# FortiGate - SD-Branch Playbook

Version 6.4.0

**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO GUIDE**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**NSE INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

January 21, 2021
FortiGate 6.4.0 SD-Branch Playbook
01-644-000000-20210121

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2021-01-19 | Initial release. |
| | |
| | |
| | |

# Introduction

The *SD-Branches Playbook* is a practical guide for architecting and securing the retail environment based on the needs of retail businesses.

*Secure SD-Branch* define the devices and security needed to defend your retail operations. As you explore the SD-WAN architecture, you will discover the need to orchestrate your SD-WAN solution at scale, linking together a massive network of underlays and overlays that connect back to regional hubs, datacenters, clouds and corporate head-quarters. We will introduce various methods of *SD-WAN Orchestration* provided by the FortiManager to simplify and automate your deployment. Further integration with third party automation solutions will outline how *Zero Touch Provisioning* streamlines the entire workflow starting from a request for a new retail location to the actual physical deployment of the necessary SD-Branch units.

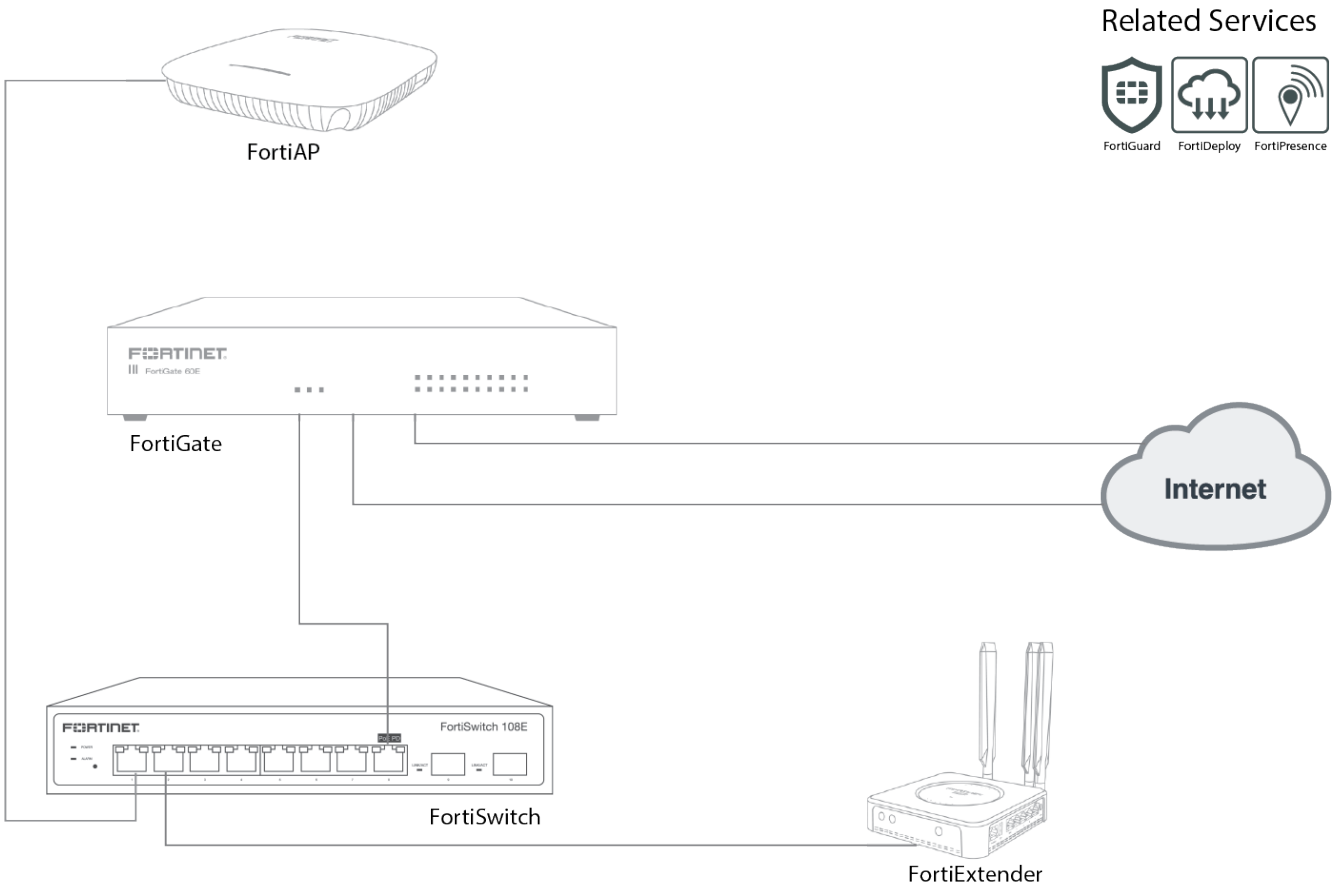
As retailers increasingly turn digital, their retail strategy must involve a secure and *Integrated Wireless*. We will explore how our FortiGate wireless controller integrates Network Access Control (NAC) with a comprehensive dashboard to provide a secure a secure wireless solution. Additionally, our *Presence Analytics* can provide key analysis of the retail branch based on wireless statistics. Finally, you will use the FortiGate switch controller, to manage your users and devices and simplify NAC policies with our *Integrated Segmentation*.

