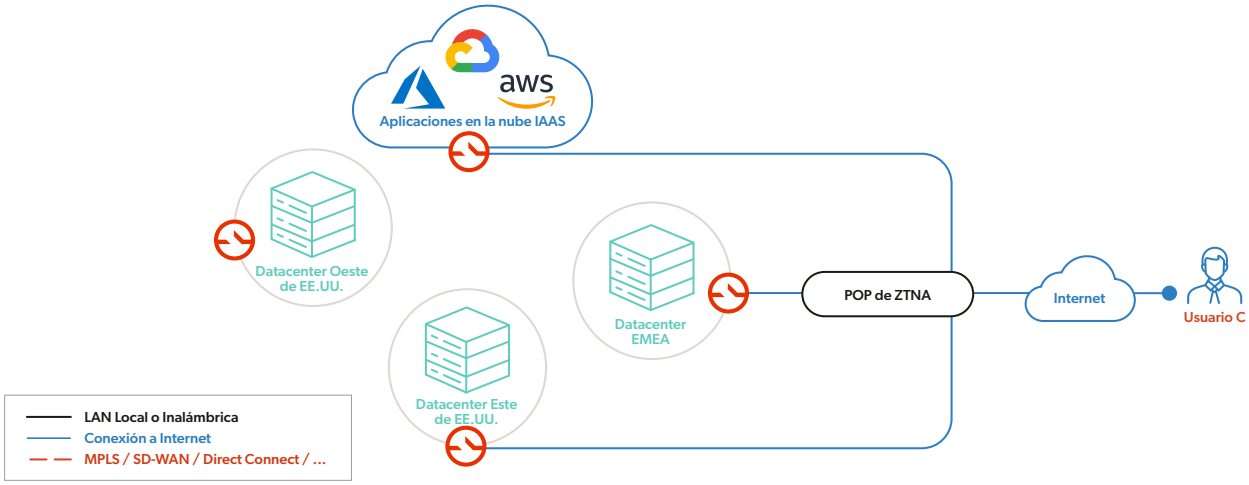
Cuando se sustituyen las tecnologías VPN por una arquitectura ZTNA enrutada en la nube, se aplican ahorros de costos y ventajas similares a los de la arquitectura enrutada directamente. Sin embargo, esta arquitectura presenta el doble de costo de ancho de banda de Internet y latencia adicional porque se requiere conectividad entre el usuario y el punto de presencia (POP) de ZTNA más cercano y entre el POP y los centros de datos regionales. La conexión entre el punto de presencia del ZTNA enrutado en la nube y cada centro de datos suele ser una conexión cifrada compartida que afecta significativamente al rendimiento general del sistema. El control del tráfico se produce en la nube y utiliza un túnel abierto compartido dentro de los centros de datos de la organización. Si la nube se ve comprometida, existe una puerta trasera abierta a todos los sitios críticos de la organización.

Además, las arquitecturas ZTNA enrutadas en la nube suelen tener limitaciones para admitir todos los protocolos o gestionar el tráfico iniciado desde abajo, lo que es fundamental para abordar los casos de uso del protocolo de voz por Internet (VoIP) y los conjuntos de herramientas operativas de TI que requieren la aplicación de parches, la gestión y la asistencia de los dispositivos. Esta limitación puede obligar a los clientes a tomar decisiones difíciles después de la compra para determinar qué se puede incluir y qué no funcionará con la solución ZTNA enrutada en la nube adquirida. La organización debe entonces bifurcar sus aplicaciones entre las que están protegidas por soluciones ZTNA enrutadas en la nube y las que no lo están, dejándolas vulnerables a los riesgos.

¿Qué es ZTNA de enrutamiento en la nube?

Las arquitecturas ZTNA enrutadas en la nube, comúnmente denominadas proxies conscientes de la identidad (IAP), son habituales en el mercado debido a su rápido desarrollo y velocidad de comercialización. En este modelo, el tráfico de datos se canaliza a través de entornos de nube multiarrendatario. Estas arquitecturas pueden tener muchos inconvenientes, como la compatibilidad limitada con protocolos de red, las limitaciones de recursos locales, las limitaciones de latencia y "giro de horquilla", así como la incapacidad para escalar eficientemente. Además, existe una confianza implícita en la seguridad, disponibilidad y escalabilidad de la nube multiusuario del proveedor. Las empresas que buscan un control exhaustivo y previsibilidad suelen encontrar más ventajosas las soluciones ZTNA de enrutamiento directo.

