Ruckus
Simply Better Wireless.

case study

SecureHotspot: InnFlux

SECURING ACCESS TO OPEN HOTSPOTS WITH ZERO HASSLE

Next to Brigham Young University (BYU) in Provo, UT, an ultra-modern student housing community (The Village at South Campus) was recently developed by property owner Peak Capital Partners that offers a premier lifestyle for BYU students, a big differentiator in the ultra-competitive higher education market.

As a new development, nothing was spared for the best student living experience available including fitness rooms, a pool, game rooms, and of course study rooms, all at a reasonable cost. During the planning process, the specifications called for a critical student requirement of high-speed wireless Internet access for all students that would be reliable, secure, and would not require an IT staff on hand to manually manage credentials.

The problem needed to be solved was: “how to provide secure Wi-Fi access automatically to users accessing open hotspots?”

Open Wi-Fi hotspots are becoming marginalized, as end users are now more skeptical of transmitting any sensitive information over these unencrypted networks. Meanwhile even typical open hotspots require some client configuration.

For The Village, providing and automating security for students accessing its open Wi-Fi hotspots, despite the device being used, was the only way to maximize the wireless infrastructure.

Because most current secure solutions, such as 802.1x authentication, pre-shared keys, etc, require tedious pre-configuration from the hotspot administrator and/or complex registration on behalf of the end-user, these solutions are impractical for the typical ephemeral hotspot user and hotspot administrator rendering them completely useless.

InnFlux, a nationally renown Internet technology provider, was commissioned to oversee the Internet services and connectivity of this deployment. They found that most WLAN vendors lacked the features and technology needed to manage the secure connectivity and bandwidth sharing required to maintain the network without extensive IT management. The only other alternative would be to set up each student with their own access point, which would limit connectivity to the room. This represented a management nightmare and would be prohibitively expensive.

REQUIREMENTS

- Providing secure access to open hotspot despite device type
- Automating the process by which secure student access could be achieved
- Minimal user or IT management involvement with credentials or credential management
- Bandwidth fairness to ensure no heavy bandwidth user(s) will inhibit the other users’ bandwidth
- The ability to dynamically direct users to specific VLANs based on authentication
- Performance and capacity for dense client environments
- Simplified and intuitive guest networking

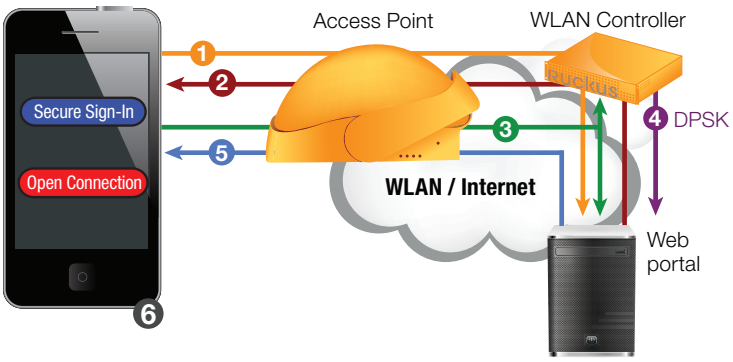
SOLUTION

- 241 ZoneFlex 7363 dual band APs
- 1 ZoneFlex 7762 outdoor APs
- ZoneDirector 3000 controller

BENEFITS

- Approximately four rooms covered per AP whereas competitive solutions required one AP per room
- SecureHotspot with ZeroIT and DPSK allows for simple, secure networks that are easy for both the end user and IT manager to maintain and use
- Device specific security key allows individual private users to ensure they receive their own allocation of bandwidth
- Reliable WLAN in high density environment that typically is impacted by self-interference
- Service provider ability to monetize the network with premium services that do not require significant overhead

SecureHotspot:
InnFlux



1. Client associates to AP; WLAN controller doesn't recognize anonymous device, sends client to Web portal
2. Web portal redirects to branded portal page, requesting user to sign in or provide credentials
3. Sign-in request sent from client to Web portal, which instructs controller to generate a unique encryption key
4. WLAN controller sends encryption key to Web portal
5. Web portal forwards encryption key along with requisite Wi-Fi configuration information to client and auto configures client
6. Client automatically reassociates to secure SSID with encryption key allowing secure hotspot transmissions

Multi-dwelling units (MDUs) typically don't offer secure connectivity – using the "open" type of guest networking available with any wireless network, nor do they have IT managers on staff. What The Village really wanted was more than typically offered in a guest network, they wanted each student to have their own reliable private network. The main challenge with this request required managing Internet access to private student residents securely without compromising bandwidth fairness, all with minimal IT manager intervention.

So InnFlux turned to Ruckus and its new Secure Hotspot technology.

SecureHotspot is a unique approach to securing clients connecting to open hotspots that leverages Ruckus' existing patented technology, ZeroIT Configuration and Dynamic Pre-Shared Key (DPSK). DPSK is used to generate unique 63-character encryption keys for each user device on an open network without the need to authenticate or preregister users. These encryption keys are then downloaded and installed within each client device automatically using Zero IT Configuration.

