FORTINET

SOLUTION GUIDE

Secure Access Architecture

Complete Security for Network Access

Introduction

Technology and market trends are rapidly changing the way enterprise organizations deploy local area networks, connect end devices, and enable business applications of every type. But the implication of these changes and the following trends impact how networks must be secured.

Growth in Unsecure Connected Devices

The number and types of network-connected wireless devices continue to grow exponentially. Enterprise networks have moved well beyond connecting laptops, smartphones, and tablets. Emerging IoT (Internet of Things) applications are bringing new device types into enterprise networks. Gartner Group predicts 33 billion endpoints will be connected by 2020. This exponential increase in connected devices presents new vulnerabilities and a growing attack surface for hackers to exploit. IoT devices in particular (such as wireless sensor nodes, location-based beacons, and other small devices) often are not capable of supporting a suite of security solutions.

Wireless Brings Perceived Vulnerabilities

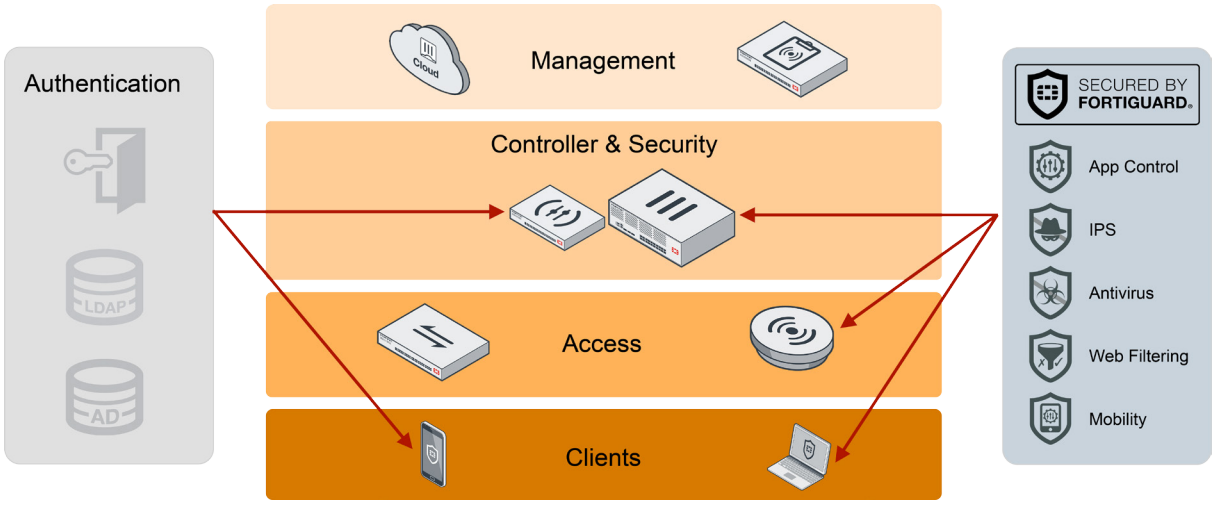
Wi-Fi is becoming the primary access medium for many of these network devices. This in turn is driving the never ending 'need-for-speed'. With the capability of delivering gigabit speeds, Infonetics forecasts that by 2019 90% of connected devices will be 802.11ac-capable. But as the device landscape shifts from corporate-owned to employee-owned, and as network usage shifts to an ever-greater reliance on wireless, the perceived vulnerabilities of devices and the wireless network is coming into question. Recent Fortinet surveys indicate strong concern from CIO and IT administrators about the vulnerabilities of their wireless access network.

Application Proliferation Enlarges Attack Surface

The growth of mobile applications goes hand-in-hand with the increased number of devices. Mobile application use shows growth of 76% year-on-year. This means enterprises are not only facing support challenges from more enterprise applications, but also new vulnerabilities that stem from applications never before seen on the network.

Operational Complexity for IT

On top of this unprecedented growth in application and device diversity, users expect a unified access experience—one that ensures consistent, secure application and device policies across both wired and wireless environments. This creates major challenges for IT organizations that are stressed to fill gaps in security if policies are inconsistently applied and not easy to manage.



Secure Access

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

Fortinet Secure Access Architecture

With these trends and challenges, the deployment and management of enterprise networks, applications and devices must be simplified. A network access layer that is not only secure but easy to manage, and continuously protected safeguards critical internal enterprise assets and users from cyberattacks.

This is where Fortinet solutions lead the way.

