From the Manhattan Project during World War II to present-day work in energy and environmental research, Sandia National Laboratories has been on the leading edge of developing and applying advanced technology for many different uses. Today, Sandia serves as a major research and development laboratory for the U.S. Department of Energy’s National Nuclear Security Administration.

Objective

A few years ago, Mark Mitchell, principal technologist at Sandia National Laboratories, started getting requests from his computing research group to add wireless LAN access to the Sandia campus. Because Sandia is a multi-program lab that performs national defense R&D and works on energy and environment projects, Mitchell was a bit apprehensive about deploying a full-scale wireless LAN.

After gaining security approvals, he initially deployed “fat” wireless access points (APs)—with onboard configuration information—in a few locations on campus. Once the next generation of “thin” wireless architectures emerged, Mitchell began testing products from a variety of other vendors, from startups to large networking companies.

Mitchell wanted a centrally managed wireless LAN system with a thin AP architecture that had no configuration information at the access point. He also needed the ability to locate and suppress rogue APs, handle multiple VLANs and support 802.11a/b/g standards.

Solution

Ultimately, Mitchell took down his first group of fat APs and replaced them with the Juniper Networks® Wireless LAN Portfolio, which is based on WLA Series Wireless LAN Access Points and WLC Series Wireless LAN Controllers.

Mitchell says the previous APs posed a security risk because configuration information is stored on the devices themselves, unlike Juniper where all intelligence is controlled centrally by the WLC Series Wireless LAN Controllers. Not only does the Juniper architecture make the network easier to manage, it also makes the wireless LAN more secure because a stolen or lost WLA Series access point will not work without the intelligence provided by its WLC Series controller. The WLC Series Wireless LAN Controllers also contain backup configurations for specific fail-over scenarios.

“The Juniper architecture is inherently more secure than what we had been using,” says Mitchell. “The value of the Juniper Networks Wireless LAN Portfolio, and the myriad features that are built into it, is just what we were looking for.”

He chose Juniper based on the responsive technical support, the price/performance gain and the time-saving capabilities of the RingMaster Software planning, management, monitoring and performance optimization suite. RingMaster Software enables IT organizations to perform pre- and post-deployment 3-D planning, remote configuration, 24 x 7 user monitoring and network-wide event reporting. It also creates detailed reports.
“I am truly impressed by all the amazing breakthrough wireless capabilities built into Juniper Networks Wireless LAN Portfolio. We pride ourselves on being in the forefront of the technology curve, and Juniper is the type of company we can rely on to help us make advancements in the way we do research.”
- Mark Mitchell, Principal Technologist
Sandia National Laboratories

RingMaster Software features greatly simplify the RF planning stage, so no RF expertise is required. RingMaster Software further simplifies the implementation process by including a library of RF attenuators defined for building obstacles, such as many types of doors, walls, ceilings, and other physical obstructions. All of which make sure that you have wireless LAN coverage exactly where you want it.

RingMaster Software also addresses the security issues Mitchell had raised by providing RF topology mapping and optimization; coverage hole mitigation, continuous, scheduled, or on-demand rogue detection; network-wide event reporting, user monitoring, location awareness, and packet tracing; as well as complete RF management and monitoring of network usage patterns to protect against unwanted intrusions and denial of service (DoS) attacks. RingMaster Software also detects, identifies and locates rogue APs, their users, DoS and probe attacks, as well as 802.11 ad-hoc networks.

Results
The Juniper Networks Wireless LAN Portfolio has proven to be a huge hit with Sandia employees by providing mobility and productivity gains to those that use the system. A majority of employees now use the Juniper Wireless LAN Portfolio to access the Internet, email and other resources during meetings and while roaming. Recently, the on-campus medical department developed specialized applications for tablet PCs that enable physicians to download the latest vital patient information in real time through the wireless LAN.

To ensure that data is secure, the Juniper Wireless LAN Portfolio uses 802.1X mutual authentication with WPA2/AES to encrypt all data between a client and the WLA Series access point. Unlike VPN-based security, Juniper encrypts the IP address itself, which is critical in a sensitive environment.

“I am truly impressed by all the amazing breakthrough wireless capabilities built into Juniper Networks Wireless LAN Portfolio,” says Mitchell. “We pride ourselves on being in the forefront of the technology curve, and Juniper is the type of company we can rely on to help us make advancements in the way we do research.”

About Juniper Networks
Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.