A common use case for protecting the retail Point of Sale (POS) is meeting necessary compliance. Through the Security Fabric on both the FortiGate and FortiAnalyzer, we will learn how our security rating engine can help monitor risks and perform *PCI Risk Assessment*. Finally, we will explore different protection platforms offered by our *FortiGuard Services*.

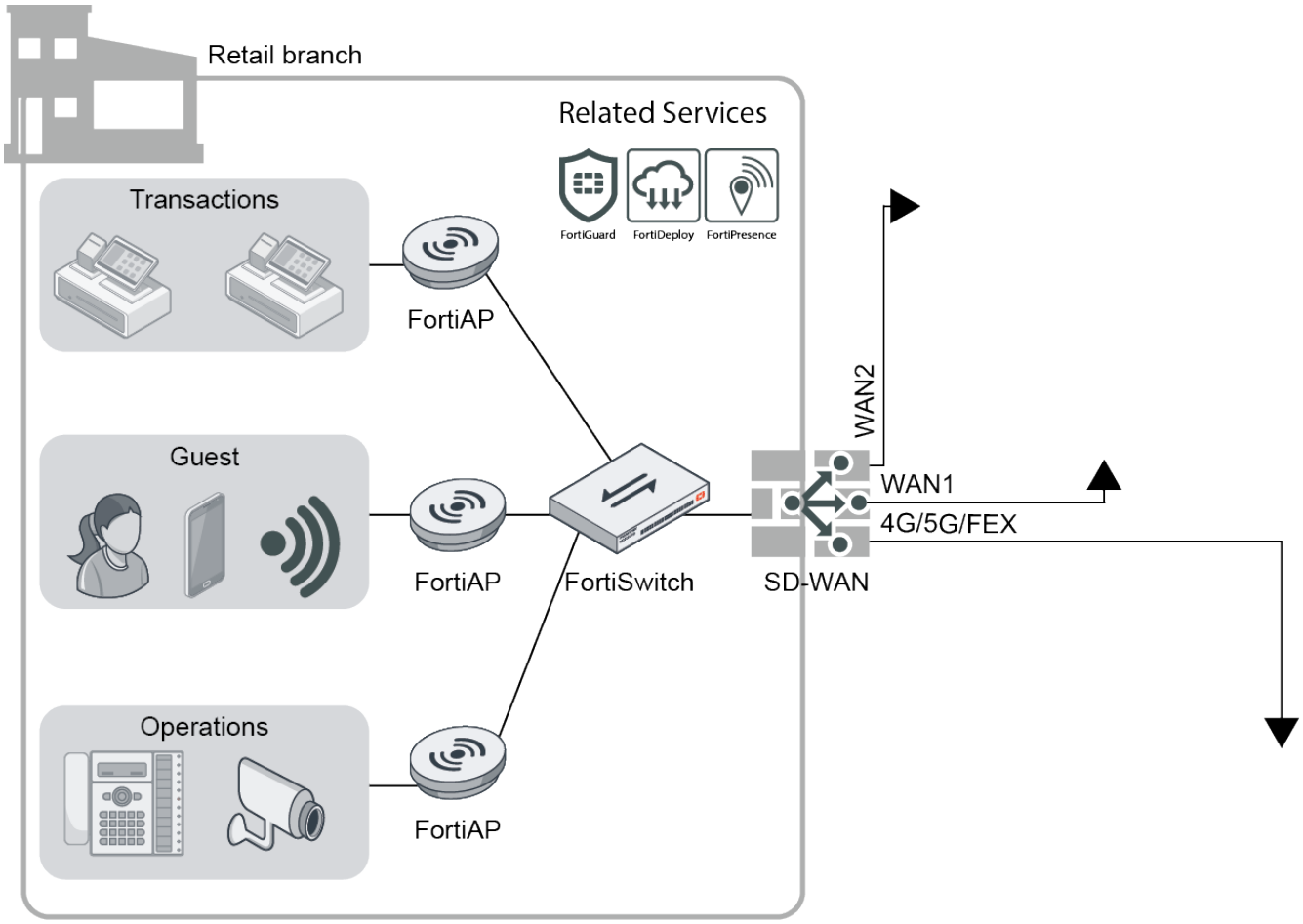
# Secure SD-Branch

FortiGate is the first line of defense at the branch level. It facilitates business critical SD-WAN connectivity, and simplifies overall branch deployments with managed wireless and switch networks. Ultimately, FortiGate secures and simplifies the branch deployments, and streamlines business critical applications.

The digital retail branch has evolved over the years, from simple protection for Point of Sales terminals to the secure SD-Branch we see today. By using the following Fortinet appliances, we provide a single pane of glass solution driven by the FortiGate and SD-WAN.




