

# **SECURE ACCESS ARCHITECTURE**

**Enterprise Network Access  
with Complete Security**

Technology and market trends are rapidly changing the way enterprises deploy local area networks, connect end devices and enable business applications of every type, and this has implications for how network access security is planned, deployed and managed.

### GROWTH IN UNSECURE CONNECTED DEVICES

The number and types of network-connected wireless devices continues to grow unabated. BYOD (Bring Your Own Device) is becoming the norm, and enterprise networks have begun to move beyond connecting laptops, smartphones and tablets. Now, emerging IoT (Internet of Things) applications are bringing new device types to the enterprise in virtually every industry.

However, the exponential increase in unsecured connected devices presents new vulnerabilities and a growing attack surface for hackers to exploit. On top of the

challenges of BYOD onboarding, IoT devices such as wireless sensor nodes, location-based beacons, and other small devices pose an additional threat, since many cannot support a suite of security solutions. This puts the onus on the network to keep these devices secure.

### WIRELESS SECURITY IS A TOP CIO CONCERN

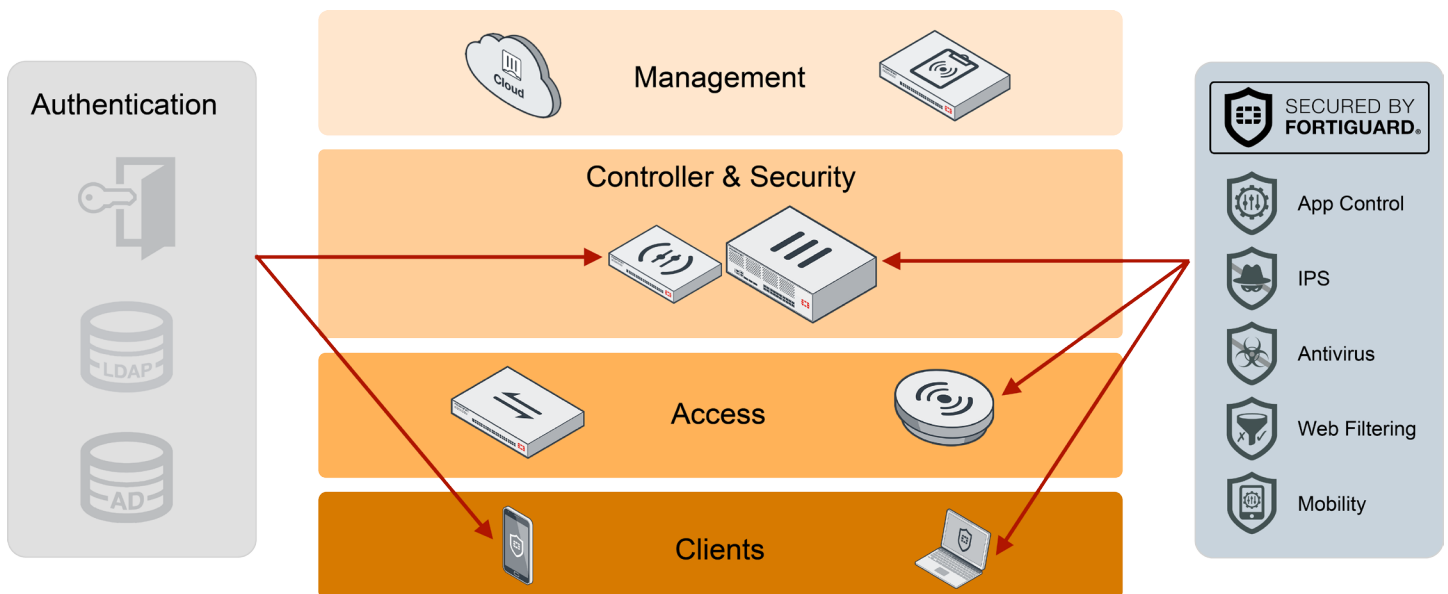
The shifting device landscape from corporate-owned to employee-owned, and users' growing reliance on the Internet, also puts device and application layer security in the limelight. Recent surveys indicate almost 50% of IT Decision Makers rate wireless LANs among the two most vulnerable areas of their IT infrastructure. Device and application proliferation go hand-in-hand. With mobile application use growing at 76% year on year, enterprises face not only support challenges from more enterprise applications, but also new vulnerabilities that stem from applications and devices never before seen on the network.