ARQUITECTURA ZTNA ENRUTADA EN LA NUBE



ZTNA UNIVERSAL: ACCESO SEGURO PARA TODOS LOS USUARIOS

Cuando el ZTNA se limita a sustituir las VPN para permitir el acceso de los usuarios remotos, el equipo de administración de TI se ve a menudo obligado a gestionar las reglas de seguridad por separado para los usuarios remotos y los locales. Esta fragmentación de los protocolos de seguridad puede aumentar la complejidad y las posibles vulnerabilidades de la infraestructura de red. El cambio a ZTNA Universal elimina la distinción entre usuarios remotos y locales, asegurando protocolos de seguridad consistentes y garantizando una latencia y rendimiento uniformes para todos los usuarios. Repasemos un ejemplo de por qué esto añade complejidad y, a continuación, destaquemos las arquitecturas de enrutamiento directo y enrutamiento en la nube.

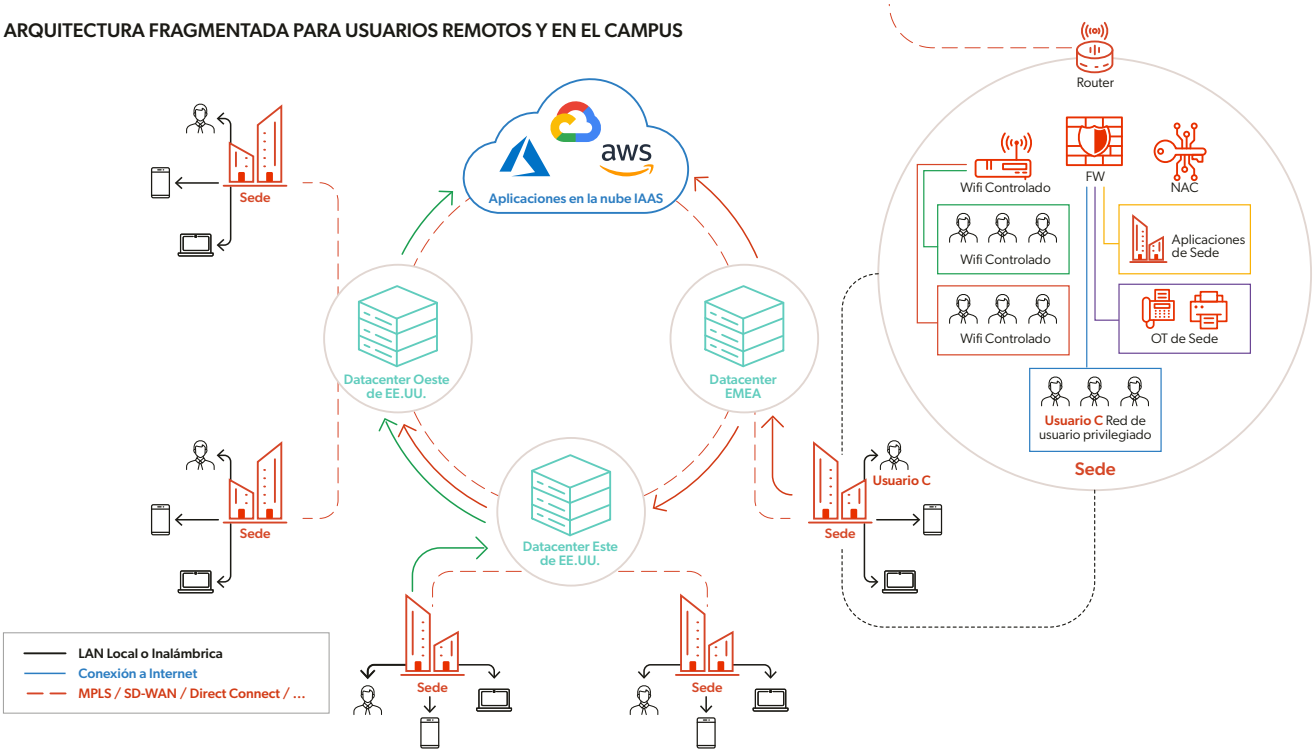
Tomemos al usuario C, que en este caso es un usuario privilegiado (administrador/ operaciones de TI) que necesita trabajar desde una sucursal en EMEA utilizando su escritorio. Debido a su condición de usuario privilegiado, necesita un amplio acceso a numerosos sistemas y aplicaciones sensibles. Para proteger a los usuarios con privilegios del resto de usuarios de la oficina, a menudo se les coloca en una red de usuarios con privilegios. Para ello, la empresa necesita una solución de control de acceso a la red (NAC), un sistema de gestión inalámbrica y conmutadores ethernet especiales para identificar el dispositivo de un usuario privilegiado.