From a logical perspective, the FortiGate helps manage wired and wireless connectivity to secure branch transactions, employee and guest WiFi, and other operational devices like VoIP phones and security cameras.




Central to the SD-Branch is the SD-WAN, which helps steer traffic dynamically over various WAN connections. Understanding the concepts behind SD-WAN will help you deploy your solution more effectively.

# Resources

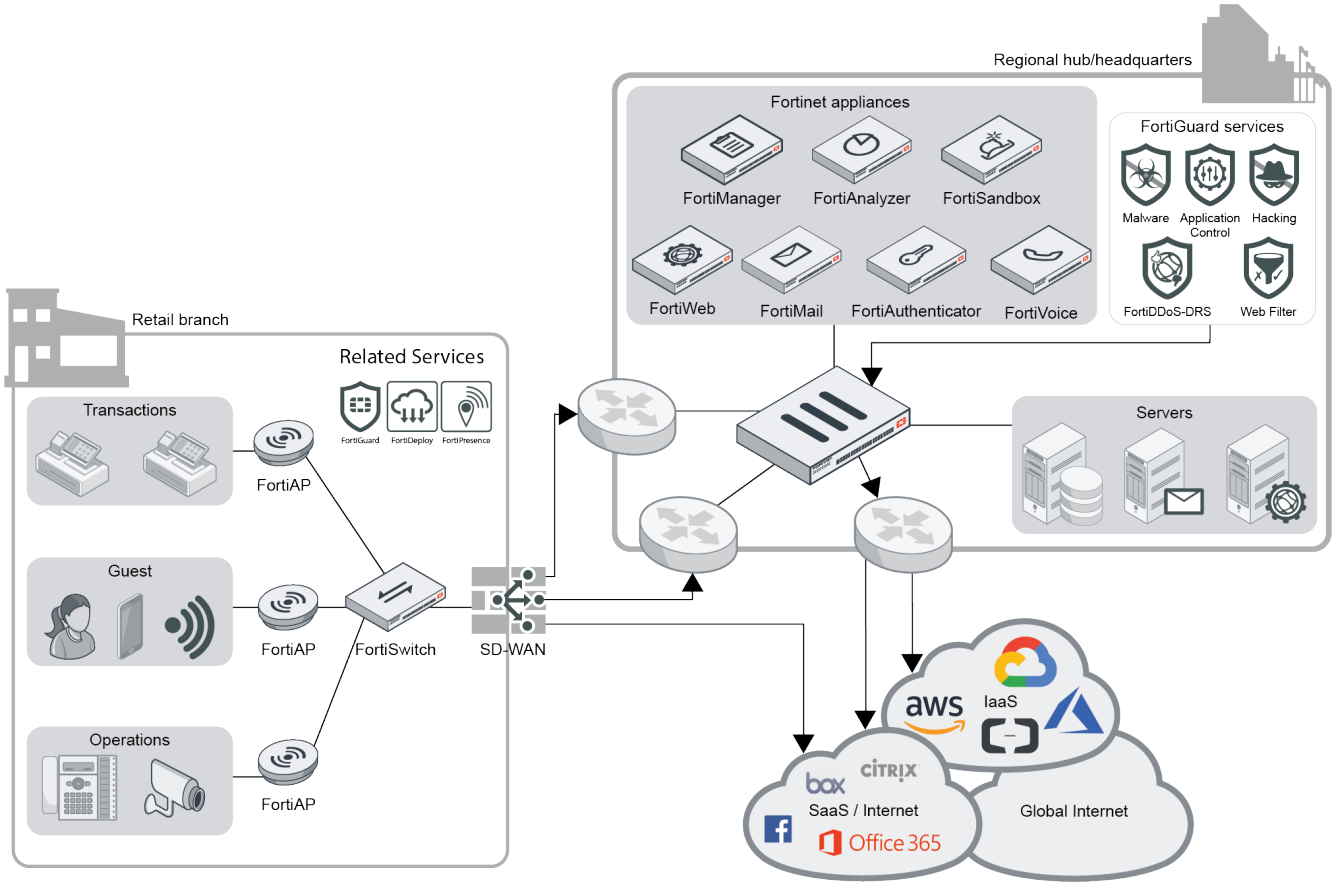
| Topic | Resource | Description |
|---|---|---|
| **Introduction to SD-WAN** | SD-WAN Quick Start Guide | A step-by-step example of how to start using SD-WAN for load balancing and redundancy. |
| | Configuring Performance SLA (Health Checks) | Learn about the health monitor, health check options, and performance SLA monitor using the REST API. |
| | Understanding SD-WAN Service Rules and load-balancing strategies | Instructions for configuring SD-WAN rules, Implicit rules, Best quality strategy, and Maximizing bandwidth (SLA strategy). |
| **Use SD-WAN to communicate with other branches, hubs, or** | Integration with ADVPN | This example illustrates how to use SD-WAN and ADVPN together. |

