aruba
a Hewlett Packard Enterprise company

DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

SEGMENTACIÓN DINÁMICA

Acceso sencillo y seguro que unifica las redes inalámbricas y cableadas

El número creciente de dispositivos de IoT y el uso de servicios en la nube y de movilidad cruciales para la empresa son los motores de las innovaciones en el lugar de trabajo digital, lo cual nos lleva a preguntarnos: ¿el perímetro de la red es lo suficientemente inteligente para conectar de forma segura todos los tipos de dispositivos y usuarios? Las redes inalámbricas y por cable anteriores se crearon sin tener en cuenta la seguridad, el acceso del IoT y la movilidad cruciales para la empresa. El enfoque actual de utilizar configuraciones manuales y estáticas para estos dispositivos del IoT y móviles en constante cambio ubicados en las redes de campus y sucursales presenta nuevos riesgos para la seguridad y se ha convertido en una tarea tediosa que los equipos de TI deben realizar cada día.

Para simplificar y proteger la red, la segmentación dinámica de Aruba unifica la aplicación de políticas en las redes inalámbricas y por cable, para mantener el tráfico seguro y separado. Ahora, la coexistencia de las operaciones orientadas hacia la empresa y las redes corporativas gestionadas con dispositivos de cliente gestionados por la TI y el IoT se ha simplificado, mientras se optimizan la experiencia de red y las operaciones de TI extremo a extremo.

La segmentación dinámica utiliza los conocimientos recopilados de la capacidad básica de generación de políticas basadas en roles, de los cortafuegos de usuario, además de la visibilidad de aplicaciones enriquecida de capa 7 y del filtrado integrado de contenidos web de Aruba.

MOTORES TÉCNICOS Y EMPRESARIALES CLAVES

Gestión de políticas simplificada

Incorporar dispositivos de cliente y del IoT solía precisar múltiples puntos de contacto, la mayoría de las veces con la configuración manual de nuevas VLAN, ACL o subredes en cada salto de la red. Los movimientos, añadidos y cambios permanentes en redes grandes y distribuidas también consumen tiempo y generan errores. Un diseño de red con una seguridad sólida pero de complejidad reducida solía implicar conceptos mutuamente excluyentes.

VENTAJAS PRINCIPALES

- **Experiencia de usuario superior y uniforme**: funciones de ampliación de rol de usuario, inspección profunda de paquetes de aplicaciones y elaboración de perfiles de dispositivos de redes inalámbricas a cableadas.
- **Operaciones de red simplificadas:** ahorra tiempo y elimina la proliferación de VLAN mediante la reducción de la configuración necesaria para SSID, ACL, subredes y puertos cableados.
- **Seguridad y visibilidad de dispositivos mejoradas:** ClearPass and Policy Enforcement Firewalls (PEF) ofrecen visibilidad y aplicación de políticas mejoradas.

Mejorar la experiencia del usuario

Cuando los usuarios se mueven entre escritorios o ubicaciones, esperan la misma experiencia de red, con independencia del lugar donde se conectan o la forma, por cable o de manera inalámbrica. Pedirles que utilicen una red privada virtual (VPN) supone un reto. Cualquier experiencia de red que requiera el soporte de la TI se percibe como negativa. La experiencia de usuario –ya se trate de un empleado, un invitado, un comprador o un estudiante– afecta al éxito de una organización. La conexión de nuevos tipos de dispositivos, como teléfonos inteligentes, impresoras o equipos de videoconferencia, suele realizarse sin los conocimientos o el soporte de la TI. La expectativa es que la TI ofrezca una experiencia fluida, al tiempo que mantiene la visibilidad y la gestión de todos los elementos en una red segura.

