DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

ARUBA SECURE CORE

La seguridad de red embebida más avanzada en la industria

Como un líder en proporcionar soluciones de acceso alámbricas e inalámbricas mobile-first, de siguiente generación, Aruba está ayudando a agencias gubernamentales y a empresas conscientes de seguridad a construir redes de alta seguridad mejores en clase que proporcionan control, visibilidad y confiabilidad necesarias para entregar una experiencia de cómputo segura desde el edge, al core, a la nube.

Como un elemento fundacional de Aruba 360 Secure Fabric, Aruba Secure Core está basado en cuatro componentes:

1. Aseguramiento de dispositivos – el uso del hardware de seguridad del módulo TPM (Trusted Platform Module) asegura que los dispositivos y sus códigos boot no hayan sido alterados y evita la personificación o la deshabilitación de los dispositivos.
2. Tráfico confiable—un rango de tecnologías, desde cifrado centralizado de grado militar a control de acceso basado en roles, certifica que los usuarios y dispositivos en la red están conectados correctamente solo a aquellos recursos autorizados a los que tienen derecho y que el tráfico previsto llegue a su destino.

Figura 1: Atributos de Aruba Secure Core

¿QUÉ TAN SEGURO ES ARUBA SECURE CORE?

- **Seguro para la Defensa:** Único proveedor de soluciones WLAN empresariales autorizado para la Fuerza Aérea de Estados Unidos
- **Seguro para Ultra Secretos:** Primer proveedor y más utilizado en el programa US Commercial Solutions for Classified
- **Seguro Certificado:** FIPS 140-2, Common Criteria, DoDIN-APL, cientos de Autorizaciones para Operar del Gobierno de Estados Unidos.

3. Preparado para Analíticos – perspectivas de la red y datos resumidos se sintonizan para apoyar detección de ataques downstream, incluyendo técnicas avanzadas basadas en tecnología de Inteligencia Artificial/aprendizaje de máquina.
4. Soluciones Abiertas – las organizaciones no están restringidas a los productos de Aruba para entregar un caso de uso específico. Las soluciones de Aruba se pueden utilizar en forma individual para acceso alámbrico y WLAN, en malla, para acceso remoto y supervisión por video, aprovechando componentes de la solución que no son parte del portafolio de Aruba.

ASEGURAMIENTO DE DISPOSITIVOS

Aruba Secure Core comienza con los access points y controladores inalámbricos y switches en el portafolio de networking de Aruba. Cada elemento ha sido diseñado cuidadosamente con extensas capacidades de seguridad embebidas que típicamente no se encuentran en otros productos de networking.

Secure boot con protección TPM

Las soluciones de networking alámbricas e inalámbricas de Aruba incluyen un uso extenso de la tecnología TPM (Trusted Platform Module), una norma internacional para un cripto procesador resistente a alteraciones, el cual es un micro controlador dedicado diseñado para asegurar hardware, integrando llaves criptográficas en dispositivos.

Un cargador boot comprometido introduce una 'amenaza persistente avanzada' que un cliente no puede eliminar. Un cargador boot corrompido puede evitar que el switch arranque ('bricking the switch') o sutilmente modificar operaciones que estén ocurriendo con el objeto de ocultar malware o de otra forma enmascarar un ataque. Al utilizar llaves resistentes a alteraciones y otros datos de confirmación contenidos en el hardware TPM, la integridad y el código boot del dispositivo que no hayan sufrido cambios se pueden validar, asegurando un proceso de arranque limpio. Las llaves de cifrado de identidad y atestación del switch de networking de Aruba se instalan durante su fabricación para habilitar el proceso.

En forma similar, toda la configuración y monitoreo de los access points, así como la atestación del boot ocurren a través del controlador, eliminando la amenaza de que un AP haya sido comprometido y que las llaves hayan sido robadas.

Protección contra Intrusiones Inalámbricas

El software RFProtect™ evita ataques DoS (denial-of-service) y man-in-the-middle y mitiga las amenazas de seguridad sobre el aire. Esto elimina la necesidad de costosos sistemas IDS sobrepuestos con sensores dedicados. RFProtect protege en contra de clientes Wi-Fi no autorizados y redes ad hoc, escaneando continuamente el ambiente RF, evaluando centralmente datos forenses, conteniendo activamente a dispositivos no autorizados y bloqueando las configuraciones de los dispositivos.

