SOLUTION OVERVIEW

ARUBA SECURE INFRASTRUCTURE

The most advanced, embedded network security in the industry

As a leader in providing mobile-first, next-generation wired and wireless network access solutions, Aruba is helping security-conscious government agencies and enterprises build best-in-class, highly secure networks that provide the control, visibility and reliability needed to deliver a secure computing experience from the edge, to the core, to the cloud.

As a foundational element of Aruba's 360 Secure Fabric, Aruba's Secure Infrastructure is based on four key components:

1. Device assurance – use of Trusted Platform Module (TPM) security hardware ensures that the device and its boot code has not been altered and prevents device impersonation or disablement.
2. Trusted traffic—a range of technologies from centralized, military-grade encryption to role-based access control certifies that users and devices on the network are properly connected to only those authorized assets to which they are entitled, and that the intended traffic reaches its destination.

Figure 1: Aruba Secure Infrastructure attributes

HOW SECURE IS ARUBA SECURE INFRASTRUCTURE?

- **Defense Secure:** Only authorized enterprise WLAN solution provider for the US Air Force
- **Top Secret Secure:** First and most widely-deployed vendor in the US Commercial Solutions for Classified program
- **Certified Secure:** FIPS 140-2, Common Criteria, DoDIN-APL, 100's of US Government Authorizations to Operate

3. Analytics-ready – network insights and summarized data is tuned to support downstream attack detection, including advanced techniques based on AI/machine learning technology.
4. Open solutions – organizations are not restricted to Aruba products to deliver a specific use case. Aruba's solutions can be used individually for wired and WLAN access, mesh, remote access and video surveillance, leveraging components of the solution that are not part of the Aruba portfolio.

DEVICE ASSURANCE

Aruba Secure Infrastructure starts with the wireless access points, controllers and switches in the Aruba networking portfolio. Each element has been carefully engineered with extensive embedded security capabilities not typically found in other networking products.

TPM-enforced secure boot

Aruba wired and wireless networking solutions feature extensive use of Trusted Platform Module (TPM) technology, an international standard for a secure tamper-resistant cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

A compromised boot loader introduces an 'advanced persistent threat' that a customer cannot remove. A corrupted boot loader can prevent the switch from booting ('bricking the switch') or subtly alter ongoing operations in order to hide malware or otherwise mask an attack. By using tamper-resistant keys and other confirming data contained in the TPM hardware, the device integrity and boot code can be validated as unchanged, ensuring a clean startup process. Aruba networking switch identity and attestation encryption keys are installed during manufacturing to enable the process.

Similarly, all wireless access point configuration and monitoring as well as the boot attestation takes place through the controller, eliminating the threat that an AP has been compromised and keys stolen.

Wireless intrusion protection

RFProtect™ software prevents denial-of-service and man-in-the-middle attacks and mitigates over-the-air security threats. This removes the need for expensive overlay IDS systems with dedicated sensors. RFProtect guards against unauthorized Wi-Fi clients and ad hoc networks by continuously scanning the RF environment, centrally evaluating forensic data, actively containing rogue devices and locking-down device configurations.

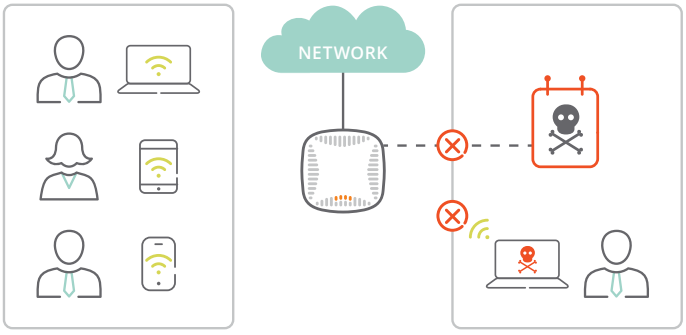

Figure 2: With hardware-based controls and integrated real-time monitoring, the Aruba Secure Infrastructure delivers the device assurance required for strong network security.

TRUSTED TRAFFIC

With the foundation of device assurance delivered by the extensive use of hardware-enforced and monitored protection, Aruba Secure Infrastructure then adds Trusted Traffic functionality to further secure the network.

