INFORME DEL SECTOR

Solución para finanzas

Red Aruba centrada en el usuario para las finanzas

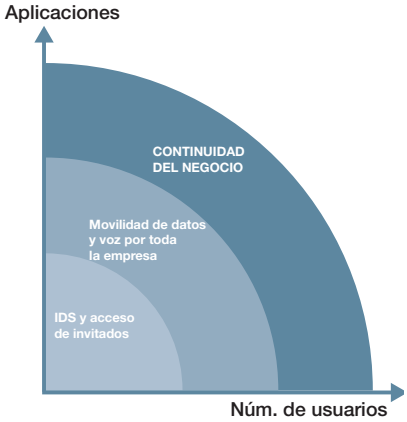
¿Cuál es su objetivo? ¿Imponer a sus usuarios una política de no usar redes inalámbricas, pero ofrecer a los invitados un acceso inalámbrico a Internet seguro? ¿Potenciar la productividad de usuario con acceso inalámbrico seguro a aplicaciones de datos y voz en todo un edificio? ¿En un campus? ¿En todo el mundo? ¿Proporcionar continuidad al negocio incluso en caso de disrupciones como las causadas por inclemencias del tiempo, sucesos imprevistos y desastres?

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 consistente de alto rendimiento para satisfacer sus necesidades de movilidad segura, desde el bloqueo del acceso a través de servicios de protección de intrusión inalámbricos (IPS) hasta la autorización de acceso a invitados para permitir una movilidad masiva y la continuidad del negocio. La red Aruba de gestión centralizada está diseñada para movilizar las aplicaciones empresariales por la LAN, la WAN e Internet, aumentando la productividad de los usuarios sin ningún impacto negativo sobre la seguridad. A diferencia de otras soluciones, la red Aruba centrada en el usuario se superpone a las redes existentes, preservando las inversiones actuales y evitando cambios de red disruptivos.

Características únicas de Aruba

UNA PLATAFORMA, VARIOS USOS: Los gestores de red están de acuerdo en que las necesidades de movilidad crecen más rápido de lo previsto. Vale la pena planificarse con tiempo y elegir un sistema que crezca con usted. Con Aruba, puede empezar bloqueando el acceso inalámbrico, desplegar un acceso de invitados, pasar lentamente hacia una movilidad masiva para toda la empresa e incluso ofrecer continuidad en el negocio mediante el acceso remoto de miles de usuarios, todos en la misma plataforma con un software subyacente común. Esta profundidad de capacidades y esa flexibilidad de aplicaciones son posibles gracias a la integración única de la LAN inalámbrica, seguridad y acceso remoto en una sola plataforma gestionada centralmente.

SEGURIDAD BASADA EN IDENTIDAD
La seguridad Aruba basada en identidad está diseñada para permitir el acceso de forma segura a los empleados, subcontratados e invitados simultáneamente, y al mismo tiempo proteger los dispositivos de red de los usuarios no autorizados y de un usuario respecto a otro. El enfoque de



Aruba combina identidad de usuario, posición del dispositivo, tipo de tráfico, hora del día y otros parámetros para crear políticas de acceso basadas en roles, que se cumplen continuamente mediante el cortafuegos con certificado ICSA y las tecnologías de cumplimiento de dispositivo. La arquitectura centralizada Aruba expande la seguridad y las normas de acceso para que acompañen al usuario en todo el edificio, el campus e incluso por Internet.

La ventaja de Aruba:

- **Plataforma integrada única**: Proporciona seguridad para políticas no inalámbricas, acceso de invitados, sistema inalámbrico seguro dentro del edificio y acceso remoto para la continuidad del negocio.
- **Seguridad basada en identidad:** Permite el acceso seguro de invitados y empleados, a la vez que cumple las necesidades de confidencialidad de datos de conformidad con la ley.
- **Gestión central**: Un único punto de control para redes en oficinas principales, sucursales y oficinas domésticas facilita la configuración, la supervisión y la solución de problemas.
- **Continuidad de aplicación**: Asegura el manejo fiable de datos, voz y vídeo convergentes de forma inalámbrica.
- **Red flexible y escalable:** El modelo de despliegue superpuesto evita actualizaciones y rediseños de red.

Con la seguridad basada en identidad, las instituciones financieras pueden facilitar de forma segura el acceso a los invitados y los empleados y a la vez cumplir los requisitos de confidencialidad de conformidad con la normativa.