Este segmento tiene acceso a los sistemas críticos de toda la red de la empresa. Como resultado, están aislados de los usuarios estándar y de los empleados invitados (es decir, contratistas y proveedores externos) cuyo acceso suele estar restringido sólo a la conectividad a Internet. En todas las sucursales se establecen reglas de cortafuegos avanzadas y complejas, que normalmente se impulsan desde un sistema central de gestión de cortafuegos. Cada nuevo segmento de usuarios que se añade en una oficina para distinguir los grupos de usuarios genera un trabajo exponencial en las reglas del cortafuegos, la solución NAC y los sistemas de gestión inalámbrica. Por lo tanto, la segregación de usuarios y dispositivos suele reducirse a cuatro o seis segmentos diferentes, lo que hace que la segmentación de la red empresarial sea de grano muy grueso.

"Las empresas gastan miles de millones en proteger las redes locales mediante una combinación de funciones de conmutación y NAC, un enfoque que está a punto de cambiar con el paso al trabajo híbrido. Los líderes de producto deben ampliar los productos ZTNA a los entornos de campus para impulsar los ingresos y el valor empresarial, pero deben actuar con rapidez".

— Gartner La Seguridad de las Redes de Campus y el NAC están Maduros para la Disrupción del Mercado

ARQUITECTURA FRAGMENTADA PARA USUARIOS REMOTOS Y EN EL CAMPUS



Cuando el usuario C se conecta desde su sede a todas las diferentes aplicaciones en el oeste de EE.UU., el este de EE.UU., EMEA y el entorno de nube IaaS de la empresa, está utilizando ancho de banda MPLS/SD-WAN en cada uno de estos enlaces. Todo ese ancho de banda para aplicaciones privadas y tráfico de navegación por Internet también se consume a través de la conexión privada de la sede al centro de datos de la empresa más cercano.

