
FORTINET
WIRELESS DEFENSE
STRATEGIES IN THE IoT ERA

CONTENTS

INTRODUCTION

Non-stop 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-a-service (XaaS), and artificial intelligence. Securing enterprise wireless LANs from unauthorized access and cybersecurity attacks are top of mind for enterprise IT decision-makers worldwide.

These trends have significant implications for the planning, deploying, and securing of WLANs.

Enterprises must plan with a “mobile-first” mentality. This is strategic. It presents a growing need for a robust end-to-end security architecture within the enterprise. Strategic changes are required to effectively secure 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 growth in number and types of Wi-Fi devices is still going strong. 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% of IT decision-makers worldwide indicated that BYOD access is supported. In North America alone, the number is 76%. In addition, these IT organizations are expected to have complete control of all devices.

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 game-changing applications.

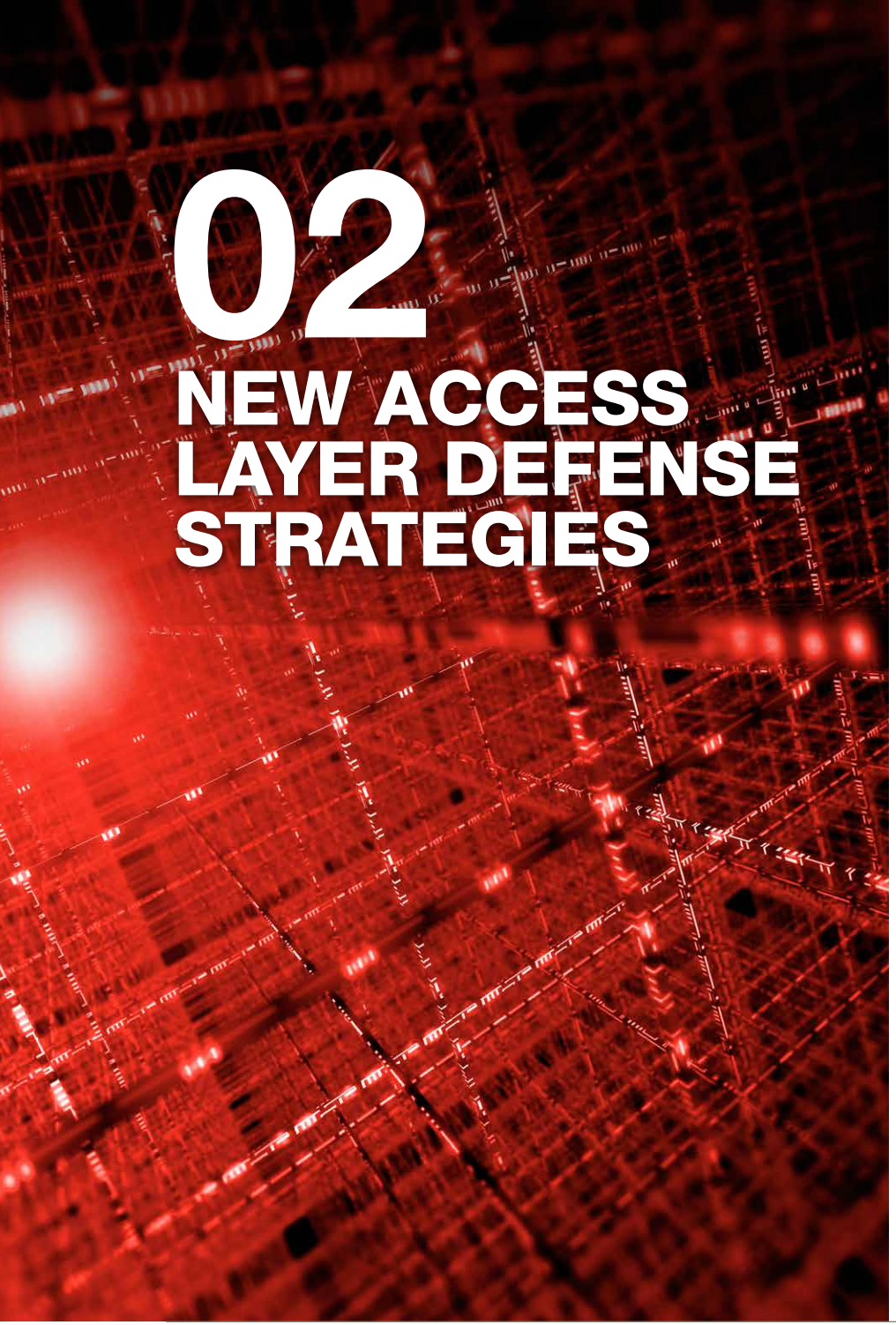
This exponential increase in a multitude of unsecured device types presents new vulnerabilities and threats. IoT is a new entry point for attack and as such presents new security challenges. Typically appliances and sensors are used for data collection and transfer. Most of these devices are open and unable to support common client-based security solutions. This puts the burden on the network to keep these devices secure.

The healthcare/pharmaceutical industry is a great example. Compared to traditional IT systems, incidents involving IoT, such as a hacked MRI machine, can carry consequences, such as policy and financial impacts. Virtually all software, applications, systems, and devices are now connected to the Internet. This is a reality that cybercriminals recognize and are actively exploiting. Some 94% of medical institutions said their organizations have been victims of a cyberattack[3]. Cybercriminals are constantly devising new ways of leveraging IoT and expanding the attack surface to carry out advanced persistent threats.

Banks and other financial institutions consider IoT-enabled ATMs, information kiosks, and credit/debit cards with sensing technology as revenue growth opportunities. As these organizations are already experiencing a huge number of cyberattacks, they face even greater risks with IoT-based services.

