Guía del arquitecto de redes para adoptar un servicio de acceso a la red de confianza cero

Mejores prácticas para utilizar ZTNA como alternativa a la VPN

zscaler™

Debido a que las aplicaciones privadas se trasladan a la nube y los usuarios trabajan a distancia, las empresas necesitan un servicio que garantice el acceso seguro a las aplicaciones privadas mientras ofrecen una experiencia de usuario sin fricciones. Incluso con todo lo que se ha hablado sobre la seguridad de confianza cero, algunas empresas intentan usar arquitecturas centradas en la red, que dependen de cortafuegos de última generación diseñados para el acceso a la red, como una manera de limitar la conectividad del usuario a las aplicaciones. Estas arquitecturas tradicionales no coinciden con las necesidades actuales y no se diseñaron para conectar a los usuarios autorizados con aplicaciones específicas. Obligan a colocar a los usuarios en la red y a menudo conducen al riesgo de movimiento lateral a otras aplicaciones, direcciones IP expuestas a Internet y ataques DDoS a través de concentradores VPN que se encuentran en el perímetro de la red y escuchan pings entrantes.

Muchas empresas están considerando los servicios de acceso a la red de confianza cero (ZTNA) como una alternativa a la VPN. De hecho, Gartner consideró que, para 2021, el 60 % de las empresas abandonarían su actual VPN por un servicio de ZTNA. Pero la realidad es que en cualquier organización grande (global) incluso un pequeño cambio en la forma en que los usuarios acceden a las aplicaciones puede convertirse en una tarea ingente. Este documento le ayudará a comprender por dónde empezar para poder adoptar ZTNA, rápidamente y sin interrupciones para el negocio.

En esta guía trataremos lo siguiente:

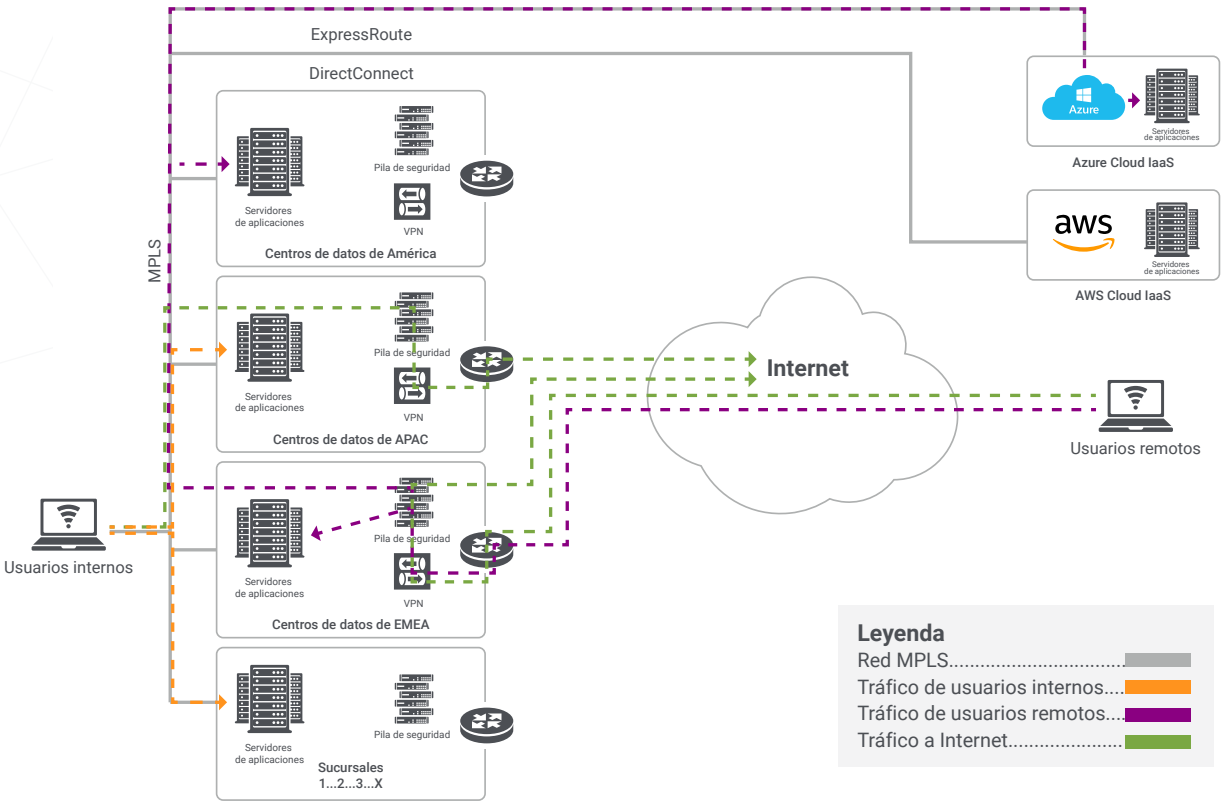
- Diferencias arquitectónicas entre la tecnología de acceso tradicional y ZTNA
- Un vistazo a la arquitectura de referencia para implementar ZTNA
- Las tres fases que hay que tener en cuenta al adoptar ZTNA en su empresa
- Consejos profesionales y consideraciones para aprovechar al máximo su implementación de ZTNA

