Arquitectura de confianza cero
Qué es y cómo conseguirla

Alcatel·Lucent Enterprise

Libro electrónico
Arquitectura de confianza cero

Contenido

¿Qué es la arquitectura de confianza cero?

¿Qué significa arquitectura de confianza cero (ZTA)? Significa que se debe autenticar y autorizar a cada usuario y dispositivo antes de permitir el acceso a los datos. Es una estrategia de "no confiar en nadie; autenticar todo".

Una analogía nos servirá de ayuda en este caso.

Si pensamos en la seguridad tradicional como una fortaleza que protege a un pueblo, construiríamos el muro de la fortaleza (también conocido como el cortafuegos) alrededor del pueblo (también conocido como la empresa). Todo lo que está fuera de la fortaleza no es de confianza y se examina, mientras que todo lo que está dentro es implícitamente fiable y está permitido. Este límite de confianza es tanto físico como implícito, dependiendo del lado de la fortaleza en el que se encuentre, ya que mientras se esté en el lado "correcto" de la muralla, no se requieren más comprobaciones. Si pensamos en este enfoque la red empresarial, puede haber alguna segmentación básica en forma de VLAN, SSID, subredes o interfaces vinculadas a un cortafuegos, pero esta segmentación es estática y tiene más que ver con la escalabilidad y la capacidad de gestión de la red que con la seguridad.

Sin embargo, hoy en día, el enfoque del cortafuegos (fortaleza) es cada vez menos eficaz por sí solo debido a varios motivos. El primero es la movilidad. Los usuarios se conectan a otras redes de fuera de la empresa y pueden traer consigo las amenazas. En segundo lugar, los invitados no son necesariamente dignos de confianza. Se podría argumentar que incluso no se debería confiar ciegamente en los empleados (los que están dentro de la fortaleza). En tercer lugar, cada vez se añaden más dispositivos IoT a la red. Estos plantean mayores riesgos de seguridad porque pueden no estar sancionados ni gestionados por TI y suelen carecer de capacidades de seguridad. Con el enfoque tradicional de "fortaleza/aldea", "cortafuegos/empresa", si un usuario o dispositivo se ve comprometido, hay poco o nada que impida que la amenaza se extienda a otros usuarios y dispositivos. Una vez dentro, hay libertad de movimiento.

En la analogía de la fortaleza, si lo único que protege al pueblo de los intrusos es la muralla, el día que los intrusos aprendan a escalar el muro de la fortaleza, y lo harán, habrá una carnicería.

La pregunta es: ¿qué podemos hacer al respecto? Pensemos en esto desde el enfoque de "no confiar en nadie", o "confianza cero".

En la confianza cero, no se confía en ningún usuario o dispositivo. Ya sea en las instalaciones o fuera de ellas, todos ellos pasan por los mismos controles. No se puede confiar en los usuarios internos. Se autentican y autorizan todos los accesos.

En la analogía de la fortaleza significaría que, además de la fortaleza que protege al pueblo de las amenazas exteriores, cada casa, cada edificio, tiene su propia seguridad para protegerse de los riesgos procedentes de los actores maliciosos que viven dentro de la fortaleza. En cuanto a la empresa, lo que se conoce como microsegmentación definida por software va un paso más allá. Además de la fortaleza y la seguridad alrededor de los edificios, también tenemos guardias de seguridad personales que nos siguen a todas partes. Y allá donde vayamos, nos pedirán el pasaporte. En la red empresarial, este límite de confianza es difuso, está distribuido y es móvil. No está vinculado a una ubicación específica, puerto de conmutador o VLAN en particular. Depende de la identidad, del dispositivo, de la situación y de la hora del día, entre otras cosas. Está definido por software y se ajusta sobre la marcha. En este enfoque, los componentes se tienen que gestionar y deben ser capaces de reaccionar y reconfigurarse según sea necesario para responder a las amenazas o a los cambios en el flujo de trabajo.

Comprender la macrosegmentación y la microsegmentación

En una arquitectura de confianza cero hay dos tipos de segmentación, la macrosegmentación y la microsegmentación. En nuestra analogía, el muro de la fortaleza es la macrosegmentación, mientras que los guardias de seguridad personal son la microsegmentación.

