Cloud Secure Access Deployment Guide

Secure Cloud-managed Wireless LAN Solution

Overview

Distributed enterprises, dissatisfied with the cost and complexity of traditional controller-based enterprise WLAN solutions, are turning to cloud-managed Wi-Fi as a more practical alternative. But most cloud Wi-Fi solutions fall short on content and application security, leaving businesses vulnerable to cyberthreats. Fortinet's *Cloud* Secure Access solution addresses this shortcoming completely.

Cloud Wi-Fi Evolution

Distributed enterprises such as retail, hospitality, health clinics and managed care facilities have historically been poorly served by enterprise WLAN vendors. Traditional controller-based solutions are generally too complex and too expensive for small businesses or those with multiple sites requiring only a few APs each.

To address this growing market, enterprise WLAN vendors have ported their management and controllers to the cloud, simplifying management and reducing CAPEX. With a cloud-managed Wi-Fi architecture, customers now only need to buy and configure APs, not controllers or management servers.

But, the apparent simplicity of cloud-management does not come without compromises. Security beyond standard Wi-Fi access control is invariably lacking. In large enterprises, content and application security is normally provided through specialized security appliances for IPS, web filtering, antivirus and so on. But in most cloud Wi-Fi solutions these functions are absent. The result is cloud-managed Wi-Fi that is inherently not as secure as controller-managed Wi-Fi.

Secure Access Architecture

Fortinet's Secure Access Architecture offers the best of next-generation firewall capabilities together with enterprise access. 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.

Beyond Wi-Fi Security

Today's Wi-Fi authentication and encryption standards (WPA2, 802.1X, etc.) are generally accepted as robust Wi-Fi access control mechanisms. Why does anyone need more security than that? Well, the threat landscape has moved up the stack, and it is constantly evolving. Our growing dependence on the Internet and cloud services, along with BYOD, has resulted in exponential growth in potential threat vectors and targets.

Threats enter your network through common applications like email, web browsers and social networking tools, as well as seemingly innocent apps and games on the mobile devices belonging to your staff, or customers. Worms and viruses on an infected mobile device can infect other Wi-Fi attached devices, even without either of them accessing the Internet.

Securing business communications, personal information, financial transactions, and the mobile devices of your users involves much more than Wi-Fi access control. It requires scanning for malware, preventing access to malicious websites and controlling application usage. But typical cloud Wi-Fi solutions do not cater to these requirements. Fortinet's novel approach completely addresses this shortcoming in existing cloud Wi-Fi offerings.

Fortinet Secure Access Architecture

There is no one-size-fits all WLAN solution - different use cases favor different deployment models. Fortinet's Secure Access Architecture ensures enterprises of any size, in any industry can choose the topology and network management that best suited to their network and organizational structure, and enjoy the same world-class cybersecurity in every scenario.

The Cloud Secure Access solution, which is recommended for SMBs and distributed enterprises, is just one of three distinctly different WLAN offerings designed to give enterprises complete flexibility over their preferred deployment model, without compromising security.

Cloud Secure Access Solution

Fortinet's *Cloud* Secure Access 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 FortiAP-S series offers the same network security capabilities typically found only in controller-managed enterprise WLAN solutions combined with supplementary security services.

Normally, if you want to apply comprehensive security for all types of traffic from access points in remote offices, you need to tunnel traffic through centralized security devices on the corporate LAN, and often hairpin it back to where it came from. All this adds latency and burns the capacity of your network links, forcing premature, costly upgrades.

Doing this is not only complicated, it also masks your visibility of client and user behavior, as it requires entire VLANs, not unique sessions, to be mapped from one security appliance to the next, to process security in multiple passes through different devices. It is highly inefficient.

Distributed enterprises in hospitality, retail and healthcare which have large numbers of guests, would rather not be tunneling video, gaming and other high-bandwidth traffic from their guests through the corporate network. But if they want to control application usage, such as preventing a guest from watching inappropriate content in their coffee shop, or if they want to fully protect devices from cyberthreats, they've had no alternative, until now.