Antes de comenzar, tómese unos minutos para leer la entrada de blog llamada "Mitigar los riesgos a través del perímetro definido por software". Esta entrada proporciona una visión general inicial de los servicios de acceso a la red de confianza cero.

Ahora es el momento de explorar la arquitectura ZTNA como medio para conectar a los usuarios autorizados con aplicaciones privadas específicas, sin necesidad de que se encuentren en la red.

¿Dónde está usted hoy? - Un repaso de la VPN en la empresa

Vemos que la arquitectura más común en muchas organizaciones se puede representar en este diagrama de alto nivel. Sí, me doy cuenta de que el número y la ubicación de los centros de datos, los enrutadores, los cortafuegos, los concentradores VPN y la red MPLS no serán idénticos a los del diagrama, pero creo que proporcionan una representación lo suficientemente acertada de los componentes. Hay muchos otros dispositivos de red y de seguridad que las organizaciones han desplegado, incluidos proxies en línea, sandboxes, cortafuegos L7, soluciones AV y DLP, etc. En aras de la simplicidad, he consolidado todo el concepto de seguridad en Internet como pila de seguridad en los diagramas.



Hay varios aspectos que quiero destacar en este tipo de arquitectura tradicional:

01 Los usuarios remotos utilizarán la VPN para entrar en uno de los centros de datos y se colocarán en la red corporativa. En mi experiencia con muchas organizaciones, la red es relativamente plana, las ACL son bastante limitadas, por lo que exponen toda la infraestructura corporativa del centro de datos y las redes a cada usuario remoto.

