# SECURE ACCESS FOR LARGE PUBLIC VENUES

## High-speed Wi-Fi with World-class Threat Protection

Large public venues such as arenas and convention centers face a constant struggle to deliver fast, reliable Wi-Fi coverage amid spiraling demands and unusually difficult environmental conditions.

Architectural and structural challenges such as high ceilings, concrete and steel barriers or walls, and large open spaces filled with reflective surfaces all make for a very hostile Wi-Fi environment. Add to that huge volumes of users and surging crowds, and large venues are among the most difficult places to deploy Wi-Fi successfully.

A secure, reliable Wi-Fi service has become critical to a venue's popularity and commercial success. In contrast, poor performance and connectivity, application security, or service delivery issues can be very damaging. Many event organizers now list Wi-Fi quality among their top five criteria when it comes to selecting a venue.

Meanwhile, sports venue owners and operators are hoping ubiquitous Wi-Fi can help reverse or slow down declining attendance by delivering a unique experience to the fans from the parking lot to the terraces and throughout the event. Venue operators need to step up the game-day experience and give fans a richer, more engaging, immersive experience, with Wi-Fi at the heart of the solution.

Fortinet's Controller-based Secure Access solution uniquely addresses the tough performance, scalability, and security challenges facing stadium, arena, and convention center operators.

## LARGE VENUE CHALLENGES

### HOSTILE RADIO FREQUENCY (RF) ENVIRONMENT

Stadiums and conference or exhibition centers are notoriously difficult places to provide reliable Wi-Fi. On one extreme, you have massive walls of concrete and steel, while at the other, the "bowl" or the "show floor" is a huge open space filled with reflective surfaces. Without walls to contain RF signals, interference is common, resulting in degraded connectivity and performance.

Capacity requirements at such venues dictate a dense deployment of access points (APs), likely to result in interference between APs. The resolution is a balancing act, requiring a significant amount of intricate planning, along with the associated investment in Wi-Fi accessories and controller features to better manage the RF footprint for the entire deployment.

### SCALING CAPACITY OVER TIME

With the venues expecting a huge number of Wi-Fi end-users and ever-growing bandwidth demand, they are caught in a vicious cycle, repeatedly needing to add more access points, shrink cell sizes, and redesign the channel plan to increase performance and capacity, without really effectively solving the problem.

### PROTECTING APPLICATIONS AND USERS

Protecting users from cyberthreats may seem out of the jurisdiction for end-users other than venue operator staff. But with so many users on one network, a single infected device could in turn infect other connected devices on the network, including those of the venue operators. Virus scanning and URL filtering is recommended to be applied to guest access and traffic, and guest traffic should of course be segregated from the venue operator's specific applications and services to ensure security and performance. A combination of user rate limiting, application prioritization,

## SECURE ACCESS

*Fortinet's Secure Access solution enables stadiums, arenas, and convention centers to keep tens of thousands of bandwidth-hungry event-goers connected, while at the same time enabling and securing critical applications and services such as point-of-sale (POS) and digital signage and communications, among others.*

- Easiest deployment and capacity scaling in the industry
- Better Quality of Experience (QoE) with faster, more reliable access and roaming
- Real-time load balancing and efficient airtime conservation deliver true fair use policy and optimized bandwidth allocation
- Superior 802.11ac performance with site-wide channel bonding
- Comprehensive threat protection consolidated on a single platform
- Exceptional visibility and control of applications and utilization
- Real-time monitoring and signature updates from our research and analysis agency, FortiGuard Labs

application throttling, and application blocking are all needed to manage network utilization so that everyone has an equally good experience, and to ensure mission-critical applications are never compromised.

But when networks are overloaded most of the time, especially if users are highly mobile, rate-limiting and QoS accuracy breaks down. What else can be done to guarantee performance for VoIP and mobile point of sale (mPOS), without needing to deploy separate parallel networks?

### MONETIZING THE NETWORK

To offset the high cost of the Wi-Fi network, venue operators must explore how the wireless LAN (WLAN) can save money or make money. Captive portal and social login are an obvious first step for harvesting visitor intelligence for online and offline marketing purposes, but that's just the beginning.

Stadiums and arenas that let fans order merchandise and concessions online, right from their seat or suite, can boost sales 10-15%. And streamlining concession purchases with mPOS can save thousands by removing cash handling and petty theft from the system. Convention centers can offer "Show Wi-Fi" sponsorship, and premium access tiers to VIPs and groups, or by location.

