Aerohive NETWORKS

South Carolina Dept. of Probation, Parole & Pardon Services

Aerohive Cooperative Control Wireless LAN Brings Security, Availability, and Manageability to Widely Distributed State Agency

Challenges

- Highly mobile workforce of parole agents and field personnel required network access, regardless of which of the 46 state-wide courtrooms they are working in

- Needed to let agents connect hassle-free to the network when they return to their home office

- Required a way to provide secure guest wireless access, which would accommodate other agents when working out of SCDPPP's offices

- Searched for a wireless solution that could provide the required level of security, resilience, flexibility, and scalability

Results

- Utilizing Aerohive security features, including 802.11i (WPA2), wireless IDS, 802.1X authentication, rogue detection, integrated stateful firewall, and guest access control

- Aerohive's controller-less wireless LAN architecture eliminates the need to backhaul all traffic, which means users can continue working locally even when the central site or WAN link is down

- Aerohive's HiveManager NMS was used to provision the new HiveAPs

- HiveManager is providing central monitoring capabilities through a single, easy-to-use console

The South Carolina Department of Probation, Parole, and Pardon Services (SCDPPPS) works with over 32,000+ offenders statewide through programs to help them become members in good standing within their communities and to lead productive lives. Fewer repeat offenders translates into lower prison populations and reduced spending of state tax dollars. In addition, a successfully employed offender pays taxes as well as enables the agency to collect millions of dollars to distribute funds to victims and their families.

The point people for these programs are the SCDPPPS agents and field personnel. These individuals are highly mobile, spending 50 to 60 percent of their time out of the office, traveling to where their clients are, including 46 courtrooms around the state. Notebook computers are an important tool for agents, providing access to

> "I appreciated the vision of how the Aerohive access points functioned, the intelligence they had, even when they were disconnected. Most other products I looked at got pretty dumb when they lost connectivity with the controller."
>
> **—David O'Berry**
> Director of IT, Systems and Services, SCDPPPS

client-related information in the Offender Management System, which is hosted in Columbia, South Carolina's state capital. "One-hundred percent of our users are now mobile capable," says David O'Berry, Director of Information Technology, Systems, and Services who is responsible for the SCDPPPS' statewide IT network. "At any point in time we could have up to 750+ mobile users."

In addition to the central site in Columbia, the SCDPPPS maintains 53 widely distributed offices around the State. When agents return to their office, they want a fast, hassle-free way to connect to the network. Locating and physically "plugging in" to an Ethernet outlet takes time. O'Berry's goal is to streamline the process by deploying wireless access points in all of the offices, giving agents as well as potentially other authorized state personnel instant connectivity as soon as they power their mobile device.

A Need for Independence

While wireless could have been potentially available at all of the offices over a year ago, O'Berry was not satisfied with the way the network had to be configured to ensure an acceptable level of security. "The solution we were testing required virtual tunneling back to a centralized controller in Columbia. It simply wouldn't scale that well."

Wireless security was an important issue not only for SCDPPPS users, but for guest users. SCDPPPS often works with other agencies connecting remotely, including Federal Probation, and local law enforcement while agencies like Vocational Rehabilitation actually work out of SCDPPPS offices at times. O'Berry wanted a way to provide secure guest wireless access for these users as well.

In addition to security, the centralized wireless network infrastructure also posed reliability and availability issues. If the central site went down, or the link to any local office failed, the local LAN would be down too. "You don't ever want users to lose connectivity to their local LAN," says O'Berry. "The wireless network must be independent to some degree."

A Matter of Scale

O'Berry kept an eye out for a wireless solution that could provide the security, resilience, flexibility, and scalability he needed. Then he learned about Aerohive. Aerohive's cooperative control access points require no network controllers or overlay networks. The result is enterprise-class security and scalability without the cost, capacity, performance, and availability issues associated with controller-based deployments. "I appreciated the vision of how the Aerohive access points functioned, the intelligence they had, even when they were disconnected," says O'Berry. "Most other products I looked at got pretty dumb when they lost connectivity with the controller. The Aerohive model scaled very well. From a scalability and resiliency perspective, I felt that Aerohive was the best choice."

After an extensive evaluation, the SCDPPPS chose Aerohive APs as part of a comprehensive solution that also included Unified Access Control (UAC) software from Juniper, an Aerohive partner. Aerohive offered the security features O'Berry was looking for, including 802.11i (WPA2), wireless IDS, 802.1X authentication, rogue detection, integrated stateful firewall, and guest access control, as well as integration with Novell directory. UAC provided additional strong security with pre-authentication and internal policy compliance.

Aerohive's controller-less APs eliminate the need to backhaul all traffic to Columbia—whether it is destined for the central site or not—

improving performance. This means that users can continue working locally even when the central site or WAN link is down. To boost resiliency, O'Berry plans to take advantage of the Aerohive APs' ability to automatically forward traffic to a default gateway, providing a failover route via SSL VPN to the central site.

Phased Deployment, Flexible Management

The SCDPPPS has completed the roll out of Phase One of the Aerohive deployment, covering the central site with 802.11n HiveAPs, and has begun subsequent deployments to distribute HiveAPs throughout 53 remote offices.

Aerohive's HiveManager Network Management System (NMS) was used to provision the new HiveAPs. The easy-to-use graphical user interface makes quick work of wireless network settings and security policies, eliminating the complexities associated with most wireless deployments. And when new HiveAPs are connected to the network, the HiveManager automatically discovers them and transparently pushes configuration settings and policies to them for a seamless plug-and-play installation.

On an ongoing basis, the HiveManager provides monitoring capabilities through a single, easy-to-use console management. "I like the flexibility that the HiveManager gives me," says O'Berry. "I can configure guest users, such as Vocational Rehab, as completely separate entities and allow them to manage their own APs if I need to with minimal hassle."

Planning for the Future

Due to their mobility, SCDPPPS Agents are potentially heavy cell-phone users. Even when they come back to the office, they are likely to continue using their cell phones based on their business efficiency needs. O'Berry sees an opportunity to deploy dual-mode phones that would work like traditional cell phones outside the office, but connect through the Wi-Fi network when in the office. "That would be a big deal from a cost savings standpoint," says O'Berry. "It also demonstrates the importance of the Aerohive network's ability to provide a scalable, resilient infrastructure."