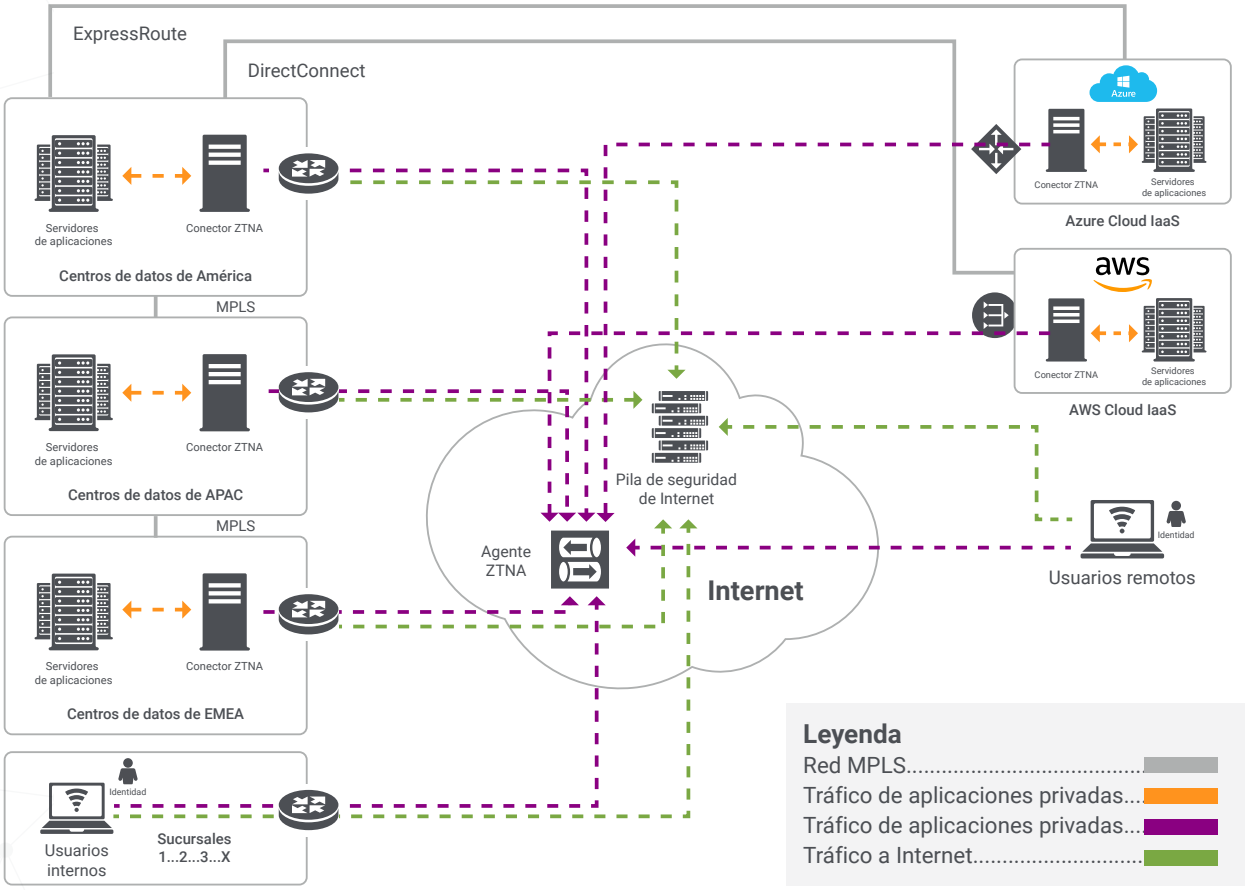
02 Todo el tráfico de Internet de los usuarios remotos retornará al centro de datos para su inspección utilizando la pila de seguridad (hardware) que la organización posee. Esto se conoce como VPN de túnel completo; es ideal para los equipos de seguridad que necesitan garantizar la seguridad de los usuarios cuando están fuera de la red corporativa, pero puede tener un impacto negativo en la experiencia del usuario cuando todas las aplicaciones de Internet/SaaS tienen que retornar en lugar de salir localmente. Muchos usuarios disponen ahora de conexiones domésticas a Internet de banda ancha más rápidas que algunas líneas WAN corporativas (incluso en una zona rural, por ejemplo, del estado de Tennessee, tengo una conexión de fibra de 1 Gbps a través de mi ISP).

03 Los usuarios internos suelen estar en redes de dispositivos/usuarios, ya sean físicas o inalámbricas, pero por lo general pueden enrutar/conectarse a todas las redes de centros de datos, ya que estas redes son tradicionalmente "de confianza". El acceso a las rutas de aplicaciones internas a través de la LAN y las aplicaciones de Internet/SaaS pasará por la pila de seguridad antes de dirigirse al ISP. El problema de esta forma de proceder es la suposición incorrecta de que solo porque usted es el "dueño" y controla la red debe confiar automáticamente en todos los usuarios y dispositivos en ella.

Tenga en cuenta el acceso entrante requerido desde Internet (VPN) para el acceso remoto y la posibilidad de que los usuarios internos se comuniquen directamente con todos los servidores de aplicaciones, independientemente de su identidad.

Una arquitectura de referencia para proporcionar acceso a las aplicaciones internas sin aumentar el riesgo

El objetivo final de una arquitectura definida por software es desvincular el acceso a las aplicaciones del acceso a la red. Ya no será necesario colocar a los usuarios en la red, las aplicaciones privadas solo son accesibles para los usuarios autorizados, las direcciones IP nunca están expuestas a Internet y desaparece la complejidad de administrar segmentos de red, las políticas de FW y las ACL. El siguiente diagrama muestra un aspecto simplificado del resultado final.



Con esta nueva arquitectura definida por software, notará que hay una separación clara de redes de centros de datos/aplicaciones, usuarios remotos y usuarios internos. No importa si su organización tiene solo dos centros de datos con sede en EE. UU., una docena de centros de datos globales, algunos entornos Azure/AWS/GCP, etc... los resultados son bastante claros:

01 Las redes privadas, como MPLS o incluso las VPN de sitio a sitio, solo deben ser necesarias entre centros de datos y entornos IaaS en la nube donde se requiere comunicación de servidor a servidor. Si su organización ha trasladado la capa web del sitio www a AWS, pero la base de datos SQL backend sigue estando en un centro de datos físico, sigue necesitando conectividad privada (baja latencia, gran ancho de banda) entre esas ubicaciones.

