DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

Aruba ESP con seguridad Zero Trust

Seguridad para el Edge

Los problemas de seguridad de las redes han evolucionado considerablemente en los últimos años, a medida que los usuarios se han ido descentralizando cada vez más y los ataques se han vuelto más sofisticados y persistentes. Los tradicionales enfoques de seguridad centrados principalmente en el perímetro de la red se han vuelto ineficaces como estrategias de seguridad autónomas. La seguridad actual de las redes debe dar cabida a un conjunto diverso y siempre cambiante de usuarios, y a amenazas mucho más frecuentes dirigidas a partes de la infraestructura de la red en las que antes se confiaba.

Zero Trust ha resultado ser un modelo eficaz para abordar mejor las exigencias de seguridad de la empresa moderna partiendo de la base de 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 estrategia general de seguridad de la red aplicando un conjunto más riguroso de mejores prácticas y controles de seguridad a los recursos de red que antes eran fiables.

ARUBA ESP: PRINCIPIOS ZERO TRUST FUNDAMENTALES

Zero Trust varía considerablemente en función del dominio de seguridad en cuestión. Aunque los controles a nivel de aplicación han sido un punto central dentro de Zero Trust, una estrategia integral también debe abarcar la seguridad de la red y el creciente número de dispositivos conectados, e incluir el trabajo desde casa. Aruba ESP con seguridad Zero Trust Security incorpora visibilidad integral, micro segmentación y control de mínimo acceso, y supervisión y ejecución continuas. Incluso las tradicionales soluciones VPN mejoran cuando se garantiza que los mismos controles que se aplican a las redes de campus o sucursales también se extienden a los hogares o a los trabajadores remotos.

En la era de la IoT, los principios básicos de una buena seguridad de red suelen resultar difíciles de implementar. En la medida de lo posible, es necesario identificar y autenticar a todos los dispositivos y usuarios antes de brindarles acceso a la red. Pero, además de esta autenticación, tanto los usuarios como los dispositivos deben disfrutar solo de un mínimo acceso a la

red para realizar aquellas actividades que sean cruciales para el negocio. Y esto implica determinar a qué recursos y aplicaciones de red puede acceder un determinado usuario o dispositivo. Por último, todas las comunicaciones entre los usuarios finales y las aplicaciones deben estar cifradas.

LA NECESIDAD DE UNA VISIBILIDAD INTEGRAL

Como consecuencia del aumento de la IoT, la visibilidad integral de todos los dispositivos y usuarios de la red resulta una tarea cada vez más complicada. Y sin visibilidad, los controles de seguridad críticos que hacen posible el modelo Zero Trust son difíciles de aplicar. La automatización, el aprendizaje automático basado en IA y la capacidad de identificar rápidamente los diferentes tipos de dispositivos son críticos.

Aruba ClearPass Device Insight utiliza una combinación de técnicas activas y pasivas de detección y perfilado para determinar todo el espectro de dispositivos conectados o que intentan conectarse a la red. Y aquí se incluyen los dispositivos más comunes utilizados por los usuarios, como portátiles y tabletas. Pero se diferencia de las herramientas tradicionales por su capacidad de ver el amplio abanico de dispositivos IoT cada vez más omnipresentes en las redes actuales.

ADOPTAR EL "MÍNIMO ACCESO" Y LA MICROSEGMENTACIÓN

Una vez queda resuelto el tema de la visibilidad, los siguientes pasos críticos pasan por la aplicación de las mejores prácticas Zero Trust relacionadas con el "mínimo acceso" y por la microsegmentación. Esto supone utilizar el mejor método de autenticación posible en cada extremo de la red (es decir, autenticación 802.1X completa y multifactor para los dispositivos de los usuarios), y aplicar una política de control que sólo facilite el acceso a los recursos que sean absolutamente necesarios para ese dispositivo o usuario.