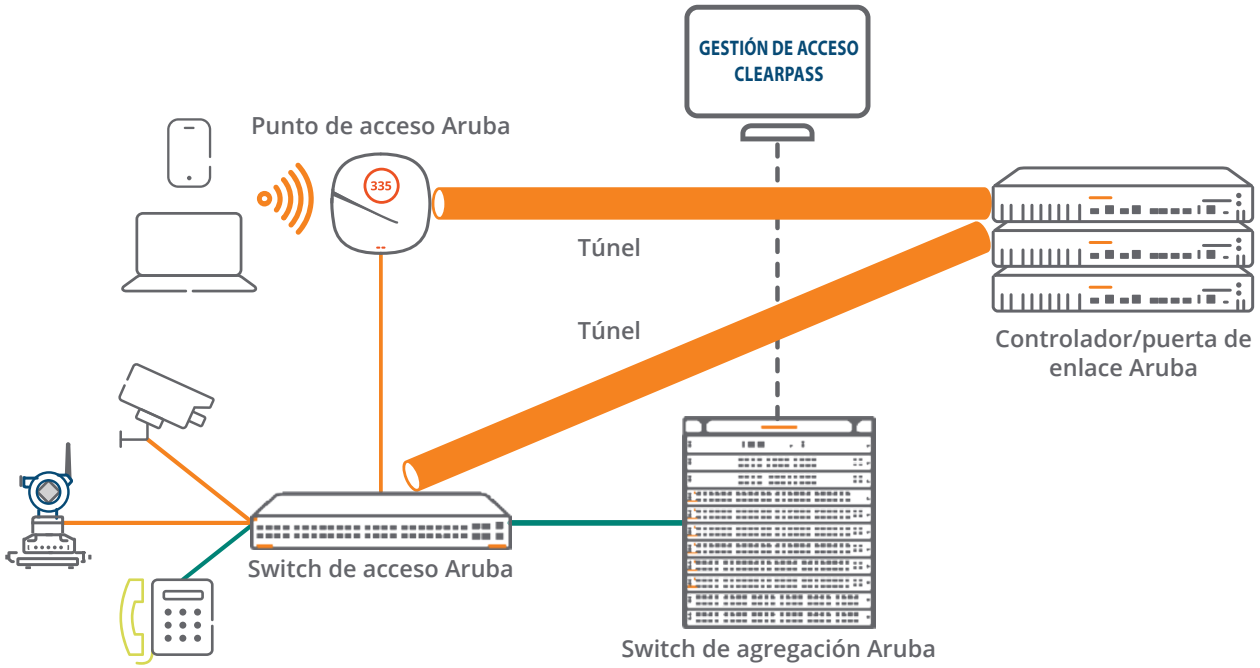
La vulnerabilidad de la red queda expuesta con el crecimiento previsto del número de dispositivos de IoT/periféricos conectados a las redes empresariales hasta superar los 20 000 millones en 2020.

Fuente: Gartner, (enero de 2017).

Desde la iluminación inteligente hasta las cámaras de seguridad o los lectores de acreditaciones, la implementación de dispositivos de IoT en redes de todos los tamaños se está produciendo a gran velocidad. Esta nueva conectividad de red aporta muchas ventajas atractivas, pero también expone la red a riesgos de seguridad, puesto que estos dispositivos «saltan» en las mismas rutas que los datos financieros, médicos y cruciales para el negocio de naturaleza confidencial. Estos dispositivos raras veces llevan una seguridad sólida integrada y carecen de un proceso de autenticación seguro. Las contraseñas se almacenan en texto legible, carecen de suplicantes seguros y suelen estar físicamente ubicadas en zonas públicas inseguras... lo que abre la puerta a accesos no autorizados a la red.

AMPLIACIÓN DE LAS INNOVACIONES EN WLAN A LA CONMUTACIÓN

La segmentación dinámica amplía la gestión de políticas segura de Aruba y las capacidades de aplicación de políticas de la WLAN para simplificar y asegurar el acceso a las redes cableadas. Esta capacidad implica que se pueden asignar dinámicamente a los dispositivos de cliente por



Segmentación dinámica, parte de The Experience Edge

cable políticas basadas en rol de usuario o puerto, algo fundamental cuando se prevé que el número de dispositivos de IoT alcance los 20 000 millones en 2020. Los switches de red Aruba, ahora respaldados por ClearPass para la gestión de políticas y por los controladores de movilidad para la aplicación, desempeñan un papel fundamental a la hora de unificar el acceso de red.

Políticas basadas en roles

Mediante la implementación de la segmentación dinámica, las decisiones de las políticas basadas en roles y los derechos de acceso se basan en el tipo de dispositivo, la aplicación utilizada e incluso la ubicación del usuario o el dispositivo. Utilizadas originalmente para abordar la seguridad inalámbrica, las políticas basadas en roles segmentaban el tráfico de red por tipo de usuario, como empleado, invitado o contratista, al tiempo que simplificaba de manera significativa la gestión de la red con la eliminación de las configuraciones de red complejas y estáticas. Esta potente capacidad optimizaba los flujos de trabajo de la TI, como la gestión de las políticas de acceso y TSPD, y garantizaba un rendimiento superior de las aplicaciones.

Ampliar la gestión dinámica de políticas basadas en roles a los PA inalámbricos y los switches por cable proporciona una manera fundamentalmente sencilla, segura pero diferente de gestionar y aplicar políticas a la movilidad, el IoT y la nube. Las puertas de enlace/los controladores de movilidad de Aruba, que aplican las definiciones de políticas de ClearPass, ya poseen la capacidad para comprender y utilizar dinámicamente los roles. Esta capacidad elimina la tarea ardua y generadora de errores de gestionar VLAN, ACL y subredes complejas y estáticas mediante la asignación dinámica de políticas.