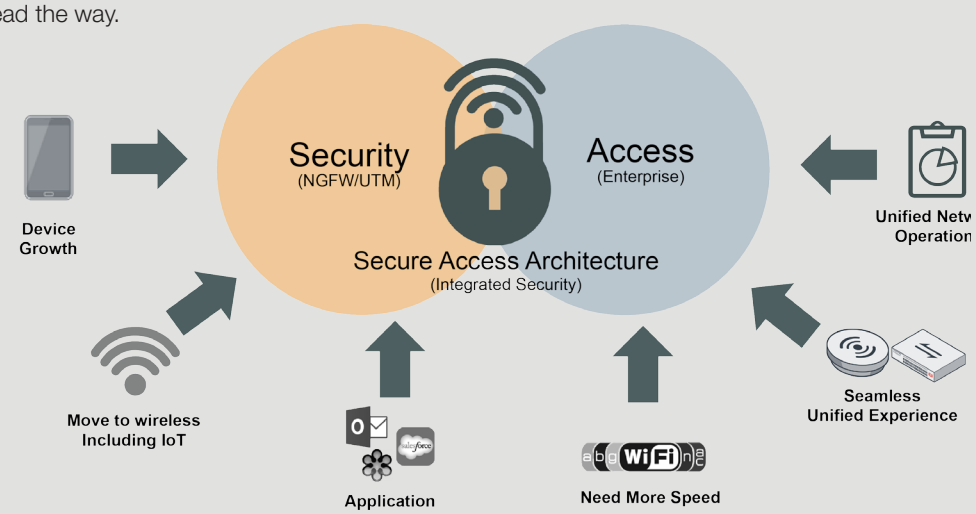


FIGURE 1
Secure Access Architecture

Fortinet networks are different. Fortinet's network access solutions offer the best of next-generation firewall capabilities together with enterprise access. As opposed to traditional wireless solutions which only address connectivity, Fortinet's secure access solutions have robust network security at their core in addition to connectivity. Fortinet secure access solutions are designed to provide the same award winning and 3rd party validated security in every type of 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. Our three product offerings enable any business to choose the topology and network management that best suits them, without having to compromise on security protection.

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 and controlling application usage. But typical Wi-Fi solutions do not cater to these requirements. Fortinet has a unique approach that addresses the shortcomings of other Wi-Fi offerings. Fortinet's secure access portfolio provides the most flexible cyber security platform with end-to-end enforcement for enterprises of all sizes and verticals of any type.

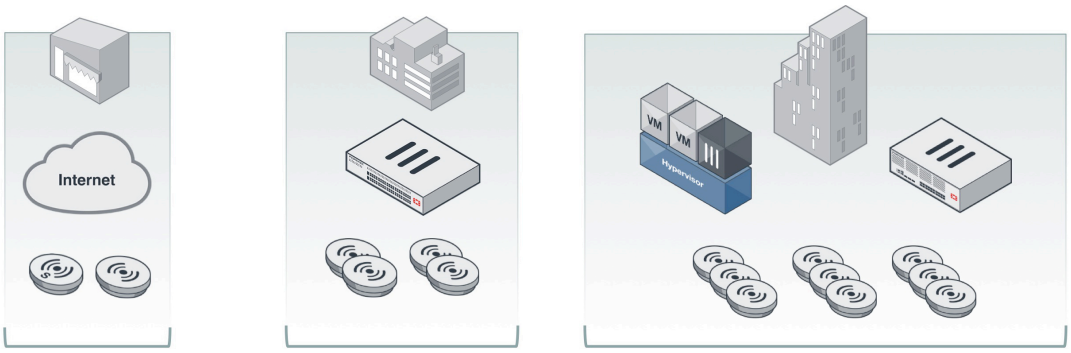


FIGURE 2
Supports Enterprises of All Sizes

Same Security on all Platforms

To provide the same levels of security as Fortinet, other vendors would need a variety of supplemental security support, depending on the product deployed. This adds to the operational complexity and TCO of their products. In contrast, the Fortinet secure portfolio offers the same comprehensive security across all our access platforms, whether controller-managed 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.

Fortinet Secure Access Offerings

With Infrastructure, Integrated, and Cloud solutions—Fortinet offers a comprehensive set of deployment options to meet the secure network needs of any size of organization in any vertical market. These three solution options are designed to extend or upgrade existing network systems. With on-site and cloud-managed solutions, Fortinet brings market-leading secure and flexible solutions.