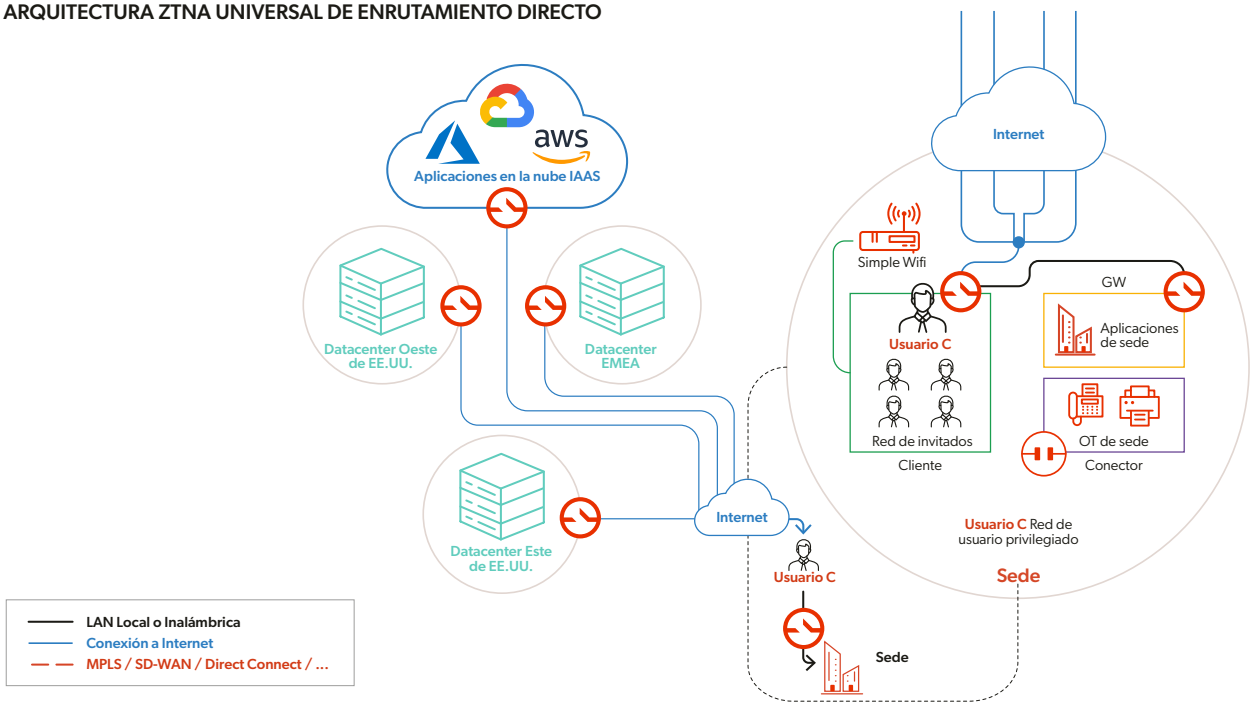
Además, las redes y la seguridad de la empresa se vuelven significativamente complejas en caso de fusión o adquisición. Serían necesarias nuevas conexiones MPLS/SD-WAN y habría que gestionar subredes solapadas para ampliar la tabla de enrutamiento de la empresa. En la mayoría de los casos, el cortafuegos central y el equipo de seguridad de la sucursal son soluciones diferentes, lo que dificulta su integración o resulta costoso sustituirlos según los estándares de la empresa.

ZTNA UNIVERSAL CON ARQUITECTURA DE ENRUTAMIENTO DIRECTO

Revisemos ahora el enfoque universal de ZTNA. Este enfoque se aplicará a todos los usuarios remotos y locales que se conecten a aplicaciones empresariales a través de la conectividad ZTNA. Este caso de uso puede ampliarse a dispositivos IoT, servidores o dispositivos en los que no se haya podido instalar un cliente ZTNA.

Es crucial seleccionar una solución que ofrezca una funcionalidad ZTNA Universal completa, junto con una arquitectura de enrutamiento directo. Normalmente, los protocolos y el número de dispositivos compatibles son mucho más complejos cuando se intenta abordar todos los casos de uso de la empresa, no sólo el acceso remoto de los usuarios. Por lo tanto, es fundamental tener en cuenta estos posibles obstáculos a la hora de seleccionar una solución ZTNA para proteger todas las conexiones de usuario a recurso y de recurso a recurso. Dado que ZTNA es una solución de software que funciona como una superposición de red segura e individual, existe la posibilidad de migrar usuario por usuario y sede por sede, lo que hace que su implantación sea relativamente sencilla y sin interrupciones para la mayoría de las empresas. El único requisito es eliminar o disminuir las interconexiones dedicadas restantes y eliminar determinadas herramientas de seguridad de las sedes una vez que todos los usuarios o toda la oficina hayan completado la migración.

ARQUITECTURA ZTNA UNIVERSAL DE ENRUTAMIENTO DIRECTO



ROI Directo: ZTNA Universal de Enrutamiento Directo

Reducción de costos y casos de uso desbloqueados:

Una vez totalmente desplegado, el tráfico de usuario ya no viaja por las conexiones MPLS/SDWAN entre el centro de datos y las sedes (a través de enlaces privados). En su lugar, todo el tráfico de usuario desde las sedes al centro de datos más cercano utilizará conexiones a Internet normales. Además, si los dispositivos IoT o los servidores locales de la oficina están protegidos por ZTNA universal, toda la conexión puede sustituirse por una simple conexión a Internet, lo que resulta significativamente más rentable.

