FORTINET

Wireless Defense Strategies in the IoT Era

Table of Contents

FORTINET

Introduction

Nonstop mobility, instantaneous network access, and a flood of new wireless devices are the new norm for enterprise wireless LANs (WLANs). Employees are no longer tethered to their desks, and they expect pervasive mobile application access. IT organizations are faced with constant technology transformations such as the Internet of Things (IoT), anything-as-aservice (XaaS), and artificial intelligence. Securing enterprise WLANs from unauthorized access and cybersecurity attacks are top of mind for enterprise IT decision-makers worldwide. These trends have significant implications for implementing and securing WLANs.

Enterprises must plan with a “mobile-first” mentality to establish a robust, end-to-end security architecture within the enterprise. This requires strategic changes to effectively secure both wired and wireless LANs while supporting business applications of every type.

Here we’ll discuss access layer protection in enterprise WLANs and why deploying ad hoc security is no longer enough to protect against threats. This eBook explains how a secure access architecture gives enterprise networks the end-to-end protection required now and into the future.

01: Access Layer Security Needs A Second Look

The number and diversity of Wi-Fi devices is still rising. The Synergy Group has reported that WLAN is the fastest-growing technology in enterprise IT infrastructure[1]. The Wi-Fi Alliance® predicts that the number of connected consumer and business devices will reach 38.5 billion in 2020[2]

Across almost every industry, people are using multiple personal and work-supplied devices to access mission-critical applications. The BYOD experience is no longer a revolution—it's the new norm. In a recent survey conducted by Lightspeed GMI for Fortinet, 56 percent of IT decision-makers worldwide indicated that BYOD access is supported. In North America alone, the number is 76 percent. In addition, these IT organizations are expected to have complete control of all devices.

Similarly, IoT has become mission critical in the enterprise, introducing new security challenges.

Emerging IoT applications are bringing new unsecured wireless devices to vertical markets everywhere. From the factory floor to the hospital recovery room, IoT devices range from industrial robotics to advanced medical sensors. They are being deployed in huge numbers for a wide range of innovative and gamechanging applications. But this exponential increase in a multitude of unsecured device types presents new vulnerabilities and threats.

Within this rapidly changing landscape, securing business communications, personal information, financial transactions, and mobile devices involves much more than network access control. It requires scanning for malware, preventing access to malicious websites, endpoint integrity checking, and controlling application usage. As a result, IT departments are faced with the difficult task of balancing the requirements of network security with the flexibility to onboard the growing number and diversity of clients.

02: New Defense Strategies

With high-profile attacks on major organizations, cybersecurity and the protection of critical company and customer data are top concerns. In many cases, however, IT organizations have yet to include key security measures such as intrusion prevention or application control, which add critically needed protections.

A more unified access layer strategy helps protect against these sophisticated attacks to assure secure communications, data, transactions, and mobile devices. This includes:

- Ensuring consistent application and device policies across both wired and wireless environments, and across multiple devices per user
- Adding multiple layers of defense, including explicit internal network segmentation, to break or mitigate the chain of infection
- Continuous scanning for malware to prevent access to malicious websites, endpoint integrity checking, and controlling application usage

Unified Access

Typical Wi-Fi strategy implementations do not cater to these strategic requirements. For example, many campus networks have become flat, creating a wide-open environment. This means that any person or device—whether legitimate or not—has unchecked access to the entire network and associated IT resources. Regardless of sophistication, cyberattacks can wreak havoc on a flat network very quickly. Multiple layers of defense are essential to protect against attacks that are getting past border defenses.

Explicit internal segmentation, with firewall policies between users and resources, limits traffic, provides logs, and helps break the infection chain.

WIPs

Implementing wireless intrusion protection (WIP) systems enables the detection of and safeguard against rogue devices, unauthorized access, and ad hoc networks. For automatic prevention, WIPs must accurately detect and classify all threats. However, the deployment of WIPs in an ad hoc network architecture is a big challenge to optimally configure and maintain.