| Topic | Resource | Description |
|---|---|---|
| **connecting to the cloud** | Integration with OCVPN | Learn OCVPN how enables SD-WAN to dynamically add its tunnel interfaces as SD-WAN members. |
| | SD-WAN Cloud On-ramp | Configure a connection to a new cloud deployment that has some remote servers. |
| **Advanced features** | Application steering using SD-WAN rules | Examples of how to use different strategies to perform application steering to accommodate different business needs. |
| | Quality of Services profiles | Use a traffic shaper to control maximum and guaranteed bandwidth, or prioritize traffic. |
| | Using BGP tags with SD-WAN rules | Learn how SD-WAN rules can use Border Gateway Protocol (BGP) learned routes as dynamic destinations. |
| **SD-WAN Solutions** | Secure SD-WAN Solution Hub | Learn SD-WAN Basics, Management and Orchestration, Overlay VPN & Advanced Routing, and more. |

Continue on in this guide to explore more component configurations of the Secure SD-Branch.

# SD-WAN Orchestration

Building on our sample SD-Branch topology, we now add in a *Regional Hub* and *Multi-Cloud* access. Here, we will require redundant connections back to the HQ for processing transactions, and additional link(s) connecting to cloud resources for other SaaS based services or custom applications on the public cloud. The connections may be physical connections or high speed VPN overlays to secure the data.




Transforming each branch into a SD-Branch can become a daunting task when hundreds or even thousands of branches are involved. Managing the connections and interconnecting the VPN overlays increase in complexity as the number of sites grow.

Central management and SD-WAN orchestration is designed to reduce the complexity by automating much of the ground work. Fortinet's *SD-WAN Orchestrator* and *SD-WAN Module* are two approaches to orchestrate your SD-WAN deployment with FortiManager.

