Contact: Marc Pinotti, WiFi4guest Suit 200

PHONE +1 (425) 285 – 4353, WEB HTTP://WWW.WIFI4GUEST.COM
EMAIL – SUPPORT@WIFI4GUEST.COM , 8201 164TH AVE NE REDMOND, WA 98052

Wifi4Guest

A New Approach to Guest Internet Access at a Global Software Company.

October 2016

Case Study

Organization
Global ISV with over 100,000 full-time employees, and over 100,000 additional contractors, partners, and guests annually.

Situation
As a leader in IT software, the company hosted hundreds of thousands of devices on the corporate network every year—all requesting access to the Internet. However, their wireless infrastructure was not sufficient to meet both the security needs of the organization and the simplicity needs of end-users.

Solution
The company turned to WiFi4guest to provide a cost-effective, simplified Internet access solution that would ease the burden on IT administrators by separating Internet traffic from guest devices onto an isolated network.

Benefits
- Safe access to the Web
- Simplified administration
- Easy to use for both guests and employees across a wide range of devices

Software
- WiFi4guest Enterprise Captive Portal
- Microsoft Windows Server, Microsoft SQL Server

Overview

BUSINESSES LOOKING TO ENHANCE NETWORK SECURITY AND OPERATIONS, WHILE STILL PROVIDING GUEST INTERNET ACCESS TO ALL USERS, NEED A SOLUTION THAT WILL SEPARATE CORPORATE FROM UNTRUSTED TRAFFIC WITHOUT INCREASING COST AND COMPLEXITY. A MULTI-NATIONAL SOFTWARE COMPANY TURNED TO WIFI4GUEST FOR A CUSTOMIZABLE, EASY-TO-USE NETWORK MANAGEMENT TOOL THAT COULD SUPPORT A BROAD RANGE OF DEVICES AND INTEGRATE WITH EXISTING INFRASTRUCTURE INVESTMENTS.

Introduction

An increasing number of companies are embracing Consumerization of IT (CoIT) as a core business principle, electing to welcome smart devices into the enterprise computing environment that were never before planned to be there. At the same time, employees are demanding a simplified, high performance Internet access experience when they are on the corporate network, regardless of the devices they are using.

One technology organization, in particular, felt this pressure more than most. A major software company with global operations and hundreds of thousands of employees, contractors, partners, and customers on their campuses every year needed a way to provide consistent Internet access for unknown devices—be they personal or business-owned.

This “Bring Your Own Device” (BYOD) trend meant there were more individuals with more devices needing Internet access, including unmanaged, non-domain-joined laptop PCs, tablets, and smartphones. Corporate IT wanted greater control over network traffic segregation, bandwidth utilization, quality-of-service, information security, and user support for the thousands of new devices joining the network each week.

So while BYOD had the potential to enable greater end-user productivity by letting them use the types of devices they wanted, the company was at a crossroads for deciding how to adapt their infrastructure accordingly.

Internet Access for Everyone

The company wanted to provide a seamless Internet experience for both employees and visitors. They hoped that a more open approach to network management could foster increased productivity by enabling a more flexible work style, and could not only reduce costs,

but result in higher overall efficiency—if only users were able to work on the devices they chose.
While the goal was to streamline the way users gain access for both business and personal tasks, it was equally important to maintain corporate network integrity in the process. This meant moving less secure personal devices off of the internal network and onto an alternate service.
The problem was that the existing infrastructure for Internet access via the corporate network placed operational burdens on end-users. Connecting a wireless device required multiple configuration changes and security settings to be managed. In addition, corporate IT had been maintaining multiple networks and administrative functions in order to separate public traffic from sensitive internal traffic, which also had the effect of increasing overall IT management and support costs.
The company needed a solution that would bridge the gaps between current infrastructure and the needs of end-users, yet not further complicate network management or risk organizational security.

Meeting the Needs of End-Users and IT

Increasingly, technology companies today need broad support for consumer PCs (laptops) and Macs, as well as other generally non-trusted devices that require Internet connections. At this company, vendors, partners and guests routinely bring such systems with them, and corporate management wants to support them without dictating what kind of device they have to use on the company network. Their goal was to support whatever form-factor the guest had.
The company's IT group settled on several criteria for choosing a guest-network solution:

- Basic authentication and access mechanism
- Transparent compliance with industry regulations
- Bi-directional security and privacy for both corporate and personal data
- Minimal support costs, but with the broadest platform acceptance

Furthermore, keeping implementation and service costs at a minimum required the solution to use readily available off-the-shelf components that would support broad access without complex software agents or client-authentication mechanisms:

- Simplify the end-user experience
- Enable employees and visitors to easily access the Internet from almost any device
- Eliminate network administrator intervention for adding devices to the network
- Improve return-on-investment by leveraging as much existing infrastructure as possible

With these requirements in mind, the software company outlined the use cases that would best address the ways employees, vendors and guests use wireless devices on the Internet. Employees frequently had multiple companion devices, including personally-owned "untrusted" (not managed by corporate IT) smartphones and tablets, as well as company-owned tablets and laptops. On-site vendors had the same range of devices, but they were all "untrusted" (personal smartphones and tablets, with laptops owned by their respective organizations). Finally, in all cases, guests used devices which were personal.