### GROWING OPERATIONAL COMPLEXITY FOR IT

On top of this unprecedented growth, users expect a more unified access experience – one that ensures consistent application and device policies across both wired and wireless environments, and across multiple devices per user.

The growing sophistication of cyberattacks is exposing the vulnerabilities in traditional flat networks. The new strategy needed to protect against sophisticated attacks is to add multiple layers of defense, including explicit internal segmentation, to break or mitigate the chain of infection.

All these changes in usage, devices and applications create an enormous challenge for IT organizations to protect the network from the ever-evolving array of threat vectors.



### SECURE ACCESS

Experience the industry's most comprehensive network access security, regardless of the size of your business, your network topology and choice of on-premise or cloud-based management.

## FORTINET SECURE ACCESS ARCHITECTURE

These trends and the challenges ahead, call for a network access architecture that is not only secure but easy to manage, to safeguard critical internal enterprise assets and users from cyberattacks.

Fortinet SAA plays a big part in the over all Fortinet Security Fabric. With Fortinet's unique approach to an inter-operative and collaborative infrastructure, SAA is able to share valuable data with the rest of the network to ensure a more comprehensive secure network. Data such as user information, BYOD, IoT, etc. can all be shared to provide a full view of your network.

This is where Fortinet's Secure Access Architecture leads the way.

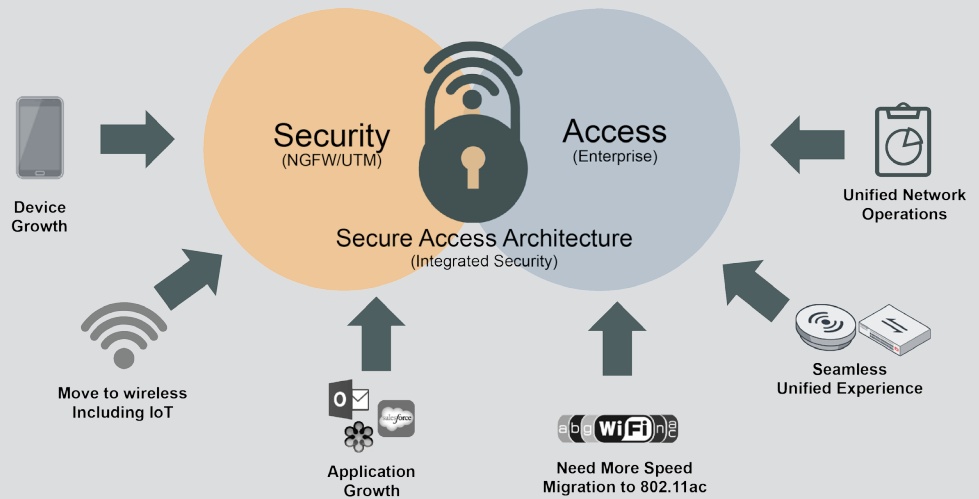


FIGURE 1: SECURE ACCESS ARCHITECTURE

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, end-point integrity checking, controlling application usage and much more.

But typical Wi-Fi solutions do not cater to these requirements. They only address connectivity and access security. Security above Layer 2 is typically provided as an overlay by a variety of security appliances. Fortinet's network access solutions are different. They include comprehensive world-class network security at their core.

Fortinet's secure access architecture ensures the same award winning security that is validated by independent certification agencies (NSS Labs, etc..) is available to every type of Wi-Fi deployment, from a stand-alone AP in an isolated office, to a

handful of APs in a retail store to thousands of APs deployed across a large enterprise campus.

To meet the diverse requirements of different use cases from large to small, on-premise versus cloud-based management, and organizational differences, different WLAN architectures and topologies have emerged. While other WLAN vendors present the same solution for every problem, Fortinet enables enterprises of any size, in any industry to choose the topology and network management that's suited for their network and organizational structure, without having to compromise on security protection.