En la **macrosegmentación**, la red física se divide en diferentes segmentos lógicos. Estos segmentos pueden ser una VLAN, una combinación de VLAN y VRF, una VPN cuando hablamos de la conexión de ruta más corta (SPB), MPLS, o incluso VXLAN o túneles GRE. Todo el tráfico entre usuarios o dispositivos en diferentes segmentos está controlado por un cortafuegos. Todas las empresas utilizan la segmentación de alguna u otra forma, pero no siempre por motivos de seguridad. A menudo, este tipo de segmentación se utiliza por razones de escalabilidad, administrativas u organizativas. Si dos dispositivos están asignados a diferentes VLAN, pero pueden comunicarse sin pasar por un cortafuegos, entonces significa que están en el mismo macrosegmento. Un ejemplo típico de este tipo de segmentación es ejecutar la telefonía IP en VLAN y VRF separadas que están lógicamente aisladas de los PC.

La cuestión es ¿cómo asignar usuarios o dispositivos a estos segmentos? Aunque se puede hacer de forma estática, por ejemplo, mediante puerto del conmutador o mediante SSID, en realidad es una forma obsoleta de hacer las cosas. Es una forma demasiado rígida y no augura nada bueno para los usuarios móviles. Lo ideal es tener un sistema de autenticación definido por software, de modo que cuando un usuario o dispositivo se conecta y se autentifica, se le asigna un perfil. El perfil aprovisionará al usuario o al dispositivo en el segmento correcto, independientemente de la ubicación física, del puerto del conmutador o del SSID.

Aunque la macrosegmentación tiene ventajas de seguridad, en muchos casos se hace por razones organizativas o administrativas. Por ejemplo, las cámaras y las cerraduras de las puertas están controladas por el grupo de seguridad de acceso, mientras que los termostatos están controlados por el grupo de mantenimiento del edificio.

La microsegmentación va un paso más allá. No todos los usuarios son iguales y no todos tienen una necesidad legítima de acceder a todos los recursos. El mismo perfil que asigna a los usuarios a un segmento también incluye un conjunto de políticas que añaden un control detallado de los privilegios de los usuarios/dispositivos que son diferentes según los roles, como RRHH vs. finanzas. Esto se conoce como **acceso basado en funciones** y está directamente relacionado con el **principio de privilegios mínimos**. Por eso, aunque las cámaras y las cerraduras de las puertas estén en el mismo segmento, no tienen por qué utilizar los mismos recursos. La cámara necesita comunicarse con el grabador de vídeo, mientras que la cerradura tiene que comunicarse con su servidor. No es necesario que una cámara se comunique con una cerradura de puerta, al igual que no es necesario que una cerradura de puerta se comunique con otra. Estos permisos detallados se implementan a través de políticas que forman parte del perfil y que se aplican de forma dinámica al dispositivo después de la autenticación. La microsegmentación debe ser definida por software por varios motivos. Ni los usuarios ni los dispositivos IoT son estáticos, sino que se mueven, se conectan y se desconectan, por lo que las políticas no pueden estar atadas a una ubicación o a un puerto. De hecho, las configuraciones de microsegmentación deben ser dinámicas en función de la combinación de múltiples factores, entre ellos, la identidad del usuario o del dispositivo, la hora del día y la ubicación.

En resumen, cuando la comunicación entre diferentes segmentos está controlada por un cortafuegos, se trata de una macrosegmentación. Cuando la comunicación dentro del mismo segmento está controlada por las políticas de control de acceso a la red (NAC, Network Access Control) asociadas al dispositivo o al rol del usuario, se trata de una microsegmentación.

Por qué necesita ambas

¿Qué ocurre si se utiliza solamente un tipo de segmentación?

