DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

Aruba ESP con seguridad Zero Trust

Seguridad para la periferia

Los desafíos de seguridad de la red han evolucionado significativamente a través de los años a medida que los usuarios se descentralizaron cada vez más y los ataques se tornaron más sofisticados y persistentes. Los enfoques de seguridad tradicionales que se centraban principalmente en el perímetro de la red se han vuelto ineficaces como estrategias de seguridad autónomas. La seguridad de redes moderna debe incorporar un conjunto diverso y cambiante de usuarios y dispositivos, como también amenazas mucho más frecuentes que tienen como objetivo las partes de la infraestructura de la red que previamente eran "de confianza".

La confianza cero (Zero Trust) ha surgido como un modelo eficaz para abordar mejor los cambiantes requisitos de seguridad de las empresas modernas, ya que supone que todos los usuarios, dispositivos, servidores y segmentos de la red son inherentemente inseguros y potencialmente hostiles. Aruba ESP con seguridad Zero Trust mejora la postura general de seguridad de la red gracias a la aplicación de un conjunto más riguroso de mejores prácticas de seguridad y controles a los recursos de redes que antes se consideraban de confianza.

ARUBA ESP: PRINCIPIOS CENTRALES DE ZERO TRUST

Zero Trust varía considerablemente según el área de seguridad que se observe. A pesar de que los controles al nivel de las aplicaciones han sido un punto de enfoque dentro de Zero Trust, una estrategia integral también debe abarcar la seguridad de la red y la cantidad cada vez mayor de dispositivos conectados, que incluye el entorno de trabajo desde el hogar. Aruba ESP con seguridad Zero Trust incorpora visibilidad integral, control y microsegmentación de menor acceso, y aplicación y monitoreo continuos. Incluso las soluciones VPN tradicionales se enriquecen garantizando que los mismos controles se apliquen a las redes de sucursales o campus, que también se extienden al trabajador remoto o desde el hogar.

En la era de la IoT, los principios básicos de una buena seguridad de redes son, por lo general, difíciles de

implementar. Cuando sea posible, todos los dispositivos y los usuarios deberán estar identificados y autenticados correctamente antes de otorgarles acceso a la red. Además de la autenticación, se les debería proporcionar a los usuarios y a los dispositivos la menor cantidad posible de acceso: lo necesario para realizar actividades importantes para la empresa una vez que están en la red. Esto significa autorizar a qué aplicaciones y recursos de la red puede acceder cada usuario o dispositivo. Por último, todas las comunicaciones entre usuarios y aplicaciones deben estar cifradas.

LA NECESIDAD DE UNA VISIBILIDAD INTEGRAL

Con la adopción cada vez más generalizada de la IoT, la visibilidad de espectro completo de todos los dispositivos y usuarios en la red se ha vuelto una tarea cada vez más dificultosa. Sin visibilidad, los controles de seguridad críticos que respaldan el modelo de Zero Trust resultan difíciles de aplicar. La automatización, el aprendizaje automático basado en la IA y la capacidad para identificar tipos de dispositivos rápidamente son cruciales.

Aruba ClearPass Device Insight utiliza una combinación de técnicas de generación de perfiles y detección pasiva y activa para detectar el espectro completo de dispositivos conectados o que intentan conectarse a la red. Esto incluye los dispositivos comunes de usuarios, como las computadoras portátiles y tablets. Lo que la diferencia de las herramientas tradicionales es su capacidad para ver el conjunto cada vez más diverso de dispositivos de IoT cuya presencia en las redes actuales ha aumentado mucho.

ADOPTAR EL "MÍNIMO ACCESO" Y LA MICROSEGMENTACIÓN

Una vez incorporada la visibilidad, los siguientes pasos fundamentales son aplicar las mejores prácticas de Zero Trust relacionadas con el "mínimo acceso" y la microsegmentación. Esto supone utilizar el mejor método de autenticación posible para cada punto terminal en la red (es decir, autenticación de múltiples factores 802.1X completa para los dispositivos de usuarios) y aplicar una política de control de acceso que solo autorice el acceso a recursos que sean absolutamente necesarios para ese dispositivo o usuario.