02 El acceso remoto ya no requiere conectividad de entrada para los usuarios, como vpn.company.com. Esta arquitectura sitúa el plano de orquestación (control) en la nube, donde se termina la comunicación de los usuarios. Las puertas de enlace, conocidas en el mundo de Zscaler como ZPA App Connectors, no requieren puertos de escucha entrantes, un registro público de IP/DNS. Estos conectores se comunican de forma saliente a través de TLS con el plano de orquestación basado en SaaS. Las aplicaciones internas solo se intermedian una vez que la identidad de los usuarios ha sido verificada y cotejada con las políticas de acceso.

- Si un usuario puede acceder a una aplicación/recursos internos, el plano de orquestación cambia las conexiones TLS salientes entre los conectores y los dispositivos del usuario. Sin embargo, este usuario no se coloca en la red, por lo que las aplicaciones basadas en DNS son ofuscadas, lo que significa que las verdaderas direcciones IP privadas de los servidores de aplicaciones no están expuestas a los dispositivos del usuario. En lugar de ello, se crea dinámicamente una dirección IP sintética en el cliente para cada aplicación a la que accede.

- Si a un usuario no se le permite acceder a una aplicación interna, nunca se habrá generado tráfico de red que llegue al centro de datos. La solicitud se bloquearía en la nube, por lo que así se eliminaría el riesgo de incluso permitir que los usuarios lleguen a la "puerta principal" de los servidores de aplicaciones críticas. La forma más fácil de verlo es parar a los usuarios en la nube antes de poder establecer una sesión SSH o RDP en un servidor. Aunque es muy probable que el usuario no pueda autenticar la sesión SSH/RDP (salvo mediante la fuerza bruta o el robo de credenciales), esta arquitectura elimina este riesgo. ¿Lo mejor de todo? Cada uno de estos intentos se registra y permite a su organización de seguridad supervisar de forma proactiva (y reactiva) lo que los usuarios intentan hacer. Un ejemplo sería enviar todos los registros a su SIEM, como Splunk, y crear una alerta si algún usuario genera X número de políticas bloqueadas en X número de minutos en los mismos servidores/puertos, como intentar SSH en sap.company.com 20 veces en 5 minutos. Si el usuario está bloqueado por la política, entonces usted está seguro y puede llegar proactivamente a ver si el dispositivo del usuario está comprometido o si el usuario tenía intenciones maliciosas. Si el usuario no estuviera bloqueado por la política, las sesiones SSH se habrían realizado, pero el servidor rechazaba las credenciales incorrectas, lo que significa que este usuario estaba autorizado pero había olvidado la contraseña de administrador (root).

03 Todas las redes de usuarios deben tratarse como cafeterías con Internet o redes wifi de invitados. Tanto si el usuario está en el edificio principal de la sede, en una sucursal, en una planta de fabricación o simplemente de viaje, nunca debería haber una razón para colocar al usuario en la red donde pueda explorar/enrutar sus servidores de aplicaciones y centros de datos. Es importante tener en cuenta que los sitios de algunas sucursales pueden tener requisitos ajenos al acceso de usuario a aplicación. En tal caso, los dispositivos IoT y las comunicaciones de servidor a servidor necesitarían conectividad de red privada. Sin embargo, aunque exista este requisito, es mejor separar estas redes de las redes de los usuarios.

04 El acceso a Internet, también conocido como la pila de seguridad, también debe modernizarse para permitir la mejor seguridad y experiencia del usuario. Al desvincular a los usuarios de la red, debe explorar el envío de tráfico de Internet directamente desde los usuarios en lugar de enviarlo a un centro de datos centralizado para su inspección. Para las sucursales, puede ser tan sencillo como usar un enrutador, cortafuegos o dispositivo SD-WAN existente para dirigir todo el tráfico de Internet a una solución de seguridad en la nube, como la plataforma Zscaler Internet Access. La pila de seguridad completa se ofrece como servicio y tiene más de 100 ubicaciones globales, lo que significa que puede enviar todas las ubicaciones corporativas a los sitios de Zscaler más cercanos para su inspección. Incluso en el caso de que un usuario esté de viaje, el cliente unificado de Zscaler App (un agente de reenvío ligero implementado en los dispositivos móviles y portátiles de los usuarios) puede proporcionar la experiencia del usuario necesaria (enviando el tráfico de Internet localmente al nodo Zscaler más cercano en lugar de retornarlo), pero aun así proporcionar al equipo de TI los controles de seguridad y visibilidad necesarios.