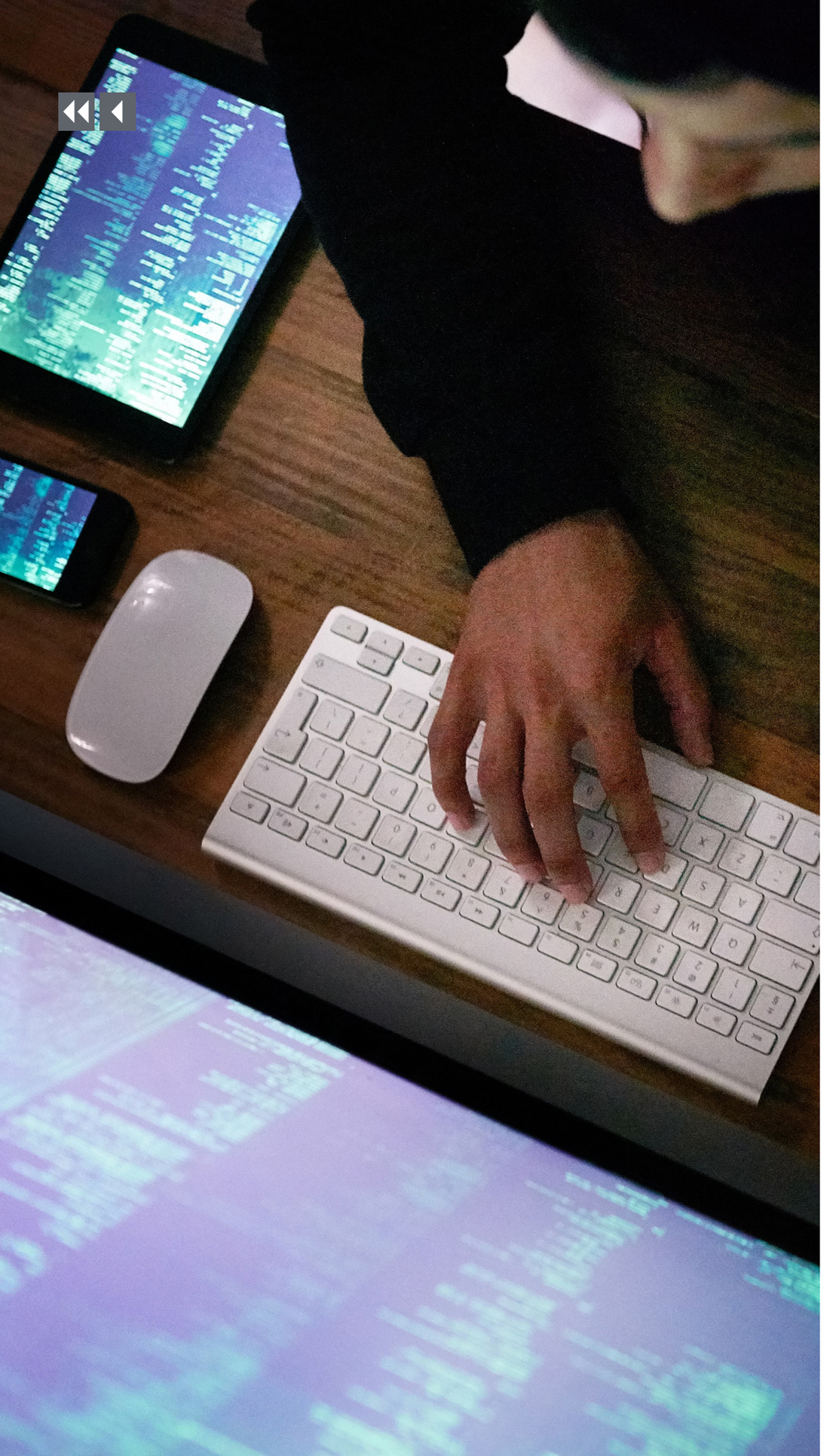
Echemos un vistazo a la macrosegmentación. El problema que surge al utilizar únicamente este enfoque es que el cortafuegos se convierte en un cuello de botella, ya que todo el tráfico debe pasar por él para su autenticación y autorización. Esto puede provocar problemas de rendimiento. Puede desplegar más cortafuegos en la capa de distribución, lo que puede resultar bastante costoso y no implica necesariamente una mejora del rendimiento, ya que los cortafuegos no presentan velocidad de cable. Además, en la actualidad se dispone de múltiples puntos de aplicación de las políticas y múltiples lugares para mantenerlas actualizadas, lo que hace que su gestión sea complicada.