The last set of requirements lied in determining the company's policies regarding Internet usage. On the one hand, individual users deserved privacy when connecting their personal devices to the network. On the other hand, a fundamental goal of the project was to enhance corporate data and application security and protect the organization from both intentional and unintentional exploits.

Thus, policies were created that could differentiate between personal and corporate network traffic in order to provide transparent Internet access without applying content inspection, yet separated sensitive internal traffic and enforced rigorous security controls.
Although the particular needs for each group differed slightly, the common elements identified above made it easier to define a solution that could meet everyone's needs: an isolated virtual network for all

devices that were not company-owned. Their Internet traffic would remain private, and company data would stay protected.

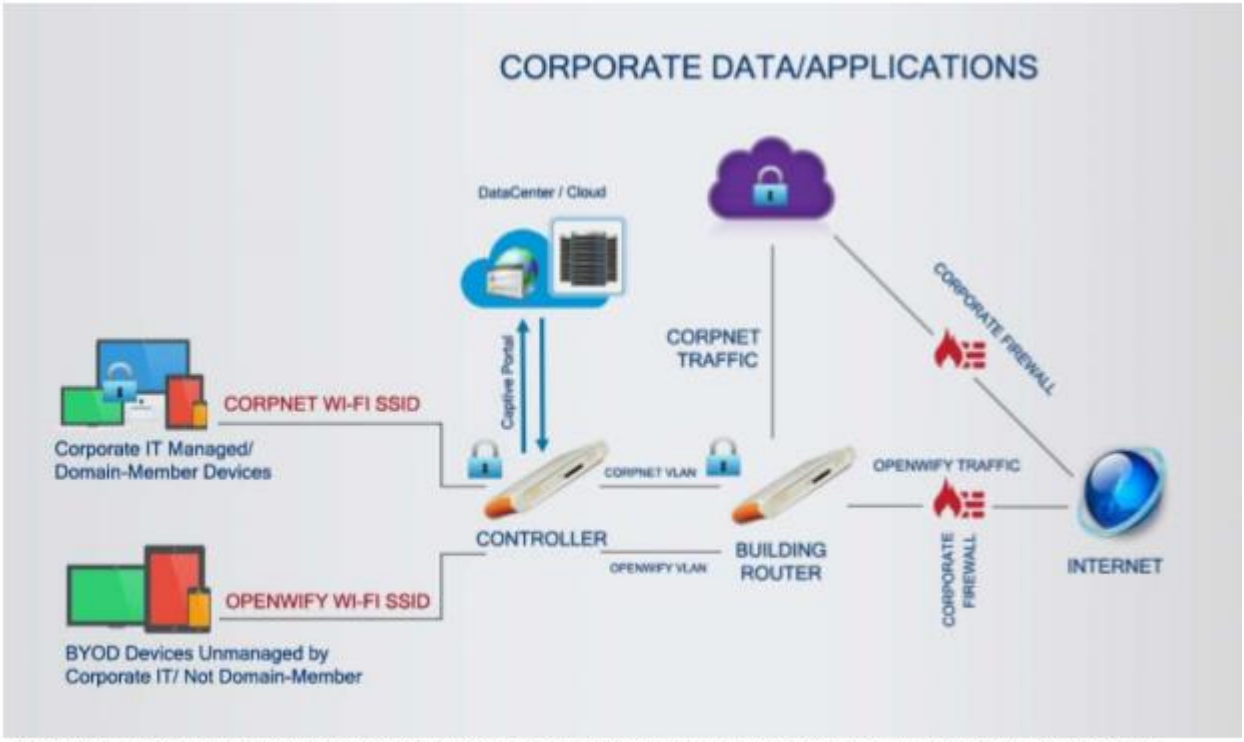


FIGURE 1: EXAMPLE TOPOLOGY FOR CONNECTING WIRELESS DEVICES THROUGH THE AMBIENTWIFI ENTERPRISE CAPTIVE PORTAL.

A Solution for Common Access

The WiFi4guest Enterprise Captive Portal is a scalable solution for open Internet access by any Wi-Fi enabled device on your corporate network without increasing security risks to your IT infrastructure. WiFi4guest delivers simplified management, monitoring, and reporting with a customizable “captive portal” experience that enables end-users to quickly and easily connect, helping to reduce network support costs and improving productivity.

WiFi4guest Enterprise Captive Portal marks a break from high-cost, monolithic open-network products by integrating seamlessly with your existing IT infrastructure to provide new access services. Instead of requiring investments in expensive hardware add-ons to create and manage a virtual network, WiFi4guest enables your IT organization to easily enhance and isolate Internet traffic coming from mobile devices—using the equipment you already have

How It Works

WiFi4guest was able deliver a solution capable of identifying untrusted devices and shunting their Internet traffic to an isolated wireless network. Any wireless device—employee or guest-owned, personal or corporate—attempting to connect to the corporate network would see two wireless SSIDs: CORPNET and OPEN. If the device is trusted (meaning domain-joined and fully managed by corporate IT), it will default to a CORPNET connection; if the device is untrusted, it will be automatically rerouted to a web page where the user can easily “click-to-connect” for Internet access to the OPEN network. WiFi4guest Enterprise Captive Portal identifies and registers the device’s MAC address, assigns an IP address for the OPEN network, and grants access to the Internet—much like a hotel or airport hot-spot that presents a web page containing terms and conditions for access, asking the user to “click-to-accept” before being fully connected.