Las tres fases para hacer posible la adopción de una arquitectura ZTNA

Los arquitectos se preguntan a menudo lo siguiente: "¿Cuál es la mejor manera de empezar?" Una de mis respuestas favoritas es que "depende". Sé que muchos ingenieros y arquitectos pueden sentirse identificados con esto porque se pueden lograr muchos resultados diferentes en función de las necesidades, los requisitos y la configuración específicos. Sin embargo, es nuestra responsabilidad proporcionar las recomendaciones de mejores prácticas a las organizaciones en este recorrido. Quiero advertir que el enfoque del recorrido por etapas que se trata en esta sección no es un conjunto concreto de pasos que cada organización debe seguir. Es un enfoque de alto nivel que hemos observado en muchos clientes para cumplir con los requisitos actuales, pero al mismo tiempo permitir que la organización adopte el concepto de red de confianza cero. La confianza nunca es implícita y el acceso es adaptable, en función de las políticas contextuales establecidas por los administradores que tienen en cuenta el usuario, el dispositivo, el servicio, etc.

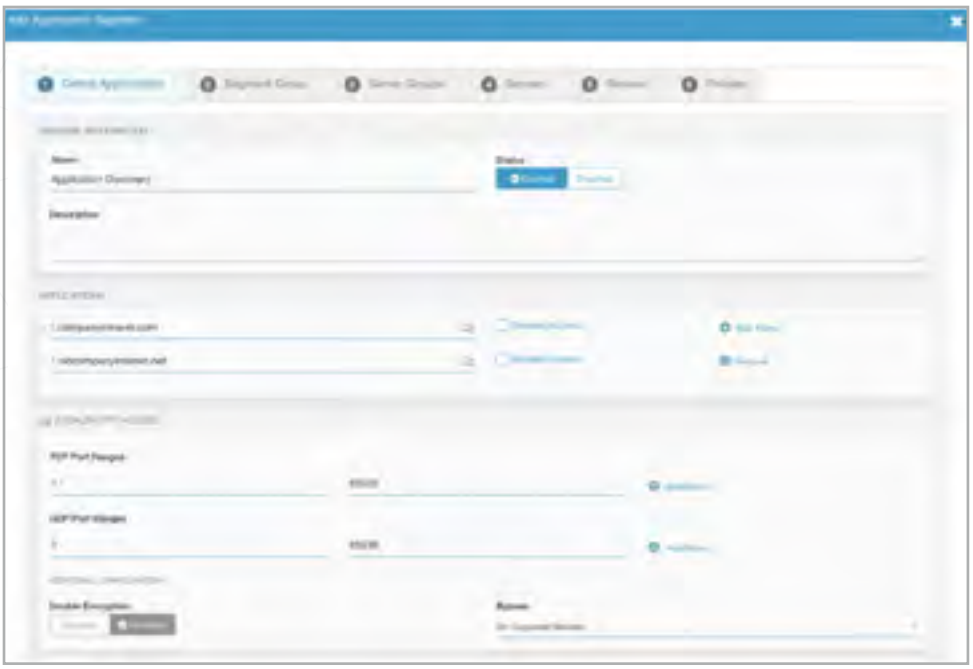
El enfoque se asemeja en parte a dar pequeños pasos: se empieza con los usuarios remotos, se desarrollan segmentos y luego se aprovecha ZTNA para el acceso a las aplicaciones privadas para todos los usuarios, independientemente de su ubicación. Deberá tener en cuenta la forma en que los usuarios acceden a las aplicaciones y servicios, la distribución (cantidades y tipos) de sus ubicaciones (centros de datos, entornos IaaS en la nube y ubicaciones físicas desde donde trabajan los empleados) y cualquier cronograma basado en proyectos. En muchos casos, una actualización de la VPN podría servir como catalizador para adoptar ZTNA en lugar de adquirir una VPN de nueva generación o "siempre activa", que trae consigo los mismos retos de su VPN actual.