Segmentación de capa 4-7

La segunda capacidad básica de los switches Aruba es la segmentación. La arquitectura WLAN de Aruba mantiene el tráfico seguro y separado mediante el uso de túneles entre los puntos de acceso y un controlador o puerta de enlace. Esta segmentación basada en túneles proporciona seguridad, como la inspección a través de cortafuegos de tráfico de alto riesgo, gracias al Policy Enforcement Firewall (PEF) integrado de Aruba. El PEF ofrece contexto granular (usuario, dispositivo, aplicación, ubicación), para reducir la necesidad de contar con cortafuegos costosos para la primera línea de interrogación y defensa. A través de las políticas contextuales basadas en identidades, tipo de dispositivo y ubicación, se pueden satisfacer las necesidades de grupos de usuarios diferentes con una única configuración de red, a medida que los flujos de tráfico se adaptan a los roles asignados.

La segmentación dinámica simplifica y protege las redes redes inalámbricas y por cable al establecer el controlador de movilidad como el motor de ejecución de políticas unificado. El tráfico de PA o Switches se encapsula en túneles GRE para su inspección por parte del Policy Enforcement Firewall (PEF).

Al utilizar esta arquitectura de creación de túneles WLAN, los switches Aruba pueden proporcionar ahora un enfoque de la segmentación basada en roles frente al uso más manual y tradicional de las VLAN locales. Esto resulta ideal para los dispositivos de IoT que no gozan de confianza o para ofrecer visibilidad de las aplicaciones, puesto que los switches Aruba pueden crear túneles dinámicos para tráfico seleccionado hacia el controlador, para la inspección profunda de paquetes y la autenticación de dispositivos, al igual que un punto de acceso. Por ejemplo, se puede asignar dinámicamente a una cámara de seguridad un rol con derechos que restringe su tráfico a un servidor único especificado, eliminando las probabilidades de que se produzcan accesos malintencionados a otras partes de la red.

Esta nueva capacidad de segmentación mejora la posición de seguridad con una creación de túneles que se puede configurar sobre la base del puerto (PBT), donde la autenticación se lleva a cabo en el controlador, o sobre la base del usuario (UBT), donde la autenticación se lleva a cabo en el switch. Debido a que esta segmentación actúa como una superposición, puede coexistir con implementaciones VLAN al hacer uso de túneles seguros en zonas seleccionadas sin desinstalar ni sustituir la infraestructura de conmutación al completo.

COMPONENTES DE LA SOLUCIÓN

Puntos de acceso inalámbricos Aruba

Rendimiento wifi 802.11ac y 802.11ax que se adapta a las necesidades de cualquier entorno. La inteligencia artificial y los servicios de ubicación integrados ofrecen a la TI la

automatización y la visibilidad necesarias para entregar una experiencia óptima, para usuarios y dispositivos de IoT.

Switches de red Aruba

Crean una base integrada cableada e inalámbrica que entrega escalabilidad, seguridad y alto rendimiento para redes de campus y sucursales. La segmentación dinámica pone a disposición de los equipos de TI una manera única y sencilla de aplicar políticas, utilizar servicios avanzados y segmentar de forma segura tráfico cableado de usuarios e IoT en cualquier punto de la red a través de túneles, bien basados en puertos (PBT) con autenticación en el controlador o basados en usuarios (UBT) con autenticación en el switch Aruba.

Controladores de movilidad y puertas de enlace Aruba

Como elementos fundamentales de la solución, las puertas de enlace o los controladores hacen las veces de responsable de la aplicación de las políticas para el tráfico inalámbrico y por cable. El controlador de movilidad Aruba (que ejecuta AOS 8.1 o posterior) permite que la TI aproveche la aplicación de políticas, los contratos de ancho de banda y otras restricciones del tráfico. En un entorno de sucursal, la puerta de enlace para sucursal con gestión centralizada de Aruba realiza esta función. El Policy Enforcement Firewall hace las veces de tecnología de red subyacente en apoyo de estos dos entornos.

Aruba ClearPass Policy Manager con elaboración de perfiles

Gestión centralizada y aplicación de políticas de acceso a la red para un control de acceso por cable o inalámbrico. Sus funciones principales son la elaboración de perfiles de dispositivos, la autenticación, la autorización y la aplicación de políticas. Utilizando ClearPass, una vez definidos el rol y los privilegios, siguen al usuario o al dispositivo en su acceso por cable o inalámbrico. Por eso, si el usuario cambia a un dispositivo desconocido o si se encuentra en una red insegura, la política cambiará automáticamente los privilegios de autorización. Los roles de usuario para descargar (DUR) se configuran en ClearPass, para eliminar así la necesidad de definir los roles o las políticas en un switch.

RESUMEN

Para gestionar mejor la movilidad crucial para la empresa y los requisitos crecientes de la conectividad del IoT, la innovadora solución de segmentación dinámica de Aruba simplifica las operaciones de TI y mejora la seguridad al aplicar de forma dinámica políticas unificadas y servicios avanzados en cualquier punto de la red. De este modo, se garantiza la distribución uniforme, la aplicación automática y la ejecución independiente de todas las políticas de acceso y seguridad pertinentes a todos los usuarios y dispositivos por cable e inalámbricos.

SO_DynamicSegmentation_SK_092419 a00058593ese