Trusted Traffic starts with ArubaOS, the software architecture designed to support hardware-based network security functionality. It is built using three key components:

- A hardened, multi-threaded supervisory kernel managing administration, authentication, logging, and other system operation functions.
- An embedded real-time operating system powers the dedicated packet processing hardware of the controller, implementing all routing, switching, and Common Criteria validated firewall functions.
- A programmable, FIPS, DoDIN-APL and Common Criteria validated encryption/decryption engine built on the controller's dedicated hardware, delivering government-grade security without sacrificing performance.

Centralized encryption

Aruba's security architecture is different from all other vendors. In the default configuration, known as tunnel mode, Aruba access points (APs) do not perform encryption/decryption and thus do not contain any encryption keys. The access points receive encrypted wireless frames from the radio interface and immediately packages these encrypted wireless frames into an IP tunnel to the mobility controller. Once at the mobility controller, the IP tunnel packet header is removed and what remains is an encrypted 802.11 Wi-Fi frame. The controller then processes this frame, decrypting it and turning it back into a standard routable IP packet. Access points never have access to encryption keys, and they are unable to process the Wi-Fi traffic locally.

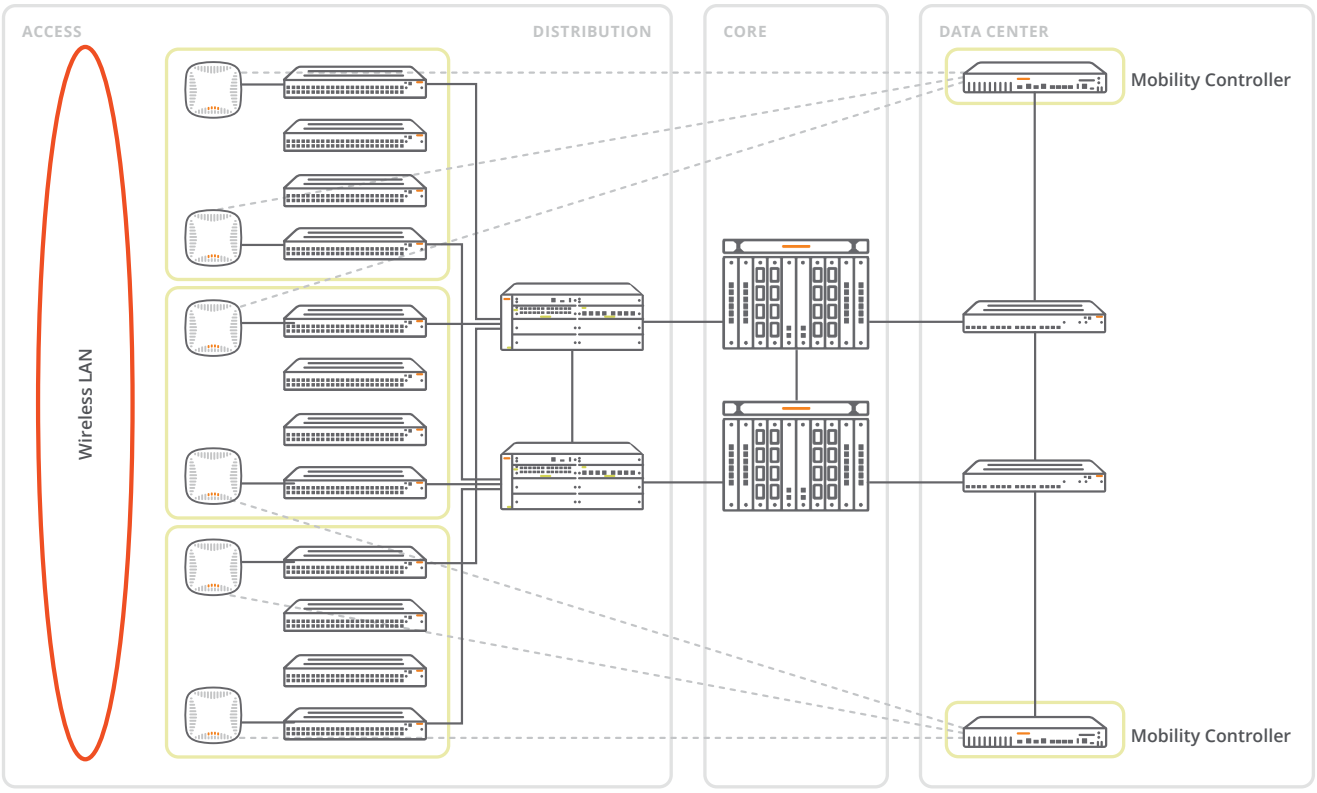

Figure 3: The Aruba wireless LAN architecture

The implication is that an attacker who gains physical control of an Aruba APs, even one who replaces the firmware with custom malicious code, will not be able to break into Wi-Fi sessions that pass through that AP. All Wi-Fi encryption is between the client and the mobility controller – the AP is simply a pass-through device. Mobility controllers must be physically protected, but access points do not.

