INFORME DEL SECTOR

Solución para la administración

Red Aruba centrada en el usuariopara administraciones públicas

¿Cuál es su objetivo? ¿Proporcionar acceso inalámbrico fiable que cumpla con la normativa FIPS 140-2 a sus usuarios? ¿Mejorar la productividad del usuario con acceso inalámbrico seguro en cualquier lugar, desde el lugar en que sucede la acción hasta la sala de instrucción, desde las oficinas civiles a las zonas donde se lleva a cabo la respuesta?

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, áreas exteriores 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 INTEGRADA DE CONFORMIDAD CON LA NORMATIVA

Las redes Aruba centradas en el usuario proporcionan soluciones móviles seguras para la gente que trabaja en la administración. La plataforma Aruba garantiza que cumple los siguientes requisitos legales:

- Cifrado de nivel 2 validada por la FIPS 140-2
- Cumplimiento con los estándares 802.11i
- Cumplimiento de la Directiva 8100.2 del Departamento de Defensa de Estados Unidos
- Seguridad de extremo a extremo en un canal asegurado
- Protección y detección de intrusiones inalámbricas
- Certificación de criterios comunes
- Autenticación 802.1x (incluye tarjeta de acceso común)
- Certificación JITC

SEGURIDAD BASADA EN IDENTIDAD:CONTROL DE ACCESO POR NIVEL DE CERTIFICACIÓN DE SEGURIDAD

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 de red, no soportan movilidad. El control de acceso móvil necesita el contexto de usuario, incluyendo su función organizativa, certificación de seguridad, tipo de dispositivo, ubicación, hora e incluso comportamiento de uso, a la hora de establecer una política. Diferentes grupos de empleados, subcontratados e invitados de diferentes suborganizaciones requerirán niveles únicos de acceso e incluso métodos de autenticación diferentes (por ejemplo, 802.1x, VPN y portal cautivo). Además, todo esto debe realizarse sin aumentar la complejidad de la red e integrándose 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 ICSA que permite crear funciones exclusivas y

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 convergentes, voz y vídeo de forma inalámbrica.
- **Red flexible y ampliable:** El modelo de despliegue superpuesto evita actualizaciones y rediseños de red.
- **Preparado para el futuro:** Software actualizable para nuevas tecnologías como 802.11n, NAC, mesh y eFMC

aplicarlas a cada usuario,según nivel de certificación de seguridad y su dispositivo. El cortafuegos también mantiene una lista negra de clientes que incumplen 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.

GESTIÓN CENTRAL Y RESOLUCIÓN DE PROBLEMAS

Desplegar y gestionar una red a nivel empresarial y 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.

Aruba permite la captura remota de paquetes para que los gestores de TI puedan solucionar los problemas en otras ubicaciones de la misma ciudad o país. Además, Aruba ofrece una visión dinámica completa del entorno RF de cada edificio, base o ubicación de la red. Los administradores de red pueden llevar a cabo todas las actualizaciones y el mantenimiento de forma centralizada desde una ubicación, recibiendo alertas de intrusión u otras señales de seguridad en tiempo real.

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 el usuario y la densidad del dispositivo, las descargas instantáneas 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 la administración

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 conforme a la normativa.

A continuación, se incluye la explicación

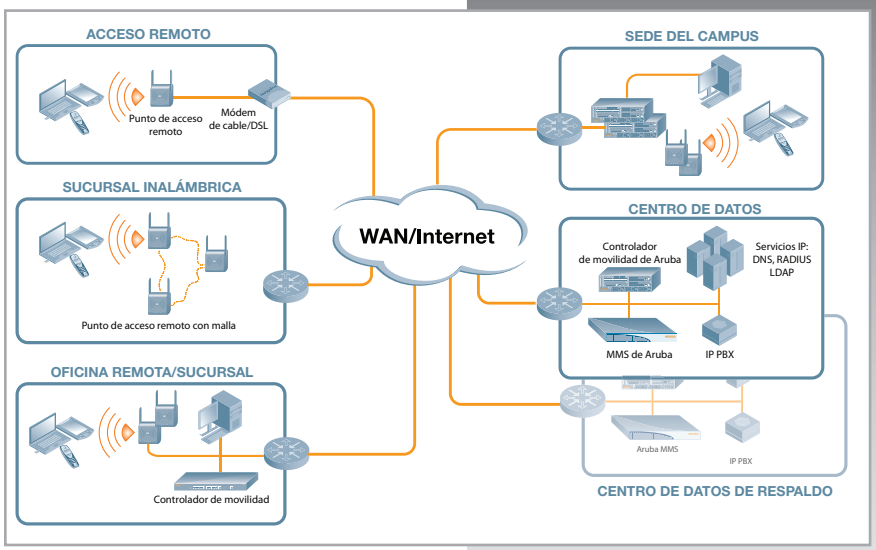
ARUBA networks

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 soportar hasta 500 controladores remotos y también puede respaldar a un controlador en una ubicación remota en caso de parada programada. 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 proporcionar 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.



SEGURIDAD COMPLETA DE EXTREMO A EXTREMO

Aruba Networks permite cifrado programable para la transición sin dificultades de AES-CCM/802.11i y AES-CBC de 256 bits hacia dispositivos alámbricos o inalámbricos sin necesidad de actualizar el hardware. Todo esto, en combinación con una seguridad de defensa exhaustiva que proporciona un soporte multicapas integrado que bloquea el aire, el cable, la red y el usuario.

Aruba también ha continuado innovando en este campo dotando de capacidades de EAP-Offload a su software validado a través de la normativa FIPS. Con EAP-Offload, la autenticación sensible y las transacciones de gestión importantes se llevan a cabo dentro del límite criptográfico seguro del controlador de movilidad centralizado, y no necesitan ser transmitidas como texto libre o usando algoritmos de cifrado débiles entre el controlador de movilidad y el servidor RADIUS externo.

Alternativamente, Aruba también protege los servidores RADIUS que soportan EAP mediante la función RADIUS sobre IPsec, como recomienda la directriz RFC 3579. Esto ofrece la primera solución FIPS del sector para un despliegue superpuestoinalámbrico no disruptivo.

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_ FED_ES_071029