

DEPLOYMENT GUIDE

# **Large Enterprise Secure Access Deployment Guide**

Secure Premise-managed Wireless LAN Solution

# Large Enterprise Secure Access Deployment Guide

Overview . . . . .	3
Fortinet Secure Access Solution . . . . .	3
Controller Secure Access Solution. . . . .	3
Controller Secure Access. . . . .	3
Fortinet Access Points . . . . .	7
Comprehensive Cybersecurity . . . . .	8
Internal Segmentation . . . . .	9
Common Deployment Scenarios . . . . .	9
Related Products and Services . . . . .	13
Controller Secure Access Summary . . . . .	13

## Overview

Large enterprise and campus networks require WLAN solutions that scale well for high-density deployment and are easy to manage and integrate within an existing network security framework.

Today, enterprise Wi-Fi networks support mission-critical mobile application traffic that spans from videoconferencing to heart monitoring systems. Enterprise class Wi-Fi has evolved beyond a best-efforts network to a utility where new applications, devices, and “things” mandate an always-on wireless infrastructure.

**Fortinet’s Controller Secure Access** solution uses a unique channel-management approach, which eases deployment and scaling and offers a number of compelling quality-of-experience advantages. It also provides a complete portfolio of security services that offer additional means of protection to combat the ever-evolving threat landscape.

By managing spectrum utilization differently, this unique technology overcomes the interference-related deployment barriers commonly encountered in large venues such as conference centers, stadiums, warehouses, and university or hospital campuses. And by dramatically simplifying initial deployment, smaller organizations such as K-12 schools, which are often understaffed, can deploy a secure, scalable wireless LAN with far less effort than competing solutions.

## Fortinet Secure Access Solution

Fortinet’s Secure Access solution ensures enterprises of any size, in any industry, can choose the topology and network management that is best suited to their network and organizational structure, and enjoy the same world-class cybersecurity in every scenario.

The days of one-size-fits-all Wi-Fi are over. How Wi-Fi is used in different-size organizations and across different industries varies tremendously. What is ideal for a small retail store is generally not suitable for a hospital or university campus and vice versa. As a result, different architectures and topologies have emerged, while still remaining fully interoperable with the thousands of different Wi-Fi-certified devices in existence.

There are four dimensions across which WLAN vendors have differentiated their solutions from one another: controller vs. controller-less, on-premise or cloud-based management, multicell vs. singlecell channel management and, finally, integrated vs. separate application security. It turns out that some technological approaches really are better suited to different use cases than others.

For these reasons, Fortinet has invested in not just one WLAN solution, but three separate and distinctly different approaches, each backed with Fortinet’s world-class cybersecurity. Fortinet’s Controller Secure Access solution is just one of three WLAN offerings designed to give enterprises complete flexibility over their preferred deployment model, without compromising security.

## Controller Secure Access Solution

The Controller Secure Access solution is best fitted for large enterprise and campus deployments, and consists of best-of-breed components for switching, WLAN, and cybersecurity.

The WLAN component provides a highperformance, premise-managed Wi-Fi network with a broad range of 802.11ac Wave 1 and Wave 2 access points (APs), while an access security overlay is provided by a FortiGate appliance, which features a comprehensive portfolio of security services along with granular application-control capabilities.

What makes this WLAN solution so unique is its single-channel management technology called Virtual Cell, which simplifies deployment and scaling, and delivers compelling reliability and quality-of-experience advantages over other WLAN systems.

Virtual Cell minimizes the complex, time-consuming process of channel planning, which can take months for a large network, through its unique single-channel deployment model, which avoids the challenges of planning around co-channel interference. In a Virtual Cell, all radios operate on the same channel, providing a layer of coverage across your venue, and appear to clients as a single radio wherever they go.

## Controller Secure Access

A key business issue has become. How do you balance the need for security with the flexibility of allowing any devices onto the network?

Fortinet’s Controller Secure Access solution simplifies wireless LAN deployment and scaling, and delivers compelling quality-of-experience advantages in high-density and videoor voice-rich environments. It also provides a comprehensive portfolio of application-layer security services that enable enterprises to augment their existing security framework with the latest protection against the ever-evolving threat landscape.

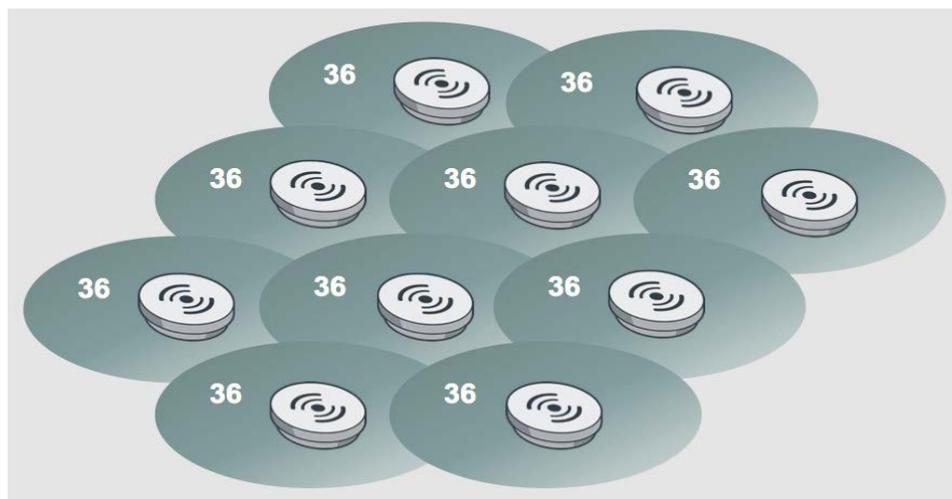


Figure 1: Fortinet Virtual Cell Deployment Model.