### FORTINET SECURE ACCESS OFFERINGS

Only Fortinet has three distinctly different WLAN offerings: An Integrated wireless solution in which WLAN control and security are combined on a single high-performance

appliance; an Infrastructure wireless solution made up from best-of-breed wireless, switching and security components; and a third, Cloud wireless solution which embeds security intelligence into cloud-managed access points.

To provide the level of security equivalent to Fortinet, other vendors need a variety of different supplementary security products which add to the operational complexity and TCO (Total Cost of Ownership) of their solutions. In contrast, Fortinet's secure access portfolio offers the same comprehensive security across all three access platforms, whether on-premise or cloud-managed. This makes it easy for businesses to mix and match deployment models for different use cases, without giving up critical security protection.

## INTEGRATED WIRELESS OFFERING – UNIFIED MANAGEMENT, SUPERIOR VISIBILITY AND CONTROL

Fortinet's *Integrated* Secure Access offering is a family of thin access points, managed via an on-premise FortiGate. Recognized in both Gartner Group's Magic Quadrants for Unified Threat Management and Enterprise Firewalls, FortiGate consolidates the functions of Network Firewall, IPS, Anti-malware, VPN, WAN Optimization, Web Filtering and Application Control together with WLAN Control in a single platform. For branch office deployments FortiGate is also available with an integrated AP known as FortiWiFi.

With security, connectivity and access control, unified through a “single pane of glass”, enterprises can centrally administer consistent user, device and application policies across wired and wireless with ease. FortiGate provides unprecedented visibility and control of applications, and enables effortless BYOD onboarding.

Complete PCI-DSS and HIPAA compliance is assured, along with the industry's most comprehensive protection for all manner of wireless and Internet threats. And like other Fortinet security products, FortiGate is Secured by FortiGuard Labs, an internal security intelligence and research agency, which delivers regular signature updates, ensuring immediate protection from emerging cyberthreats.

The combination of FortiGate security and FortiAPs gives enterprises of all sizes in various industries, the scalability to deploy thousands of APs, and enable secure access for tens of thousands of clients, without the complexity of additional point security products in order to provide comprehensive world-class threat protection.

### KEY BENEFITS

- Unified management of wired, wireless and security
- Intuitive “Single pane of glass” management interface
- Comprehensive threat protection provided by a single appliance
- One-box, all-inclusive solution for remote office network
- Unmatched visibility and control of applications and utilization
- Security kept up to date through regular signature