There are advertising options and much more. However, unless you can guarantee a reliable user experience, none of the above matters. Managing applications and controlling the service quality is therefore critical for success.

## FORTINET SECURE ACCESS

As enterprise Wi-Fi has matured, different enterprise WLAN architectures emerged and feature sets have commoditized. In most enterprise deployments, there is little to separate vendors from a performance and connectivity perspective.

However, in some use cases, one deployment model can stand out with clear advantages over others, and large public venues are a prime example—they face special coverage and capacity challenges that overshadow most other considerations.

While other WLAN vendors present the same solution for every scenario, Fortinet's Secure Access embraces all common WLAN topologies and deployment models with no less than three distinctly different wireless offerings, each backed with world-class cybersecurity.

Fortinet's Controller solution is made up of best-of-breed wireless, switching, and security components; the Integrated solution combines WLAN control and security on a single, high-performance appliance; and the Cloud solution embeds security intelligence into cloud-managed access points.

With Fortinet, large public venue operators don't need to compromise security for performance. Fortinet's Secure Access provides comprehensive protection from classic wireless intrusion threats to all types of malware and application threats, while delivering an outstanding Wi-Fi experience to hordes of bandwidth-hungry fans or attendees.

## FORTINET CONTROLLER WIRELESS SOLUTION

Because of the extraordinary environmental challenges in large public venues, Fortinet recommends its Controller-based wireless offering. This solution gives large public venue operators scalable, high-performance, high-density Wi-Fi with everything they need to handle tens of thousands of mobile devices, manage application usage and priorities, and enjoy world-class protection from current and evolving threats.

The Controller-based secure access solution consists of best-of-breed components for switching, WLAN, and management. The WLAN component provides a high-performance, premise-managed Wi-Fi network with a broad range of APs including indoor and outdoor dual 11ac radio APs.

What makes it so different is its unique single-channel management architecture called Virtual Cell, which simplifies deployment and scaling and delivers compelling reliability and traffic isolation advantages over the traditional multi-channel approach used in other solutions.


FIGURE 1: FORTINET VIRTUAL CELL DEPLOYMENT MODEL

Virtual Cell minimizes the complex, time-consuming process of channel planning, which can take months for a large venue, through its unique single-channel deployment model, which avoids the challenges of planning around co-channel interference.

In a Virtual Cell, all radios operate on the same channel, providing a layer of coverage across your venue, and they appear to clients as a single radio wherever they go. In addition, the network, not the client, controls how and when clients roam. This unique approach renders co-channel interference harmless and ensures that clients use the best available connection at all times.

This network-based traffi c control also makes it possible to perform real-time AP load balancing based on actual traffic, not crude, round-robin algorithms based on station count. It even governs station airtime so every client gets a fair turn on-air, and the slowest devices don't hog resources.

## RAPID DEPLOYMENT AND SCALING

To increase coverage or incrementally boost capacity in one particular area—say, extending coverage to the parking lot—you don't need to survey the site, move other APs around, or adjust channel and power settings. Just add APs wherever it is physically convenient and you're done.

Doubling or tripling capacity, which normally requires a highly disruptive redesign of the network, is also a cinch using a non-disruptive approach called channel layering.

For large-capacity gains, multiple Virtual Cells can be configured to each use a different channel, while occupying the same coverage area, by adding additional sets of APs. Layering cells in this way can be limited to a small zone requiring more capacity, or Virtual Cells can span the entire venue.

What's more, you can roll out new Virtual Cells at your own pace. Layering a new Virtual Cell alongside another does not require any changes to existing cells, so the stability and performance of your existing environment is never put at risk each time you need to scale capacity.

### TRAFFIC ISOLATION AND VIP SERVICES

Channel layering can also be used as a strategy to physically segregate mission-critical corporate traffic from guest traffic, or to guarantee more capacity to select groups of users such as staff, press and VIPs, or mPOS.

If not for day-to-day operations, in emergency situations facilities staff will need 100% reliable access to voice services and public-address systems, without risk of network congestion from guest traffic. Using Virtual Cells to isolate critical traffic types can provide dedicated spectrum for such requirements.

