



La solución de acceso para invitados de Aruba

El acceso para invitados suele ser la primera aplicación implementada por las organizaciones que despliegan una WLAN. El acceso para invitados proporciona una interacción visible con las empresas colaboradoras y los visitantes y da una impresión positiva de la organización. Un buen sistema de acceso a invitados proporcionará en primer lugar un acceso fiable y de alto rendimiento a Internet sin que sea necesario que el invitado deba superar innumerables dificultades para reconfigurar su PC para conectarse. La conectividad follow-me de Aruba y sus servicios de continuidad de la aplicación permiten que el invitado disfrute de un rendimiento óptimo.

Una red de acceso de invitados debe separar y segregar el tráfico interno y el de invitados para conseguir una seguridad de acero para las LAN y los servidores de la organización. Puesto que el acceso a invitados se provee desde la misma infraestructura WLAN y LAN que lleva el tráfico interno, se trata de un reto muy importante que está directamente solucionado por la seguridad follow-me de Aruba.

Uso del acceso para invitados

Existen numerosas ventajas de productividad del hecho de proporcionar a los invitados, contratistas y empleados temporales acceso instantáneo a la información de la empresa. Al ofrecer un acceso a Internet seguro, estos usuarios pueden acceder por VPN a su red corporativa o de casa para utilizar el correo electrónico y otros recursos no almacenados en su escritorio o en su dispositivo móvil.

PROTECCIÓN DE LA INTRANET: Una solución de acceso a invitados segura debe garantizar que los invitados se conecten directamente a Internet, pero que no tengan acceso a los recursos de la red interna aunque el tráfico del invitado corra por la infraestructura LAN y WLAN de la organización junto con el tráfico informático corporativo. Las arquitecturas más viejas utilizan una VLAN dedicada a ofrecer esta protección. Sin embargo, la gestión de VLAN es engorrosa y el menor error de configuración puede provocar brechas de seguridad, permitiendo que algún intruso utilice la red de acceso de invitados para atacar a los servidores y recursos de la organización. Aruba implementa una seguridad basada en

la identidad para identificar, categorizar y contener el tráfico de invitados sin importar por dónde naveguen en la WLAN y todo ello sin configuraciones en la VLAN.

Los portales cautivos están bien establecidos como medio de acceso a Internet, ya sea en hoteles, centros de conferencias o hotspots Wi-Fi. Cuando el invitado abre por primera vez un navegador Web, el flujo es interceptado y al invitado le aparece una página de autenticación. Este portal cautivo, que puede personalizarse con el diseño propio de la organización, puede solicitar una dirección de correo electrónico, una contraseña y/o que acepte los términos del acuerdo de utilización.

ASIGNACIÓN DE CREDENCIALES FLEXIBLE Y NADA ENGORROSA:

Algunas organizaciones se enorgullecen de proporcionar acceso abierto a Internet a cualquiera. Sin embargo, esto es cada vez más inusual debido al riesgo para la organización pues se les culpa del mal uso de su red. Por ejemplo, si un ataque a un objetivo a través de Internet se origina desde una red de empresa y no se han realizado

Ventajas:

- **Separación del tráfico:** El cortafuegos stateful certificado por ICSA garantiza que los invitados no accedan a la Intranet de la organización
- **Característica integrada:** El acceso de invitados puede agregarse a cualquier red centrada en el usuario de Aruba
- **Control flexible:** De un acceso abierto para todos a contraseñas individuales únicas
- **Hospitalario:** Se integra con sistemas de terceros para la verificación de tarjetas de crédito

los pasos adecuados para proteger su red, podrían ser considerados responsables. La mejor manera de controlar el acceso de invitados es mediante contraseñas individuales temporales, pero puede ser una tarea engorrosa si no hay sistemas de soporte disponibles. La mejor opción es proporcionar a cada invitado una tarjeta que incluya su contraseña en el momento en que entren en la recepción. De esta manera se minimizan los inconvenientes a la vez que se maximiza la seguridad.

COSTES MÍNIMOS DE

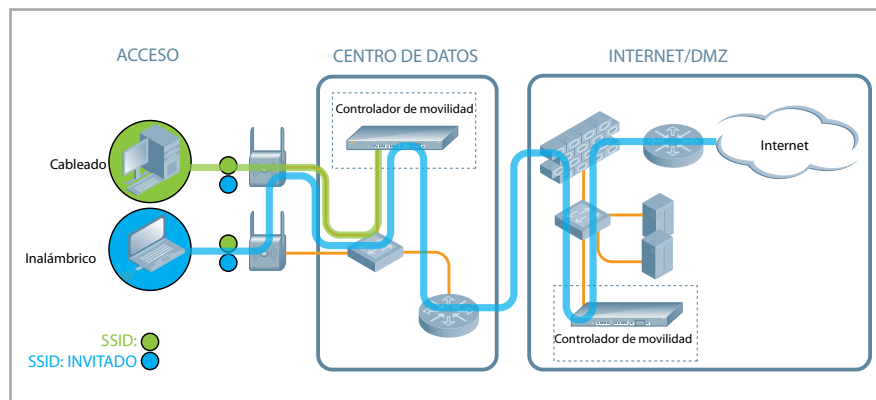
ADMINISTRACIÓN: Las aplicaciones TI deberían funcionar sin la necesidad de soporte frecuente y con el menor número de llamadas a la hotline por parte