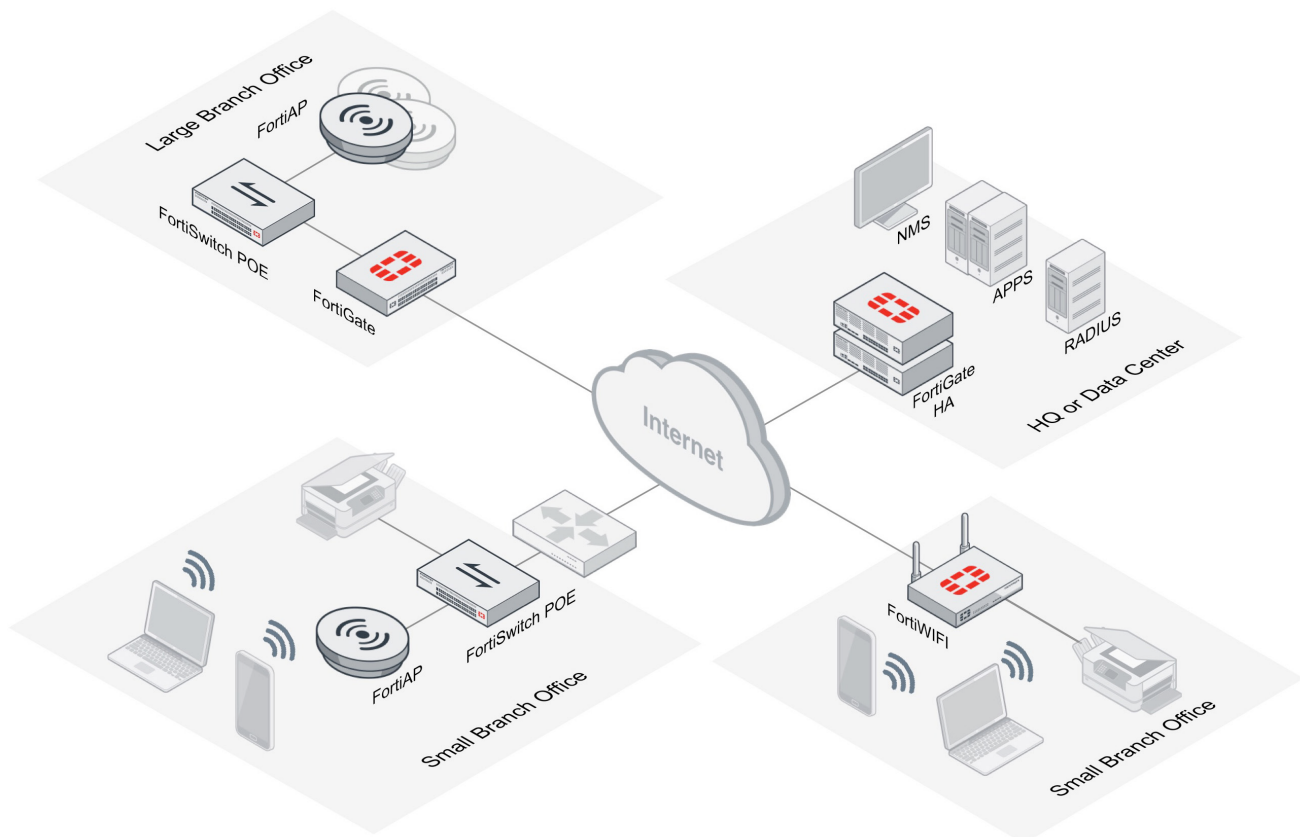


FIGURE 2: FORTINET INTEGRATED WIRELESS OFFERING

## INFRASTRUCTURE WIRELESS OFFERING – EASY DEPLOYMENT AND SCALING, UNIQUE QOE FEATURES

Fortinet's Infrastructure Secure Access offering consists of best-of-breed components for switching, WLAN and cybersecurity. This is the ideal solution when it makes sense for an organization to separate the management of network access infrastructure from the network security infrastructure.

The WLAN component provides a high-performance, premise-managed Wi-Fi network with a broad range of 802.11n and 802.11ac access points (APs). While FortiGate provides an access security overlay featuring a comprehensive portfolio of security services and granular application control, consolidated on a single, high-performance appliance.

What makes the Infrastructure wireless offering so different is its unique Wi-Fi

channel management architecture called Virtual Cell which simplifies deployment and scaling, and enables a number of compelling quality-of-experience advantages. These include superior voice mobility due to zero-handoff roaming, and more reliable user connections due to real-time load balancing based on actual traffic.

Virtual Cell minimizes the complex, time-consuming process of channel planning, which can take months for a large installation, and it makes capacity scaling easy and disruption-free, because existing access points don't need reconfiguration. Virtual Cell also enables mission critical traffic isolation on dedicated spectrum – a physical form of internal segmentation which assures optimum performance and combats sophisticated cyberattacks.

## KEY BENEFITS

- Easiest deployment and capacity scaling in the industry
- Better Quality of Experience with faster, more reliable roaming
- Superior 802.11ac performance with site-wide channel-bonding
- Bonjour multicast suppression to prevent bandwidth waste
- Comprehensive threat protection provided by one appliance
- Exceptional visibility and control of applications and utilization
- Security kept up to date through regular signature updates from FortiGuard Labs