NGFWs

Because threats are constantly changing and mutating, there is a strong trend towards implementing next-generation firewalls (NGFWs). Now more than ever the need to be part of any security system in order to effectively fight advanced threats and respond to new cybercriminal tactics. NGFW systems enhance existing security methods by extending the capabilities of traditional firewalls. This includes intrusion prevention, SSL/SSH, deep-packet inspections, malware detection, and application awareness. NGFWs bring additional context and the ability to understand the details of web application traffic passing through the network, while taking action to block traffic that might exploit vulnerabilities.

Visibility and Control

Configuration and management is a highly critical aspect of implementing this broad range of security measures. Even as enterprise organizations deploy new security capabilities, breaches can still occur as a result of ineffective configuration and management. Deploying and managing disparate security systems for access control, WIPs, and firewalls is resource-intensive and open to error. These challenges can be addressed by deploying an integrated, end-to-end security strategy.

03: How To Select a Secure WLAN Solution

Enterprise organizations need a security fabric that provides flexible end-to-end protection across all their IT environments. Multiple layers of defense present the best way to protect against the highly sophisticated attacks that are getting past border defenses. Explicit internal segmentation, with firewall policies between users and resources, limits traffic and can break an infection chain. In addition, security mechanisms must be integrated into the network to protect access from unsecure IoT and BYO devices.

Any WLAN security strategies should include an integrated wireless solution where control and security are combined in a single portfolio. Optimal security should be comprised of all network components including wireless, switching, and security. In addition, embedding security intelligence into WLAN appliances and access points (APs), regardless of architecture, reduces total cost of ownership (TCO).

Fortinet's Secure Access solution delivers three WLAN deployment options designed to meet the different WLAN requirements of today's enterprises. In addition to WLAN services, our secure access portfolio also provides the most flexible security platform with end-to-end enforcement. These options enable any organization to choose the topology and network management that best fits its needs, without having to compromise on security.

On-Premise WLAN Management

- **Integrated:** This option includes an integrated Wi-Fi controller within a FortiGate next-generation firewall. So in addition to consolidating all the functions of a network firewall, IPS, anti-malware, VPN, WAN optimization, web filtering, and application control in a single platform, the FortiGate also provides full control to connected APs, local or remote. Fortinet also offers the FortiWiFi solution where the APs themselves are integrated within the FortiGate, designed to support smaller offices. In addition to local management, our Integrated solution can also be managed via the cloud.
- **Controller:** This option combines traditional WLAN controller-based management, network applications, and a range of high-performance indoor and outdoor APs. This offers an ideal solution Continuous scanning for malware to prevent access to malicious websites, endpoint integrity checking, and controlling application usage for organizations that need a dedicated wireless network that can be separated from the underlying security infrastructure. Our Controller solution offers flexible channel deployment options to drastically reduce site survey and channel planning work while securing traffic through wireless traffic segmentation. It can also scale for different implementations— ranging from medium to large enterprises.

Cloud Managed

FortiCloud: This solution is unlike any other cloud Wi-Fi offering. Based on the FortiCloud Provisioning and Management Service and a new class of APs, the FortiAP-S series combines the elements of advanced firewall protection in the AP itself, at the network edge, to offer complete security with the simplicity and convenience of cloud management.

Conclusion

The access landscape is evolving with the unrelenting increase in the number and types of networked devices. IoT applications and the continued growth of user devices bring new and ever-changing cybersecurity threats.

Enterprise-wide network access control is an integral part of any IT strategy and implementation. Growing requirements to support new devices and device types necessitate an end-to-end wireless, wired, and security system—a solution that minimizes device deployment interoperability issues, simplifies manageability of network devices, and supports mobile applications.

A flexible, secure access architecture (such as Fortinet's Secure Access solution) provides the maximum protection that every enterprise must have.

[1] Synergy Research Group, January 2016 press release.

[2] Wi-Fi Alliance® 6 for '16 Wi-Fi® predictions, January 2016.

www.fortinet.com

485444-A-0-EN

September 18, 2019 1:00 AM

eb-wireless-defense-strategies-in-the-iot-era