Role-based access control

The Policy Enforcement Firewall™ enforces application-layer security and prioritization based on user roles, device types, app flows, location and more. With policies based on identities, devices and location, the needs of different groups of users can be satisfied with a single wireless network configuration. Traffic flows simply adapt to the mobility state of the mobile user and device.

This eliminates the cost and complexity associated with manually configuring static VLANs, access control lists and the wired switch infrastructure.

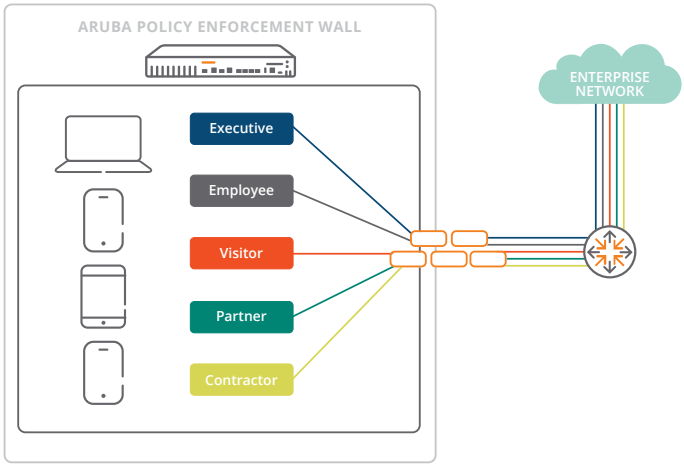

Figure 4: Aruba's Policy Enforcement Firewall provides the flexibility to separate any type of traffic flow.

Remote access

Aruba offers two types of VPN access where the mobility controller acts as the VPN head-end. The VPN services in ArubaOS™ include the Virtual Intranet AccessTM (VIA), a hybrid IPsec/SSL VPN client that runs on a host operating system. By supporting VPN connections to third-party systems, there is no need to invest in additional VPN appliances.

Employees who work remotely can easily install an Aruba RAP (Remote Access Point) to securely access the corporate network through a VPN tunnel. Once they're connected, the experience is just as if they're at the office, thanks to a zero-touch VPN link to an Aruba controller in the data center.

Figure 5: VIA automatically scans the air, finds the best connection, and launches VPN-on-demand to the corporate network.

The Trusted Traffic capability of Aruba Secure Infrastructure means that not only are the switches, access points and controllers secure, but also that the use of those resources are tightly controlled.

ANALYTICS READY

Networking data and insights are becoming increasingly important in helping security teams detect and respond to advanced, targeted attacks. When a user opens up the wrong email attachment or clicks on a bad web link, that device and the user's credentials can become the launching pad for ransomware and other damaging attacks on the inside. Often it is only by seeing small changes in behavior that are contained in network traffic that the security team can spot an attack and react before the damage is done.

Aruba IntroSpect is a User and Entity Behavior Analytics solution that applies machine learning models to network and log data to detect these attacks on the inside. Aruba switches directly provide packets via a span or tap port to the IntroSpect packet processor, which in turn performs the deep packet inspection required to extract the most relevant data for the machine learning models. IntroSpect also analyzes AMON feeds from Aruba mobility controllers which provide a very detailed security view of wireless traffic.

Aruba Secure Infrastructure provides the deep networking insights that advanced attack detection such as IntroSpect's machine learning can leverage to monitor and identify compromised users and devices.

SUMMARY

With mobile, BYOD, virtualization, cloud and the emergence of things coming from operations technology, it is more important than ever to have a highly secure and trusted network.

For over 15 years Aruba has been at the forefront of delivering a high performance, highly reliable and secure wired and wireless network infrastructure – from access points to core switches. As a security provider, Aruba has consistently introduced ground-breaking innovations in the areas of encryption, physical hardening, and remote access to ensure that user, system and device traffic can be trusted. Chief Information Security Officers around the world have come to rely on the security "head start" that Aruba Secure Infrastructure has provided.

SO_SecureInfrastructure_091318