



The Federal Deposit Insurance Corporation banks on Aruba for portable wireless network access

The banking crisis of 2008 drastically increased the workload of the compliance audit and bank assumption teams within the Federal Deposit Insurance Corporation (FDIC). These teams, charged with the on-site inspection or transition of a bank’s business, require deployment to banks all across the country.

Seemingly overnight, the number of bank assumptions skyrocketed and the FDIC found that the model used to connect these teams from their remote locations to the FDIC had become both antiquated and expensive.

FDIC employees and contractors needed to connect their laptops and PDAs to the agency network from each deployed location, including staging areas and bank facilities. The challenge the FDIC faced was to provide its traveling teams with a network that would provide secure, portable and seamless connectivity to the agency’s servers, documents and applications. To quickly and effectively manage the banking crisis, the FDIC needed an innovative, secure and scalable solution.

Increased workload drives the need for a scalable solution

Prior to 2008, the FDIC’s compliance audit and bank assumption teams traveled on average three or four times per year. To connect these teams, the FDIC used costly, labor-intensive dedicated circuits and virtual private network (VPN) services between its data center and the field teams.

As the banking crisis ensued, this design proved difficult to scale as the number of teams and deployments escalated. It was also out of step with the mobile access needs of the field teams who moved regularly and desired that their remote networking solutions easily follow them.

A secure network on the go

To address the needs of the field teams, the FDIC looked to Aruba Networks to provide deployable remote wireless network kits. These kits contain a pre-configured full wireless LAN (WLAN) system comprised of an Aruba Mobility Controller, Aruba access points (APs) and a full complement of software – all packaged into a fly-away protected case.

All of the kits are plug-and-play, and require no field configuration. Management is centrally handled by Aruba Mobility Controllers at the FDIC data center. Collaborative, real-time applications such as voice, chat and whiteboard sharing work from any local/remote PC to any other local/remote PC, with no special configuration requirements on the clients and applications.



Requirements

- Instant on network that is secure, portable and seamless
- Scalable solution that is easy to deploy at remote sites without on-site support
- Centralized management
- Secure authentication and access control
- Adherence to federal requirements including FIPS, Common Criteria and TAA

Solution

- Aruba 800 Mobility Controller
 - Policy Enforcement Firewall (PEF) software enforcing per-user and per-application security policies
 - AP mesh software allowing instant connectivity of APs into the network without requiring Ethernet cable drops
 - Site-to-site security software securely tunneling all traffic from the remote site to the data center
 - Adaptive Radio Management (ARM) automatically configuring every AP to idealize the RF/WLAN based on their neighbors and the environment
- AP-70 indoor APs and AP-85 outdoor APs

CASE STUDY
Government

The FDIC typically uses business-class Internet services (metro Ethernet, DSL, cable) at the staging locations and each target-bank facility. These IP connections are then attached to the Aruba Mobility Controller. With no configuration changes required, a secure WLAN is instantly activated in the facility from the controller, which in turn securely connects to a master Aruba Mobility Controller at an FDIC data center.

Security is end-to-end, as user authentication, traffic validations and encryption extend from the laptop or PDA endpoint to the master controller at the FDIC data center. Replacement of the application-limiting VPN system provides a seamless user network and application experience, where all users simply authenticate to their laptop or PDA using built-in WLAN hardware/software to securely connect to the FDIC network.

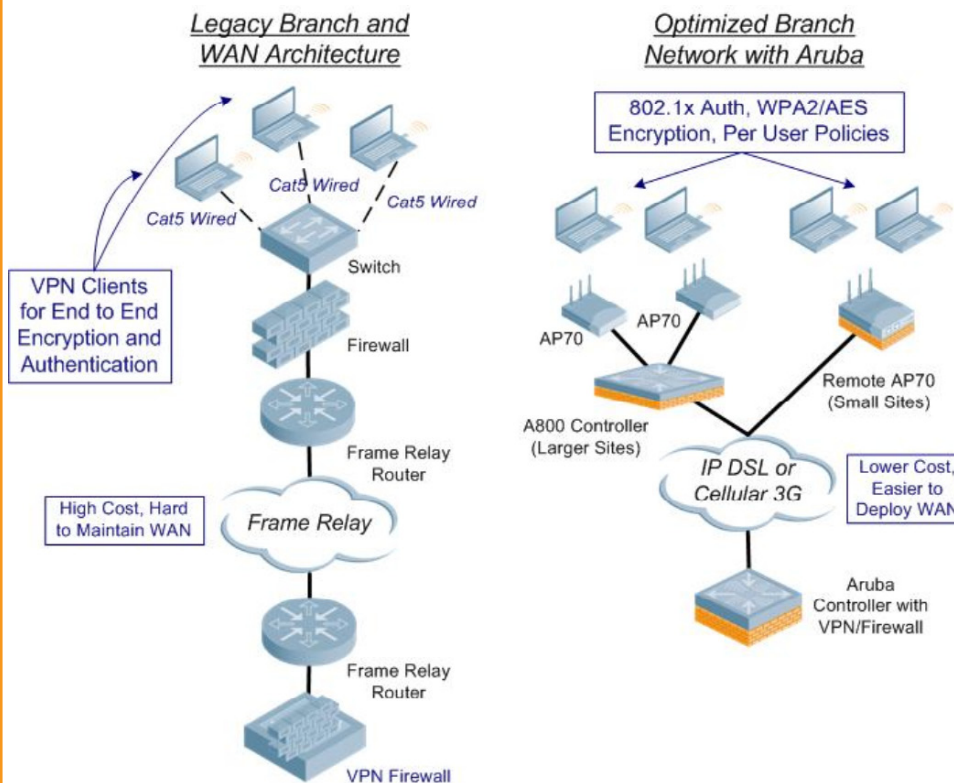
The deployment of Aruba remote wireless network kits enabled the FDIC to rapidly scale their ability to manage the national banking crisis. The agency can now support a large number of field teams that may include as many as 100 members with upwards of 25 teams deployed at any given time.

The Aruba kits provide the field teams with a secure “instant on” network that can be easily set up and taken down with minimal IT involvement, significantly reducing the time-to-activate from days to a matter of minutes. With a lower cost of ownership, the Aruba WLAN solution successfully meets the needs of the FDIC and saves money. That’s something to bank on.



Benefits

- Plug-and-play installation and automatic configuration
- Mobile, easy-to-transport WLAN with low cost of ownership
- Integrated firewall enabling differentiated user access
- End-to-end security and user-application security from remote location to FDIC data center



WWW.ARUBANETWORKS.COM | 1344 Crossman Avenue. Sunnyvale, CA 94089
1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com