La otra opción, utilizar solamente la microsegmentación, también resulta problemática. Si la única aplicación de políticas se realiza a través de las políticas de NAC, las listas de políticas se vuelven más largas y complejas, pudiendo agotar los límites de capacidad del dispositivo.

La conclusión es que es mejor tener un equilibrio entre estas dos formas de segmentación. Esto permite que el cortafuegos controle el tráfico entre diferentes segmentos (vertical) y que las políticas de NAC controlen el tráfico dentro de un determinado segmento (lateral).

Al combinar ambas formas, se puede hacer frente a las amenazas a la seguridad que se extienden de un segmento de seguridad a otro, así como a las que se desplazan lateralmente por el mismo segmento. De forma más tangible, la microsegmentación es lo que impide que un atacante que ha logrado comprometer una cámara, utilice la brecha como pivote para comprometer otros recursos, como la cerradura de una puerta.

El objetivo es autenticar cada conexión y asignar permisos a cada usuario o dispositivo. Esto significa utilizar tanto la segmentación para evitar la propagación de las amenazas a través del movimiento lateral, como la supervisión continua y la puesta en cuarentena de cualquier usuario o dispositivo que no cumpla las normas.



Cómo conseguirla

En una situación de nueva implementación, sería relativamente fácil construir una arquitectura de confianza cero utilizando la microsegmentación desde el principio. Sin embargo, en situaciones de antigua implementación, la adaptación de la red con microsegmentación puede dar lugar a que los usuarios, los dispositivos y las aplicaciones se queden fuera de la red debido a autenticaciones fallidas o políticas incompletas. Sería difícil o incluso improbable que una empresa pudiera migrar de golpe, en un solo ciclo de actualización.

En los entornos de antigua implementación, habrá un período durante el cual coexistirán las arquitecturas de confianza no cero y de confianza cero, y la migración se producirá de uno en uno, esto es, una capa o una ubicación cada vez. Lo importante es asegurarse de que los elementos de la infraestructura que se implementan, y la forma en que lo hacen, sean flexibles y capaces de funcionar en modo de confianza cero o microsegmentado cuando otros elementos de la infraestructura estén listos. Esto significa que la infraestructura tendrá que interoperar con los componentes existentes y futuros.

Metodología

Hay cinco pasos hacia una arquitectura de confianza cero: supervisar, validar y evaluar, planificar, simular y aplicar.

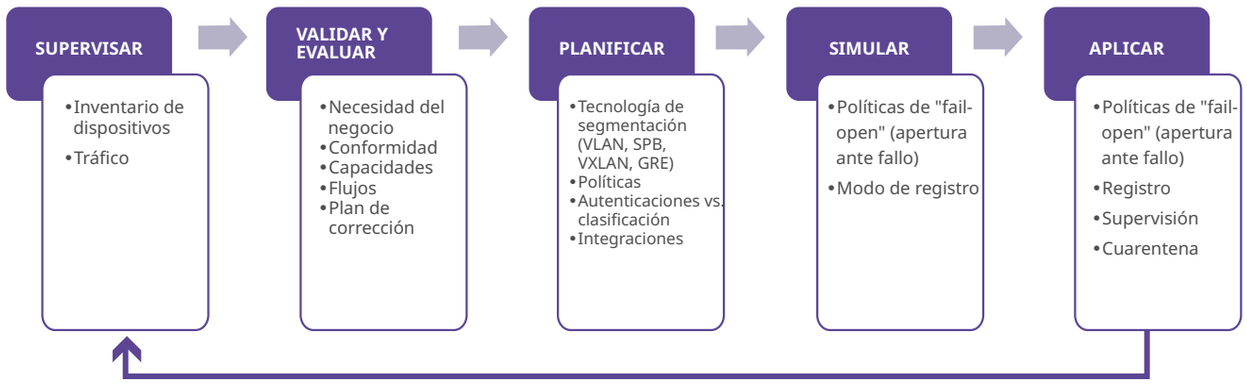


Figura 1 - Metodología

Paso 1: supervisar

Antes de hacer cualquier otra cosa, hay que empezar a supervisar y construir un mapa y un inventario de lo que se tiene en la red.

