



CASE STUDY

Regional Athletic Complex Lights Up Outdoor Wi-Fi

Business Challenge

Salt Lake City is the capital of the state of Utah, with a population approaching 250,000. Its local government, Salt Lake City Corporation (SLCC), employs over 2,800 people and has an IT staff of around 60. As part of a longer-term vision to get its parks and recreation areas connected, the city's regional athletics complex turned on Wi-Fi.

The 140-acre complex near Rose Park features 16 soccer/multipurpose fields, including a stadium field equipped with a scoreboard, restrooms, and concessions. The complex is used for city-sponsored programs and is available to rent for tournaments, instructional camps, and league play by local schools, clubs, and businesses.

When the complex was first built in 2014, with funds from a bond measure and a donation from major league soccer, the city had been prudent to lay conduits under the fields, connecting lighting poles to a maintenance building near the center of the complex. Now they were ready to light it up and bring internet access to its users.

Since this was to be a free service, they needed a solution that would be economical and easy to operate, yet it also required high-end capabilities. They would need full security and the ability to allocate bandwidth and application priorities differently according to the ever-changing calendar of events and activities at the complex.

One Throat to Choke

The incumbent provider of wired and wireless network infrastructure across SLCC's offices was contacted for a possible solution, but with budget cuts and limited funds, they had to look for an alternative solution.

A big factor affecting the design was the relatively low-speed broadband connection to be available at the complex. With only 100 Mbps downlink capacity to play with, they would need to manage that bandwidth carefully from the edge of the network.

This ruled out most cloud-managed Wi-Fi options, because the high-end security and application controls are absent. A controller-based option would have required multiple security appliances—too many boxes to manage and high software maintenance fees.

SLCC didn't want any finger-pointing either. "We were determined to find one provider that could handle it all," says Jason Struck, network and security manager at SLCC. As existing users of FortiGate, FortiMail, and FortiWeb, they were familiar with Fortinet security, so they approached Fortinet too. "Nothing else came close to the economics and flexibility offered by FortiGate," notes Dustin Phillips, network engineer at SLCC.



"The Wi-Fi deployment at the Regional Athletic Complex has been a great success. It was brought online quickly, and we have the security and application controls we were looking for with very low support and operating costs."

– Bill Haight, CIO, Salt Lake City Corporation

Details

Customer: Salt Lake City Corporation

Industry: Government

Location: Salt Lake City, Utah, USA

Business Impact

- Integrated security and wireless local-area network (WLAN) management reduce complexity
- Complete set of security services included, with no hidden fees
- Comprehensive protection from cyber threats on an open network.
- Security future-proofing through frequent automated updates from FortiGuard Labs
- Low day-to-day energy costs due to consolidated platform
- Affordable, easy-to-replicate blueprint for future parks and recreation projects

Consolidated Solution

FortiGate appliances consolidate unified threat management (UTM) and wireless local-area network (WLAN) control on one high-performance appliance, equipped with wide-area network (WAN) and Power over Ethernet (PoE) switch ports. Wired and wireless network management and security are unified through a single pane of glass.

The complete portfolio of security services—from intrusion prevention system (IPS) to URL filtering and virus scanning—are included under a single license. There are no hidden fees or surprises when you want to enable a security option. With a single FortiGate 200D-POE, SLCC had all the security and controls they needed in a single box.

Secure Outdoor Wi-Fi

Six FortiAP 222C 11ac access points were mounted on the lighting poles using copper-to-fiber transceivers to utilize dark fiber laid in the conduits, and two more were installed on the exterior of the maintenance building, connected directly to the FortiGate over PoE.

The network was configured, secured, and running smoothly within three days. They could stream high-definition (HD) video at the extreme edges of the complex, but not in volume because of the small internet pipe. This and other applications would need to be throttled using FortiGate's application control functionality.

"Although Wi-Fi is offered as a free service, we have a civic—if not moral—duty to protect all of its users from cyberattacks and the spread of viruses," says Struck. "We also must ensure it is used appropriately, given this is a public venue for people of all ages," he adds.

Total Application Control

SLCC has enabled IPS, URL filtering, antivirus protection, and firewall features that are all kept up to date with regular updates by FortiGuard Labs, providing immediate protection against newly discovered threats and malicious sites.

"Having security and Wi-Fi management controlled through the same interface and implemented on the same platform makes the network really easy to understand and administer," says Struck. "And getting security updates automatically is tremendously reassuring," he continues. "But what is really amazing is the control we have over individual applications—we can prioritize, throttle, or block just about anything."

Solutions

- FortiGate
- FortiAP
- FortiGuard Labs

"Nothing else came close to the economics and flexibility offered by FortiGate."

– Dustin Phillips, Network Engineer,
Salt Lake City Corporation