Infrastructure Wireless Offering – Mobility, Flexibility, and Choice

The Fortinet Infrastructure offering combines on-premise controller-based management, open application appliances, and a range of high-performance indoor and outdoor APs. This offers an ideal solution when an organization needs to separate access infrastructure from the underlying network's security infrastructure. With network-controlled roaming, users benefit from the best possible mobility experience. Our Infrastructure solution offers the most flexible channel configuration and layering to simplify deployment while increasing performance, traffic segmentation, and capacity. On top of this infrastructure is the wireless industry's first open application platform to help IT build a more agile and open network. This product family scales for implementation in small, medium, and large enterprises of all types.

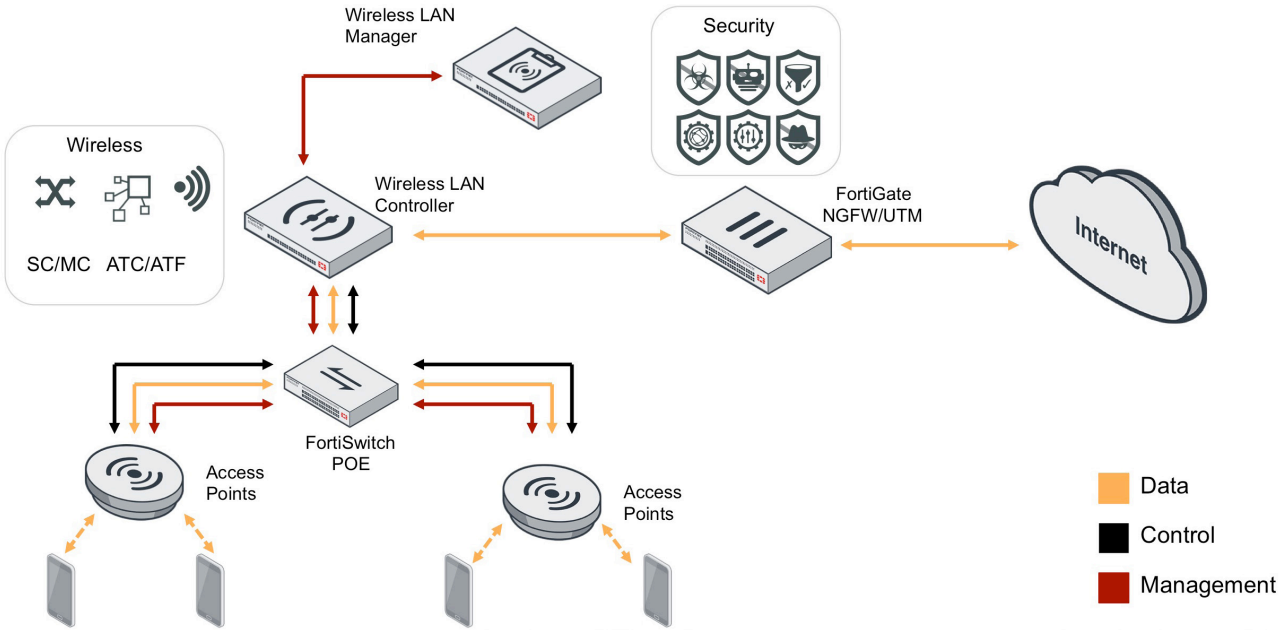


FIGURE 3
Fortinet Infrastructure Wireless Offering

Benefits include:

- **Air Traffic Control and Airtime Fairness** – The network determines optimal client roaming between access points for the best possible mobility experience in time-sensitive applications
- **Multi-Channel** - Maximizes spectrum reuse and performance
- **Virtual Cell plus Single Channel** - Simplifies deployment and seamless roaming
- **Virtual Cell plus Channel Layers** - Multiple channels segment application traffic and add capacity
- **Mobile Center** – An application platform that helps IT build a more agile and open network
- **Mobile Center Applications** – Centralizes management, automates client on-boarding, and integrates SDN applications such Skype for Business (formerly Microsoft Lync)

Integrated Wireless Offering—Integrated, Scalable, Unified Management

The Fortinet Integrated offering is a family of controller-managed APs that function in cooperation with a FortiGate. In addition to consolidating all the functions of a network Firewall, IPS, antimalware, VPN, WAN Optimization, Web Filtering, and Application Control in a single platform, **FortiGate also has an integrated Wi-Fi controller**. Fortinet APs can then be connected directly to FortiGate, providing comprehensive wireless coverage. FortiGate is also available with an integrated AP known as FortiWiFi.