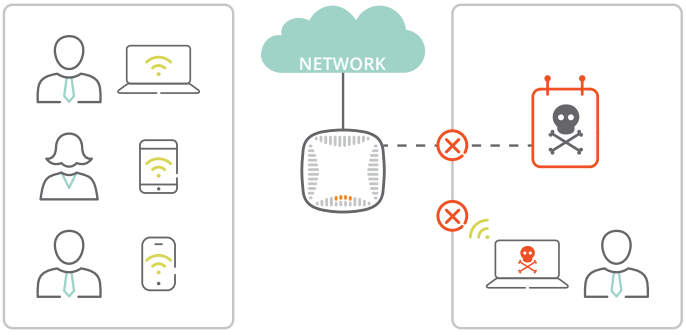

Figura 2: Con controles basados en hardware y monitoreo integrado en tiempo real, Aruba Secure Core entrega el aseguramiento de dispositivos requerido para una sólida seguridad de red.

TRÁFICO CONFIABLE

Con la fundación del aseguramiento de dispositivos entregada por el extenso uso de protección y monitoreo de hardware, Aruba Secure Core entonces agrega funcionalidad Trusted Traffic para asegurar aún más a la red.

Trusted Traffic comienza con ArubaOS, la arquitectura de software diseñada para soportar funcionalidad de seguridad de la red basada en hardware. Se construye utilizando tres componentes clave:

- Un kernel de supervisión, con múltiples hilos, mejorado en seguridad, manejando la administración, la autenticación, el logging y otras funciones de operación del sistema.
- Un sistema operativo en tiempo real embebido alimenta el hardware dedicado de procesamiento de paquetes del controlador, implementando todo el enrutamiento, el switching y las funciones de firewall validadas por Common Criteria.
- Una tarjeta programable de cifrado/descifrado con validación por FIPS, DoDIN-APL y Common Criteria, construida en el hardware dedicado del controlador, entregando seguridad de grado gubernamental sin sacrificar el rendimiento.

Cifrado centralizado

La arquitectura de seguridad de Aruba es diferente a la de todos los otros proveedores. En la configuración por omisión, conocida como el modo túnel, los access points (APs) de Aruba no efectúan cifrado/descifrado y, por lo tanto, no contienen ningunas llaves de cifrado. Los access points reciben tramas inalámbricas cifradas de la interface del radio e inmediatamente empaquetan estas tramas inalámbricas cifradas en un túnel IP al controlador de movilidad.

Una vez que se encuentran en el controlador de movilidad, el encabezado del paquete del túnel IP se elimina y lo que permanece es una trama 802.11 Wi-Fi cifrada. El controlador entonces procesa esta trama, descifrándola y regresándola a un paquete IP enrutable estándar. Los access points nunca tienen acceso a las llaves de cifrado y, por lo tanto, no son capaces de procesar el tráfico Wi-Fi en forma local.