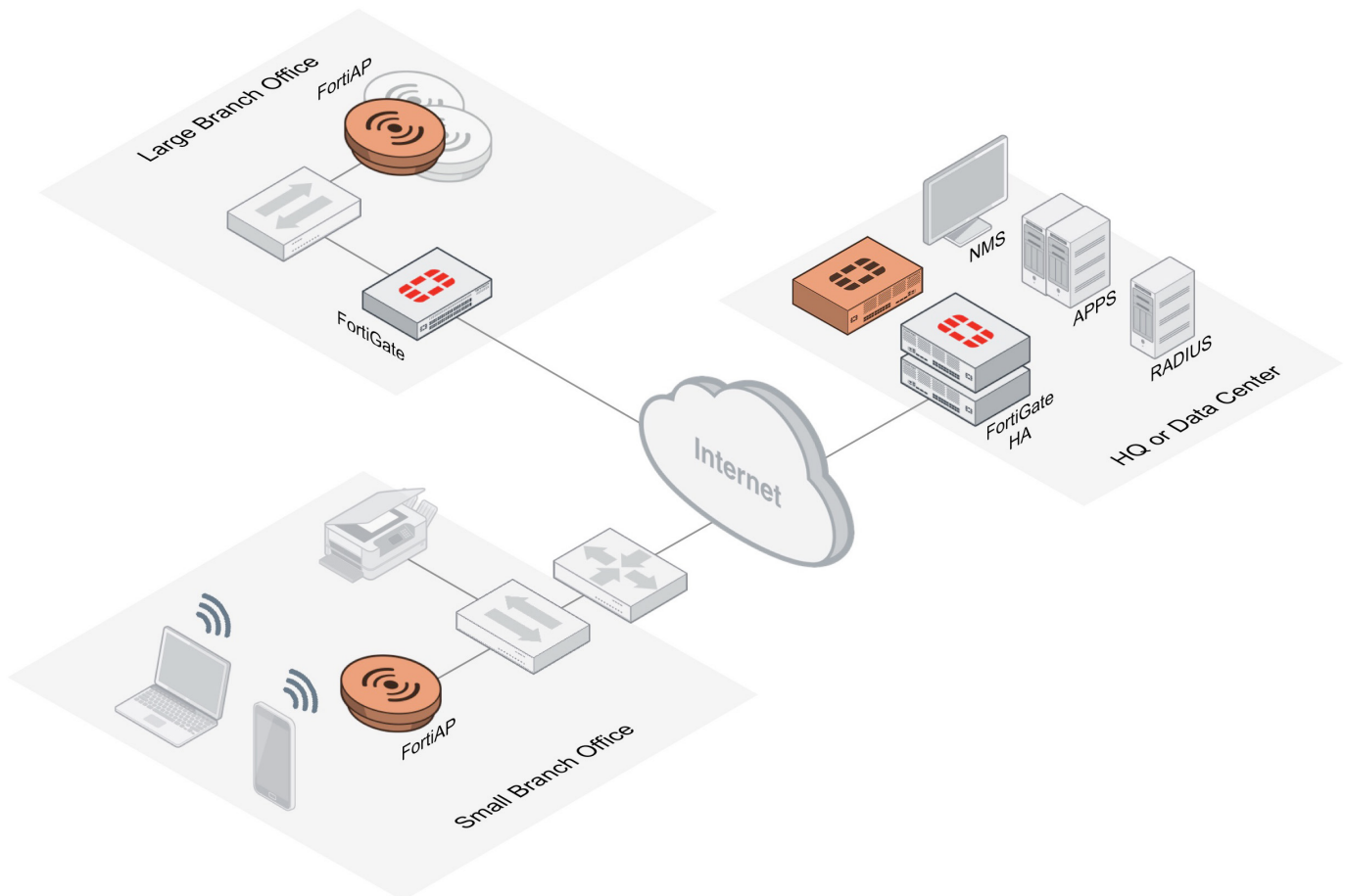


FIGURE 3: FORTINET INFRASTRUCTURE WIRELESS OFFERING

## CLOUD WIRELESS – INDUSTRY’S MOST SECURE, CONTROLLER-LESS CLOUD WI-FI

Fortinet's Cloud wireless solution is unlike any other Cloud Wi-Fi offering. Based on the FortiCloud Provisioning and Management Service, and a new class of access points, the solution combines advanced security protection at the network access edge, with the simplicity and convenience of cloud management.

Equipped with extra memory and twice the processing power of typical thin access points, the FortiAP-S series performs real-time security processing on the Access Point itself, while configuration management and reporting via FortiCloud provides complete visibility of user, device and application usage, comprehensive threat analysis, and all the identity management tools needed for BYOD onboarding and guest access through captive portals.

Combining Wi-Fi access and network security into the compact footprint of a single AP provides an exceptionally elegant and affordable WLAN solution for SMBs (Small Medium Businesses) and distributed enterprises. It lets users at small and remote sites connect to the Internet safely, without sacrificing security.