Recognized in both Gartner Group's Magic Quadrants for Unified Threat Management and Enterprise Firewalls, FortiGate consolidates security, connectivity, and access control in a single platform. Regardless of access method, FortiGate applies a common security policy to all users 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. Enterprises can centrally administer security policies through a "single-pane-of-glass" management interface. Like other Fortinet security products, FortiGate is secured by FortiGuard—receiving regular signature updates to ensure continuous protection against attacks and zero-day cyber threats.

The combination of FortiGate security and FortiAPs gives enterprises of all sizes, hospitals, and schools scalability for thousands of APs and tens of thousands of clients, providing complete threat protection without the complexity of additional point security products.

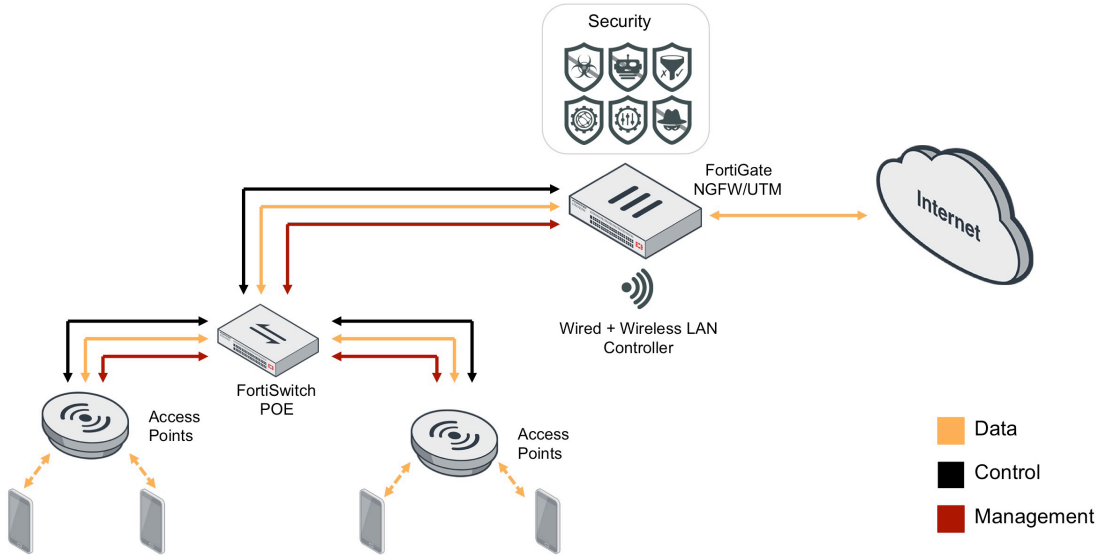


FIGURE 4
Fortinet Integrated Deployment Diagramt

Cloud Wireless – Secure, Cloud and Controller-less

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

Equipped with extra memory and twice the processing power of typical thin APs, FortiAP-S series performs real-time security processing on the AP itself. Combining Wi-Fi access and network security into the compact footprint of a single AP provides an exceptionally elegant and affordable WLAN for SMBs and an additional wireless option for distributed enterprises.

Configuration management and reporting is provided through the FortiCloud provisioning and management portal, providing comprehensive details on per-user and device application usage, bandwidth, and traffic analysis. It includes all the management tools needed for: adds, moves, and changes; user management, including BYOD onboarding; and guest access captive portal management. What's more, FortiCloud is completely free. There is no recurring management license per AP.

Complete Security at the Network Edge

The FortiAP-S Series enables distributed enterprise sites to connect to the Internet safely, without sacrificing security. Corporate users can still be authenticated against RADIUS servers over the WAN if desired, or via FortiCloud. All traffic from employees or guests is protected by enterprise-class layer 7 security directly at the AP, without squandering WAN bandwidth.

The FortiAP-S series allows distributed enterprises to benefit from superior security at all remote sites, without altering their existing security infrastructure at corporate or backhauling traffic through the corporate network.