Aruba ClearPass Policy Manager permite la creación de políticas de acceso basadas en roles que permiten a los equipos de seguridad y TI poner en práctica estas mejores prácticas utilizando un único rol y los privilegios de acceso asociados que se aplican en cualquier punto de la red, ya sea una infraestructura estándar o inalámbrica, una sucursal o un campus. Una vez perfilados, los dispositivos quedan automáticamente asignados a la correspondiente política de control de acceso, y se segmentan a partir de otros dispositivos gracias las capacidades de segmentación dinámica de Aruba. La ejecución se realiza a través del cortafuegos de ejecución de políticas de Aruba, un cortafuegos de aplicación completa que se encuentra integrado en la infraestructura de red de Aruba. La infraestructura de Aruba también utiliza los protocolos de cifrado más seguros, como el estándar WPA3 a través de conexiones de red inalámbricas.

ClearPass Policy Manager también se integra con una gran variedad de soluciones de autenticación que permiten el uso de la autenticación multifactor y la capacidad de forzar la reautenticación en puntos clave de toda la red. Gracias al ecosistema ClearPass, los clientes también pueden incorporar fácilmente otras soluciones para reunir los requisitos Zero Trust relacionados con la información contextual y demás telemetría de seguridad.

Esto significa que ClearPass se puede integrar con una gran variedad de soluciones, como las herramientas Endpoint Security, para tomar mejores decisiones de control de acceso basadas en la posición de un dispositivo. Las políticas de control de acceso también se pueden modificar en función del tipo de dispositivo que se utilice, del lugar desde el que se conecta el usuario y de otros criterios dependientes del contexto.

CONTINUA SUPERVISIÓN Y EJECUCIÓN

Gracias al control de acceso basado en roles para imponer una segmentación granular, la supervisión continua de los usuarios y los dispositivos en la red constituye otra de las mejores prácticas de Zero Trust. Esto permite hacer frente a los riesgos derivados de amenazas internas, malware avanzado o amenazas persistentes que hayan podido eludir las defensas perimetrales tradicionales.

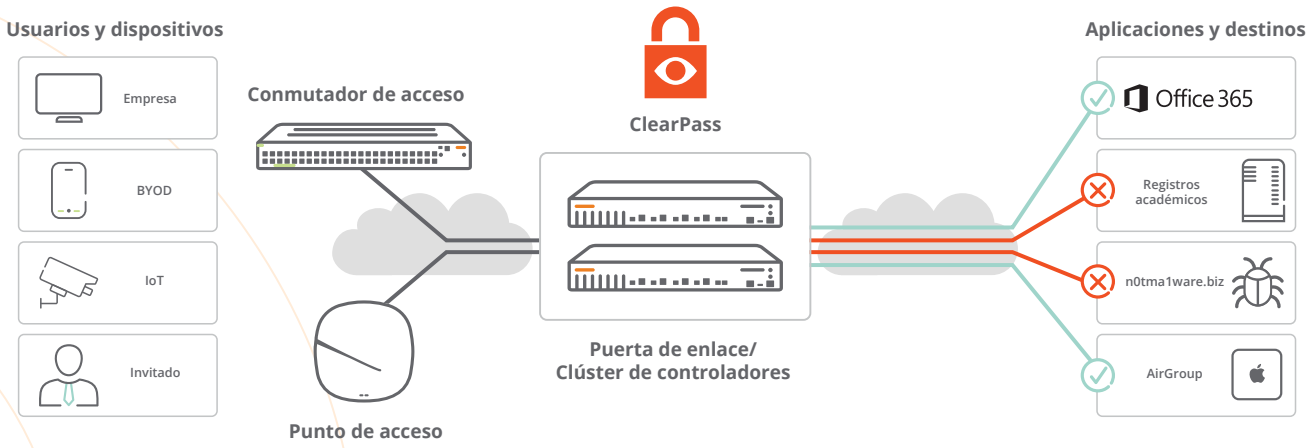

Figura 1: Aruba ClearPass asigna automáticamente políticas de control de acceso basadas en roles que se aplican empleando la segmentación dinámica

ARUBA ESP (PLATAFORMA DE SERVICIOS EN EL EDGE)

La primera plataforma del sector con un sexto sentido basado en IA para automatizar y proteger