# SD-WAN Orchestrator

The *SD-WAN Orchestrator* simplifies the SD-WAN deployment. It is ideal for a multi-region enterprise network, where hub and edge devices interconnect to create a complex mesh of underlays and VPN overlays. SD-WAN Orchestrator automates the configuration based on profiles that you define for hub and edge devices, allowing you to scale your SD-WAN deployment with ease.

Once the hub and edge device profiles are defined, you add a FortiGate to the SD-WAN Orchestrator by specifying one of the profiles and the region. The orchestrator is able to create the necessary overlays between the hub and the edge device, and a full mesh overlay between multiple hubs. Finally, policies templates are added based on the profiles you created.

The SD-WAN Orchestrator is a *Management Extension Application (MEA)* that can be installed on the FortiManager. To learn more, see the SD-WAN Orchestrator Administration Guide.

# FortiManager's SD-WAN module

FortiGate's native ADVPN support is a powerful solution for building a scalable VPN overlay network between a hub, or hubs, and many spokes.

Spokes (or SD-Branches) can communicate with other branches through dynamically built tunnels called *shortcuts*. The FortiManager SD-WAN module and the VPN Manager work together to help scale your FortiGate configurations and manage the important components by grouping together your VPN overlays, objects, policy packets, etc.

The SD-WAN template then takes the shared objects and creates different profiles to perform health checks and dynamically steer your traffic. The deployment method allows very granular control over your SD-WAN profiles and is suited for administrators with deep understanding of the underlying technologies.

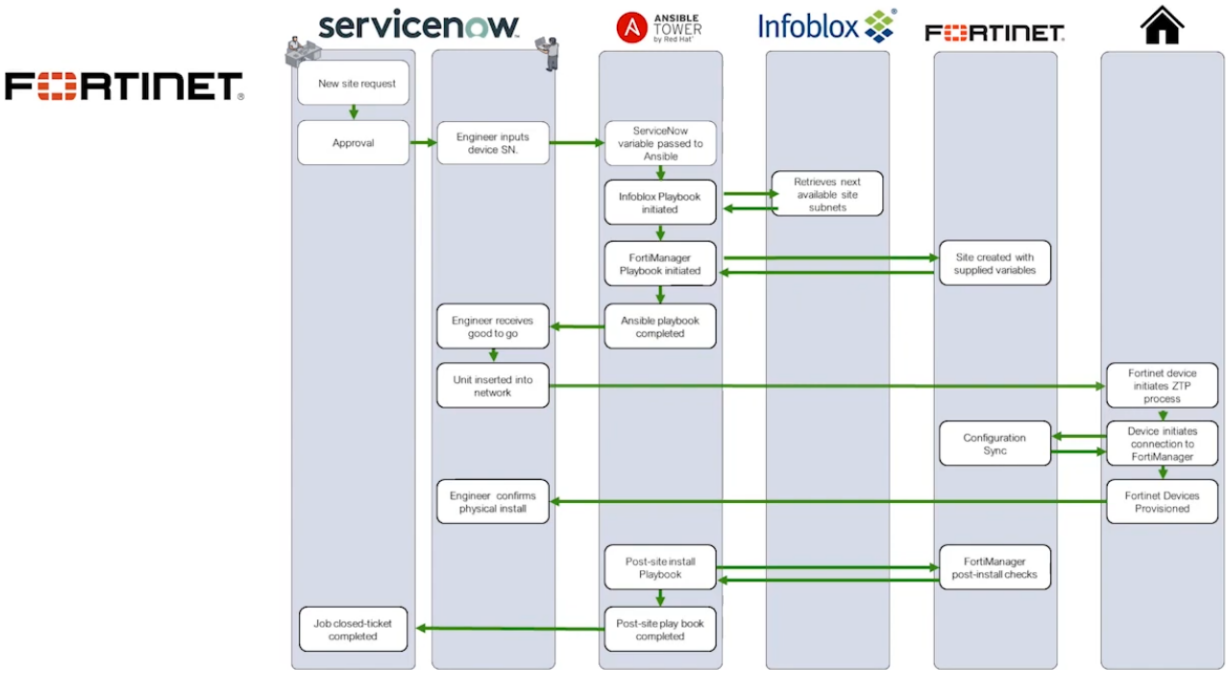
## Resources

| Topic | Description |
|---|---|
| SD-WAN / ADVPN configuration guide | Provides an understanding of the Fortinet Secure SD-WAN configuration. |