Many vendors' controller based WLAN solutions, including Fortinet's own solutions, allow split routing at remote offices, whereby corporate traffic is tunneled over the WAN to undergo security processing at the head office or data center, while Internet traffic goes directly to the Internet. But this Internet traffic is no longer protected by corporate IPS, antivirus and web-filtering appliances.

Alternatively, all traffic from authenticated corporate users may be tunneled through the WAN, while only guest traffic goes directly to the Internet. In this case, only guest traffic is unprotected and uncontrolled. Still, neither approach is ideal.

With the FortiAP-S series, all traffic from any type of user can be protected and controlled regardless of whether it is corporate or Internet traffic, without tunneling everything through the corporate WAN. Not only is this efficient and cost-effective, it is also the most secure and least complex of all options.

What makes the FortiAP-S series access points so special is they contain advanced security functions embedded in the AP hardware. This new class of AP is equipped with extra memory and twice the processing power of typical thin APs, which enables them to perform real-time security processing at the network access edge, not in the cloud or on the corporate LAN. Processing L2-L7 security at the AP in one pass is efficient. Plus, it allows exceptionally granular user and device policies and preserves complete visibility of session-level behavior.

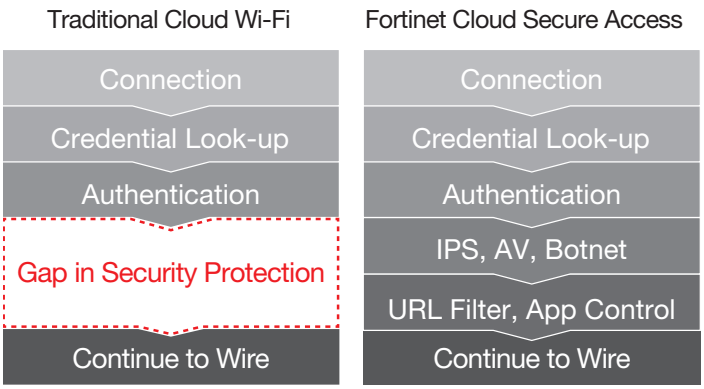

Figure 1. Fortinet Cloud Wi-Fi and Application Security Enforcement

FortiCloud Provisioning and Management

FortiCloud is a cloud-based provisioning, configuration management and analytics service for FortiGate, FortiWiFi, FortiAP and FortiAP-S series product lines. It lets you quickly initialize and then maintain centralized control and visibility of your wireless network all from the cloud, avoiding the cost of WLAN controller and management gear.

Hosted by Fortinet, it gives businesses a single dashboard for managing the infrastructure and security for the entire network, and offers unlimited network scalability with all the benefits of centralized management.