Corporate users can still be authenticated against RADIUS servers over the WAN if desired, or via user accounts provisioned in FortiCloud, while all employee and guest traffic is subjected to enterprise-class cybersecurity protection locally at the network edge. Distributed enterprises can at last implement comprehensive security at remote sites, without needing to alter the security framework at corporate, or backhaul all traffic through the corporate network.

### KEY BENEFITS

- Comprehensive cybersecurity in remote offices without the cost and complexity of WAN backhaul
- Provisioned and managed remotely through FortiCloud
- Industry's most compact Wi-Fi access with layer 7 security
- No recurring per AP licenses for full-featured cloud-management
- Layer 7 control to prioritize, block or throttle any application
- PCI-DSS compliance with rogue AP detection and mitigation
- Security kept up to date through regular signature updates from FortiGuard Labs

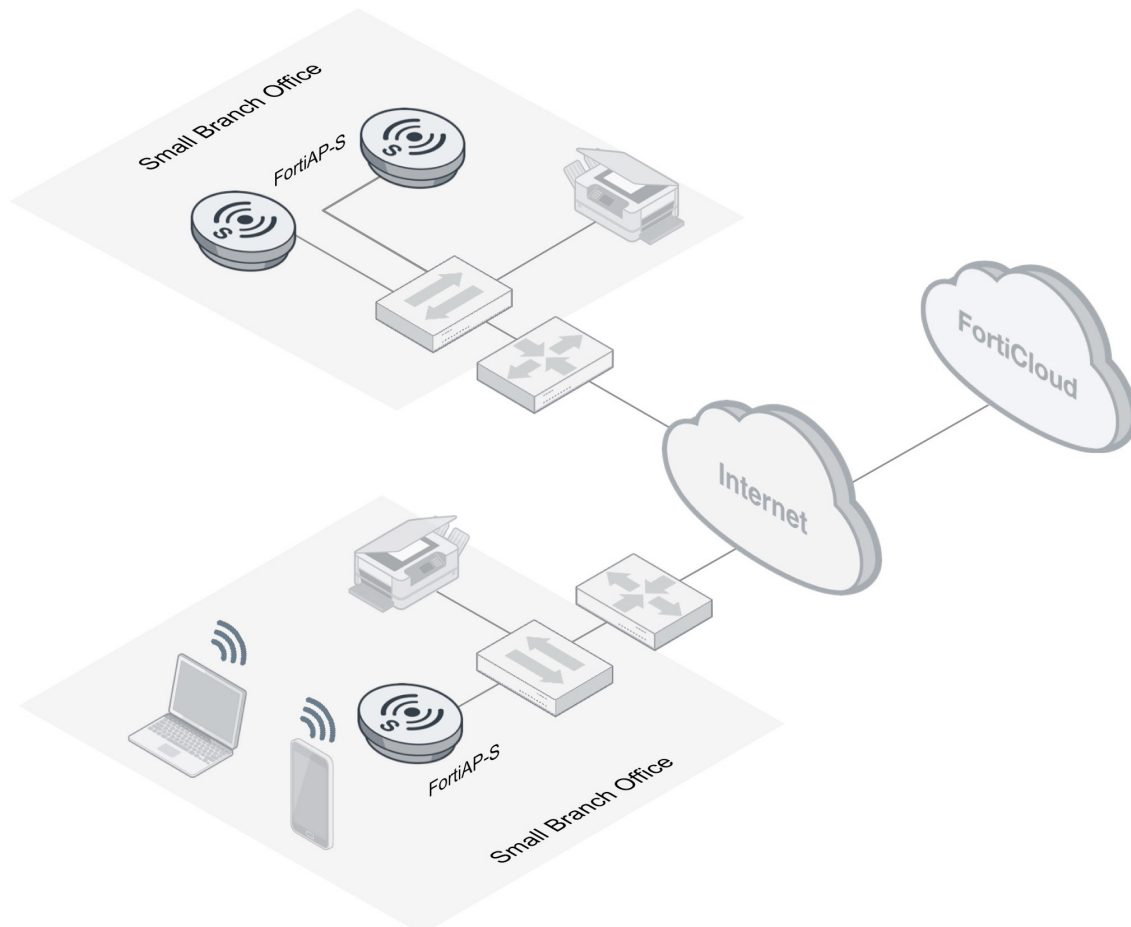


FIGURE 4: FORTINET CLOUD WIRELESS OFFERING

## FORTISWITCH – SECURE ACCESS SWITCHING

FortiSwitch Secure Access Switches are feature-rich, yet cost effective, supporting the needs of enterprise campus and branch office network connectivity. With high density 24 and 48 port models, which support 802.11at Power over Ethernet (PoE), you can power anything from access points to VoIP handsets and surveillance cameras.