### Rapid Deployment and Scaling

Virtual Cell dramatically simplifies deployment because it dispenses with site surveys for adds, moves, or changes. It also cuts out the time-consuming, constant tinkering with channel plans that is normally necessary in an evolving wireless LAN.

To increase coverage or incrementally boost capacity in one particular area—say extending coverage to the parking lot—you don’t need to survey the site, move other APs around, or adjust channel and power settings—just add APs wherever it is physically convenient and you’re done.

Scaling capacity, which normally requires a highly disruptive redesign of the network, is also a cinch using a non-disruptive approach called channel layering.

For large-capacity gains, multiple Virtual Cells can be configured to each use a different channel, while occupying the same coverage area, by adding additional sets of APs. Layering Virtual Cells in this way can be limited to a small zone requiring more capacity, or they can span the entire venue.

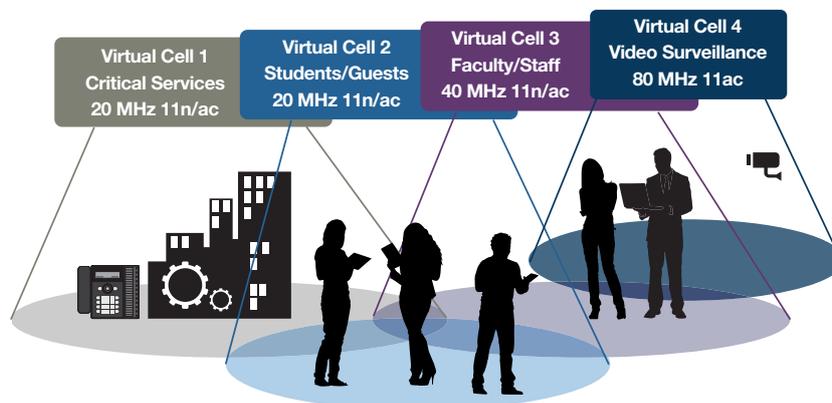


Figure 2: Campus-wide capacity scaling with channel layering.

What’s more, you can roll out new Virtual Cells at your own pace. Layering a new Virtual Cell alongside another does not require any changes to existing cells, so the stability and performance of your existing environment is never put at risk each time you need to scale capacity.

### Traffic Isolation and VIP Services

Channel layering can also be used as a strategy to physically segregate missioncritical corporate traffic from guest traffic, or to guarantee more capacity to select groups of users, such as executive staff, or for mission-critical applications such as VoIP, telepresence, or mobile point-of-sale (mPoS).

Hospitals, for example, can use it to provide total RF isolation for critical applications such as VoIP, heart monitors, and location tracking, or by clinical function. This allows critical services to be assigned dedicated spectrum and high QoS, on the clearest channels, with immunity to congestion on other channels.

Large venues and schools typically segregate out voice and important facilities resources such as building automation and security systems. If not day to day, in emergency situations facilities staff needs 100% reliable access to voice services and public-address systems, without risk of disruption by less-important traffic.

### More Reliable Connections

A major benefit of Virtual Cell is instantaneous zero-handoff roaming, which dramatically impacts the quality and reliability of real-time services such as VoIP and telepresence. This is because Virtual Cell controls how clients roam between APs.

In traditional multi-channel WLAN architectures, clients continuously probe for APs in order to know which AP to roam to, as the signal strength of their current AP weakens. Not only does this waste bandwidth, due to the large number of probe requests being sent by every client, but it leaves the client to make a poorly informed roaming decision based solely on signal strength, with zero awareness of the load on that AP it is about to associate with.

With Virtual Cell enabled, it is the network, not the client, that dictates when and where a client should roam to get the best service. This network-directed roaming technique, which mimics the way roaming occurs in cellular networks, can fully take account of the AP loads and other criteria, and ensures that every client enjoys the best available connection at all times. It also fixes common problems like sticky clients, further reducing unnecessary probes and retransmissions.

Under network control, roaming is almost instantaneous (3 ms vs. the typical 100+ms), which makes voice calls and any type of real-time traffic more reliable. And when thousands of sports fans race to the bar at halftime, or conference attendees surge from the keynote to breakout conference rooms or the show floor, they stay connected and whatever they were doing is not interrupted.