Como se ha señalado anteriormente, los concentradores VPN se sustituyen por una solución de software puro que facilita la adición de más puntos de entrada sin necesidad de comprar o mantener costosos dispositivos VPN de hardware adicionales. Además, facilita el escalado automatizado de la nube, permitiendo el aprovisionamiento y desaprovisionamiento de recursos en respuesta a la fluctuación de la demanda. Además, durante conflictos geopolíticos, epidemias o catástrofes naturales que afecten a regiones concretas, ahora se puede dar soporte a un cambio repentino al trabajo remoto para todos los usuarios sin ninguna interrupción.

Además, los costos de las herramientas de seguridad de las sedes se reducen considerablemente. Teniendo en cuenta a todos los usuarios, todos ellos pueden trabajar desde una red a Internet inalámbrica (o por cable) de invitados al estilo de un café. Sólo se requiere acceso a Internet, y la red de la sede no tiene acceso a las aplicaciones de la empresa. Cuando el usuario utilice su dispositivo, el cliente ZTNA se conectará a todas las ubicaciones para las que tenga derechos, que podría ser incluso una conexión de red de área local (LAN) dentro de la sucursal para utilizar aplicaciones locales (es decir, impresora local o servidor VoIP). Cuando el usuario se conecta, su dispositivo local puede delimitarse para impedir que otros usuarios vean el dispositivo en la red local. Esto elimina la necesidad de segmentar la red de usuarios diferentes, las soluciones NAC, las complejas configuraciones inalámbricas gestionadas y las complejas reglas de cortafuegos necesarias para garantizar el acceso adecuado de los usuarios.

Con fusiones o adquisiciones, las puertas de enlace adicionales para nuevos centros de datos o ubicaciones en la nube son el único requisito. La incorporación de nuevos usuarios que utilicen una solución de gestión de identidades y accesos (IAM) existente se realiza mediante la implementación del software del cliente ZTNA en los respectivos usuarios. Las soluciones de enrutamiento directo no requieren una tabla de enrutamiento empresarial central, ya que la red de cada usuario se construye según las especificaciones dictadas por el motor de políticas, eliminando así cualquier problema de superposición de subredes IP. Esto agiliza la integración de fusiones y adquisiciones, permitiendo que los primeros usuarios se conecten a la empresa adquirida en cuestión de horas o días, en lugar de meses o trimestres.

La ampliación de los casos de uso para abarcar dispositivos IoT u otros dispositivos mediante conectores también conlleva ahorros de costos y ventajas de seguridad, una mayor eficiencia operativa y una gestión de red más completa. Al integrar los dispositivos IoT en el marco de ZTNA, las organizaciones pueden extender sólidas medidas de seguridad y control de acceso a una gama más amplia de dispositivos conectados. Esta integración permite la aplicación centralizada de políticas, la gestión simplificada del acceso y protocolos de seguridad coherentes en diversos tipos de dispositivos, lo que reduce la complejidad de gestionar la seguridad de muchos puntos finales.

ROI Indirecto: ZTNA Universal de Enrutamiento Directo

Reducción del riesgo de infracciones:

Con SPA, se puede aprovechar la Internet estándar para el tráfico de red crítico de la empresa. Como los puntos de borde son invisibles, se eliminan las posibilidades de ataques DDoS, de parcheo de vulnerabilidades VPN y de día cero. Según informa SecurityWeek, el tiempo de inactividad debido a un ataque DDoS a una aplicación con éxito cuesta a las organizaciones una media de 6.000 dólares por minuto. Como resultado, se pueden conseguir ahorros tanto en la gestión de DDoS como en los costos y riesgos operativos y se puede mantener la continuidad del negocio.

La implementación de políticas de grano fino garantiza que no se conceda a los usuarios un amplio acceso a la red, lo que reduce significativamente el vector de ataque, especialmente si un usuario o dispositivo malicioso intenta conectarse desde una ubicación remota. Además, las políticas de grano fino permiten adaptar los privilegios de acceso en función de factores contextuales, lo que mejora la capacidad de la organización para proporcionar un acceso seguro a los usuarios al tiempo que evita los intentos de acceso no autorizado por parte de agentes maliciosos.