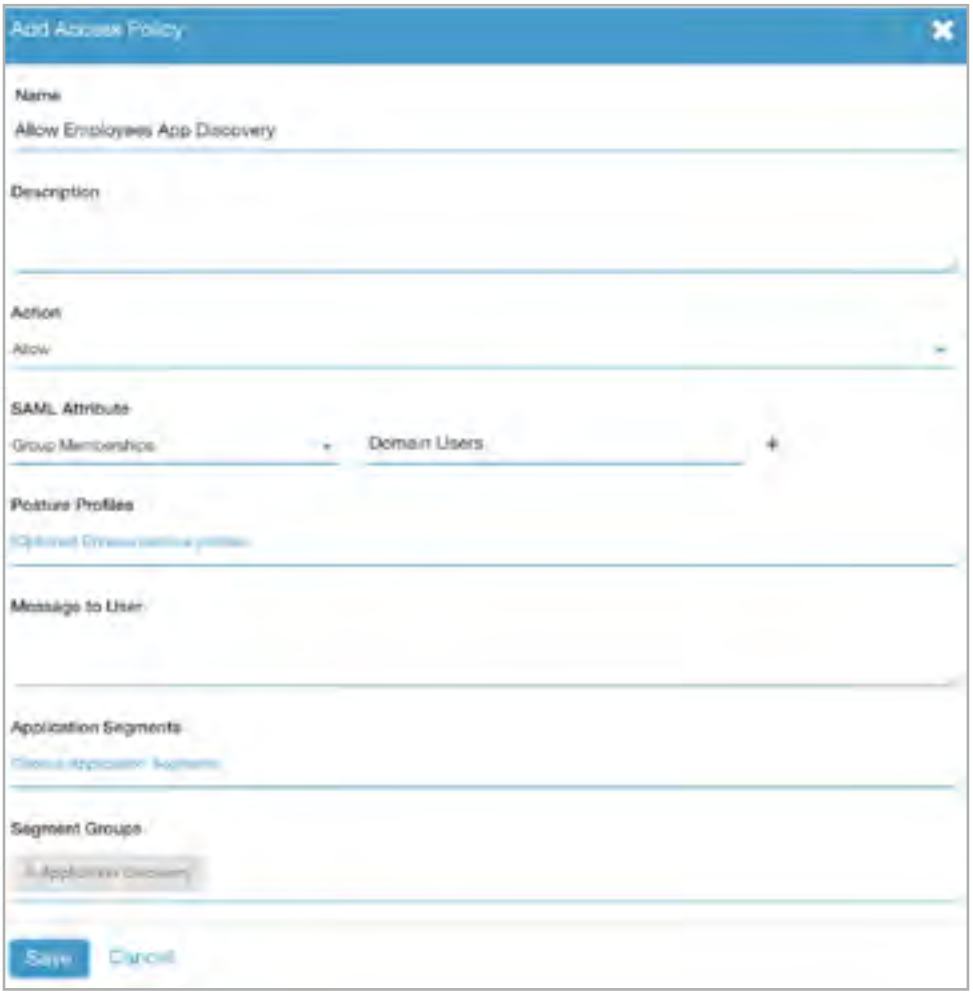
Fase 1 Conseguir desplegar ZTNA para el acceso remoto y el descubrimiento de aplicaciones

En esta fase, querrá empezar por sustituir la solución VPN de acceso remoto existente. Para ello, es posible que tenga que desplegar ZTNA con niveles de acceso similares a los de su actual VPN de acceso remoto. Esto es clave, ya que quiere asegurarse de que su nueva iniciativa no sea vista como un inhibidor de la productividad de los usuarios remotos.

También tendrá que entender qué aplicaciones privadas se están ejecutando en su entorno para reducir su superficie de ataque y erradicar la TI en la sombra. Es muy probable que haya muchas más aplicaciones de las que usted conoce actualmente. Nuestra solución llamada Zscaler Private Access (ZPA) resuelve esto con nuestra función Application Discovery (descubrimiento de aplicaciones). Es imposible conocer todas las aplicaciones/servicios internos a los que cada usuario necesita acceder, por lo que Application Discovery le permite básicamente trabajar con comodines, como *.company.com, *.company.net, todos los puertos TCP y UDP.