The solution was deployed on existing network routers, controllers, firewalls and wireless access points (shown in Figure 1), using Microsoft Windows Server and Microsoft SQL Server as the foundation for web authentication and MAC address storage (as well as detailed log data for usage reporting).
Both the web-based Enterprise Captive Portal Management Console and the user-facing authentication page run on an isolated virtual server with Internet Information Services. It connects through a secure link to the main network controller hardware to gather the MAC address, query the database for connection details, and then instructs the controller to allow Internet access.

Simplified Management for BYOD Scenarios

WiFi4guest Enterprise Captive Portal provides easy-to-use tools that are highly customizable and designed for a wide variety of scenarios. Examples include business portal pages displaying marketing or support details, terms-and-conditions for Internet use, or integration with numerous authentication providers.
In particular, the software company wanted to display a simple end-user agreement outlining fair usage of corporate network resources, and inform the user about the privacy policy. This straightforward mechanism made it easy for end users to connect to the Internet through any device—even those without web browsers (for instance, a device set to sync e-mail with an Exchange Server).
The guest network solution also provided IT administrators with monitoring, logging, and reporting to help maintain security and troubleshoot both deployment and end-user connectivity issues. With an intuitive web based management console, support costs could be kept to a minimum, and network information could also be linked to a security incident or enterprise management system using the .NET Framework.

Safe and Secure

All traffic from the OPEN network must pass through the same corporate firewalls as MSFTCORP traffic in order to maintain network security (protection from malware, exploits, etc.), but completely isolated on its own virtual LAN. Traffic from trusted devices (such as employee laptops) is further inspected for information leakage prevention and compliance, while untrusted devices on the OPEN network route directly to the Internet through the firewalls. This way, all devices—regardless of their origins—are protected by common infrastructure for intrusion prevention, anti-malware, and application-layer security.

Improved Productivity

One of the consistent needs expressed by users was that every visitor—contractor, customer, partner, or guest—that came to the company's offices needed Internet access, but the corporate network was locked down, blocking connections without someone calling the helpdesk. The WiFi4guest Enterprise Captive Portal alleviated this problem by letting end-users manage their own access requests quickly and easily, further enabling enterprise IT to provide transparent Internet connectivity without adversely affecting costs.
In addition, when users are able to get tasks done on the kinds of devices that work best for them, they are more efficient. Since the WiFi4guest Enterprise Captive Portal does not require any client-side agent installation or configuration, any Wi-Fi-enabled device can connect through both a web browser and an application.
The result is that both employees and visitors can be more productive on their preferred companion devices, since they can stay in contact a use network resources no matter where they go on the corporate campus.

Contact: Marc Pinotti, WiFi4guest Suit 200

PHONE +1 (425) 285 – 4353, WEB HTTP://WWW.WIFI4GUEST.COM
EMAIL – SUPPORT@WIFI4GUEST.COM , 8201 164TH AVE NE REDMOND, WA 98052

Summary

The company enabled both employees and visitors to access the corporate network and get to the Internet using the devices that they preferred. WiFi4guest Enterprise Captive Portal reduced network maintenance costs and improved user productivity, without sacrificing security and performance. WiFi4guest Enterprise Captive Portal addresses an emerging market trend that sees enterprise organizations taking a commoditized approach to the increasing demands of mobile device users. The Consumerization of IT means that support staff are being overwhelmed with users wanting to place their WiFi enabled smartphone, tablet, or personal laptop on MSFTCORP. It is difficult for customers to manage a manual access process, and does not make sense to open their sensitive internal network to any and every user's device.

WiFi4guest Enterprise Captive Portal helps network and security administrators enhance the end-user experience, provide richer connectivity options, and improve control over mobile Internet traffic. Centralizing network access and routing all unmanaged devices through a single point lets administrators enforce usage policies, detect malicious activity, require authentication, and gather statistics on guest access.

With WiFi4guest, the company was able to:

- Enhance employee productivity by permitting them use their own devices and applications, in the way they want to, while greatly simplifying support requirements.
- Implement a more secure corporate computing environment by isolating traffic from unmanaged devices.

About Us

Founded in 2013, UnifyCloud LLC specializes in software innovation that leads the industry with cost effective IT solutions to real-world problems. Visit us and learn more about our product portfolio at http://www.Wifi4guest.com.

The information contained in this document is provided for informational purposes only, and WiFi4guest makes no warranties, express or implied, with respect to the document or the information contained in it. WiFi4guest is a trademark of UnifyCloud LLC, 2016. All rights reserved.