La migración a ZTA requiere un conocimiento detallado de los activos (físicos y virtuales), de los sujetos (incluidos los privilegios de los usuarios) y de los procesos de negocio que tocan o se montan en la red. Los conocimientos incompletos suelen conducir al fracaso cuando se deniega el acceso por falta de información. Esto es especialmente un problema si hay "TI en la sombra" o "IoT en la sombra" desconocidos dentro de la organización.

Comience supervisando los dispositivos y los flujos de tráfico. Cree un informe de inventario con todos los dispositivos vistos en la red, categorizados por tipo de dispositivo, fabricante, modelo y sistema operativo, entre otros. El informe también debería mostrar dónde y qué puerto del conmutador o SSID se vio por última vez el dispositivo. Esta información puede obtenerse de elementos como la dirección MAC, la firma DHCP y el agente de usuario HTTP.

La mayoría de las herramientas de terceros solamente proporcionan una dirección IP, pero no el tipo de equipo. Sería ideal disponer de una herramienta para crear un inventario de IoT/dispositivos que facilite la creación rápida y sencilla de perfiles NAC para cada tipo de dispositivo.

La otra información necesaria para crear políticas son los flujos de tráfico. Dependiendo del equipo que tenga, puede obtener esta información a partir de herramientas de supervisión de flujos tales como sFlow, Netflow o Deep Packet Inspection (DPI).

Este proceso será iterativo. La primera vez que se activa la supervisión, los informes pueden no ser muy significativos, pero a medida que se avanza en los otros pasos, serán más específicos y útiles. La información que recopile en este paso será clave para los siguientes.

Paso 2: validar y evaluar

El siguiente paso es validar estos resultados. Evalúe las necesidades de la empresa. Cualquier IoT en la sombra que no pueda justificarse debe eliminarse, ya que aumenta innecesariamente la superficie de ataque. Por lo demás, hay que identificar los sujetos (usuarios y dispositivos), los flujos de tráfico y los flujos de trabajo, ya que deberán reflejarse en las políticas. Por ejemplo, quién tendrá acceso a determinados activos y qué podrá hacer con ellos. Aplique el principio del menor privilegio.

La microsegmentación no significa relajar otras políticas de seguridad, como las políticas de contraseñas o las actualizaciones de firmware. Se deben evaluar las capacidades individuales. ¿Estos dispositivos son compatibles con la autenticación basada en certificado? ¿Existe una herramienta de gestión que permita emitir y aplicar esos certificados? ¿Cuáles son los flujos de tráfico necesarios? Es posible que tenga que pedir esta información al fabricante, pero también deberá contrastarla con sus propios informes de análisis de tráfico. Si se encuentran activos que no cumplen con la política de la empresa, se necesita un plan de corrección para que cumplan con la normativa, o bien se tendrán que implementar controles adicionales.

Paso 3: planificar

En esta fase ya conoce los activos, los sujetos (usuarios), el tráfico y los flujos de trabajo. Ahora tiene que convertir estos conocimientos en políticas de autenticación y seguridad para implementar la arquitectura de microsegmentación necesaria. Como se ha mencionado anteriormente, para obtener los mejores resultados se deberá incluir una combinación de macrosegmentación y microsegmentación. Tenga en cuenta que en la mayoría de los escenarios de antigua implementación se verá limitado por la arquitectura ya existente.

Para la macrosegmentación existen múltiples opciones tales como VLAN, VRF, SPB VPN, VXLAN o túneles GRE, y características especiales tales como VLAN privada. Cada una de estas opciones tiene sus pros y sus contras, y pueden ser útiles en diferentes situaciones. Para la microsegmentación, necesitará saber qué políticas debe incluir en el perfil para cada usuario o tipo de dispositivo. Por último, tendrá que definir cómo asignar usuarios y dispositivos a su segmento y políticas. Esto se reduce a la autenticación o clasificación, que puede incluir la creación de huella digital del dispositivo.

