



Red Aruba centrada en el usuario para la empresa

¿Cuál es su objetivo? ¿Proporcionar acceso inalámbrico seguro a sus usuarios en todo un edificio? ¿En un campus? ¿En todo el mundo? ¿Proporcionar una seguridad y una experiencia de usuario al alcance de todos sus usuarios independientemente de dónde se conecten? Reducir los costes de telefonía y potenciar la productividad del usuario con voz sobre LAN inalámbrica y convergencia fijo móvil (FMC)?

Aruba ha elaborado un nuevo enfoque para ayudarle a conseguir su objetivo. Las redes Aruba centradas en el usuario integran WLAN adaptativas, seguridad basada en identidad y servicios de continuidad de aplicación en un sistema de alto rendimiento para campus empresariales, edificios de oficinas, sucursales y teletrabajadores. El resultado es una red de gestión centralizada que distribuye las aplicaciones empresariales por la LAN, la WAN e Internet, aumentando la productividad de los usuarios sin ningún impacto negativo sobre la seguridad. Frente a otras soluciones, la red Aruba centrada en el usuario se superpone a las redes existentes, preservando las inversiones existentes y evitando cambios de red disruptivos.

Características únicas de Aruba

SEGURIDAD BASADA EN IDENTIDAD

Las aplicaciones móviles en la empresa requieren que la red cubra de manera segura a los usuarios allí donde vayan. Los métodos de control de acceso tradicionales, determinados por el punto de entrada a la red, no admiten movilidad. El control de acceso móvil necesita el contexto de usuario, incluyendo su función organizativa, tipo de dispositivo, ubicación, hora e incluso comportamiento de uso, a la hora de establecer una política. Diferentes grupos de empleados, subcontratados e invitados requerirán niveles únicos de acceso e incluso métodos de autenticación diferentes (por ejemplo, 802.1x, VPN y portal cautivo). Por último, todo esto debe conseguirse sin aumentar la complejidad de la red y consiguiendo una integración sin fisuras con las estructuras de directorios existentes como RADIUS, LDAP o Active Directory.

Los controladores de movilidad de Aruba Networks y los puntos de acceso están especialmente capacitados para ofrecer esas funciones. Frente a otras soluciones que asignan políticas a

SSID/VLAN específicas para proteger y segmentar una red, Aruba implementa un cortafuegos de estado basado en funciones con certificado ICASA que permite crear funciones exclusivas y aplicarlas a cada usuario y dispositivo. El cortafuegos también admite una lista negra de clientes que violen la política, finalizando la sesión y denegando el acceso a la red de ese momento en adelante. Las redes Aruba centradas en el usuario se superponen a las redes ya existentes y se integran con cualquier estructura de directorios instalada con anterioridad.

CONTROL Y GESTIÓN CENTRALES

Desplegar y gestionar una red empresarial global puede resultar una ardua tarea si no se enfoca correctamente. La red Aruba centralizada y su gestión de políticas está diseñada para facilitar su despliegue y funcionamiento. Con la gestión centralizada Aruba, la configuración de los datos se propaga de forma automática y segura por toda la red, los puntos de acceso y los controladores locales y remotos. Se proporciona una única interfaz para TI con el fin

La ventaja de Aruba:

- **Seguridad basada en identidad:** La seguridad acompaña a los usuarios que se desplazan por la LAN, la WAN e Internet
- **Gestión central:** De fácil configuración, supervisión y resolución de problemas con control centralizado
- **Reconocimiento de aplicaciones:** Optimizado para soportar datos, voz y vídeo convergentes de forma inalámbrica
- **Red flexible y escalable:** Con el modelo de despliegue superpuesto no son necesarias las actualizaciones y los rediseños de red.
- **Preparado para el futuro:** Software actualizable para nuevas tecnologías como 802.11n, NAC, mesh y eFMC

de implementar y proteger las políticas subyacentes que aseguran la integridad, la seguridad y el funcionamiento de toda la red. La función de control centralizado también incluye perfiles de rendimiento que son utilizados por los puntos de acceso Aruba para optimizar su operación y soportar con garantías las aplicaciones esenciales. El resultado es una red de gran escalabilidad que es lo suficientemente simple como para ser utilizada por usuarios no especializados.