FortiSwitch integrates directly into FortiGate, allowing switch administration and access port security to be managed from the same “single pane of glass”. Regardless of how users and

devices are connected to the network (wired, wireless or VPN), you have complete visibility and control over your network security and access.

FortiSwitch VLANs appear just like any other interface on a FortiGate, meaning you can apply policies to FortiSwitch ports just as you can with FortiGate “WLAN” ports. You even have visibility of per port and switch level PoE power usage. Unified control of switches through FortiGate together with security administration, simplifies remote management and troubleshooting.

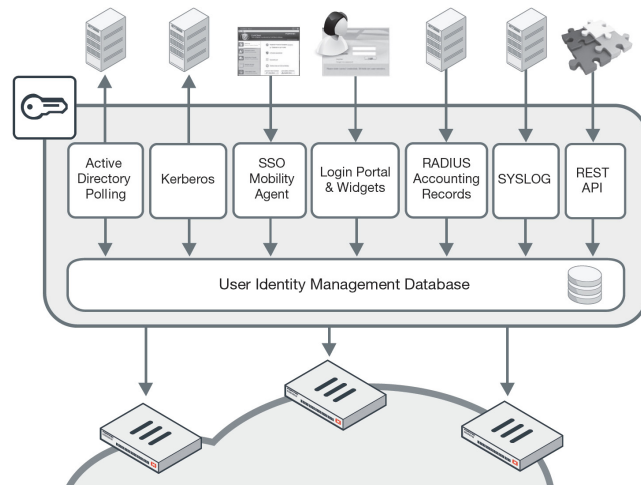


FIGURE 6: FORTIAUTHENTICATOR SINGLE SIGN-ON USER IDENTIFICATION METHODS

## INTERNAL SEGMENTATION FIREWALL – UNPRECEDENTED PERFORMANCE

Many campus networks have become flat. But as cyberattacks become more sophisticated, we now know from recent documented exploits that once hackers breach perimeter defenses, they can wreak havoc on a flat network very quickly.

Multiple layers of defense is the new standard to protect against highly sophisticated attacks that are getting past border defenses. Explicit internal segmentation, with firewall policies between users and resources, limits traffic, gives you logs and helps to break the infection chain.

But software-based firewalls designed for the perimeter are too slow. Fortinet is first to market with a purpose built Internal Segmentation Firewall (ISFW) appliance with multi-gigabit line-rate performance.

## FORTINET AUTHENTICATION – SCALABLE AUTHENTICATION ECOSYSTEM

Network and Internet access is critical for almost every role within the enterprise; however, this requirement brings with it associated risks. The key objective of every enterprise is to provide secure but controlled network access, enabling the right person the right access at the right time.

Fortinet Authentication solutions include a broad range of flexible options. With support for up to millions of users, Fortinet provides authentication solutions that span the Infrastructure, Integrated and Cloud offerings. Capabilities include single-sign, social login, and captive portal authentication options which can be integrated with internal or external RADIUS, LDAP and certificate management systems. Fortinet authentication can also be part of a complete ecosystem with third party partners for applications such as, payment gateways, booking systems, and Mobile Device Management (MDM).

