ESCRIPCIÓN GENERAL DE LA SOLUCIÓN

aruba
a Hewlett Packard Enterprise company

LA ARQUITECTURA MOBILE FIRST DE ARUBA

Marzo 2018

Tabla de Contenido

Introducción

La arquitectura de networking de Aruba para la empresa definida por software está diseñada para ser mobile first y entrega una red que es abierta, segura y autónoma. La velocidad, variedad y volumen de usuarios y cosas que se conectan a las redes han obligado a TI a cambiar la forma en la cual construyen y operan redes de siguiente generación.

- Mobile First—Permite que los usuarios y cosas se conecten a la red y reciban la misma política y permisos, independientemente de cómo se conecten, alámbrico o inalámbrico, haciéndolos verdaderamente móviles. Diseñada a propósito para entregar una experiencia de networking continua para ambientes en donde la movilidad, IoT y la nube son de misión crítica.

- Abierta—Las redes son multi proveedor y necesitan ser abiertas. Esto significa no tan sólo soportar normas abiertas, sino proporcionar soporte enriquecido de APIs para permitir fácil integración y automatización de extremo a extremo en la red por TI, línea de negocios y hasta usuarios. Las organizaciones necesitan ser capaces de innovar a su propio paso y no estar atadas y limitadas por la arquitectura de un solo proveedor.

- Segura—La seguridad en todas las capas de la red es crítica. Aruba asegura la infraestructura alámbrica e inalámbrica con código firmado, boot seguro y protección criptográfica de hardware. Los datos de los usuarios se protegen con cifrado fuerte y una política a nivel de cada usuario, ambos otorgando acceso apropiado y protegiendo a los dispositivos de amenazas. Seguridad basada en analíticos, administración de políticas líder en el mercado y un ecosistema extenso de partners de seguridad confiables permite que TI diseñe y opere su red.

- Autónoma—El aprendizaje de máquina utiliza cantidades masivas de datos analíticos con el objeto de entender el estado operacional y de seguridad de la red. Los sistemas automatizados optimizan el rendimiento y alertan a los administradores de cambios o resaltan cambios potenciales que requieran aceptación mediante operaciones de red en sitio y administradas en la nube.

Las redes tradicionales se han convertido en un verdadero entramado de VLANs y ACLs debido a que las organizaciones han hecho cumplir las políticas y la seguridad sobre una infraestructura que nunca fue diseñada para manejar políticas basadas en aplicaciones. Los switch ports tienen configuraciones estáticas y las interfaces VLAN tienen cientos y en ocasiones miles de ACLs—provocando que los diseños de las redes sean frágiles y que TI tenga miedo de tocarlas.

Diseño

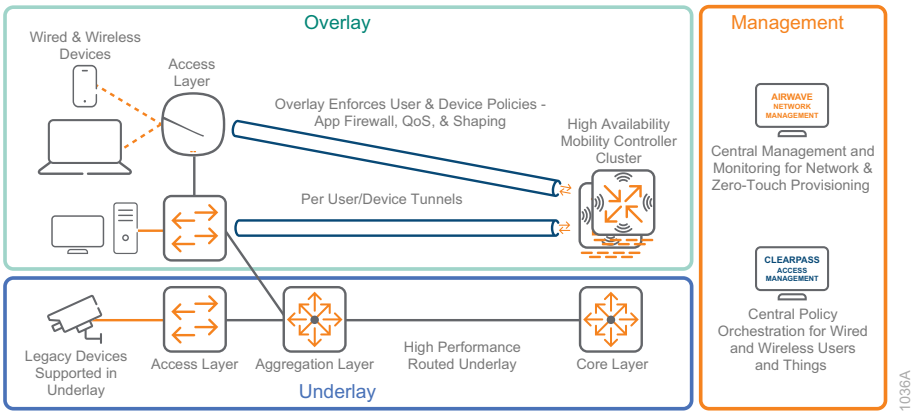
No existe una red en el futuro; existen miles y Aruba está entregando la infraestructura con un modelo para soportar la diversidad y complejidad requerida en redes definidas por software de siguiente generación. En la empresa definida por software, TI opera la infraestructura y la red subyacente y les otorga a los usuarios y a la línea de negocios la capacidad de auto aprovisionar redes sobrepuestas.