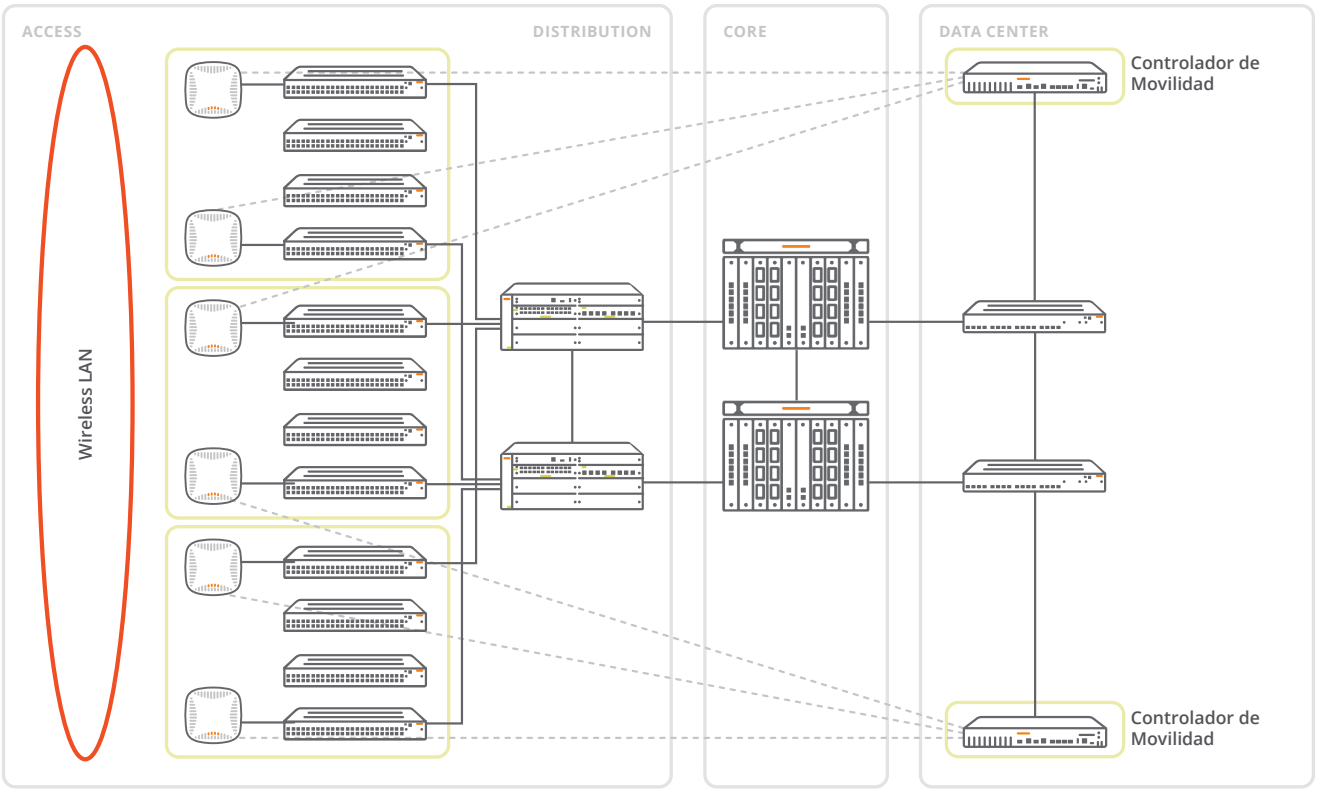

Figura 3: La arquitectura LAN inalámbrica de Aruba

La implicación es que un atacante que obtiene control físico de un AP de Aruba, aun uno que reemplace el firmware con código malicioso personalizado, no será capaz de intervenir en las sesiones Wi-Fi que pasen a través de ese AP. Todo el cifrado Wi-Fi se efectúa entre el cliente y el controlador de movilidad – el AP es simplemente un dispositivo pass-through. Los controladores de movilidad deben estar protegidos físicamente, pero los access points no.

Control de acceso basado en roles

El firewall Policy Enforcement Firewall™ hace cumplir seguridad y priorización en la capa de aplicaciones en base a roles de usuario, tipos de dispositivos, flujos de aplicaciones, ubicación y más. Con políticas basadas en identidades, dispositivos y ubicación, las necesidades de diferentes grupos de usuarios se pueden satisfacer con una sola configuración de red inalámbrica. Los flujos de tráfico simplemente se adaptan al estado de movilidad del usuario móvil y del dispositivo.

Esto elimina el costo y la complejidad asociada con configurar manualmente VLANs estáticas, listas de control de acceso y la infraestructura del switch alámbrico.