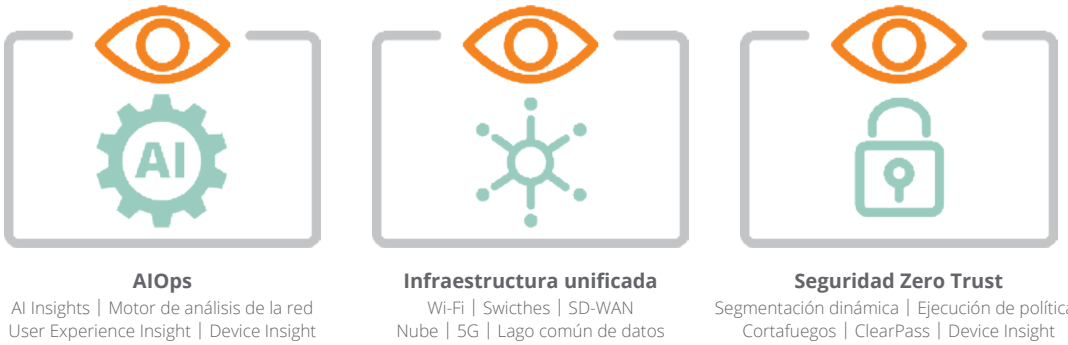

Figura 2: La seguridad Zero Trust es uno de los pilares fundamentales de Aruba ESP

Defensa contra amenazas con IDS/IPS

Las capacidades de defensa de Aruba permiten hacer frente a infinidad de amenazas, entre las que se incluyen el phishing, la denegación de servicio (DoS) y los cada vez más extendidos ataques de ransomware. Las puertas de enlace Aruba 9000 SD-WAN permiten detectar y prevenir intromisiones basadas en la identidad (IDS/IPS) al trabajar en conjunto con Aruba Central, ClearPass Policy Manager y el cortafuegos de ejecución de políticas. La IDS/IPS basada en la identidad realiza una inspección de tráfico a partir de firmas y patrones tanto en el tráfico LAN de la sucursal (este-oeste) como en el tráfico SD-WAN (norte-sur) que pasa a través de la puerta de enlace, de modo que la seguridad queda integrada en la red de la sucursal. El avanzado panel de seguridad de Aruba Central proporciona a los equipos de TI visibilidad en toda la red, métricas de amenazas multidimensionales, datos de inteligencia ante amenazas, así como correlación y administración de incidentes. Las amenazas se envían a los sistemas SIEM y a ClearPass para su corrección.

360 Security Exchange

Gracias a sus más de 150 integraciones compuestas por las mejores soluciones de seguridad, entre las que se incluyen conjuntos de herramientas de operaciones y respuestas de seguridad (SOAR), ClearPass Policy Manager es capaz de proporcionar de manera dinámica un acceso basado en la telemetría de amenazas en tiempo real procedente de múltiples fuentes. Se pueden crear políticas para tomar decisiones en tiempo real sobre el control de acceso basadas en las alertas procedentes de cortafuegos de última generación (NGFW), herramientas de gestión de información y eventos de seguridad (SIEM) y muchas otras fuentes. Las acciones de ClearPass son totalmente configurables, ya que permiten desde limitar el acceso (es decir, sólo a Internet) hasta eliminar por completo un dispositivo de la red para su rehabilitación.

ARUBA ESP (PLATAFORMA DE SERVICIOS EN EL EDGE)

Para ayudar a nuestros clientes a capitalizar las oportunidades en el Edge, hemos desarrollado Aruba ESP, la primera plataforma del sector basada en IA y diseñada para unificar, automatizar y asegurar el Edge. La seguridad Zero Trust es un componente clave del Aruba ESP que, cuando se combina con AIOps y una infraestructura unificada, permite a las organizaciones reducir costes, simplificar las operaciones y permanecer seguras.

RESUMEN

En la actualidad, las redes y sus diferentes amenazas requieren una estrategia diferente. La antigua seguridad de red centrada en el Edge no fue diseñada para el personal móvil ni los dispositivos IoT de hoy en día. Aruba ESP con seguridad Zero Trust brinda un conjunto completo de capacidades que abarcan visibilidad, control y ejecución, que permiten hacer frente a los requisitos de una infraestructura de red descentralizada basada en la IoT.

SO_ZeroTrustSecurity_051120 a00097694ese