This approach also makes it possible to perform real-time AP load balancing based on actual traffic, not crude round-robin algorithms based on station count. Any client can be roamed to a different AP completely transparently, with no roaming delay penalties, as loads change.

### Better Airtime Utilization

The system also uses sophisticated air traffic control mechanisms to govern station airtime so every client gets a fair turn on-air, which prevents the slowest, or the fastest, devices from hogging resources. It also employs dynamic contention adaptation algorithms, which involves on-the-fly adaptation of WMM parameters to minimize the contention window that the AP advertises, based on the number of instantaneous contenders. This reduces collisions and improves aggregate utilization of the medium, as the number of contenders goes up.

### High-Availability Options

The **Controller Secure Access** solution offers various options to maximize availability: Support for active-active or active-standby link-level redundancy allows controllers to be connected to two or more network switches via GbE or 10 GbE ports, depending on the controller selected.

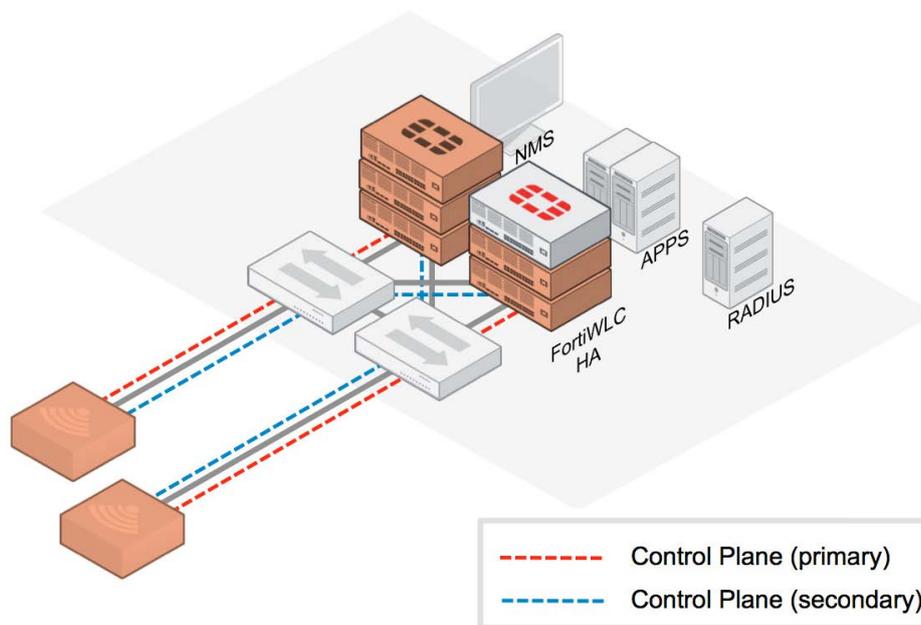


Figure 3: Link-level and N+1 controller redundancy.

N+1 controller redundancy allows clusters of up to five active controllers to be backed up by one standby controller. Controller configuration changes are synchronized between master and slave controllers, ensuring that in the moment of truth, the standby controller contains a valid, secure configuration.

APs can be configured for redundancy too. If their primary controller is unavailable, APs can automatically fail over to a secondary controller via a DNS resolvable host name or IP address provided by DHCP option 43.

### **Powerful Identity Management**

Secure, role-based access with granular policy management, based on user and device type, time of day, or other criteria, is provided through Fortinet Connect, an identity-based, onboarding solution that allows IT to easily segment users or client devices based on unique business and compliance needs. Fortinet Connect enables IT staff to configure unique access profiles for different individuals and groups within an organization (e.g., faculty, students, and guests in a school or clinicians, nurses, administrators, and facilities in a hospital) using separate SSIDs with specific authentication options.

Fortinet Connect includes support for multiple types of captive portals for guests and employees, enabling self-service guest provisioning and BYOD onboarding using a variety of authentication options including social login, 802.1x, and twofactor authentication, and is compatible with RADIUS, active directory, LDAP, etc. Fortinet Connect also provides an API to enable integration with third-party provisioning platforms such as guest registration systems used by hotels or student registration systems in universities.

### **Self-Service BYOD Onboarding**

Like it or not, BYOD has taken hold in almost every industry, and with approximately 30% of users replacing their smartphones annually these days, onboarding new devices is a never-ending task. Doing it manually simply does not scale and can quickly bring IT support to its knees.

In higher education, device onboarding is even more challenging—it is not just smartphones and tablets being connected, but game consoles, printers, and more. Some of them are headless, which adds further complexity. Healthcare faces similar challenges with all manner of proprietary operating systems on medical devices.

The solution is of course a self-provisioning system in which every user is identified and authenticated against a trusted network source (e.g., active directory) using IT-defined profiles to handle the different user types and mobile operating systems. The system must also cater to users having multiple types of devices (e.g., a corporate laptop and a personal tablet), each requiring a different security profile and users being connected on more than one device at a time. So the network must be able to recognize not just users, but each user/device pair.