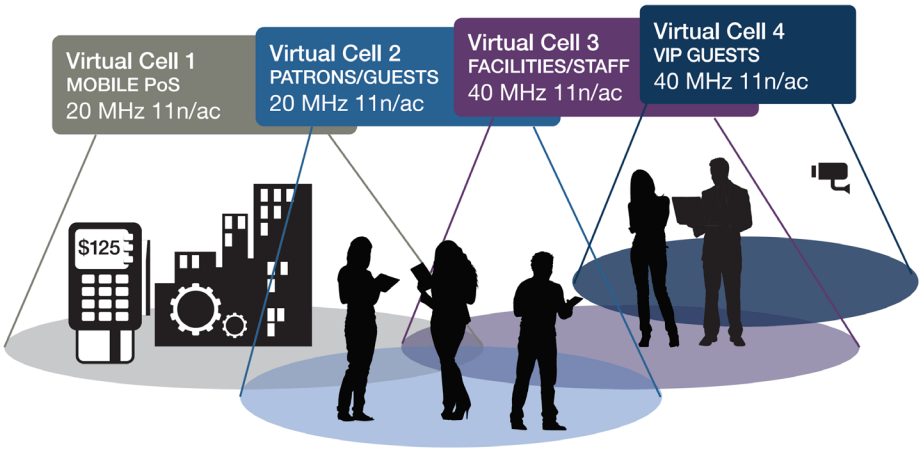


FIGURE 2: RISK-FREE CAPACITY SCALING WITH CHANNEL LAYERING

### MORE RELIABLE CONNECTIONS

In Virtual Cell it is the network, not the client, that dictates when and where a client should roam to get best service.

This network-directed roaming technique, which mimics the way roaming occurs in cellular networks, delivers a number of performance and reliability benefits.

It conserves airtime and utilizes network resources more efficiently than when clients control their own destiny, by dramatically reducing airtime-eroding beacons and probes. It also ensures each client uses the best connection available to it, and it fixes common problems like sticky clients, further reducing unnecessary probes and retransmissions.

Under network control, roaming is almost instantaneous roaming (3ms vs. 100+ms), which makes voice calls and any type of real-time traffic more reliable. And when thousands of fans race to the bar at halftime, or conference attendees surge from the keynote to other conference rooms, they stay connected and whatever they were doing is not interrupted.

### COMPREHENSIVE CYBERSECURITY

In this solution, comprehensive access security and granular application control is provided as an overlay with Fortinet's award-winning FortiGate cybersecurity platform, which features a complete portfolio of security services.

FortiGate consolidates the functions of more than seven individual security devices, including firewall, VPN gateway, network IPS, DLP, anti-malware, web filtering. and application control, in a single, high-performance platform.

With signatures for over 4,000 applications, FortiGate's Application Control provides the utmost visibility and control of the priorities and resources assigned to different apps. You can prioritize, throttle, or block literally any application. Complementary URL filtering can also be used to block end-users from navigating to known phishing and botnet websites or adult content.

With a FortiGate appliance in your network, you have an "all-you-can-eat" buffet of security features that can be selectively applied to different groups of users, to prioritize apps, control bandwidth, and detect all classes of cyberthreats from wireless intrusion to malware.

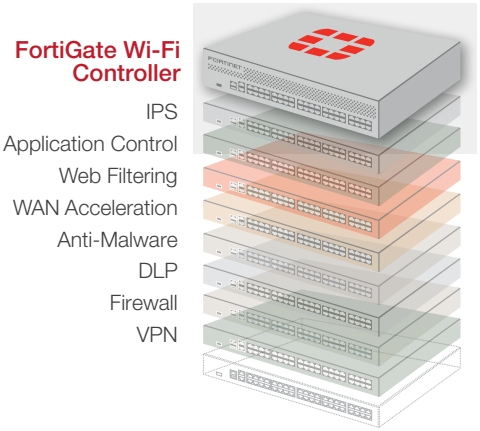


FIGURE 3: FORTIGATE CONSOLIDATED SECURITY PLATFORM

FortiGate is a recognized cybersecurity performance leader. The appliance's Security Processor-assisted, high-performance architecture allows any number of different security policies to be applied to traffic in a single pass, which keeps latency to a minimum.

FortiGate security is kept continually up to date through frequent automated updates from FortiGuard Labs, which researches the latest attacks to provide your network with immediate protection.

## SUMMARY

Arenas and convention centers are some of the most difficult places to successfully deploy Wi-Fi. But make no mistake, whether your business is hosting conferences and expos or sports events, providing a fast, reliable Wi-Fi service throughout your venue is a strategic imperative. The challenge is how to overcome the deployment barriers common to large venues.

Fortinet's Secure Access solution takes a completely different approach, which eliminates deployment complexity and eases capacity scaling. The high-performance WLAN offering is also complemented with unprecedented application control and threat management, to ensure complete control over network traffic and comprehensive protection from cyberthreats.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990



**March 03, 2017**