de los usuarios. En el caso del acceso para invitados, esto significa que los recepcionistas tendrán que poder crear cuentas para invitados fácilmente y emitir credenciales de forma rápida. El invitado debería poder acceder reconfigurando su PC mínimamente y el servicio de Internet debería ser ligero y rápido.

USO Y DATOS DE AUDITORÍA: Even guest access services must provide historical data accounting for who used the network, when they used it and how it was used.

La solución de acceso de invitados de Aruba consta de tres componentes clave: puntos de acceso (PA) ligeros, controladores de movilidad

Cómo habilita Aruba el acceso de invitados



centralizados y módulos de software de seguridad para el controlador de movilidad. También existe un sistema de gestión de la movilidad para redes más grandes. Los PA proporcionan una conectividad inalámbrica segura a los dispositivos y se conectan mediante sistemas LAN/WAN existentes para llevar 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. El acceso de invitados es una característica inherente de todas las redes de Aruba centradas en el usuario.

ACCESO DE INVITADOS EN UNA

WLAN EXISTENTE: Una red de Aruba centrada en el usuario desplegada para uso corporativo tendrá puntos de acceso para proporcionar cobertura Wi-Fi. Al añadir el acceso para invitados, es posible que sea necesario cubrir áreas nuevas del edificio con PA adicionales.

En instalaciones más grandes es posible que deba instalarse un controlador de movilidad en la DMZ del cortafuegos de la empresa. Todo el tráfico de invitados se transporta de forma encriptada desde los PA a través de los túneles GRE hasta un controlador de movilidad y luego a través de otro túnel encriptado a la DMZ, donde se conecta de forma segura al cortafuegos y a Internet. Los controladores de movilidad de Aruba disponen de un cortafuegos stateful certificado por ICSA que les permite realizar esta función tan exigente.

PORTAL CAUTIVO: Los dispositivos de los clientes conectados a la red están bloqueados de todo acceso hasta que se abra un navegador Web y se introduzcan las credenciales de autenticación. El intercambio de las credenciales de autenticación está protegido mediante SSL estándar. El sistema puede solicitar un nombre y una contraseña válidos o se puede configurar para que únicamente solicite las direcciones de correo electrónico que no son validadas. Las páginas del portal cautivo se pueden

configurar con el logotipo de la empresa, con fondos, políticas de uso aceptables y más texto. La configuración de acceso por tarjetas de crédito y sistemas de facturación es posible gracias a la integración de aplicaciones de terceros.

SEPARACIÓN DEL TRÁFICO DE INVITADOS: El tráfico de invitados se puede separar del tráfico corporativo mediante un módulo de software en el controlador de movilidad. Es posible dar a los trabajadores subcontratados diferentes políticas de seguridad que no concedan privilegios totales a la red corporativa. Esto es una ventaja de la seguridad única de Aruba basada en la identidad. El cortafuegos de aplicación de políticas permite un control preciso

del usuario, aplicando políticas a individuos o grupos de usuarios.

CONFIGURACIÓN EN FUNCIÓN DEL ROL: El acceso de invitados se proporciona mediante una página Web de manera que el recepcionista puede agregar de forma rápida y fácil la cuenta del invitado y darle una contraseña única. De otra forma, las cuentas pueden configurarse previamente y asociarse a los invitados al registrarse. Otra opción es publicar una contraseña de invitados común para todos los usuarios que sean invitados.

Ventajas de la solución de acceso de invitados de Aruba

- Permite que solo los invitados autorizados utilicen la red
- Evita que los usuarios invitados accedan a la red interna: controla el acceso a Internet en función de la hora, la ubicación, el contrato de ancho de banda, etc.
- Proporciona un sistema sencillo de creación de cuentas de invitados que puede ser usado por los empleados y los recepcionistas sin involucrar al personal técnico
- Lleva un registro de quién está utilizando la red, cuándo se está utilizando y cómo se está utilizando
- Controla el acceso de invitados tanto en la red cableada como la inalámbrica
- Proporciona acceso de invitados sin tener que reconfigurar los ordenadores de los invitados y sin necesidad de llamar al personal de soporte de TI para solicitar ayuda
- Integración con el controlador de movilidad de Aruba



WWW.ARUBANETWORKS.COM

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