Fortinet Connect manages BYOD onboarding with minimal IT involvement: It provides identity-based access, device fingerprinting and registration, and policy management for corporate- and user-owned devices of all types, and enables one-click self-provisioning of client devices for secure 802.1x connectivity. Users simply access a provisioning web portal, enter identifying information (name and password), and a suitable service profile is created automatically.

### **Easy Guest Management**

BYOD and guest management go hand in hand. For the majority of visitors and guests, placing them on a guest SSID, which only permits access to the Internet, is usually sufficient. However, certain groups of guests, such as auditors and contractors, need limited short-term access to corporate resources.

Fortinet Connect allows corporate “sponsors” to create temporary guest accounts in a secure, controlled manner to give their guests network access, which may be limited by location, time of day, and so on, and automatically expires after a predefined period of time. Options also exist for visitor self-registration to enable more restricted access to network resources (e.g., printers) beyond merely offering Internet access.

### **Bonjour Multicast Suppression**

Wherever you have a lot of Apple fans, which is often the case in higher-education networks, you'll likely run into problems with Apple's Bonjour technology, which can ravage bandwidth with thousands of irrelevant multicast packets while students connect to their Apple TVs and wireless printers in student dorms.

The multicast advertisements may be small, but they propagate everywhere and affect everyone. Fortinet's Personal Bonjour application overcomes these issues by maintaining an internal table of devices advertising services via Bonjour, and then mediates the discovery process, converting multicast probes and advertisements into unicast traffic. This approach completely neutralizes the harmful effects of AirPlay and AirPrint proliferation in student dorms by slashing Bonjour-related traffic to less than 1% of its former levels.

## Fortinet Access Points

Fortinet provides a broad range of high-performance 802.11ac Wave 1 and Wave 2 access points for indoor and outdoor deployment. Most indoor AP models are available with either internal omnidirectional antennas or external omnidirectional antennas, which can be replaced or upgraded with directional and high-gain antennas as applicable.

Automatic radio resource provisioning and zero-touch deployment features let you roll out Fortinet APs quickly, even in remote offices with no on-site controller. All enterprise features such as fast roaming, mesh and bridging support, spectrum scanning, guest access, rogue AP detection, WMM, and QoS are supported as standard, without needing to purchase expensive feature licenses.

802.11ac Wave 2 4x4			FAP-U421EV FAP-U423EV
802.11ac 3x3	 AP122	 OAP832E	 AP832
802.11ac 2x2			 AP822
	Wall Jack	Outdoor	Indoor

Figure 4: Fortinet AP Models.

**Highest Gigabit Wi-Fi Performance:** Fortinet offers the industry's largest enterprise-class Wi-Fi portfolio and blazing-fast 802.11ac Wave 2 access points. Our enterprise-class universal APs offer the ability to support multiple deployment options from on-premise to cloud, all from the same AP.

**802.3af PoE Support:** Carefully designed for thermal efficiency to reduce power consumption during full operation of both radios and 3x3 MIMO, all indoor APs run on the 802.3af PoE standard, which is rated at 12.9 W. So there is no need to upgrade your LAN switches to support 802.3at.

**Zero-touch Deployment:** Fortinet APs are truly plug and play. They use several robust discovery mechanisms to find and connect to a home controller completely automatically. Controller discovery operates over L2 or L3 connected networks, ensuring it is fast and easy for non-IT personnel to physically install an access point at any location, including home and remote offices. Once an AP has found a controller, it sets up an L2 or L3 tunnel for management control, automatically downloads the latest firmware and the security profile assigned to it, and starts operating immediately.

**Spectrum Analysis:** Any radio can be configured to periodically scan the spectrum for interference, rogue APs, etc., in the background, when it is idle. Alternatively, the AP832 and PSM3X access point radios can also be dedicated to operate in sensor mode. Unlike most other WLAN solutions, Fortinet AP can support background spectrum scanning even while handling multiple concurrent voice calls. With Fortinet's triple-radio PSM3X, two radios can be used for client access, while the third is assigned as a dedicated spectrum sensor.

With Fortinet's Spectrum Manager, you can detect and classify Wi-Fi and nonWi-Fi sources of wireless interference such as microwave ovens, Bluetooth devices, and adjacent Wi-Fi networks. The system even estimates the channel utilization impact of the interfering source. By proactively keeping you informed about Wi-Fi interference, Spectrum Manager lets you take actions to alleviate problems by removing, adjusting for, or working around external interference sources, to ensure optimal spectrum availability and high service levels.

**Wireless Intrusion and Rogue AP Detection:** To prevent clients from accessing the network via unauthorized APs, radios can be set to scan for rogue APs and mitigate the client traffic originating from them. These features are set globally, with the controller managing the lists of allowable and blocked WLAN BSSIDs and coordinating the set of APs (the mitigating APs) that perform mitigation when a rogue AP is detected. Rogue AP mitigation prevents stations from associating with or attempting to access the network through rogue APs. A customizable wireless intrusion prevention system (WIPS) software module comes with a base set of signatures corresponding to common wireless attack types such as honeypot, man-in-the-middle, etc., while the PCI compliance manager module audits and verifies a network's security posture to ensure PCI compliance.

