



Descripción breve del cumplimiento del PCI

El 4 de mayo de 2007, la peor pesadilla de todo comerciante se hizo realidad: el *Wall Street Journal* publicó un artículo en su portada describiendo la violación de la seguridad de la LAN inalámbrica teniendo como resultado el mayor robo de tarjetas de crédito de la historia. El Consejo del PCI, compuesto por las cinco principales marcas de tarjetas de crédito –American Express, Visa, Mastercard, Discover y JCB– publicó el Payment Card Industry Data Standard (PCI DSS) para evitar precisamente este tipo de violaciones. El PCI exige que todos los comerciantes del mundo traten las LAN inalámbricas como redes públicas y apliquen controles de seguridad estrictos para ambas aplicaciones a través de LAN inalámbricas e impedir entradas no autorizadas a través de la LAN inalámbrica.

Sin embargo, cumplir los estrictos requisitos de cumplimiento del PCI es costoso y complejo. Las redes cableadas e inalámbricas existentes deben rediseñarse y actualizarse para permitir la seguridad necesaria. Deben instalarse servicios de seguridad adicionales. Rediseñar y actualizar las redes de forma rápida es muy caro y desalentador, especialmente si se deben hacer cambios en cientos o hasta miles de tiendas. Las redes de Aruba centradas en los usuarios proporcionan la única solución integrada de seguridad, LAN inalámbrica y acceso remoto para hacer que el cumplimiento del PCI sea lo menos pesado y costoso posible. Aruba ofrece una solución de seguridad centralizada que se ajusta a las redes existentes excluyendo la necesidad de rediseñar y actualizar. Y como ventaja añadida, la plataforma de Aruba es una plataforma de activación de aplicaciones; la misma solución que se utiliza para la seguridad se puede utilizar para soportar de forma segura las aplicaciones inalámbricas existentes y activar otras nuevas.

Requisitos del PCI para proteger las LAN inalámbricas

El PCI Security Standards Council publicó un Data Security Standard (DSS, estándar de seguridad de datos) actualizado en mayo de 2006 que entró en vigor el 1 de enero de 2007. El Consejo del PCI impone la implementación de controles de seguridad específicos diferentes en función del uso de la LAN inalámbrica

Tal como se muestra en el diagrama, incluso si no se utiliza una LAN inalámbrica, los comerciantes deberán implementar “analizadores inalámbricos” para garantizar que no haya redes inalámbricas accidentales o no permitidas. Además, si las LAN inalámbricas se utilizan para aplicaciones de puntos de venta de tal manera que la información de la tarjeta de crédito se transmite por el aire, los comerciantes deberán implementar una encriptación fuerte (no WEP), utilizar un cortafuegos con certificado ICASA entre las LAN inalámbricas y la red POS y controlar la LAN inalámbrica de

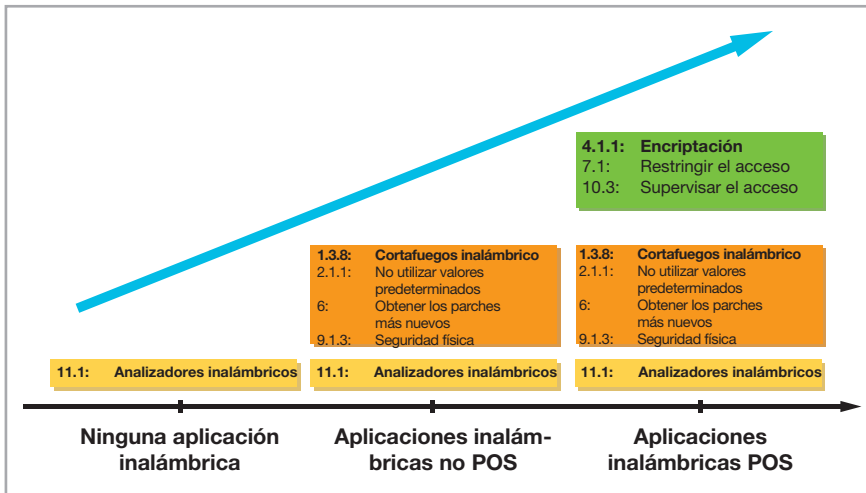
forma regular.

El cumplimiento del PCI es una necesidad imperativa. En primer lugar, el cumplimiento del PCI significa asegurar las redes frente a violaciones que protegen a su marca y sus clientes. En segundo lugar, las marcas de tarjetas de crédito han aplicado iniciativas adicionales para incrementar la velocidad y el grado de cumplimiento del PCI, donde podrá:

- Evitarse multas de incumplimiento por un importe de 25.000 dólares por tienda al mes
- Gozar de tarifas preferenciales en las transacciones
- Estar protegido bajo la provisión “puerto seguro”, donde los comerciantes que cumplen el PCI no son responsables ni multados con un cargo aproximado de 160 dólares por cada caso de tarjeta de crédito robada, en caso de violación.