Una vez que un usuario se ha inscrito correctamente en el servicio, el cliente detecta automáticamente cuando el usuario ya no está en la red corporativa; ahora todas las aplicaciones internas circularán a través de ZTNA cuando el usuario está fuera de la red. Ya no es necesario lanzar un cliente VPN y el usuario puede acceder a los recursos internos como antes. Todos estos registros de acceso se encuentran en la consola de administración de ZPA y también se pueden transmitir casi en tiempo real a su SIEM de elección, lo que permite una visibilidad granular de las aplicaciones a las que acceden los usuarios.



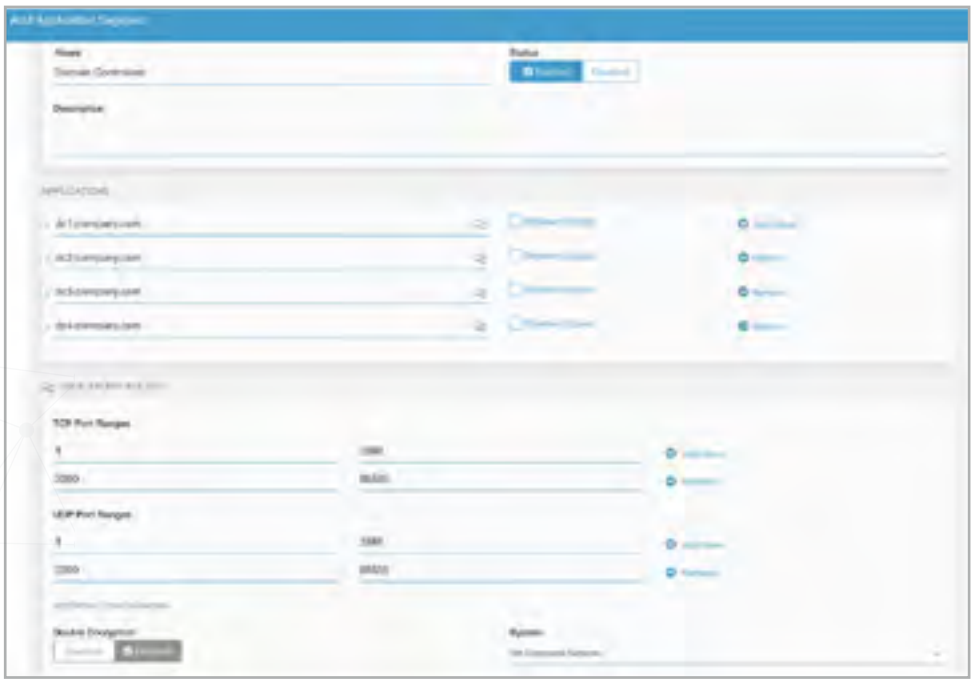


Dado que la red privada interna (MPLS, VPN de sitio a sitio) probablemente aún exista, el cliente de Zscaler App desactivará automáticamente ZPA cuando el usuario vuelva a la red corporativa. Ahora, todo el acceso a las aplicaciones internas se produce en la LAN sin Zscaler en la ruta.

Fase 2 Aprovechar la microsegmentación para garantizar la conectividad con menos privilegios

En esta fase, deberá definir políticas que separen las aplicaciones privadas en segmentos y proporcionar acceso a esos segmentos a través de atributos de identidad de usuario.

Puesto que las grandes organizaciones pueden tener cientos o miles de aplicaciones/servicios únicos, muchas organizaciones pueden querer empezar con la segmentación de los puertos de gestión, como TCP 22 (SSH) y TCP/UDP 3389 (RDP), y proporcionar acceso exclusivamente a estos puertos de forma global para los usuarios de TI. Por supuesto, siempre pueden existir requisitos únicos, pero esta segmentación puede ayudar a reducir la superficie de los usuarios que se conectan a servidores a los que ni siquiera deberían poder acceder. Por ejemplo, es muy probable que su personal de ventas no pueda acceder a TCP 3389 en un servidor de Windows que aloja su aplicación SAP; solo debería acceder a la parte web de front-end, que sería la misma que la de los servidores, pero únicamente en puertos TCP 80/443.



Lo ideal es que los servidores de infraestructura, que pueden ser controladores/servicios de dominio, clientes de software de seguridad, clientes de despliegue de software, etc., se puedan segmentar fácilmente, ya que los hosts son bien conocidos.

La segmentación de las aplicaciones es un proceso continuo, y una recomendación general es priorizar las aplicaciones que son más importantes para la empresa y a las que solo deberían acceder los usuarios conocidos.