Acceso de invitados: Invitados y subcontratados necesitan acceso a Internet, pero el uso de segmentación VLAN no es una solución segura, ya que está expuesta a ataques de suplantación. La seguridad basada en identidad que encapsula y separa el tráfico de la empresa del tráfico de invitados asegura que no se revela ninguna información secreta. La solución Aruba termina todo el tráfico de invitados encapsulado en GRE directamente en un enrutador de la DMZ.

Confidencialidad de datos de conformidad con la normativa legal: Con Aruba, los datos están protegidos en la capa 2 y en la capa 3. Además, todos los datos están cifrados y se mantienen así desde el cliente hasta el centro de datos. En ningún punto de esa transmisión la información está sin cifrar o disponible en texto. En un entorno de uso mixto, donde pueden darse conflictos de intereses, la solución de Aruba asegura un total control de acceso y una separación de información basada en el cifrado como marcan las regulaciones SOX y GLBA.

Continuidad del negocio: La planificación de la continuidad del negocio es esencial en las empresas actuales que dependen de la información porque las interrupciones del negocio debidas a las inclemencias del tiempo, las amenazas pandémicas y los desastres son cada vez más frecuentes. Sin embargo, el desarrollo de la continuidad del negocio puede resultar muy cara y compleja dada la falta de soluciones para oficinas domésticas de tipo empresarial. Ni los productos para el consumidor ni las soluciones para sucursales de tipo empresarial cumplen los requisitos. Por un lado, se encuentran las preocupaciones relativas a la seguridad y la fiabilidad y, por otro, se necesita gestión e instalación profesional bastante costosa. La solución de AP remoto de Aruba cubre esta laguna con un diseño innovador que ofrece en los hogares de los empleados la misma conectividad de voz y datos que en la oficina. Con el AP Remoto, Aruba ha revolucionado el campo de los puntos de acceso ligeros y ha aplicado dicha revolución al acceso remoto. Trasladando la gestión a la sede, los AP remotos son instalables por el usuario y gestionados centralmente, eliminando, por tanto, el gasto de operaciones y reduciendo el gasto de capital.

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 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.

CONTINUIDAD DE APLICACIÓN

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.

ARUBA networks

INFORME DEL SECTOR

Solución para finanzas

La solución de Aruba Networks para la industria financiera

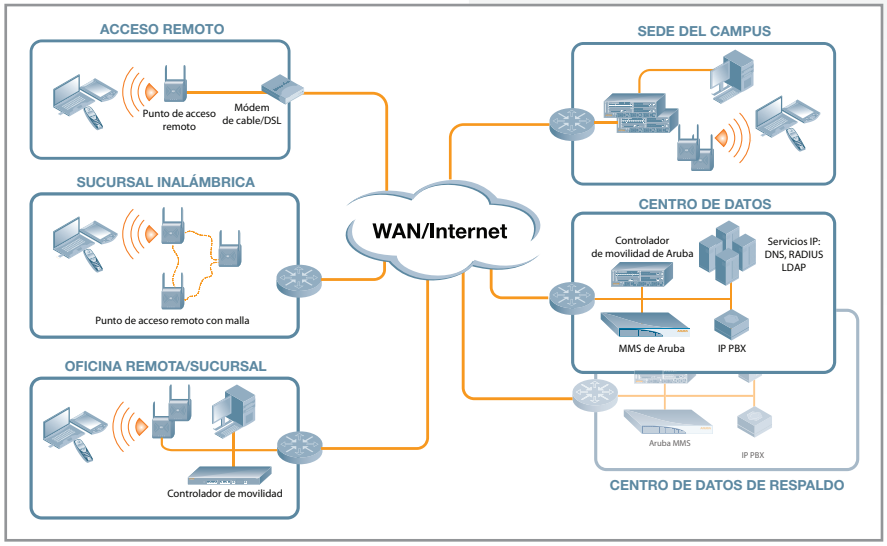
La solución Aruba está formada por tres componentes clave: puntos de acceso ligero (AP), controladores de movilidad centralizados y módulos de software para los controladores de movilidad; además de los equipos opcionales de protección frente a amenazas y análisis de la gestión. Los AP proporcionan una 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 controladores de movilidad, Aruba ofrece la seguridad necesaria de conformidad con la normativa.

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 operan con 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 también locales ofrecen protección contra intrusiones inalámbricas y pueden ofrecer servicios de autenticación local 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 pequeñas oficinas: 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.



ARUBA networks

WWW.ARUBANETWORKS.COM

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

© 2007 Aruba Networks, Inc. Todos los derechos reservados. Aruba Networks es una marca comercial de Aruba Networks, Inc. Todas las otras marcas comerciales o marcas registradas son propiedad de los respectivos propietarios. Se reserva el derecho de modificar los productos sin previo aviso.

IB_FIN_ES_071029