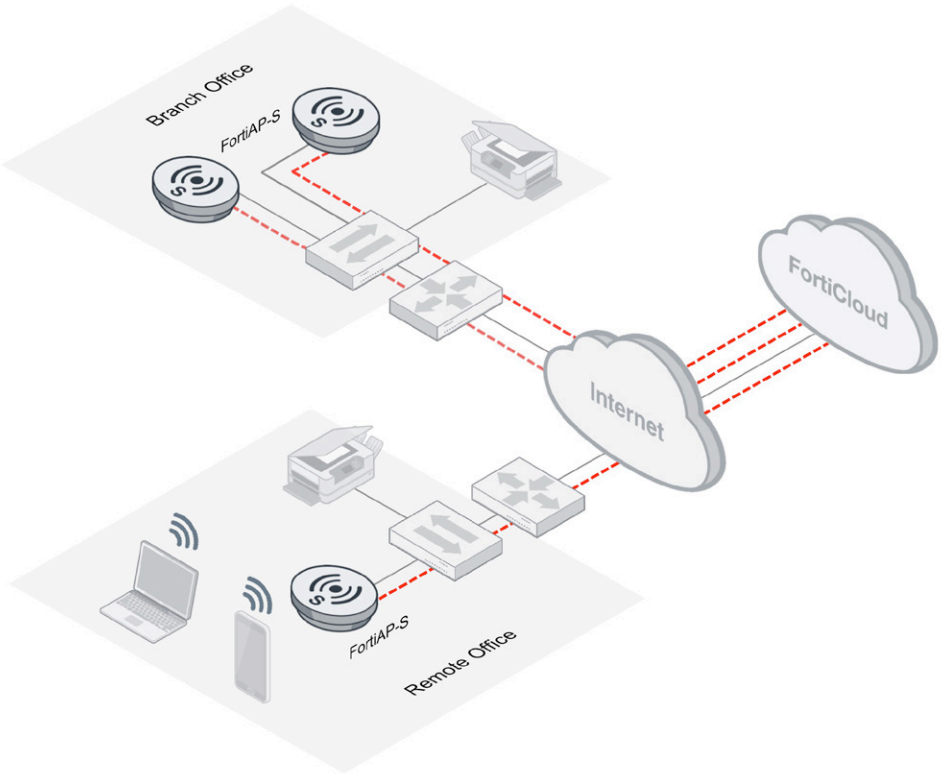

Figure 2: Secure Remote Offices with FortiAP-S Series

FortiCloud simplifies provisioning of access points and other Fortinet security devices at remote sites where there is no on-site IT expertise. FortiAP-S series access points include FortiCloud registration functionality in their firmware, which enables zero-touch provisioning. When installed, the APs will discover and connect to FortiCloud and provision themselves, automatically.

From rogue AP detection to guest access management to application usage reporting and threat analysis, FortiCloud gives you everything you need to manage the Wi-Fi access points and the complete security landscape at any remote location, while maintaining full visibility of wireless health and the quality of experience for clients.

FortiCloud Highlights

Fast Centralized Provisioning: You can deploy new APs remotely with no on-site expertise, anywhere in the world. Single and bulk configuration options in FortiCloud let you identify the serial number of APs that belong to your business. As each AP powers on for the first time, it registers with FortiCloud and automatically downloads the latest firmware and default profiles for your network. Within minutes the AP reboots and is fully operational. Once it is activated, easy-to-use provisioning lets you assign custom profiles to any AP, or push common profiles to multiple APs simultaneously.

FortiPresence Analytics: FortiPresence analytics is supported on FortiCloud that delivers a real-time location based analytics experience to customers. Configuration is applied on FortiCloud dashboard and statistics are received via an API push from each AP. FortiPresence analytics include functionality to determine in real time location metrics around total visitor traffic, visitor dwell time and heat maps with animated flows. It provides retailers with the tools they need to better understand and influence consumer shopping behavior.

Robust Authentication: FortiCloud supports authentication using 802.11i with either pre-shared keys or 802.1X. When 802.1X is enabled, users can be authenticated against the user database hosted in FortiCloud, or against a RADIUS server on the corporate network.

Roaming between Access Points: FortiCloud enables fast roaming between AP's on your network. With 802.11i Pre Authentication protocol, there is no need to re-authenticate clients when moving across AP's. This provides users with a seamless roaming experience; not having to stop and wait while the client reassociates with another access point and gets the proper security credentials.

Role / Identity-based Access: Role-based access control lets IT staff configure separate access profiles for different groups within an organization (e.g. faculty, students and guests or medical staff, admins and patients). Different policies can be assigned to different groups, allowing you to segment users or client devices based on unique business and compliance needs.

Guest Access Captive Portal: Many distributed enterprises need to provide secure Internet access for guests and visitors. FortiCloud allows businesses to associate any number of SSIDs with a fully customized captive portal, and to operate multiple branded captive portals simultaneously if needed. Guests connect to a seemingly open SSID, but the AP responds to the client's first HTTP request with a web page requesting user name and password.