RECONOCIMIENTO DE APLICACIONES

Cada vez son más frecuentes en la empresa los servicios de vídeo y voz sobre IP con la introducción de teléfonos móviles con Wi-Fi y la creciente popularidad de las comunicaciones multimedia. Para soportar servicios como el de voz, la red debe ser capaz de implementar la calidad de servicio (QoS) por aire y por cable, protegiendo las llamadas de voz y ajustando los patrones de tráfico para optimizar la calidad de voz. La solución de Aruba reconoce la voz totalmente, aprovechando un cortafuegos basado en la aplicación que asegura y prioriza la voz. Como la arquitectura mantiene un contexto centralizado para la QoS y la seguridad, puede seguir con facilidad la voz de los usuarios mientras se mueven por la red. El tráfico de voz se prioriza usando etiquetas QoS 802.1p y DSCP. El sistema reconoce automáticamente los protocolos de voz más comunes (especialmente SIP, SVC, y SCCP) y aplica una prioridad estricta al tráfico de voz. La priorización de llamadas también puede realizarse a través del control de admisión

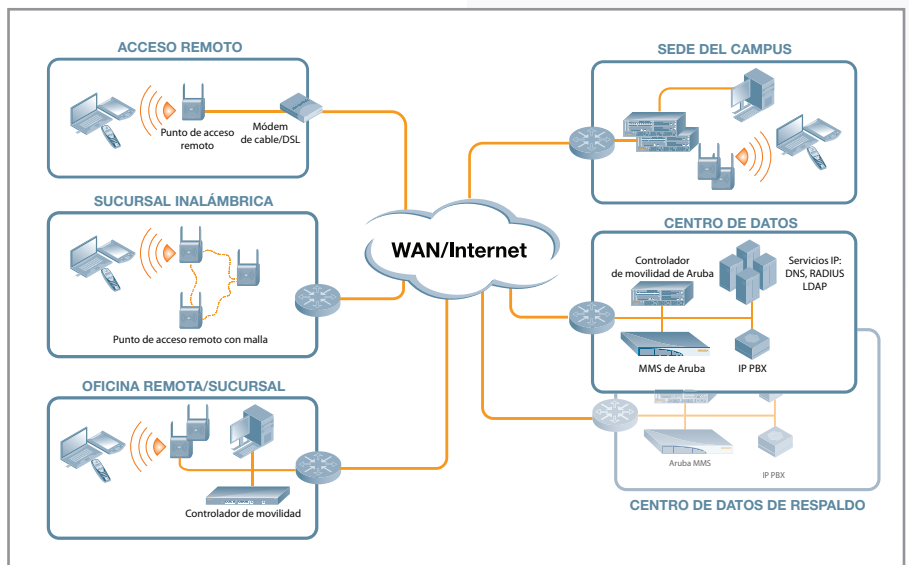
de llamadas (CAC). CAC establece un máximo de llamadas de voz por AP, moviendo de forma dinámica cualquier llamada por encima de este límite a otros AP vecinos y manteniendo una calidad de la voz excepcionalmente elevada.

ESCALABLE Y PREPARADO PARA EL FUTURO

Un sistema WLAN debe ser compatible con los requisitos existentes de una empresa, además de adaptarse al crecimiento y la adopción futura de dispositivos y aplicaciones móviles. Los retos clave de ampliar una LAN inalámbrica de empresa están relacionados con la densidad de usuarios y dispositivos, la carga instantánea durante el uso en horas punta, y la movilidad de los usuarios por diferentes áreas a través de la LAN, la WAN e Internet. Aruba Networks ha desarrollado innovaciones para automatizar la configuración RF, descargar los servidores backend AAA y hacer más escalable el diseño de VLAN para adaptarse a diferentes patrones de uso. Adicionalmente, Aruba ofrece plataformas de alto rendimiento específicas, de gran escalabilidad y potente capacidad que implementan las aplicaciones existentes, la infraestructura de TI y los clientes estándar. Diseñados para adaptarse a las necesidades de los usuarios de hoy y de los años venideros, la mayoría de los productos Aruba cuentan con una arquitectura de software modular y actualizable que se puede mejorar fácilmente con el tiempo a medida que estén disponibles nuevas funciones.