ClearPass Policy Manager de Aruba permite la creación de políticas de acceso basado en roles que permiten que los equipos de seguridad y TI pongan en funcionamiento estas mejores prácticas utilizando privilegios de acceso asociado y rol único que se aplican en cualquier parte de la red, se trate de infraestructuras inalámbricas o cableadas, en sucursales o en campus. Una vez generados los perfiles, se les asigna automáticamente a los dispositivos la política de control de acceso que corresponda y se los separa de otros dispositivos mediante las capacidades de segmentación dinámica de Aruba. El firewall de aplicación de políticas (PEF) de Aruba provee la aplicación de políticas; se trata de un firewall de aplicación completa integrado en la infraestructura de redes Aruba. La infraestructura de Aruba también utiliza los protocolos de cifrado más seguros, como el estándar de WPA3 en conexiones de redes inalámbricas.

ClearPass Policy Manager también se integra con una gran variedad de soluciones de autenticación que permiten el uso de la autenticación de múltiples factores y la capacidad de forzar la autenticación en puntos clave de toda la red. A través del ecosistema de ClearPass, los clientes también pueden incorporar fácilmente otras soluciones para cumplir con los requisitos de Zero Trust relacionados con la información contextual y otra telemetría de seguridad.

Esto significa que ClearPass puede integrarse con una gran variedad de soluciones, como las herramientas de seguridad de puntos terminales, para tomar decisiones de control de acceso más inteligentes basadas en la postura de un dispositivo. Las políticas de control de acceso también pueden cambiarse en función de qué tipo de dispositivo se utiliza, desde dónde se conecta el usuario y otros criterios basados en el contexto.

APLICACIÓN Y MONITOREO CONTINUOS

Con el control de acceso basado en roles implementado para aplicar la segmentación granular, el monitoreo en curso de los usuarios y dispositivos en la red conforman otra de las mejores prácticas de la Zero Trust. De esta manera, se abordan los riesgos relacionados con amenazas internas, *malware* avanzado o amenazas persistentes que han eludido las defensas perimetrales tradicionales.

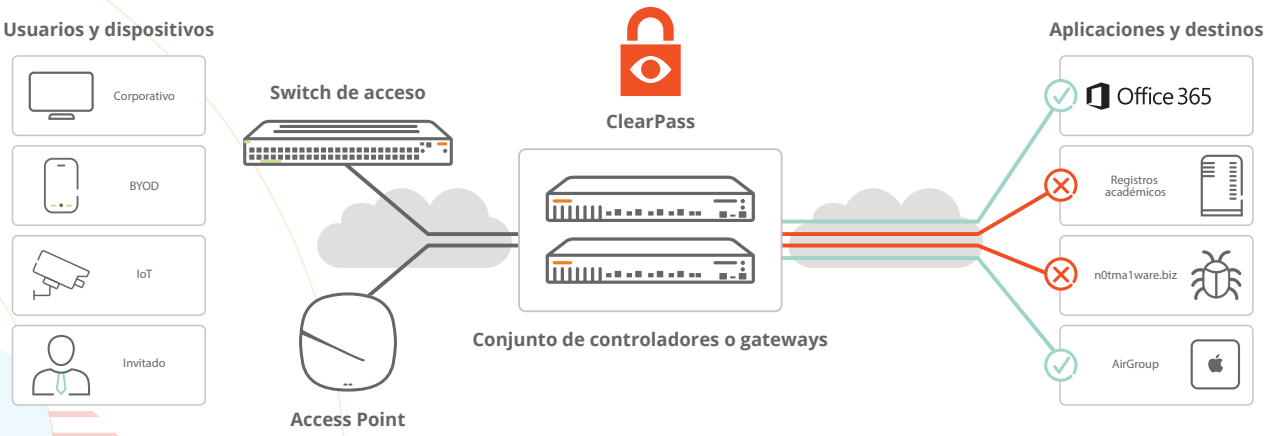

Figura 1: Aruba ClearPass asigna automáticamente las políticas de control de acceso basado en roles que se aplican mediante el uso de la segmentación dinámica