**Strong Authentication and Encryption:** As one might expect, all Fortinet APs support the full range of enterprise authentication types including WPA2-802.1X and standards-based encryption types including AES and TKIP. Extended user authentication against RADIUS servers is secured by EAPMD5, EAP-TLS, EAP-TTLS, and PEAP.

## Comprehensive Cybersecurity

In this solution, comprehensive application security and granular application control is provided through Fortinet's Cooperative Security Fabric and Fortinet's award-winning FortiGate cybersecurity platform, which features a complete portfolio of security services.

Enterprises considering Fortinet's Controller Secure Access solution over its integrated offering are likely doing so because they favor best-of-breed Wi-Fi, switching, and security and already have an adequate network security framework in place that they could leverage for wireless traffic. That said, using FortiGate for all-around wired and wireless threat protection has numerous advantages over using multiple-point products, which include easier management and superior performance.

While the WLAN Controller solution provides tremendously efficient and flexible utilization of the spectrum, FortiGate provides maximum control over users, devices, and applications, and makes it easy to administer sophisticated security policies and ensure complete threat protection.

FortiGate consolidates the functions of more than seven individual security devices, including firewall, VPN gateway, network IPS, DLP, anti-malware, web filtering, and application control, into a single high-performance platform.

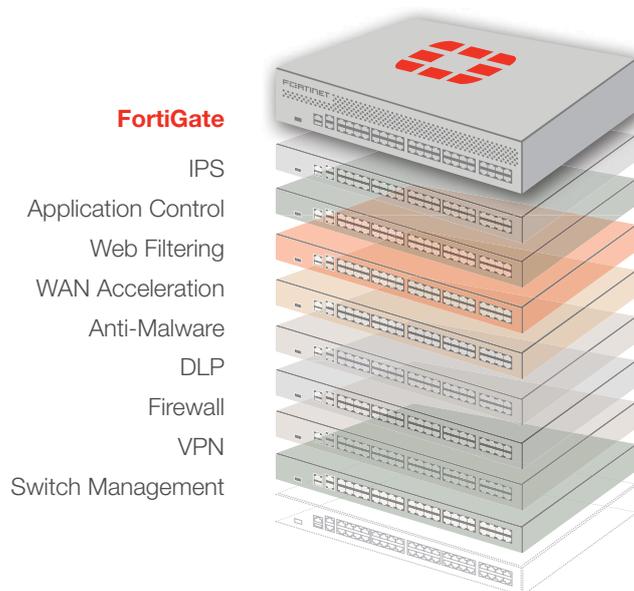


Figure 5: FortiGate Consolidated Security Platform.

With a FortiGate appliance in your network, security features can be selectively applied to different groups of users to prioritize apps, control bandwidth, and detect all classes of cyberthreats, from wireless intrusion to malware.

The FortiGate appliance's ASIC-assisted, high-performance architecture allows any number of different security policies to be applied to traffic in a single pass. This improves performance and minimizes latency over passing data through multiple single-function security appliances.

### FortiGate Highlights

The FortiOS license for any size FortiGate provides all of the following security capabilities, and much more, as standard. There are no additional licenses and fees for firewall, IPS, application control, and any other security measures.

**Firewall:** FortiGate is one of the fastest firewall platforms in the industry, with flagship models outperforming all competitors.

**VPN Gateway:** No need for a separate VPN device or WAN accelerator to manage at head offices or branch offices. FortiGate has high-performance SSL and IPsec VPN services built in. Fortinet also provides a free remote access VPN client for PCs, tablets, and smartphones on all major operating systems.

**IPS:** Fortinet Intrusion Prevention System (IPS) technology protects networks from both known and unknown threats, blocking attacks that might otherwise take advantage of network vulnerabilities and unpatched systems. You can enable IPS on any FortiGate at the edge of your network or within the network core to protect critical business applications from both external and internal attacks.

**DLP:** FortiGate can also be used to protect information privacy and prevent unauthorized leaks. Sophisticated pattern matching is used to prevent unauthorized communication of sensitive or regulated data through the corporate perimeter.

**Anti-malware:** Thanks to a combination of hardware-assisted Layer 7 deep packet inspection and a massive library of malware and exploit signatures, FortiGate provides real-time protection against viruses, botnets, web exploits, Trojans, and other malicious software variants. Regular FortiGuard Labs updates ensure immediate protection against newly discovered zero-day vulnerabilities.

**Web URL Filtering:** FortiGate can block access to any known harmful websites that may contain phishing/pharming attacks or malware, or any other site you specify. Beyond reducing exposure to malware, this can also be used to control access to age-inappropriate content in schools, or to disallow people from viewing potentially objectionable content in public areas.

**Application Control:** With signatures for over 4,000 applications, FortiGate offers unrivalled control over application priority and bandwidth management. FortiGate distinguishes unique applications, not just broad Wi-Fi priority classes. You can treat YouTube, HD YouTube, Netflix, Facebook, LinkedIn, SIP, and Skype all differently. You can ensure mission-critical traffic always prevails over low-priority applications.