With SecureHotspot, all of the 'authentication' is done in the background. After the client associates to a Ruckus hotspot AP with SecureHotspot enabled, the ZoneDirector takes over and sends the client device to the web portal. The end user then receives a request to log in either securely or in the open network.

After signing in securely, a unique pre-shared key with a limited life is sent to the device and the encrypted handshake is then completed from the ZoneDirector, Web portal, and the client device thus completing an encrypted session. The only thing the end user sees is the option to connect securely or not. There is no need on the part of the hotspot administrator to pre-configure any users, however, administrators can log details on users and usage within the hotspot.

To ensure seamless operation between the Web server and the WLAN infrastructure, InnFlux created a simple script that allowed the Web server to tell the Ruckus ZoneDirector that it was OK to generate DPSKs for a given users. And that was it.

For The Village, student credentials expire when they finish school for the year. SecureHotspot technology is also able to automatically direct student traffic to a specific VLAN to assure promised bandwidth and fair allocation of traffic among students as well as to provide explicit resource access, etc.

InnFlux offers BYU students a tiered plan for connectivity. The initial plan is a free service, included as part of the housing cost, and the other two plans charge an incremental monthly fee for increasing bandwidth, the ability to connect more devices to the network, differentiated security policies, as well as other service enhancements.

Ruckus®
Simply Better Wireless.

SecureHotspot:
InnFlux

"Ruckus helped us resolve the fundamental problem of setting up a viable, simple to use private network for each student resident without extensive IT set-up and management. Now we can offer MDU student residents a manageable private network that is rarely offered in the student housing market."

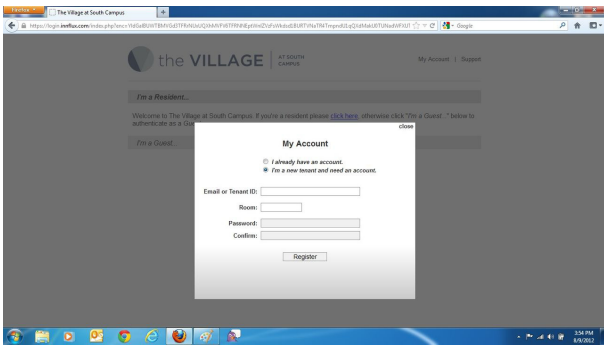
Chris Wieland
CTO, InnFlux

Additionally, with high performing Ruckus APs, InnFlux was able to cover almost 1,000 student rooms and almost 2,000 registered devices (not including guest access) over two buildings including outdoor courtyard, pool, office, and retail coverage with 242 Ruckus dual band APs. This resulted in the ability to deploy one AP to support four or more rooms. Alternative Wi-Fi suppliers specified the deployment of an AP for each room. This would have dramatically increased management and maintenance efforts as well as upfront costs for more equipment and the ongoing costs for maintenance.

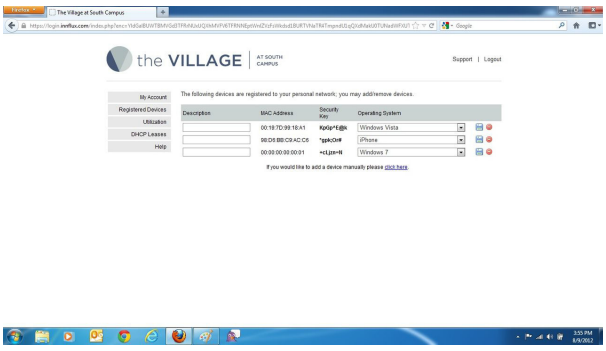
Aside from Ruckus' SecureHotspot capability, Chris Wieland, CTO of InnFlux, noted that the key RF capabilities of Ruckus saved on upfront costs because of the high performance with BeamFlex, and less maintenance hassles typically created by AP self-interference in a densely packed network with Ruckus interference mitigation. Furthermore, the PD-MRC polarization diversity capabilities of Ruckus APs provide added performance benefits to students who rely on hand held devices for connectivity challenging the RF environment with traditional stationary antennas.

As a provider offering services to students, InnFlux is impressed with Ruckus' performance and feature set. "Ruckus has allowed us to implement a viable private resident network for the MDU market, among others, that does not require high upfront costs or ongoing costs to maintain." Said Wieland, "We thought there would be much more call volume coming into our call centers, but it is much lighter than we anticipated."

Noting the advantages of the differentiation that SecureHotspot offers, Wieland stated that not only has it helped them create new business in other student housing markets, but this technology has helped them enter other segments as well, such as the other MDUs including apartments and condominiums.



Simple one time registration allows for entire year of private dedicated secure network for each individual student



Students can individually manage their registered clients at any time as well as monitor their own usage patterns

Ruckus®
Simply Better Wireless.