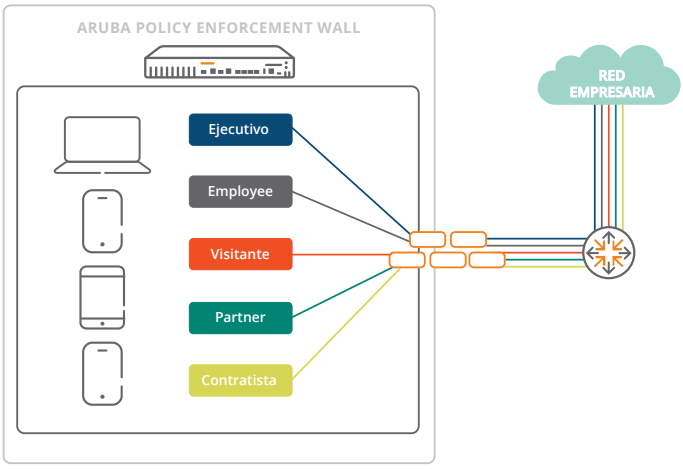

Figura 4: El Policy Enforcement Firewall de Aruba proporciona la flexibilidad de separar cualquier tipo de flujo de tráfico.

Acceso remoto

Aruba ofrece dos tipos de acceso VPN, en donde el controlador de movilidad funge como el VPN cabezal. Los servicios VPN en ArubaOS™ incluyen el VIA (Virtual Intranet AccessTM), un cliente VPN híbrido IPsec/SSL que corre en un sistema operativo host. Al soportar conexiones VPN a sistemas de terceros, no existe la necesidad de invertir en dispositivos VPN adicionales.

Los empleados que trabajan remotamente pueden instalar fácilmente un Aruba RAP (Access Point Remoto) para acceder en forma segura a la red corporativa mediante un túnel VPN. Una vez que se conectan, la experiencia es exactamente igual como si estuvieran en la oficina, gracias a un enlace VPN zero-touch a un controlador de Aruba en el data center.

Figura 5: VIA escanea automáticamente el aire, encuentra la mejor conexión y lanza VPN bajo demanda a la red corporativa.

La capacidad Trusted Traffic de Aruba Secure Core significa que no tan sólo están seguros los switches, los access points y los controladores, sino que también el uso de esos recursos está fuertemente controlado.

PREPARADO PARA ANALÍTICOS

Los datos y las perspectivas de networking se han vuelto cada vez más importantes en ayudar a los equipos de seguridad a detectar y a responder a ataques enfocados avanzados. Cuando un usuario abre un archivo adjunto desconocido en el correo electrónico o hace clic en un vínculo web malicioso, ese dispositivo y las credenciales del usuario se pueden volver la plataforma de lanzamiento para ransomware y para otros ataques dañinos en el interior. Frecuentemente, es tan sólo pudiendo ver los pequeños cambios en comportamiento que están contenidos en el tráfico de la red que el equipo de seguridad puede detectar un ataque y reaccionar antes de que efectúe daños.

Aruba IntroSpect es una solución de Analíticos de Comportamiento de Usuarios y Entidades que aplica modelos de aprendizaje de máquina a datos de la red y de logs para detectar estos ataques desde adentro. Los switches de Aruba directamente proporcionan paquetes mediante un puerto span o tap al procesador de paquetes de IntroSpect, el cual, a su vez, lleva a cabo la inspección profunda de paquetes (DPI) que se requiere para extraer los datos más relevantes para los modelos de aprendizaje de máquina. IntroSpect también analiza canales de datos AMON de los controladores de movilidad de Aruba, los cuales proporcionan una visión de seguridad muy detallada del tráfico inalámbrico.

Aruba Secure Core proporciona las perspectivas profundas de networking que la detección de ataques avanzada, como el aprendizaje de máquina de IntroSpect, pueden aprovechar para monitorear e identificar usuarios y dispositivos comprometidos.

RESUMEN

Con movilidad, BYOD, virtualización, la nube y el surgimiento de cosas provenientes de la tecnología de operaciones, es más importante que nunca tener una red altamente segura y confiable.

Durante más de 15 años, Aruba ha estado en el primer plano de la entrega de una infraestructura de red alámbrica e inalámbrica de alto rendimiento, altamente confiable y segura – desde los access points a los switches core. Como proveedor de seguridad, Aruba consistentemente ha introducido innovaciones de vanguardia en las áreas de cifrado, mejora de seguridad física y acceso remoto para asegurar que se pueda confiar en el tráfico de usuarios, sistemas y dispositivos. Chief Information Security Officers alrededor del mundo han dependido del "arranque rápido" en seguridad que Aruba Secure Core ha proporcionado.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com/latam