**Zero-day Threat Protection:** FortiGate security is kept continually up to date through frequent automated updates from FortiGuard Labs, which researches the latest attacks to provide your network with immediate protection from newly found threats.

## Internal Segmentation

Over the last decade, the trend has been to flatten corporate networks. However, 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 are the new standard to protect against highly sophisticated and persistent 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 hardware-assisted internal segmentation firewall with multi-gigabit line-rate performance.

## Common Deployment Scenarios

Both the Fortinet WLAN controllers and FortiGate security appliances come in all sizes suitable for small offices all the way up to very large enterprise and campus deployments, enabling centralized or distributed security and access control.

Flexibility and rightsizing are important; you may prefer a distributed security model over centralized, or you may have a data center. The Controller Secure Access solution supports multiple deployment options to meet your needs and preferences. Below are some common deployment scenarios. For the sake of simplicity, where we refer to FortiGate for the security component, this could equally be your preferred security appliances.

### Enterprise Campus/HQ Deployment

Distribute controllers throughout your campus for very high-density deployments by putting wireless controllers at the access switching layer. This improves capacity scaling for high density, especially as you migrate to 802.11ac, and spreads the WLAN processing load. AP traffic is tunneled to the nearest controller, and optionally may be dual homed to allow failover to a second controller for resiliency. A pair of midsize FortiGate appliances provides a secure connection to the campus backbone and internal segmentation.

## Here is a more complete list of what is in FortiOS:

- Advanced Threat Protection
- Client Reputation Analysis
- Contextual Visibility
- Extended Single Sign-on
- Sandbox Integration
- Per-device Security Policies
- Secure Guest Access
- Enterprise-class Firewall
- IPsec and SSL VPN
- SSL-encrypted Traffic Inspection
- Antivirus/Anti-spyware
- Anti-spam Filtering
- Intrusion Prevention System (IPS)
- Data Loss Prevention (DLP)
- Flow-based Inspection Options
- Web Filtering
- Application Control
- Network Access Control (NAC)
- Vulnerability Management
- Monitoring, Logging, and Reporting
- WAN Optimization
- Wireless Controller
- VoIP Security
- Central Management
- Virtual Domains
- High Availability
- Layer 2/3 Routing Services

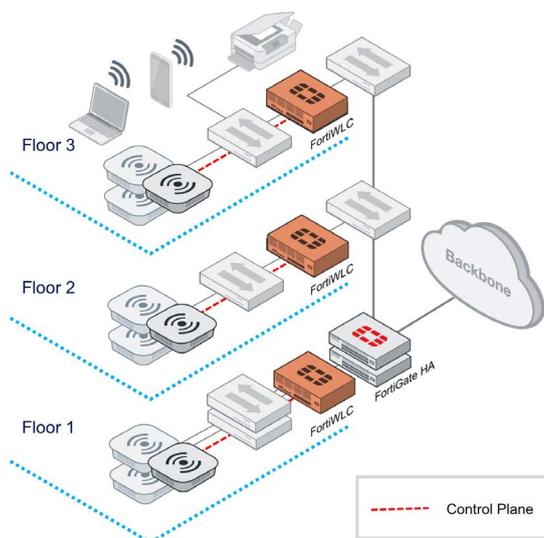


Figure 6: Enterprise Campus/HQ Deployment.

### Enterprise Edge Gateway Deployment

Use FortiGate to secure your network edge alongside a midsize FortiWLC controller. In this deployment model, SSIDs are mapped to different VLANs in the FortiGate and subjected to security inspection. FortiGate provides protection from network threats from the Internet or from wireless devices.

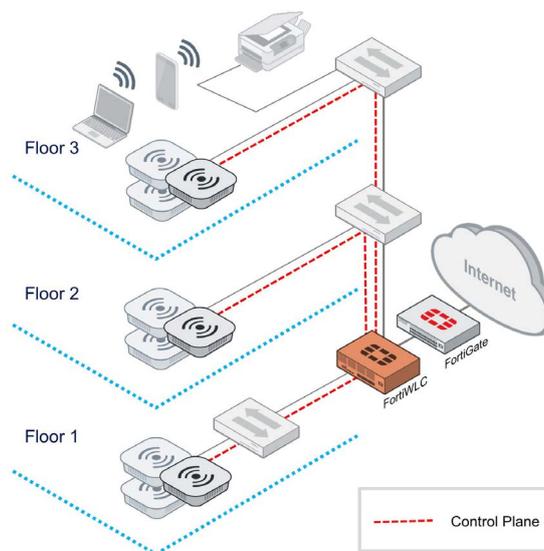


Figure 7: Enterprise Edge Gateway Deployment.

### Branch Office Deployment

Use an entry-level FortiWLC controller together with an entry-level FortiGate to provide complete threat protection if you don't already have local security appliances.