La solución de Aruba Networks para empresas

La solución Aruba está formada por tres componentes clave: puntos de acceso ligeros (AP), controladores de movilidad centralizados y módulos de software para los controladores de movilidad; además de las aplicaciones opcionales de protección frente a amenazas y análisis de gestión. Los AP proporcionan una conectividad inalámbrica segura a los dispositivos y se conectan mediante sistemas LAN/WAN existentes para conducir todo el tráfico LAN inalámbrico por un túnel GRE o IPsec a un controlador de movilidad instalado en el centro de datos. El controlador de movilidad es el punto central de configuración, gestión, servicios de continuidad de la aplicación y seguridad. Con los módulos de seguridad para



A continuación, se incluye la explicación de una red inalámbrica en un entorno empresarial con servicios de TI centralizados:

Centro de datos: Uno o varios controladores de movilidad se encuentran instalados en el centro de datos, que puede ser usado como el punto de gestión y configuración para toda la red internacional. Estos controladores también terminan AP usados para conectividad inalámbrica en la sede, así como AP utilizados por teletrabajadores, trabajadores domésticos y oficinas ad-hoc. Un controlador principal puede admitir hasta 500 controladores remotos y también puede respaldar a un controlador en una ubicación remota en caso de caída. Para alcanzar un mayor despliegue, varios controladores principales pueden compartir la tarea de gestionar los controladores locales y AP en ubicaciones remotas, y el sistema de gestión de movilidad (MMS) puede usarse como interfaz única de gestión y configuración.

Oficinas de mediano y gran

tamaño: En función del número de AP necesarios para cada ubicación, se instala un modelo diferente de controlador de movilidad Aruba, llamado controlador local. Todos los modelos de controladores Aruba usan el mismo software y tienen la misma funcionalidad, pero difieren en su capacidad de AP, que oscila entre 4 y 512 AP. Cada controlador local obtiene su configuración del controlador principal. La continuidad de aplicación y las políticas de seguridad se aplican a nivel de usuario por el controlador local. Los diferentes roles de usuario se aplican en función de la política de

grupo definida en la infraestructura de autenticación y los invitados pueden ser redireccionados mediante un túnel fuera de la red para terminar en la zona desmilitarizada o DMZ. Los controladores locales ofrecen protección contra intrusiones inalámbricas y pueden proporcionar servicios de autenticación o enviar peticiones al centro de datos. Cada controlador local calibra automáticamente la cobertura de RF para optimizar el rendimiento de la aplicación y tapar cualquier hueco de cobertura. Además, para extender la cobertura inalámbrica a áreas que sean difíciles o costosas de cablear, los AP de Aruba tienen capacidad de backhaul (red de retorno) sobre Wi-Fi mediante la tecnología galardonada de malla empresarial segura.

Usuarios remotos y oficinas

temporales: Los AP remotos son una solución económica para ofrecer conectividad inalámbrica segura y gestionada centralmente a las ubicaciones que sólo necesitan uno o dos AP. Los AP remotos se pueden conectar directamente vía Ethernet a una conexión de Internet pública o privada o a la LAN. Los AP remotos detectan automáticamente el controlador principal, establecen un túnel VPN al centro de datos y extienden la conectividad inalámbrica segura al usuario. El tráfico de la aplicación se puede dirigir mediante un túnel al centro de datos o bien se puede puentear localmente.



WWW.ARUBANETWORKS.COM

1322 Crossman Avenue. Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550