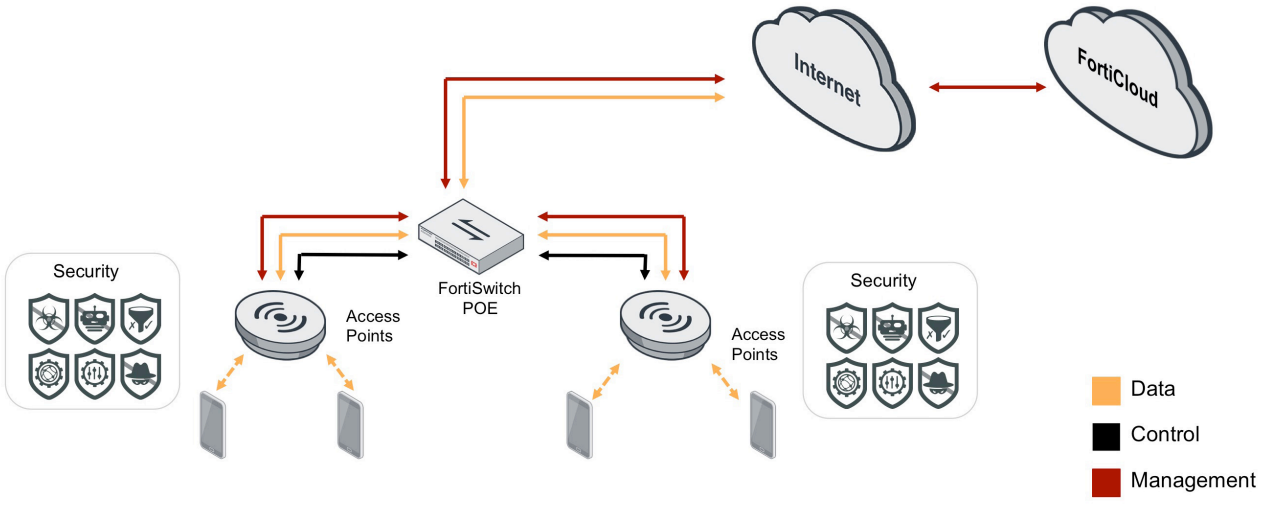


FIGURE 5
Fortinet Cloud Wireless Offering

FortiSwitch – Secure Access Switching

FortiSwitch Ethernet Access and Data Center Switches are feature-rich yet cost effective—supporting the needs of enterprise campus and branch offices, as well as data center environments. The FortiSwitch product series integrates directly into the FortiGate with switch administration and access port security managed from the FortiGate interface. Regardless of how users and devices are connected to the network, users have complete visibility and control over network security and access—perfectly suited to threat-conscious organizations of any size.

Virtualization and cloud computing have created dense, high-bandwidth Ethernet networking requirements in the data center, pushing the limits of existing data center switching. FortiSwitch Data Center switches meet these challenges by providing a high-performance switching platform with a low TCO. Ideal for top-of-rack server or firewall aggregation applications (as well as enterprise network core or distribution deployments), these switches are purpose-built to meet the needs of bandwidth-intensive environments.

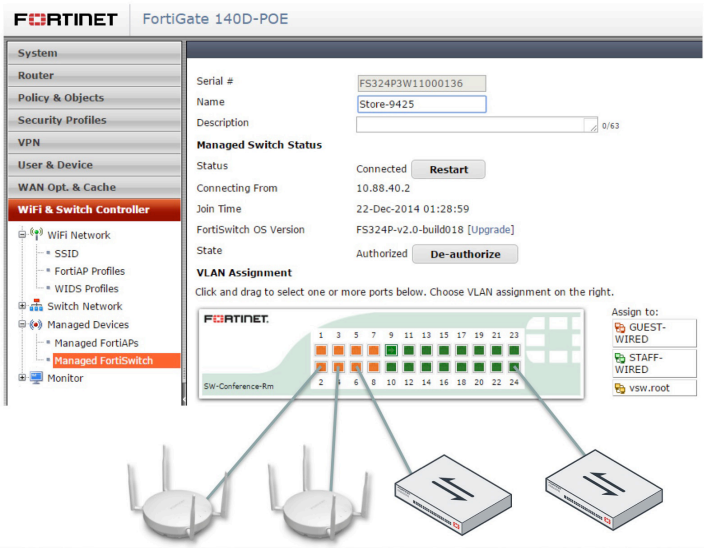


FIGURE 6
FortiGate Switch Management

Fortinet Authentication – Secure, Scalable Ecosystem

Network and Internet access is key for almost every role within the enterprise; however, this requirement must be balanced with the risk that it brings. The main objective of every enterprise is to provide secure but controlled network access—enabling the right person the right access at the right time, without compromising on security.