SSIDs are mapped to VLANs on the FortiGate to provide policy enforcement and security threat inspection for all traffic, regardless of its destination. Distributing security to branches improves performance, reduces the security bottleneck at corporate, and protects all traffic at its source. To reduce the WAN load heading to your HQ or data center, the on-site FortiGate enables only corporate traffic to be routed to the HQ or data center, while the rest of the traffic is inspected locally before going directly to the Internet.

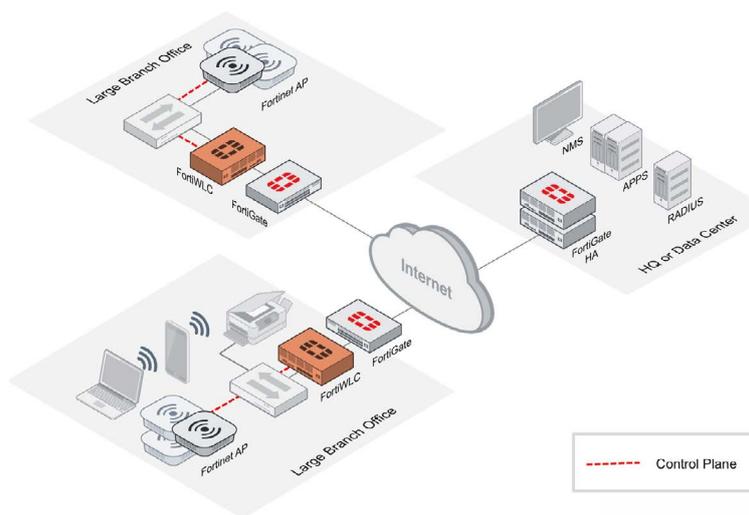


Figure 8: Large branch office deployment.

### Small Branch Office Deployment

In small branch office or home office deployments, an on-site FortiGate may be cost-prohibitive. Yet you still want to secure Internet traffic. In this case, APs can be installed without requiring a local controller, allowing non-local traffic to be tunneled back to HQ or your data center where the controllers reside. Traffic is then forwarded to your centralized FortiGate or other security appliances for security processing before it is forwarded to the Internet, and vice versa.

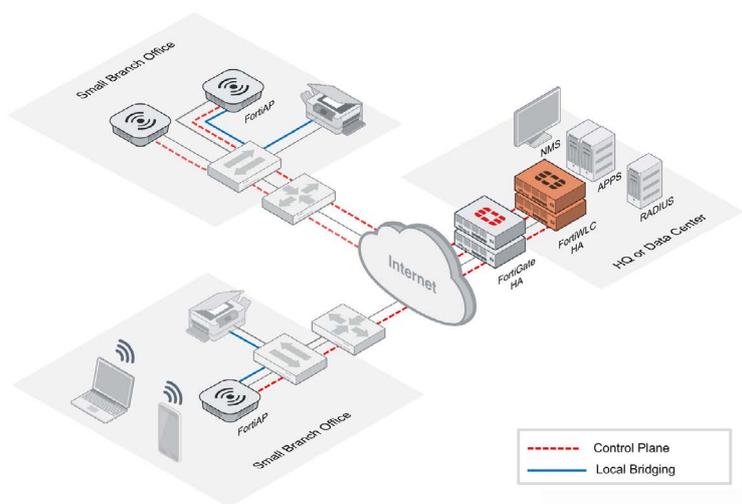


Figure 9: Fortinet AP Bridge and Tunnel Modes.

**Bridge and Tunnel Modes:** In their default configuration, SSIDs tunnel all traffic to the wireless controller. However, it is also possible to configure SSIDs to bridge traffic directly to the local LAN.

There are many use cases where it is undesirable to forward traffic through the controller. For example, in a remote office with local servers and printers but no local controller, it is preferred to bridge traffic locally and avoid the delay and bandwidth waste of a round trip over the WAN.

Both bridged and tunneled SSIDs can exist simultaneously on the same radio. For example, VoIP might be served by an enterprise-wide SSID, which is tunneled from the remote office, while a different SSID for data services is locally bridged.

**Scaling:** Virtual Cell scaling is mostly a matter of increasing AP densities and layering channels (channel layers) appropriately, and there are a few general guidelines to consider regarding AP densities and when and how to layer additional Virtual Cells.

The general rule of thumb is to layer Virtual Cells across the same footprint as others, both horizontally and vertically. For example, in a multi-story building the Virtual Cells would be present on all floors. The coverage area of each Virtual Cell is only limited by the controller and densities chosen. Devices can roam across controller boundaries, virtually eliminating limitations on cell boundaries and the size of a Virtual Cell. Nevertheless, roaming between Virtual Cells is slower than within a cell, so the Virtual Cell boundaries should be minimized.