CASOS DE USO

- **Acceso temporal guest a los recursos de la red**—Los usuarios pueden crear cuentas guest temporales y otorgar permiso para acceder a los recursos de la red, como sistemas de video de las salas de conferencias, impresoras e Internet mediante una capa superpuesta asegurada efímera.
- **Las instalaciones necesitan permitir acceso de proveedores a los sistemas IoT de edificios**—El administrador del edificio puede crear una capa superpuesta IoT segura para los sistemas de control del edificio y aprovisionar un servicio VPN para el proveedor para que pueda acceder y monitorear al equipo.
- **Los usuarios tienen dispositivos y desean su propia red personal**—Usuarios con múltiples dispositivos alámbricos e inalámbricos necesitan ser capaces de integrar en forma segura sus dispositivos y permitirles comunicarse entre sí, independientemente de la forma en la cual se conectan a la red de la organización.

El entregar la red como un servicio a usuarios es el core de la empresa definida por software. BYOD y su normalización han demostrado que TI necesita ser capaz de soportar una amplia gama de dispositivos de usuario y la avalancha de dispositivos IoT significa que la escala de lo que necesita ser soportado va más allá de lo que un grupo de TI al frente de un sistema de administración de TI por sí solos puede manejar. Herramientas que permitan que TI delegue la creación de servicio a usuarios en base a privilegios definidos son necesarias para habilitar a la empresa y evitar una nueva ola completa de TI en las sombras.

Figura 1 Arquitectura Mobile First de Aruba



CAPA SUBYACENTE

Las redes empresariales necesitan soportar los puntos terminales actuales, incluyendo muchos sistemas legados, mientras transicionan a un modelo definido por software. Los diseños que requieran un rediseño completo de la red, incluyendo hardware y el stack de protocolos de la red, pueden provocar una interrupción grave y problemas de riesgo-compatibilidad, especialmente con sistemas legados. Mobile First mantiene la red enrutada existente, utilizando un protocolo de gateway interior (IGP), como OSPF, como una capa subyacente, permitiendo que TI continúe corriendo y operando el hardware existente cuando la nueva red sea desplegada. Los dispositivos legados pueden continuar operando en la capa subyacente y las mejoras a la política permiten seguridad y control adicional sobre la capa subyacente de la red, más allá de lo que se despliega comúnmente en redes tradicionales.

CAPA SOBREPUESTA

La capa sobrepuesta permite que las organizaciones envíen tráfico Layer 2 o Layer 3 por túneles en forma segura encima de la red existente. Aruba ha estado entregando redes inalámbricas con un modelo de capa superpuesta desde el principio, permitiendo que TI entregue servicio, que de otra forma no sería seguro ni estable, a través de redes de múltiples proveedores. Aruba está extendiendo esta funcionalidad a las redes alámbricas, permitiendo que el switch de la capa de acceso actúe como un "punto de acceso alámbrico". El tráfico de red desde usuarios y dispositivos alámbricos e inalámbricos se envía mediante túneles a clusters de controladores de movilidad centralizados. Toda la política a nivel de usuario y dispositivos se puede hacer cumplir en la capa sobrepuesta utilizando el firewall del controlador de movilidad, QoS y conformación de tráfico y el contexto de usuario se comparte fácilmente con otros dominios. Las estructuras de direcciones VLAN e IP existentes se pueden mantener, pero debido a que la política se hace cumplir a los niveles de usuario y de grupo, las direcciones VLAN e IP no están amarradas a política.

SEGMENTACIÓN DINÁMICA

La Arquitectura Mobile First de Aruba no depende de configuraciones de puertos estáticos, VLANs, o listas de acceso en access points—o switches de acceso en la red—para aplicar política a usuarios y dispositivos.

- Nodo Túnel—Permite que un switch de acceso actúe como un "punto de acceso alámbrico". Los usuarios que se conecten al switch, se pueden conectar por túnel al controlador de movilidad para proporcionar la misma de política y experiencia de usuario que cuando se conectaban a la red inalámbrica. Para alta disponibilidad, se crean múltiples túneles y, si un controlador necesita ser sacado de la línea para mantenimiento o si ocurre una caída no planificada, el sistema efectúa failover transparentemente y envía al usuario a un controlador de respaldo.

- Roles descargables—Si los usuarios o los dispositivos legados se conectan a la red alámbrica y necesitan conectividad directa a la capa subyacente, roles descarga hables permiten que la configuración del puerto de acceso se cargue dinámicamente en base a la postura y política del usuario y el dispositivo.