Ventajas de Aruba:

- Menor coste con seguridad integrada para el cumplimiento del PCI
- Protege las redes cableadas e inalámbricas existentes con una arquitectura superpuesta
- Impide actualizaciones de dispositivos únicamente WEP con seguridad basada en identidad
- Migración sencilla a LAN inalámbricas de nueva generación con una plataforma multi-propósito
- Diseñado para alcanzar mayor número de centros remotos

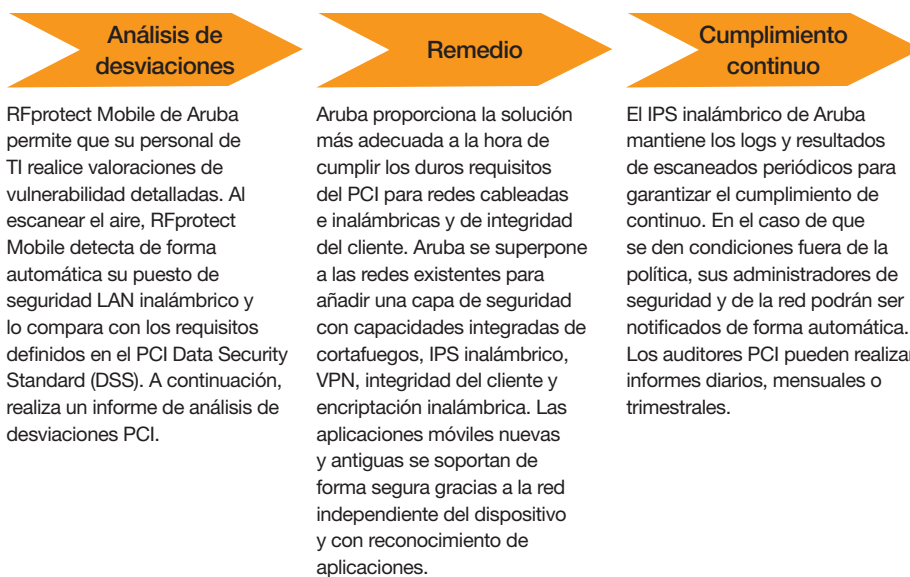


Cómo habilita Aruba el cumplimiento del PCI

Aruba Networks ha elaborado un enfoque único para cumplir los requisitos del PCI de forma poco sencilla y barata. Con una solución integrada de seguridad, LAN cableada e inalámbrica y acceso remoto, los comerciantes pueden activar la seguridad necesaria para el cumplimiento del PCI y activar las aplicaciones empresariales al mismo tiempo sin actualizar las redes anteriores. Puede encontrar más información sobre la solución para el cumplimiento del PCI de Aruba en

http://www.arubanetworks.com/pdf/company/wp_PCI-Primer.pdf.

Aruba proporciona una solución global para garantizar que su LAN inalámbrica cumpla los requisitos tan exigentes del PCI y, lo más importante, protege su red. Desde el análisis de desviaciones a la identificación de brechas de seguridad potenciales, a la búsqueda de soluciones y remedios, o a la monitorización y auditorías de cumplimiento, Aruba cubre todos los aspectos.



SEGURIDAD PCI COMO SUPERPOSICIÓN:

Las capacidades de Servicio de Protección de Intrusión (IPS) inalámbrico pueden utilizarse como una capa superpuesta sobre las redes inalámbricas existentes. La solución de Aruba consta de un monitor de aire (o varios) en las tiendas y un servidor de protección de intrusiones inalámbrico en el centro de datos. Los monitores de aire escanean el entorno cableado e inalámbrico de la tienda. Luego, los servidores centralizados agregan y analizan los escaneados en cada informe para generar informes de escaneado PCI que garantizan el cumplimiento. En el caso de un acceso no autorizado, el IPS inalámbrico de Aruba también generará alertas y evitará los ataques de forma automática. La solución de Aruba es única puesto que en el mismo hardware que se utiliza para el IPS inalámbrico también se puede configurar el acceso inalámbrico, suministrando una vía de migración sencilla y barata para las LAN inalámbricas de nueva generación.

IMPEDIR LAS ACTUALIZACIONES Y REDISEÑOS DE LA LAN CABLEADA:

Al integrar Aruba el cortafuegos stateful con certificado ICASA, VPN y las funciones de encriptación y autenticación LAN inalámbrica, los productos de red existentes como routers o cortafuegos no deberán actualizarse para permitir la segmentación VLAN, la función VPN o los servicios AAA para seguridad inalámbrica.

SEGURIDAD BASADA EN IDENTIDAD PARA PROTEGER LOS DISPOSITIVOS

SÓLO WEP: Impide que los dispositivos WEP abran una puerta trasera hacia el centro de datos gracias a los roles de dispositivo y de usuario de Aruba. Incluso si la encriptación WEP está comprometida, el acceso a la red se restringirá mediante la inspección profunda del paquete y el cortafuegos stateful integrados de Aruba.

UNA PLATAFORMA, VARIOS USOS:

Además de las potentes capacidades de seguridad, la solución de Aruba ofrece conectividad LAN inalámbrica, mallada y cableada segura a nivel empresarial, para una gran variedad de aplicaciones. También incluye el soporte simultáneo de las aplicaciones de datos, voz y vídeo en cualquier dispositivo.

GESTIÓN CENTRALIZADA: Aruba proporciona opciones a medida para diferentes tamaños de tienda que pueden gestionarse de forma centralizada como una sola red. La solución de Aruba se ha diseñado para actuar de forma segura en redes públicas y privadas, que abarca miles de ubicaciones remotas con todas las políticas de seguridad definidas y supervisadas de forma centralizada.



WWW.ARUBANETWORKS.COM

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