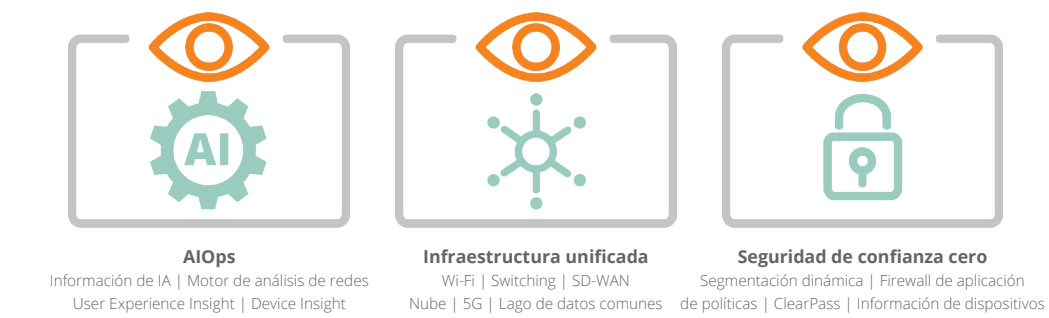

Figura 2: La seguridad Zero Trust es el pilar clave de Aruba ESP

Defensa contra amenazas con IDS/IPS

Las capacidades de defensa de amenazas de Aruba brindan protección contra una infinidad de amenazas, que incluyen la suplantación de identidad, la denegación de servicio (DoS) y los ataques cada vez más extendidos de secuestro de datos. Los gateways SD-WAN 9000 de Aruba realizan la detección y prevención de intrusos basadas en la identidad (IDS/IPS), ya que trabajan en conjunto con Aruba Central, ClearPass Policy Manager y el firewall de aplicación de políticas. La IDS/IPS basada en la identidad realiza inspecciones de tráfico basadas en patrones y en firmas tanto en el tráfico de LAN de oficinas de sucursales (este-oeste) como en el tráfico SD-WAN (norte-sur) que circule a través del gateway para brindar seguridad de redes de sucursales incorporada. Un panel avanzado de seguridad dentro de Aruba Central proporciona a los equipos de TI visibilidad en toda la red, métricas de amenazas multidimensionales, datos de inteligencia sobre amenazas, correlación y administración de incidentes. Los eventos de amenazas se envían a los sistemas SIEM y ClearPass para su corrección.

360 Security Exchange

Con más de 150 integraciones compuestas por las mejores soluciones de seguridad de su clase que incluyen conjuntos de herramientas de respuesta y operaciones de seguridad (SOAR), ClearPass Policy Manager es capaz de aplicar dinámicamente el acceso basado en telemetría de amenazas en tiempo real provenientes de múltiples fuentes. Pueden crearse políticas para tomar decisiones de control de acceso en tiempo real basadas en alertas provenientes de firewalls de próxima generación (NGFW), herramientas de administración de eventos e información de seguridad (SIEM) y muchas otras fuentes. Las acciones de ClearPass son completamente configurables, desde la limitación del acceso (es decir, solo Internet) hasta la eliminación total de un dispositivo de la red para la corrección.

ARUBA ESP (EDGE SERVICES PLATFORM)

Para ayudar a nuestros clientes a capitalizar oportunidades en la periferia, hemos desarrollado Aruba ESP, la primera plataforma potenciada por IA de la industria diseñada para unificar, automatizar y asegurar la periferia. La seguridad Zero Trust es un componente clave de Aruba ESP que, en combinación con AIOps y una infraestructura unificada, permite que las organizaciones reduzcan costos, simplifiquen operaciones y permanezcan seguras.

RESUMEN

El panorama actual de las amenazas y el entorno de redes requieren un enfoque diferente. La antigua seguridad de redes centrada en el perímetro no fue diseñada para la fuerza laboral móvil actual o los dispositivos de IoT emergentes. Aruba ESP con seguridad Zero Trust provee un conjunto integral de capacidades que abarcan la visibilidad, el control y el cumplimiento para abordar los requisitos de una infraestructura de redes impulsada por IoT y descentralizada.

SO_ZeroTrustSecurity_051120 a00097694enw