- Política centralizada—Aruba ClearPass maneja a todos los usuarios y dispositivos conectados a la red. Los dispositivos se pueden perfilar cuando se conectan a la red, su postura se verifica y después, la política adecuada se descarga al puerto de acceso.

- Confianza adaptativa—Después de que se les otorga acceso a la red a los dispositivos, su comportamiento se monitorea continuamente por herramientas de analíticos de comportamiento, firewall y sistemas IPS. Si la postura de seguridad del dispositivo cambia, un analista de seguridad puede tomar un número de acciones manuales o automatizadas, como reautenticación para verificar al usuario, poner en cuarentena al dispositivo con acceso limitado a los recursos de la red para permitir remediación sencilla, o aislar completamente al dispositivo de la red mientras se investigan los incidentes. Si se encuentra que todo está correcto, o que el dispositivo se remedia, el analista de seguridad puede restaurar rápidamente el acceso normal.

La segmentación dinámica de Aruba permite que las organizaciones conecten a usuarios y a dispositivos a puertos alámbricos y, a través de un túnel, conectarlos a un controlador o a una VLAN o subred adecuada y descargar una política dinámica (con parámetros de seguridad y de QoS) al puerto al cual estén conectados. Esto extiende la funcionalidad de redes tradicionales alámbricas 802.1X a flujos de trabajo que se desplegaban típicamente sólo en redes inalámbricas, como una integración sencilla por usuarios de dispositivos desconocidos (BYOD), acceso guest alámbrico con el mismo portal cautivo en la red inalámbrica y soporte y remediación automatizados para dispositivos que fallen las verificaciones de política o de postura con el portal cautivo.

NETWORKING CONTINUO (NON-STOP)

La conectividad inalámbrica se visualiza como un servicio a nivel de utilería en las redes empresariales de hoy, lo cual significa que los usuarios esperan que siempre esté disponible y que tenga un rendimiento óptimo. La arquitectura de Aruba entrega un número de características alámbricas e inalámbricas para soportar redes inalámbricas desplegadas como un servicio continuo con alta disponibilidad, lo cual es una parte inherente del diseño.

- Clustering de Controladores—Hasta 12 controladores de movilidad de Aruba pueden formar un cluster de alta disponibilidad que comparte carga y que puede escalar a cientos de Gbps de tráfico y a decenas de miles de usuarios.

- Actualizaciones en Servicio—Con Aruba OS 8, la red inalámbrica es capaz de actualizar el software de access points y controladores de forma que sea transparente para los usuarios en la red inalámbrica. A los usuarios se les desvía elegantemente de APs y controladores selectos mientras se actualizan y después se agregan de regreso a la red en forma transparente.

- Failover Transparente—Access points se conectan a múltiples controladores en un cluster y, en el caso de una falla del controlador primario, los access points cambien al secundario sin ninguna interrupción que sea observable por el usuario.

- Switching Continuo (Non-Stop)—Aruba OS-CX en el core y en las capas de agregación de la red entrega alta disponibilidad y actualizaciones sin hits, permitiendo que TI proporcione servicio a la red sin provocar una caída.

En conjunto, estas características permiten que una red Aruba entreguen conectividad inalámbrica que pueda correr en forma continua en la red de una organización. La red se puede actualizar mientras los usuarios estén conectados, sin ninguna interrupción. Y debido a la alta disponibilidad mejor en clase, la red puede manejar fallas en los access points y en los controladores sin que los usuarios experimenten ninguna interrupción.

Resumen

La Arquitectura Aruba Mobile First permite que las organizaciones transicionen en forma elegante su red existente a una empresa definida por software, habilitando nuevas características y funcionalidad mientras se soportan sistemas legados. Una infraestructura de red abierta, de múltiples proveedores, permite que las organizaciones innoven a su propio paso y que no se sientan atados a una solución de un proveedor único, sino que también aprovechen sus inversiones existentes. La seguridad interconstruida en todas las capas de la red protege a la infraestructura, a los usuarios y a los dispositivos de amenazas existentes y emergentes del exterior y del interior. El uso inteligente de analíticos por administradores y el aprendizaje de máquina basada en automatización proporcionan aseguramiento de la red y comienza la transición a una red que "auto opera", en dónde TI mantiene la infraestructura y la política y los usuarios aprovisionan servicios dinámicamente.

Puede utilizar la forma de retroalimentación para enviar sugerencias y comentarios acerca de esta descripción general de la solución.

a Hewlett Packard Enterprise company

B-000110A-1 03/18