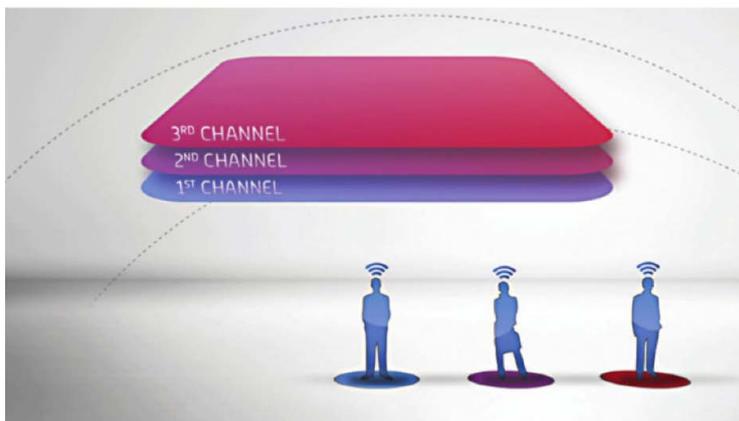


Figure 10: Multiple Virtual Cell Channel Layers can be deployed enterprise-wide.

In large horizontal spaces such as stadiums, conference and expo centers, and even warehouses the same principles apply, using natural physical boundaries, at the preferred demarcation from one group of Virtual Cells to another.

In this example, to layer additional Virtual Cells you would put additional APs in more or less the same places as the first set (ideally with a few feet of separation), and choose the two new channels to operate on. You may not need more 2.4 GHz capacity, since 2.4 GHz is considered a lifeline service these days, so both could be on the 5 GHz band.



Figure 11: 14 APs providing One 2.4 GHz and One 5 GHz Virtual Cell.

**AP Density:** The goal should be that at any location a client can always hear a minimum of two APs, preferably three. Stagger APs on different floors so clients hear APs from all sides, above and below, when layering a second Virtual Cell channel layer.

**Channel Selection:** The Virtual Cell technology is designed to avoid co-channel and adjacent-channel interference, but there are still interference sources beyond your control—including other networks and non-Wi-Fi sources such as microwave ovens, radar, etc. Therefore, you should always seek out the cleanest available channel for each Virtual Cell.

**Legacy Clients:** Although airtime fairness stops slow clients from hogging the channel, slower clients beacon at a slower rate, which can be heard farther away, thus preventing a greater number of clients from seeing a clear channel and being able to transmit. It is good practice to isolate legacy clients on their own channel and to disable those lower rates on other Virtual Cells.

**Roaming Between Virtual Cells:** Roaming from one Virtual Cell to another is just like roaming between APs in a traditional multicell network. It requires re-association and is suboptimal. So it is best to minimize the number of places where clients are exposed to Virtual Cell boundaries. For example, in a four-story building you might have one Virtual Cell covering floors 1 and 2 and another covering floors 3 and 4, so clients only need to roam when moving between floors 2 and 3. Alternatively, capabilities such as the Roaming Across Controller feature reduce the re-association friction across Virtual Cell boundaries.

**Load Balancing with Channel Layering:** When APs are colocated, they should be placed 7-10 inches apart to minimize sideband or adjacent channel interference, while not too far apart that the coverage pattern varies greatly. With two channels in each band, you can provide load balancing and redundancy on both bands.

**Full Power:** Many deployments are a replacement of an aging legacy WLAN. Because Virtual Cell allows AP radios to operate at full power, when you do a one-for-one replacement, you often end up with more APs than you really need. This is especially true if the legacy WLAN was already high density. Instead, you can scale capacity by putting half of the APs on each of two different Virtual Cells covering the same footprint.

## Related Products and Services

### FortiSwitch

FortiSwitch Secure Access Switches integrate directly into FortiGate, allowing switch administration and access port security management from the same “single pane of glass.” With feature-rich, high-density 24- and 48-port models supporting 802.3at PoE, you can power anything from APs to VoIP handsets and surveillance cameras.

### Fortinet Wireless LAN Manager

FortiWLM is a wireless application platform for managing network-based applications via a common dashboard, accessible through single sign-on. It includes preinstalled Fortinet Network Manager, Service Assurance Manager, and Spectrum Manager and comes as a network appliance or can be downloaded as a VMware application.

### FortiGuard

FortiGate and all other Fortinet security products are secured by FortiGuard, meaning they continuously receive updates of exploit, virus, and application signatures, ensuring immediate protection from zeroday 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.

## Controller Secure Access Summary

As bandwidth demand and the number and types of network-connected wireless devices grow unabated, large venues such as conference centers, stadiums, warehouses, and university or hospital campuses often face considerable deployment and scaling challenges, many of which are directly attributable to the complexity of channel planning in high-density networks based on traditional WLAN solutions.

Breaches is at an all-time high, and the threats enterprises are exposed to are becoming more sophisticated and persistent. The increasing sophistication of cyberattacks is also uncovering vulnerabilities in overly flat networks, calling for a new paradigm—using internal segmentation to break the chain of infection. Consequently, large enterprises need to reevaluate their end-to-end application-layer security.

Fortinet's Infrastructure Secure Access solution is truly unique in the wireless networking industry. It optionally supports a completely different channel management approach to extract the maximum capacity from the available spectrum. This doesn't just improve per-user and aggregate performance; it simplifies deployment and scaling as well. The solution also provides a complete portfolio of award-winning security services that enable enterprises to augment their existing security framework with additional protection against the evolving threat landscape.