Mayor productividad:

ZTNA Universal agiliza el proceso para que los usuarios autorizados accedan a los recursos necesarios, lo que permite a los propietarios de las empresas acelerar el despliegue de las aplicaciones en producción. También permite a los equipos de seguridad informática proporcionar a terceras entidades un acceso preciso a sistemas críticos, como los sistemas HVAC o los robots de fabricación, reduciendo eficazmente el riesgo de ataques de terceros. El retorno de la inversión se refleja en la mejora de la productividad y la eficiencia de los empleados o contratistas que necesitan un acceso seguro a los recursos de la empresa.

Cumplimiento simplificado:

El ZTNA Universal de enrutamiento directo puede ayudar a las organizaciones a cumplir diversas normativas y estándares, y proporciona políticas basadas en identidades que son más fáciles de auditar en comparación con las reglas y registros de los cortafuegos de red tradicionales. El retorno de la inversión puede medirse a través de la automatización de la recopilación de datos y la elaboración de informes, que a menudo requiere un enfoque manual con los enfoques tradicionales de seguridad de acceso. ZTNA puede ayudar a reducir el alcance del cumplimiento de los informes y evitar el incumplimiento de diversas normativas del sector.

ROI Comprobado de Appgate SDP para la sustitución de NAC:

Un proveedor de soluciones de alojamiento gestionado, que evolucionaba más allá del alojamiento básico, adoptó ZTNA Universal para un control exhaustivo de las comunicaciones de red y los puntos de acceso. La implementación dio como resultado una notable reducción del 98% en los tiempos de aprovisionamiento de usuarios y modificación de accesos. El aprovisionamiento de usuarios en la nube, que antes tardaba tres días, ahora sólo requiere 10 minutos, y las modificaciones de cuentas, de una hora de duración, se completan en 30 segundos. Con la adopción de ZTNA, la organización cambió el 30% de sus sistemas para alinearlos mejor con los principios de Zero Trust. La organización mejoró el acceso a la red y a los sistemas y, al mismo tiempo, aumentó la visibilidad de los eventos de acceso a la red, lo que se tradujo en un descenso significativo de los incidentes de seguridad. Los planes futuros incluyen la eliminación progresiva de un NAC independiente que protege el 60% de sus puntos finales, reduciendo esa cifra a cero.