Fortinet Authentication solutions include a broad range of flexible options. With support for up to millions of users, Fortinet provides authentication solutions for Infrastructure, Integrated, and Cloud offerings. Capabilities include single-sign-on and captive portal login options. Fortinet provides authentication solutions across wireless and wired networks with public and private systems. We enable integration with RADIUS, LDAP, and certification management. Fortinet Authentication solutions work as part of a complete ecosystem with third-party partners for applications such as social login, payment gateways, Property Management Systems (PMS), and Mobile Device Management (MDM).

Most data breaches can be traced back to login credentials stolen via phishing attacks as the initial intrusion vector. Two-factor authentication goes a long way in closing that loophole, with standards-based secure authentication that works in conjunction with FortiTokens to 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.

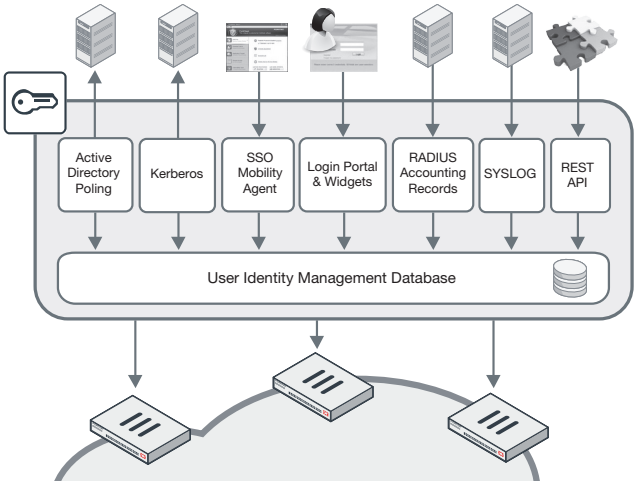


FIGURE 5
FortiAuthenticator Single Sign-On User Identification Methods

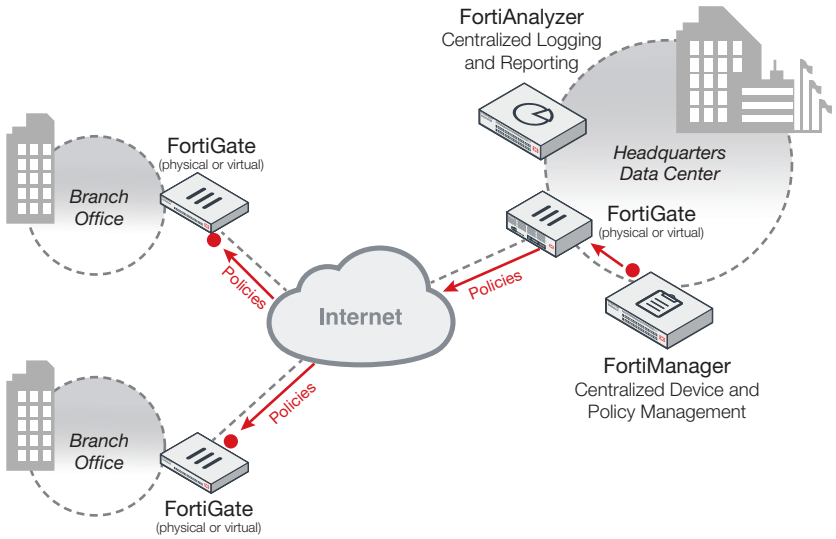
Fortinet Management – Policy Management, Analytics, Reporting

Fortinet Management solutions support all network architecture options—including physical, virtual, and public/private cloud. These solutions deliver the versatility needed to effectively manage a Fortinet-based security infrastructure. Fortinet drastically reduces management costs, simplifies configuration, and accelerates deployment cycles.

FortiManager provides crucial timesaving features like device auto-discovery, group management, global policies, auditing facilities, and the ability to manage complex VPN environments.

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 a service. Our analytics tools provide deep security, wireless analysis, and reporting—including usage, security logs/forensics, and PCI compliance. Fortinet centralized management provides the most flexible and scalable policy, analytics, and reporting system.

FIGURE 6
FortiManager Centralized Device and Policy Management



Complete Secure Access, No Compromises

As a global leader in network security, Fortinet provides complete and comprehensive security for the entire access network. From campuses, to large offices, to branch offices, to the corner shop—Fortinet offers the industry's most extensive network access security, regardless of business size, network topology, or choice of controller versus cloud-based management. Fortinet's secure access portfolio delivers the same enterprise-class security in every scenario, without compromises.

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

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

October 9, 2015