Lo ideal es invertir en tecnología (segmentación definida por software) que permita crear políticas de autenticación flexibles para poder actualizar fácilmente los perfiles de la red.

Le sugerimos que diseñe el flujo de autenticación en este orden:

1. Autenticación a través de certificados 802.1x utilizando el servidor RADIUS. La autenticación genera un registro de autenticación. Esta es una información que se puede compartir con un cortafuegos.

2. Si no se puede autenticar el dispositivo a través de los certificados 802.1x, entonces se debe intentar la autenticación MAC a continuación. La autenticación MAC no es tan segura como la 802.1x, pero es mejor que no tener ninguna autenticación.

3. Si no se devuelve ningún perfil, se puede intentar la creación de una huella digital, la cual también se puede utilizar para asignar un segmento y reglas a un perfil. Esto no genera un registro de autenticación o de tarificación, pero sí se registra en la base de datos del inventario de IoT.

4. Por último, se puede disponer de una "captura general" predeterminada en caso de que no se devuelvan los perfiles, o bien si todo lo demás falla. En las primeras etapas todavía se tendrá que asignar el dispositivo a un perfil que llevará al mismo segmento y reglas, y que registrará el dispositivo en la base de datos de inventario.

Este flujo debe estructurarse de forma flexible para que pueda modificarse a medida que se avanza. Por ejemplo, es posible que se quiera eliminar la autenticación MAC al principio y añadirla más tarde, después de tener la lista de direcciones MAC obtenida del informe de inventario. Y a medida que se perfecciona el proceso, se puede, por ejemplo, cambiar el segmento y las reglas asociadas al perfil predeterminado por reglas muy restrictivas que solamente permitan el acceso a un host bastión.

También es posible que quiera compartir el rol del dispositivo con el cortafuegos, de modo que las reglas del cortafuegos puedan basarse en el rol del dispositivo y no únicamente en la subred/dirección IP. Las ventajas de esta integración son dobles. En primer lugar, el cortafuegos puede aplicar políticas detalladas a esos dispositivos IoT. En segundo lugar, las políticas del cortafuegos se basan ahora en los usuarios o en los roles, por lo que ya no están vinculadas a una subred o a una dirección IP; esto permite rediseñar y resegmentar la red en el futuro.

El proceso será iterativo y se tendrá que ajustar, afinar y perfeccionar a medida que se vaya mejorando en el uso de la autenticación y la segmentación.

Paso 4: simular

Por mucho que planifique, es poco probable que lo haga bien a la primera. Cualquier error en el diseño del esquema de autenticación, cualquier omisión que se haga en la "lista de permitidos" de la política de seguridad resultará en un proceso de negocio interrumpido. Deberá aplicar políticas de autenticación y acceso en modo "fail-open" (apertura ante fallo). Esto significa que los dispositivos y usuarios que no se autentiquen seguirán estando permitidos en la red y que los flujos de tráfico inesperados seguirán estando permitidos. Pero todo esto se registrará, y con estos registros se pueden perfeccionar los esquemas de autenticación y política.

Paso 5: aplicar

Tras algunos ajustes, ya no se observarán fallos de autenticación o denegación de flujos legítimos. A continuación, puede pasar esas políticas de "fail-open" (apertura ante fallo) a "fail-close" (cierre ante fallo), lo que significa que se bloquearán los dispositivos no autorizados y se descartarán los flujos inesperados.

Ni que decir tiene que se tendrán que seguir vigilando los dispositivos y flujos de tráfico inesperados, repitiendo todo el ciclo si es necesario.

Una cosa más

Como parte de la supervisión, el registro y la cuarentena continuos, le recomendamos que también invierta en un sistema de detección de intrusiones (IDS) externo. Aunque hay una serie de ataques de denegación de servicio distribuido (DDoS) que el propio conmutador puede identificar directamente, un IDS externo también puede detectar una gama más amplia de ataques, como virus u otras anomalías. Quizá recuerde que hace unos años varias cámaras de videovigilancia se infectaron con el malware Mirai, o quizá recuerde el día que estos dispositivos lanzaron un ataque coordinado a los servidores DNS globales que afectó a servicios como Twitter, Spotify o Paypal. Es posible que estos ataques no sean detectados por sus conmutadores, pero un IDS dedicado sí lo hará.