FortiCloud also provides Social Media Captive portal. Visitors can easily connect to Guest Wi-Fi by checking into their Facebook, LinkedIn or Twitter accounts. Social media login greatly simplifies on boarding of guests. There is no need to generate codes or temporary login passwords.

Health and Utilization Analytics: The FortiCloud dashboard provides visibility and control of the health of the wireless network. FortiAP-S series APs may be positioned on a global map, with the ability to drill down to AP status, performance information and connected client statistics. FortiCloud also provides complete Layer 7 application visibility, with detailed information on the applications being used and by whom, bandwidth consumption by AP, client or application, and much more.

FortiCloud analytics includes granular drill-down and filtering functionality to instantly determine how applications, websites, users and threats are impacting your network. To aid you in management and compliance reporting, detailed preconfigured and custom reports are available, including specialized PCI-DSS compliance reports. They can be run on-demand or scheduled for certain times and distributed by email to interested parties.

Application Visibility and Control: Unlike other vendors' cloud Wi-Fi solutions, which can only classify up to a few hundred applications at best, FortiCloud has application signatures for over 3,300 distinct applications. It can distinguish between Netflix, Vimeo, YouTube, YouTube HD, etc., and between Skype, SIP, H.323, etc. The application control settings are configured in the cloud and then downloaded to FortiAP-S series access points for real-time local enforcement.

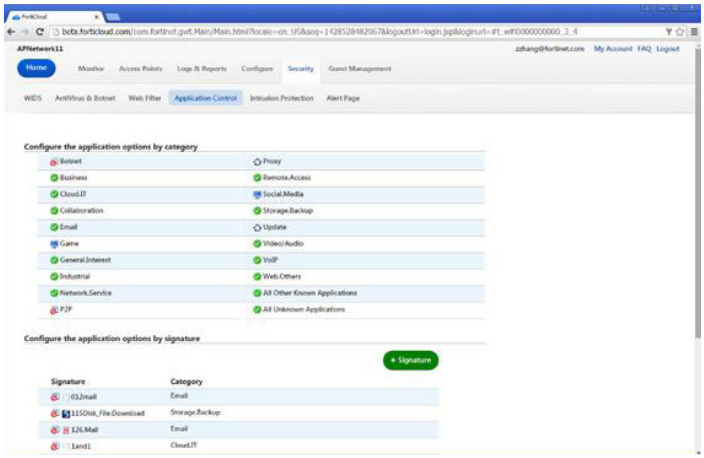

Figure 3: Category-based Application Control

Enhanced AP configuration: FortiCloud allows you to choose the subnet you wish to use when the AP joins the network. You can now get the latest FortiAP-S software through FortiGuard services linked to your FortiCloud.

FortiAP-S Series Access Points

The FortiAP-S series provides secure indoor wireless access with a range of single and dual-radio 3x3 MIMO 802.11ac APs. Some models are equipped with internal antennas, while others support external antennas to provide flexible directional and long-range coverage for both indoors, and outdoors.

Figure 4. FortiAP-S Series access points with internal or external antennas

As with other Fortinet AP product lines, zero-touch deployment enables rapid provisioning. While all enterprise features such as roaming, bridging support, guest access, WIDS and rogue AP suppression, air monitor, WMM and QoS and WAN failure survivability are supported as standard, without additional feature licenses.

Where FortiAP-S series APs differ from other Fortinet AP product lines, and conventional thin APs from other WLAN vendors, is how they handle real-time content and application security. Once configured and operational, they download the latest threat, exploit and application signatures from FortiGuard Labs to memory on the AP hardware itself, and can immediately enforce web filtering and application controls and offer protection against network intrusions, viruses and a host of other cyberthreats. The added processing capacity at the AP ensures deep security processing can take place, without impacting throughput or latency.

By enforcing network security at the network access edge, rather than in the cloud, FortiAP-S series APs can instantaneously thwart threats originating on infected client devices, such as botnets, worms and other malicious activities, from zombie computers before they even reach the Internet. This not only conserves precious Internet bandwidth for real work, it eliminates any risk of your IP address getting blacklisted and protects all the other devices in your network.

