Secure access for federal networks

Government law enforcement agency adds managed Wi-Fi across sites.

Challenges

- Lacked Wi-Fi in offices
- Required high data security
- Needed multiple-vendor cooperation

Solutions

- Lumen MPLS backbone
- Cisco wireless infrastructure
- Managed Wi-Fi
- Security architecture

Results

- Device-level authentication and visibility to secure network
- Richer cabinet-level briefings using data and video delivered wirelessly
- Secure access for traveling agency staffers in all offices
- Voice mobility with soft-phones add-on to move between offices and still receive calls to home-office desk line.
- Introduced rolling office space concept with workers moving between offices seamlessly connecting to the network
- Increased productivity of mobile workforce

Challenge

Create secure Wi-Fi for federal law enforcement agency

A US federal agency wanted to install highly reliable, secure Wi-Fi in all its sites as part of mandates to modernize government IT services. The information flowing through this agency sometimes has national security stakes.

Authentication of guest devices needed to be bullet-proof. At any time, every device on the network had to be known and authorized. Because many buildings were quite old, careful planning to avoid Wi-Fi blind spots was required.

Because the agency uses a variety of IT providers for different services and those services are purchased through different General Services Administration (GSA) contracts, the Wi-Fi integrator needed to work with those other vendors cooperatively, including managing interfaces and financial accounting against the various contracts.

LUMEN® TECHNOLOGIES

Solution

Adding wireless layer to end-to-end network makeover

The agency had already turned to Lumen for its MPLS backbone. The Wi-Fi layer was seen as an extension of this effort.

The buildings were surveyed to establish coverage zones. Cisco equipment was chosen for the project including routers, switches and appliances. The first locations were deployed in a production environment with parallel wired and wireless networks to ensure full compatibility of all applications and zero disruption in service during the upgrade. This required careful scheduling and efficient work so that office space is usable– with added Wi-Fi capability.

Interfacing to the backbone was straight forward. All data is encrypted once it hits the backbone. Architects worked with multiple vendors and government stakeholdersto create all handshakes and interfaces for authentication and security for the new wireless network. All access points were visible to administrators down to the device level to enhance security.

Results and future plans

Untethered action, secure information on a managed network

The Wi-Fi network at this agency has added mobility to the 15,000 employees and contractor staff and provided them access to future technologies and increased productivity. This was accomplished by building on top of the Lumen backbone deployed across the region for this agency.

The agency acquired the solution as a managed service and is free of the management burden while still in control of the network. The wireless equipment passes through a refresh cycle as technology evolves over time without burdening the government with added capital expense. The solution also constantly inventories all devices hitting the network – both wired and wirelessly – comparing that to the agency's inventory so the agency is always up to date on its device deployment.

Lumen Solution Set

- Lumen® Managed Network Services
- Lumen® MPLS Networks

LUMEN® TECHNOLOGIES