Una vez detectado el ataque, el IDS notificará a su sistema de gestión de red (NMS) las direcciones IP de los dispositivos afectados. Idealmente, su NMS será capaz de localizar estos dispositivos en su base de datos y cambiar sus perfiles a un "rol de cuarentena".

El "rol de cuarentena" es un rol muy restrictivo, normalmente solo permitiría la comunicación con un host bastión para que el dispositivo pudiera ser corregido, por ejemplo, estableciendo una contraseña fuerte o actualizando su firmware, entre otras opciones.

Por qué elegir Alcatel-Lucent Enterprise

Las soluciones de Digital Age Networking de Alcatel-Lucent Enterprise incorporan una segmentación robusta y flexible definida por software con políticas DPI NAC dinámicas que permiten una evolución gradual hacia una arquitectura de confianza cero.

Digital Age Networking es el proyecto de Alcatel-Lucent Enterprise que permite que las empresas y organizaciones entren en la era digital y hagan crecer sus negocios digitales. Se basa en tres pilares:

- Una red autónoma que conecta de forma fácil, automática y segura a personas, procesos, aplicaciones y objetos. La red autónoma de ALE se basa en una cartera racionalizada que se completa con una verdadera plataforma de gestión unificada que ofrece políticas de seguridad comunes en toda nuestra LAN y WLAN. La red autónoma también proporciona flexibilidad de implementación en interiores, exteriores y en entornos industriales. La gestión de la red puede realizarse en las instalaciones, en la nube o en un despliegue híbrido, según la preferencia del cliente.
- Incorporación segura y eficiente de dispositivos IoT: la segmentación mantiene los dispositivos en sus segmentos específicos y minimiza el riesgo de ataques de piratas informáticos contra el dispositivo y la red. La segmentación de IoT puede ayudar a que las empresas sepan de forma fácil y automática si el dispositivo se está comportando correctamente o no, y ayuda a mantener segura la red.
- Innovación empresarial mediante la automatización del flujo de trabajo: la integración de las métricas de usuario, aplicaciones e IoT en tiempo real, con datos de geolocalización, en plataformas de colaboración simplifica la creación y puesta en marcha de nuevos servicios y procesos de negocio digitales automatizados, incluyendo la notificación a los administradores de seguridad y de la red sobre todos los ataques en el momento en que se producen.

¿Dispone de una herramienta para crear un inventario de IoT/dispositivos? ¿Dispone de una herramienta que le permita supervisar los flujos de las aplicaciones? ¿Sus conmutadores y puntos de acceso inalámbricos actuales están preparados para la segmentación definida por software? Si no dispone actualmente de estas herramientas, póngase en contacto con nosotros y le ayudaremos a conseguirlo.

Lo que sabemos con seguridad

Concluyamos con algunos puntos clave:

- Para tener una ZTA realmente eficaz se deben utilizar tanto la macrosegmentación como la microsegmentación
- Una ZTA consta de cinco pasos: supervisar, validar y evaluar, planificar, simular y aplicar
- La ZTA basada en la microsegmentación se basa en tres pilares: la autenticación, con 802.1x EAP-TLS como estándar de oro; las políticas diferenciadas asociadas al rol del usuario o del dispositivo que se remontan al principio de mínimo privilegio; la supervisión continua y la cuarentena
- En los entornos híbridos y móviles, la microsegmentación debe estar definida por software, es decir, debe ser dinámica y estar basada en políticas, no definida estáticamente, ya que de lo contrario sería poco práctica

La migración a una ZTA a través de la microsegmentación es todo un proceso y es poco probable que una empresa de un tamaño considerable lo consiga en un solo ciclo de actualización. Pero, con cada actualización o rediseño o ciclo de mejora continua se puede estar más cerca de ese objetivo si se ponen en marcha la infraestructura y el diseño adecuados.

Alcatel-Lucent Enterprise se compromete a desarrollar la tecnología y las soluciones de red que ayudan a las empresas a desplegar todo el potencial de su negocio mediante la transformación digital.

Alcatel·Lucent Enterprise