A medida que se segmentan las aplicaciones, se eliminan del grupo de descubrimiento de aplicaciones. Esto significa que puede mezclar y combinar para garantizar que los usuarios puedan seguir accediendo a las aplicaciones de sus dominios que no ha definido explícitamente, pero que también puedan acceder a las aplicaciones conocidas en los puertos de servicio requeridos.

NOTA: No olvide también la seguridad en Internet

Aunque en esta guía nos centramos en las aplicaciones privadas, es importante darse cuenta de que también es igual de importante proporcionar una pila de seguridad para todo el tráfico que se dirige a Internet. Muchas organizaciones están explorando una pila de seguridad entrante y saliente más moderna que esté totalmente basada en la nube en lugar de depender de aparatos o dispositivos virtuales (es decir, cortafuegos). En Zscaler nuestra solución de seguridad en la nube saliente se llama Zscaler Internet Access (ZIA).

Fase 3 ZTNA para acceder a aplicaciones privadas para todos los usuarios (no solo los remotos)

Ahora ya está usted listo para la fase final. Esto significa que a partir de ahora todo el acceso a las aplicaciones privadas se basa en una configuración precisa que permite la conectividad explícita y de mínimos privilegios, por defecto.

ZPA proporciona esto a través de la conectividad de dentro hacia afuera a través de microtúneles de doble cifrado TLS que van variando en cada sesión y crean un segmento seguro único entre un usuario autorizado y una aplicación privada específica.

Quizá recuerde que anteriormente mencioné que Zscaler App puede detectar la red corporativa, ¿verdad? Esto significa que en ZPA, cada segmento de aplicación tiene una opción de configuración para (1) omitir ZPA cuando está en la red corporativa, (2) omitir siempre ZPA o (3) nunca omitir ZPA. En la fase 1 ha desplegado segmentos de aplicaciones utilizando la opción 1, pero ¿qué pasa con el acceso seguro no solo de los usuarios remotos, sino de todos? Para ello, simplemente cambie los segmentos de la aplicación a no omitir nunca ZPA. Esto significa que incluso cuando los usuarios están en una oficina física, todo el acceso a los recursos internos se gestiona a través de esta solución explícita de arquitectura de confianza, nunca se enruta simplemente en la LAN directamente a los servidores de aplicaciones en su centro de datos.

Pasar de

A

Fácil, ¿verdad? Bueno, creo que los desafíos relacionados con este cambio están fuera de nuestra propia plataforma. Como quizá recuerde, el objetivo final suele ser eliminar completamente las redes del servidor de aplicaciones/centro de datos de todas las redes de usuarios. Esto significa que no hay conectividad desde ninguna sucursal, planta de fabricación, etc., al centro de datos (para que quede claro, quiero decir que no hay conectividad desde las redes de los usuarios en estas ubicaciones).

Reflexiones finales y consejos profesionales:

Puede ser más fácil comenzar con una nueva oficina pequeña que aún no esté en la red. Abra esa oficina con solo una conexión a Internet de banda ancha. Haga que todo el tráfico que llega a Internet vaya a una plataforma de seguridad en la nube (como ZIA) y que todo el tráfico de aplicaciones privadas fluya a través de la plataforma ZPA.

Trate la nueva oficina como si fuese un cibercafé. De nuevo, tenga en cuenta que hoy en día podemos proporcionar esta conectividad para los usuarios a las aplicaciones; es probable que algunas ubicaciones, como una planta de fabricación con sensores, dispositivos IoT y servidores, necesiten comunicarse con sus centros de datos a través de MPLS o VPN privados. Trate las redes de esos lugares como centros de datos, y simplemente remita a los usuarios desde ellas; todos los usuarios estarán en "wifi de invitados" y el acceso a la aplicación interna estará permitido a usuarios autorizados.

Al final, hay mucha expectación y entusiasmo en torno a las arquitecturas ZTNA, pero el verdadero objetivo es ofrecer la experiencia que quieren los usuarios, con la seguridad necesaria cuando se trata de aplicaciones privadas. Su organización tardará en adoptar este nuevo método, pero usted, como arquitecto de redes, puede sentar las bases (plataformas) para facilitarlo.

Puede experimentar ZPA por sí mismo registrándose para una prueba alojada de 7 días en **https://www.zscaler.es/zpa-interactive.**

Zscaler, Inc.
110 Rose Orchard Way
San José, CA 95134
+1 408.533.0288
www.zscaler.es