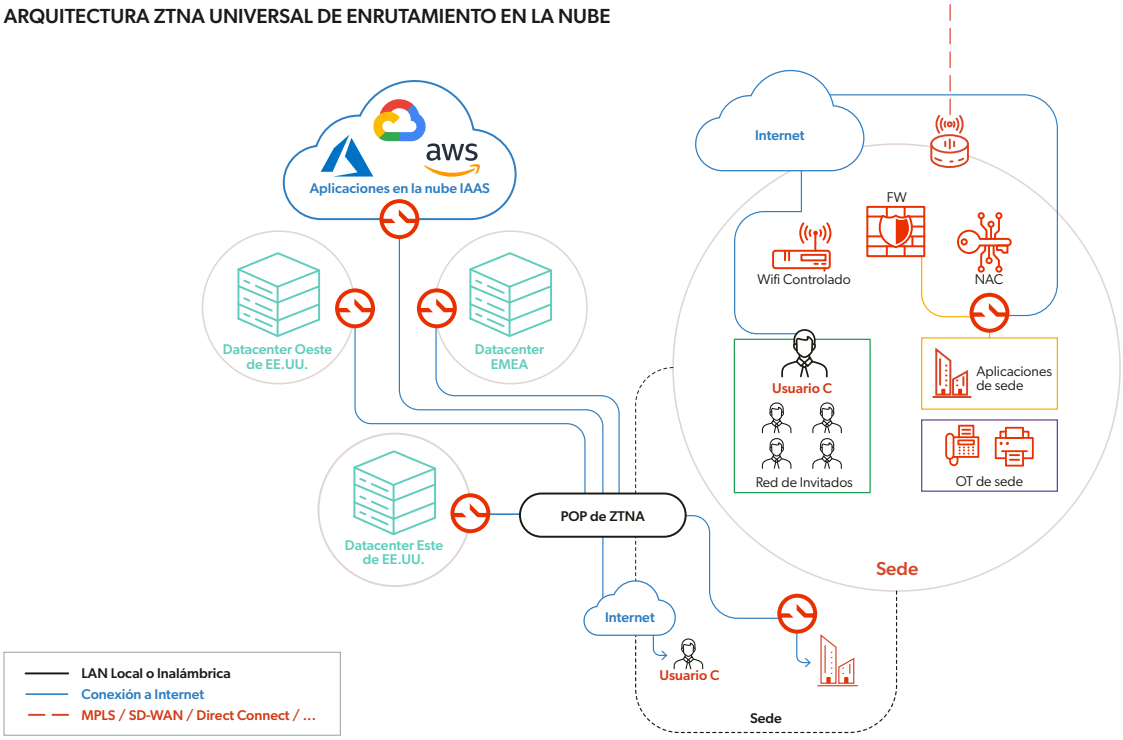
ZTNA UNIVERSAL CON ARQUITECTURA DE ENRUTAMIENTO EN LA NUBE

El despliegue de una solución ZTNA enrutada en la nube puede presentar varios retos que repercuten negativamente en el retorno de la inversión. Estas arquitecturas presentan numerosas restricciones de protocolo, muchas de las cuales no admiten tráfico descendente o no ofrecen opciones sin cliente que se adapten a escenarios IoT. Por ello, las herramientas de seguridad de la sede local no pueden sustituirse. Además, las soluciones ZTNA enrutadas en la nube a menudo se dirigen exclusivamente a aplicaciones basadas en web, excluyendo los recursos no web de la sede local, como servidores de archivos, impresoras y sistemas VoIP.

Esta limitación obliga a redirigir todo el tráfico a la nube y de vuelta a la sede local, lo que provoca un aumento de la latencia y una duplicación de los costos de ancho de banda de Internet, lo que incrementa los gastos operativos.

Además, la conexión compartida desde el POP de ZTNA enrutado en la nube hasta la sede es utilizada colectivamente por todos los usuarios y dispositivos, lo que provoca una degradación sustancial del rendimiento. Aunque algunos proveedores ofrecen un POP local para mitigar este problema, requieren recursos informáticos adicionales e incurren en elevados costos de licencia para cada sucursal, lo que repercute aún más en el retorno de la inversión. En un modelo ZTNA enrutado en la nube, la aplicación del tráfico se gestiona en la nube, lo que supone un riesgo adicional. Si un POP de ZTNA se ve comprometido, podría servir como puerta de entrada para que los atacantes se infiltren en la red.

ARQUITECTURA ZTNA UNIVERSAL DE ENRUTAMIENTO EN LA NUBE



CONCLUSIÓN

La adopción del ZTNA Universal permite a las empresas obtener un ROI sustancial y ser más eficientes desde el punto de vista operativo, especialmente con arquitecturas de enrutamiento directo. La consolidación de políticas de acceso Zero Trust para todos los usuarios y dispositivos proporciona una definición de políticas de acceso unificada y coherente en toda la empresa. Este enfoque garantiza una experiencia de usuario más segura y coherente para los empleados, independientemente de su ubicación de trabajo, al tiempo que permite a los equipos de seguridad agilizar el despliegue y la gestión de los controles y políticas de acceso en toda la red. Mediante una planificación cuidadosa y la asociación con el proveedor adecuado, la adopción de ZTNA Universal ofrece un enfoque rentable para reforzar la seguridad en las redes empresariales más complejas.

Acerca de Appgate

Appgate es la empresa del acceso seguro. Potenciamos la forma en que las personas trabajan y se conectan proporcionando soluciones creadas específicamente sobre los principios de seguridad de Zero Trust. Este enfoque de seguridad definido por las personas permite conexiones rápidas, sencillas y seguras desde cualquier dispositivo y ubicación a cargas de trabajo a través de cualquier infraestructura de TI en entornos de nube, locales e híbridos. Appgate ayuda a organizaciones y agencias gubernamentales de todo el mundo a empezar donde están, acelerar su viaje hacia Zero Trust y planificar su futuro. Más información en appgate.com.

appgate