FortiAP-S Series Highlights

Zero-touch Provisioning: When powered on for the first time, FortiAP-S series APs use a robust discovery mechanism based on serial numbers, which results in them being automatically assigned to your account. Once connected, they download the latest firmware and their assigned radio profiles, then automatically select the best channel and power settings for the prevailing RF conditions.

WAN Failure Survivability: In the event of a WAN outage, the FortiAP-S series continues to provide connectivity and threat protection for all authenticated clients, even for clients roaming back to an AP after temporarily being connected to another AP. Each AP already has user state information and threat signatures, etc, stored in memory, so it has everything it needs to continue performing IPS, application control and antivirus scanning.

Air Monitor: All FortiAP-S series models can perform channel scanning as an air monitor. In PCI compliance applications, dual-radio APs can be used to provide both client access and monitoring simultaneously.

WIDS and Rogue AP Suppression: FortiAP-S series APs can provide continuous monitoring for rogue APs and possible wireless intrusion events, and report suspicious behavior to FortiCloud, which generates appropriate alerting and reports for network managers. The rogue AP list shows MAC address, manufacturer, security profile, speed and last seen time, enabling administrators to rapidly classify trusted or untrusted APs and take corrective action to locate and remove rogues.

Easy Policy Assignment: Each configured SSID is treated as a virtual network interface that can undergo IPS checks, A/V scanning, web filtering and application control as needed. This allows security policies to be applied easily, whether a single set of policies applies to all SSIDs or unique policies apply separately to each SSID.

IPS: Fortinet Intrusion Prevention System (IPS) technology embedded in the FortiAP-S series APs protects the network from both known and unknown threats, blocking attacks that take advantage of device and network vulnerabilities, and unpatched systems. IPS protects client devices, local servers and critical business applications in the cloud from attacks.

Anti-malware: Exploiting its powerful processor for Layer 7 deep packet inspection, the FortiAP-S series AP provides real-time protection against viruses, botnets, web exploits, Trojans and other malicious software variants, while regular updates from FortiGuard Labs ensure immediate protection against newly discovered zero-day vulnerabilities.

Web URL Filtering: The AP can block access to any known harmful websites that may contain phishing/pharming attacks or malware. Beyond reducing exposure to malware, this can also be used to control access to age inappropriate content in schools, or to prevent viewing of potentially objectionable content in public areas in hospitality, retail and healthcare settings. It can also be used to limit time-wasting personal use of devices in the workplace.

Application Control: With signatures for over 4000 applications, FortiAP-S series APs offer unrivalled control over application priority and bandwidth management. They can distinguish unique applications and treat each one differently. This goes far beyond the scope of crude Wi-Fi priority classes. When bandwidth is scarce, you can ensure mission-critical applications prevail, while lower- priority applications are throttled.

Complete Security, Exceptional Value

Aside from simplified deployment and management, one of the value propositions of cloud Wi-Fi is the shift from CAPEX to OPEX. While this might seem attractive, some vendors are gouging 15%-20% of the AP hardware price as an annual cloud-management subscription fee for each managed AP. That's a high premium to pay for management services that don't change substantially from year to year.

In contrast, cloud management through FortiCloud is free. There are no per-AP subscription fees for management at all. Fortinet only charges per-AP subscriptions for the real-time application security capabilities provided through regular updates from FortiGuard Labs – a capability that no other vendor offers.

So, for roughly the same overall OPEX Fortinet's *Cloud* Secure Access solution delivers world-class security, without any CAPEX investment in security appliances, with no latency penalties and no WAN upgrade costs. No matter what happens out there in cyberspace, or to guest-and employee-owned devices connected to your network, you have up-to-date protection against the very latest cyberthreats. No other vendor delivers this value.