# Zero Touch Provisioning

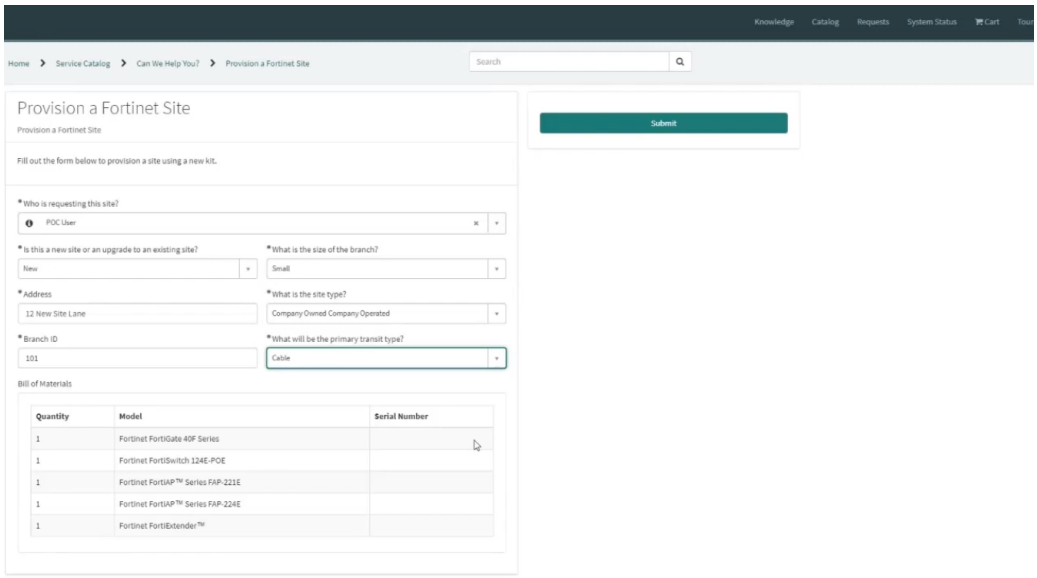
To streamline the workflow for provisioning SD-Branches, the FortiManager orchestration solution can be integrated with 3rd party services to cover the full end to end deployment.

The example below illustrates the steps involved using *ServiceNow*, *Ansible Tower*, and *Infoblox*. Other vendors and services can also be used.




## Service Portal

The ServiceNow interface in our example allows a site manager to request the provisioning of a new site or upgrade to their existing site. The manager provides information such as the size, location, and connection type for the branch. The system is then able to determine a *Bill of Materials* of all the devices that are necessary for the deployment.




After approvals, new tasks are generated for different teams to procure the equipment, services and connections. Equipment is then shipped to the provisioning engineer, who enters the Serial Number of the devices into the system for further configuration preparations.