Rightfully so, IT decision-makers are worried about the challenges of securing IoT devices and are including them as a major component of their overall security strategy.

[1] Synergy Research Group, January 2016 press release
[2] Wi-Fi Alliance® 6 for '16 Wi-Fi® predictions, January 2016
[3] SANS Institute Health Care Cyberthreat Report 2014



02 NEW ACCESS LAYER DEFENSE STRATEGIES

Enterprise organizations need a security fabric that provides flexible end-to-end protection across their entire IT environments. With these high-profile attacks on major organizations, cybersecurity and the protection of critical company and customer data are top concerns. However, in many cases, IT organizations have yet to include key security measures such as intrusion prevention or application control, which add critically needed protections.

In Section 1, we discussed the drivers that demand a more unified access layer strategy to protect against these sophisticated attacks to assure secure communications, data, transactions, and mobile devices. This strategy 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, end-point 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.

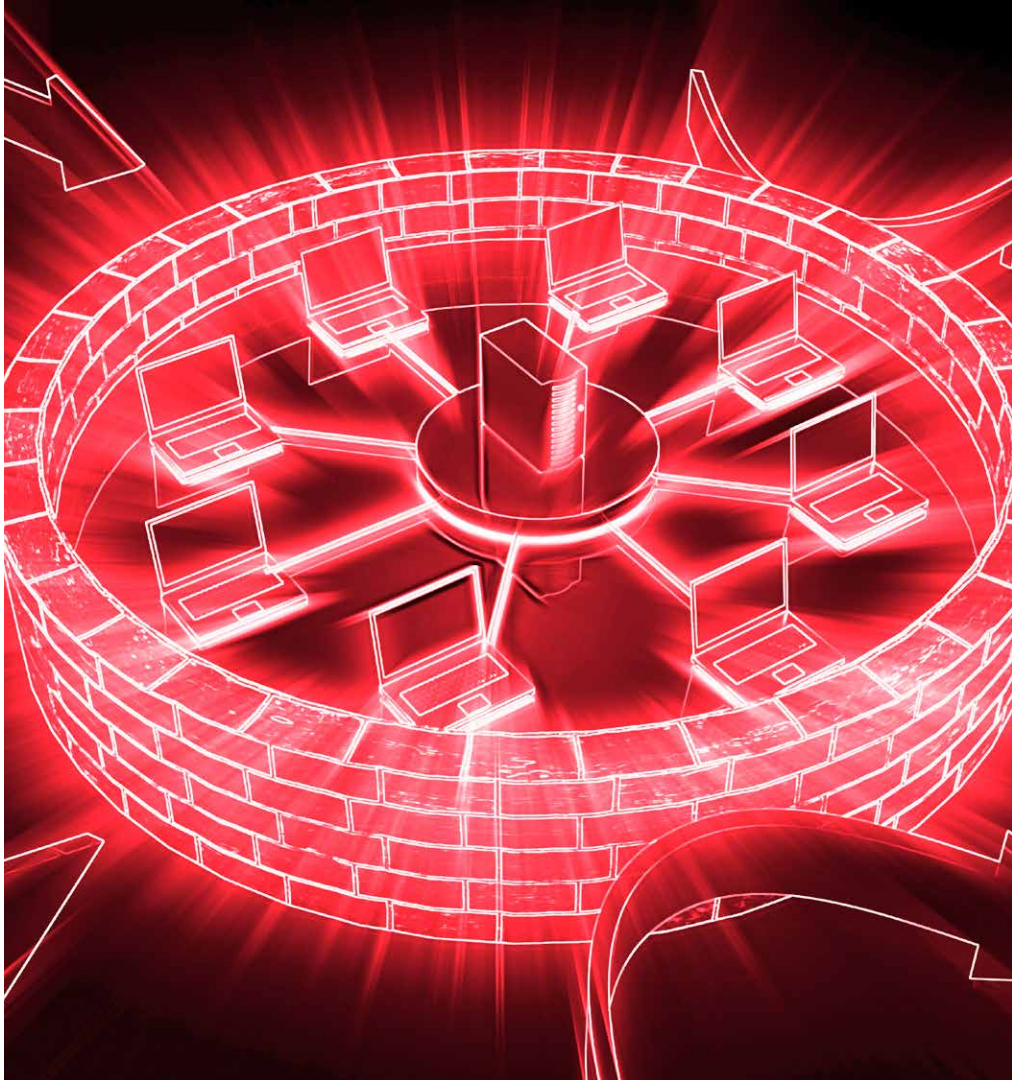
WIPs

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.

NGFW

Because threats are constantly changing and mutating, there is a strong trend towards implementing next-generation firewalls (NGFW). Now more than ever they 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

Multiple layers of defense are the best way to protect against 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 in order 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 APs, regardless of architecture, reduces total cost of ownership (TCO).

Look for the most flexible WLAN options to mix and match deployment models for different use cases, locations and IT resources. WLAN premise- or cloud-managed, controller or controllerless solutions should best suit your network and organizational structure—without giving up critical security protection. Integrated, end-to-end protection enables an overall secure, scalable and cost-effective solution.

Deployment and management of enterprise networks, applications and devices must be simplified. Even with a broad range of security measures in place, IT administrators may be uncertain about optimal configurations. Network and security implementation needs a “single-pane-of glass” view. One consistent user interface into the wired and wireless network, enabling end-to-end configuration, monitoring and management, is clearly the way to go.

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 brings the maximum protection that every enterprise must have.

Compare Fortinet's Secure Access Architecture Solution
www.fortinet.com/secureaccess