Cloud Secure Access Deployment

Fortinet's secure cloud-managed Wi-Fi is suitable for single office SMBs all the way to large distributed enterprises with thousands of locations, and it is especially attractive in small locations, where oftentimes there simply is no physical space for additional local security appliances, regardless whether such an option would be economically viable. With Wi-Fi access and security combined in the footprint of a single AP, there is no secure wireless solution, more compact. Here are some common deployment scenarios and use cases for some of the FortiAP-S series security capabilities in different industries:

Hospitality: Hoteliers want to monetize Wi-Fi and other high-margin services while ensuring their patrons have an all-round pleasant experience on or off the Internet!

In order to maximize revenue from video entertainment in rooms, they can use web filtering or application control features to block access to OTT video services such as Netflix, and preserve capacity on their Internet connection for vital applications such as email for business guests. Similarly, they can restrict Internet access in the lobby, to drive Internet access sign-up in rooms, and to prevent age-inappropriate content from being viewed in public areas, while permitting it in the privacy of one's room.

In recent years, hotels have endured backlash against blocking of personal Wi-Fi hotspots, which resulted in the 2014 FCC ruling and January 2015 advisory that Wi-Fi blocking is prohibited. This leaves hospitality with a fine line to tread between FCC compliance and protection from rogue APs and malicious use. Fortinet's *Cloud* Secure Access solution provides the rogue AP information, threat protection and threat analysis to enable businesses to thwart malicious use, while remaining FCC compliant and auditable.

K-12 Education: School districts continually struggle with insufficient funds and a shortage of IT resources. Computers are few, Internet pipes are small and network infrastructure is limited. One way to alleviate the funding dilemma is to spend less on

computers and more on infrastructure by encouraging BYOD. Yet this is a double-edged sword, as it increases the security risks, and opportunity for network abuse by students. Furthermore, they have a moral if not legal obligation to protect students from age-inappropriate content.

Fortinet's *Cloud* Secure Access provides an elegant solution to meet all of these requirements in one fell swoop: It frees up capital expense from security appliances, WLAN controllers and management for more APs. It allows blocking of inappropriate or malicious sites, neutralizes infected devices and protects the network from all cyberthreats. All while conserving precious Internet bandwidth and even more precious IT staff resources through centralized management.

Retail, Restaurants and QSR: Stores and restaurants don't want to discourage patrons from using their mobile devices. They'd rather encourage usage so they can collect consumer analytics and opt-ins, which they can use for online and offline marketing. All vendors provide a branded captive portal to enable secure access and keep guests segregated from mobile point of sale (mPOS), store operations and back-office traffic, while also capturing visitor opt-ins.

However, a captive portal alone does not provide the required protection for PCI DSS compliance, and it offers no bandwidth protection for mission-critical POS transactions. Fortinet's *Cloud* Secure Access solution goes far beyond captive portals and minimum PCI DSS compliance requirements such as scanning for and mitigating rogue APs.

It provides complete protection from any type of virus or cyberthreat, which could potentially compromise mPOS terminals and Wi-Fi enabled barcode readers, while providing complete control over the bandwidth allocated to business applications. User behavior can also be controlled, by blocking or throttling high-bandwidth applications such as video, so every patron has a good Internet experience. Retailers could even block access to the websites of direct online competitors in order to curb showrooming.

Healthcare: Health clinics and managed care facilities increasingly need to offer guest access services to guests and patients. Yet they must ensure that caregivers and life-critical medical devices get the security protection and priority service they require. More and more, medical staff are bringing their own devices to work and using them in the provision of patient care – dealing with highly sensitive patient information through those devices. To ensure HIPAA compliance, those devices should be properly screened before they access patient data and should be protected from cyberthreats from the Internet or other wireless devices.

VoIP phones, RFID/barcode scanners and many Wi-Fi enabled medical devices such as heart monitors and I/V pumps are based on Linux or even Windows operating systems. Such "headless" devices often suffer from long lapses in firmware updates, that leave them vulnerable to worms and other viruses which can quickly render your fleet of devices useless, potentially putting patients' well-being, if not their lives, at risk.

