Paliton.net

Paliton Networks: A Federal Case Study

How Federal Agencies Can Get Highly Secure Wi-Fi – Without Going Through the ATO Process

A federal regulatory agency needed a highly secure, controlled Wi-Fi system for employees to conduct official and non-official business. Paliton Networks and CommScope designed and deployed a highly scalable solution that enables all employees within that agency to conduct official business on their GFE laptops.

The challenge

Installing a modern, secure Wi-Fi system in a federal facility sounds easy enough, but for many federal agencies it's an enormous challenge. Agencies frequently lack the expertise needed to design and deploy a Wi-Fi system that can be used for official or non-official business and comply with the many complex security controls required by FISMA that are typically required.

One federal regulatory agency confronted this challenge in 2020. The agency wanted a Wi-Fi system that was on a FedRAMP-compliant infrastructure, was a managed service, and that would provide secure, controlled Wi-Fi coverage at its five locations across the country for 1,300-plus end users.

The solution

The solution is called the Controlled Non-Official Business Internet, or CNOBI from Paliton. As the name suggests, it was designed to provide Wi-Fi coverage for government non-official business — however, it can be utilized to provide Wi-Fi coverage for official business as well.

As a managed service, CNOBI and its components are owned, operated, and maintained by Paliton. It is highly secure, meets many NIST security controls, is FIPS-compliant, and operates on a FedRAMP-authorized infrastructure (Azure Gov).

The CNOBI solution starts with a FIPS certified RUCKUS SmartZone™ multi-tenant controller from CommScope that allows Paliton to securely manage both wired and wireless equipment installed at the customer's facility. Paliton's management traffic and the customer's data traffic are isolated on different planes. CNOBI offers RUCKUS URL filtering features to block access to inappropriate content.

Another component of CNOBI is the RUCKUS Cloudpath Enrollment System, an EAP-TLS-based solution that uses certificates to connect devices to the network. Mobile devices can connect only when they and the CNOBI service WLAN establish a two-way trusted relationship. RUCKUS Analytics helps ensure reporting compliance and provides information to speed trouble calls and predict faults.

To learn more about how Paliton can help your agency set up a highly secure Wi-Fi system for both official and non-official business, **please visit: Paliton.net**

Like many agencies during the pandemic, this federal customer issued government furnished equipment (GFE) laptops to its employees so they could work at home. Those laptops are outfitted with security software and features that force them to automatically connect with the agency's highly secure VPN immediately after connecting to a trusted Wi-Fi network. The VPN is an agency-operated network that complies with all relevant security controls. If it can be done at home, why not in the office?

The marriage of the two solutions provides the ability for agency employees to use a trusted service to perform official work on the GFE laptops while maintaining mobility within office. A user can simply undock and be automatically reconnected over VPN via Wi-Fi anywhere CNOBI has coverage. FIPS-certified RUCKUS hardware and software residing on top of FedRAMP infrastructure provides service assurance and enables GFE devices to negotiate higher encryption standards.

The benefits

With the CNOBI solution in place, agency employees can be at any agency facility, using their GFE laptops, and — wirelessly and securely — be able to conduct official business. The agency achieved this capability without having to go through the complex, time-consuming security accreditation process. Also, the agency's IT department does not maintain the Wi-Fi system, so they don't need to hire or augment staff to maintain it or address any issues that may arise because it is a managed service. The solution is highly scalable, supporting up to 30,000 access points.

A critical security benefit of CNOBI is that it is not vulnerable to the series of CVEs that are collectively known as Frag Attacks. Frag Attacks were a zero-day vulnerability that affected every Wi-Fi device, both client and network. Users of the CNOBI service were already protected. This is because the system relies upon the 802.1X EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) protocol to authenticate individual certificate-based identities instead of shared passwords. EAP-TLS-based systems mitigate cracking, man-in-middle, or frag attacks because each side of the Wi-Fi connection — the Wi-Fi system and the end user device — authenticates each other. If either side mistrusts the other, they cannot connect. This prevents the end user from accidently connecting to a rogue malicious device; it ensures that only authorized users can connect to the Wi-Fi system; and it is simple for the end users because once they enroll their devices, they never have to enter a password again.

RUCKUS Analytics software helps drive improved management and efficiencies for the agency. These include predictive analytics to alert agency officials about anticipated resource utilization metrics to enable pre-emptive policy or control adjustments, if necessary.

Finally, CNOBI allows the agency to avoid the expense and engineering challenge of having to deploy two Wi-Fi networks: one for official business and one for non-official business. This is a significant benefit because installing two distinct Wi-Fi systems in the same space — in which access points of both systems are competing for the same RF spectrum — can create severe performance and coverage problems. Having a single system in place removes one of biggest potential adverse impacts on Wi-Fi quality.

> "Implementation of Paliton's enterprise WIFI solution simplified our administrative responsibilities. Paliton's centralized management model makes it easy for our small IT staff to support users across multiple geographically scattered offices seamlessly. This transition has proven to be reliable, cost-effective, scalable, and secure."

To learn more about how Paliton can help your agency set up a highly secure Wi-Fi system for both official and non-official business, **please visit: Paliton.net**

Paliton Networks

Taking the complexity out of IT, Paliton Networks is small Virginia based company founded by engineers. With a strong focus in managed services, Paliton strives to bring big IT solution expertise to all sectors from small business to public education to the Federal Government