Many data breaches can be traced back to compromised login credentials obtained via phishing attacks and being used as the initial intrusion vector. Two-factor

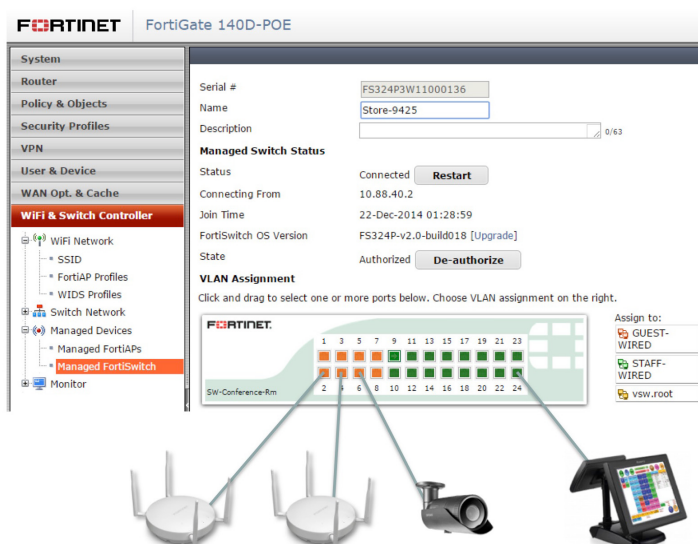


FIGURE 5: FORTIGATE SWITCH MANAGEMENT

authentication with FortiToken goes a long way in closing that loophole with standards-based secure authentication to further secure the network. Additionally, Certificate Authority functionality simplifies CA management and delivers user certificate signing, FortiGate VPN, or server x.509 certificates for use in certificate-based two-factor authentication.

## FORTINET MANAGEMENT – POLICY MANAGEMENT, ANALYTICS, REPORTING

Fortinet Management solutions support all network architecture options including physical, virtual, and public or private cloud. These solutions deliver the versatility you need to effectively manage your Fortinet-

based security infrastructure. Fortinet drastically reduces management costs, simplifies configuration, and accelerates deployment.

Key capabilities of Fortinet Management solutions include, SSID and radio policy configuration, centralized AP firmware upgrades, real-time client monitoring and deployment planning. In addition Fortinet management includes a multi-tenant portal for delivering Wi-Fi as service. Our analytics tools provide deep security and wireless analysis and reporting including usage, security logs and forensics, and industry regulatory compliance. Fortinet centralized management is the most flexible and scalable policy, analytics and reporting system.

## COMPLETELY SECURE ACCESS, NO COMPROMISES

As a global leader in network security, Fortinet provides complete and comprehensive security for the entire access network, no matter how large or small the enterprise. From campus, large office, branch office, to the corner shop, Fortinet offers the industry's most extensive network access security, regardless of the size of your business, your network topology and choice of premises or cloud-based management. The Fortinet secure access portfolio delivers the same enterprise-class security in every scenario, without compromises.

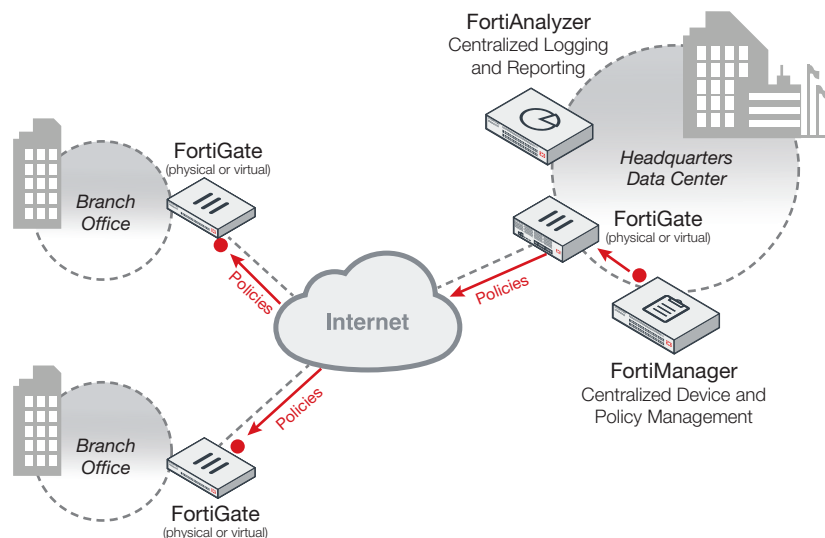


FIGURE 7: FORTIMANAGER CENTRALIZED DEVICE AND POLICY MANAGEMENT

1. Flurry Analytics – 2014 - <http://flurrymobile.tumblr.com/post/115194992530/shopping-productivity-and-messaging-give-mobile>

**FORTINET**

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