With built-in IPS, web filtering, antivirus protection and application control, Fortinet's unique cloud-Wi-Fi approach provides complete protection for medical devices and the smartphones and tablets of caregivers. Guest and patient devices can be isolated from business and medical traffic, while enjoying the same threat protection. And all medical applications can be assured prioritized service and bandwidth protection while guest bandwidth consumption and application use is kept in check.

Transportation: At a large passenger terminal, transportation providers may already have the Wi-Fi and security infrastructure they need to offer secure Wi-Fi hotspots for passengers. But at suburban and rural bus or rail stations it is a different matter; the cost of Wi-Fi deployment is often prohibitive. However, passengers want Internet access wherever they are.

Using FortiAP-S series APs and branded captive portals, transportation services operators can cost-effectively offer free or pay-per-use secure Wi-Fi hotspots that redirect users to a landing page with up-to-date timetables, service status and loyalty programs. In addition, operators can offset the cost and perhaps even turn a profit by offering tiered Wi-Fi access services to retail tenants at the same premises, which is an obvious win-win.

MSP-managed Wi-Fi: The unique security capabilities of the FortiAP-S series together with FortiPrivateCloud (see below) make it practical and profitable for managed service providers to target the massive SMB and distributed enterprise opportunity. It is no longer necessary to deploy a full security appliance and APs on premises. Just one or a handful of cloud-managed FortiAP-S series APs now provides an equivalent level of security, at a fraction of the cost. This dramatically impacts the economics of managing secure Wi-Fi access as a service, making it more attractive to businesses and more profitable for managed services providers.

Overlay Hotspots: As mentioned earlier, if you want to control or secure guest traffic, it must be tunneled through the corporate WAN. Using the FortiAP-S series as an overlay to an existing network lets businesses control and protect guest traffic and devices, while bringing relief to the corporate network.

One of the most compelling aspects of the various use cases described above is that Fortinet's Cloud Secure Access solution makes it possible for distributed enterprises to implement world-class wireless security at remote sites without altering their corporate security framework, and without burdening the corporate network in any way.

Related Products and Services

FortiGuard

FortiGate is *Secured by FortiGuard*, meaning that it receives continual exploit, virus and application signature updates, ensuring immediate protection from zero-day cyberthreats. FortiGuard Labs is a global team of over 200 threat researchers who continually research the latest attacks, and figure out how to neutralize them. Their work results in regular security updates that are downloaded to Fortinet products as a FortiGuard subscription service, to provide your network with the latest protection against new and emerging threats.

FortiPrivateCloud

FortiPrivateCloud is a feature-rich VM software platform similar to FortiCloud, which is designed specifically for MSPs to enable them to deploy cloud Wi-Fi and security management solutions as a managed service upon their own hosted services infrastructure. Its multi-tier, multi-tenant capabilities allow MSPs to manage all their customers' networks through one console, while also extending management access to their customers and enabling different privileges for different users.

Cloud Secure Access Solution Summary

Fortinet's cloud-managed Wi-Fi solution is truly unique. While other vendors require additional security appliances for antivirus, web filtering and intrusion protection, Fortinet provides this functionality as standard from the cloud. These services are enforced directly on FortiAP-S series APs where they provide immediate protection at the session level, without complicated traffic-flow mapping to external security appliances.

With regular security updates from FortiGuard Labs, the *Cloud* Secure Access solution assures instant protection against the very latest cyberthreats with no administrative effort involved. No matter how the cyberthreat landscape evolves, specialized business-centric mobile devices and those of your guests and employees connecting to your network are protected, or rendered harmless.

This unique distributed security model reduces costs and eliminates the complexity of providing wireless LAN security for distributed enterprise locations. With FortiCloud providing a single dashboard to unify infrastructure and security management, businesses can enjoy unlimited scalability and the convenience of centralized cloud management, without sacrificing enterprise-class security.

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

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

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

April 26, 2016