# Configuration Automation

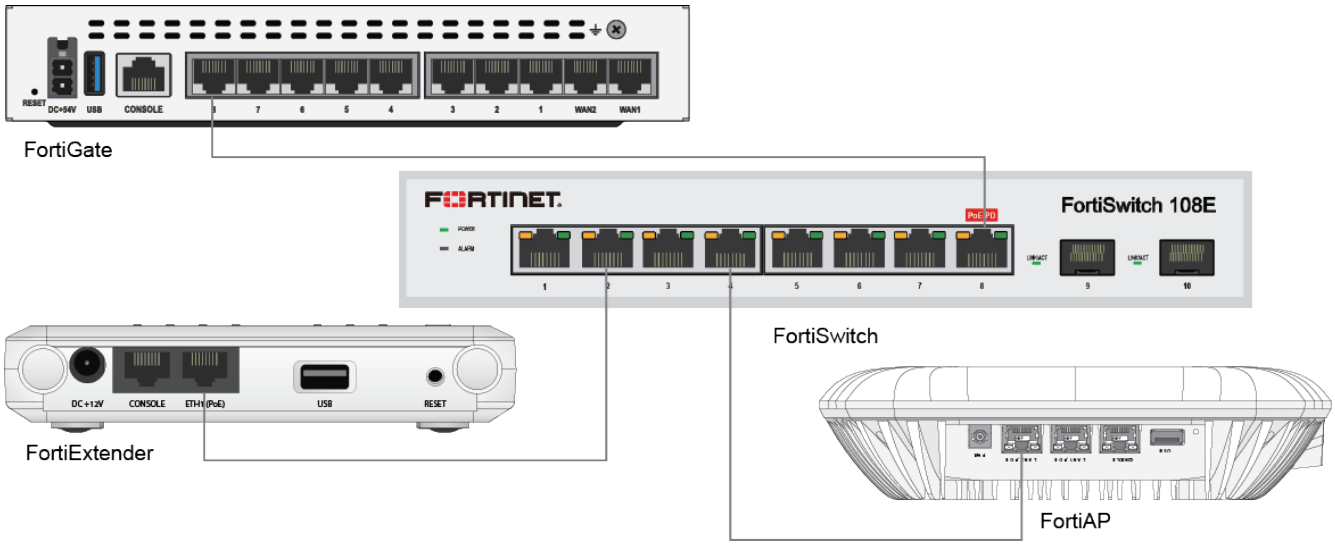
In our example, the serial number of the devices are passed from ServiceNow to Ansible Tower, which allocates an IP subnet block from an IP Address Management service such as Infoblox. The Ansible Playbook feeds these variables to the FortiManager and initiates the device configurations on the FortiManager. This may include triggering the creation of VPN overlays, routing, policies and SD-WAN rules as defined in the SD-WAN Orchestration chapter. As well, the FortiSwitch and FortiAP for the branch are also provisioned on the FortiManager.

To learn more about FortiManager automation configurations through Ansible or Terraform, visit the links below:

- FortiManager Ansible Collection
- FortiManager Ansible Collection Documentation
- Terraform FortiOS / FortiManager Provider

# Physical Installation

The provisioning engineer may schedule and install the devices at the branch as soon as the Configuration Automation has been completed. This involves making the physical connection as outlined below.




Once connected to the Internet, the FortiGate initiates a connection to the FortiManager to trigger a configuration sync. This may require a one-step manual configuration of the FortiManager IP, or other means. The site is now provisioned, and post installation checks are triggered to conclude the site deployment.

# Resources

To learn how *Zero Touch Provisioning* works on the FortiManager, visit the following links:

| Topic | Description |
|---|---|
| Adding a FortiGate by Pre-shared Key | Learn how to add a FortiGate model by using the pre-shared key for FortiGate. |
| Adding a FortiGate by Serial Number | Learn how to add a FortiGate model device to FortiManager by using the serial number for the FortiGate. |
| Zero touch Provisioning with FortiManager - DHCP method | Use the CLI to configure a DHCP server with option 240, or spoof a DHCP server with a fake FortiManager IP. |
| Zero touch Provisioning with FortiDeploy | Review the FortiGate zero touch provisioning workflow. |
| Zero touch deployment for FortiSwitch | Learn how model devices used for ZTP can also be linked to model FortiSwitches, enabling provisioning of switch settings when first connected. |
| Zero touch deployment for FortiAP | Learn how model devices used for ZTP can also be linked to model FortiAPs, enabling provisioning of switch settings when first connected. |
| Zero touch firmware rectification | Learn how a target firmware version can be associated with model devices, forcing the mapped device (serial number) to upgrade when first connected. |
| Zero touch provisioning - CLI Template with Variables | Learn how to define a CLI template using variables, and to assign those variable definition per-device. |

# Integrated Wireless

## Topology

On the SD-Branch, the FortiGate acts as the wireless controller to manage the FortiAP(s) on that site. Depending on the size of the store, this may mean the deployment of more than one FortiAP. As such, consider the different topologies outlined in the links below.

- Wired Network topology: FortiAP unit can be connected to the FortiGate unit using a *Direct*, *Switched*, or *Connection-over-WAN* deployment.
- Wireless mesh topology: A wireless mesh eliminates the need for Ethernet wiring by connecting WiFi access points to the controller by radio. This is useful where installation of Ethernet wiring is impractical.

## Getting Started

Once you have chosen the topology, you can configure the basic settings. Continuing with our earlier example, each branch may require a guest network for visitors, and a private network for employee devices. The following guide describes how to launch a wireless network for employees and guests.

- Configuring multiple wireless networks using custom AP profiles

## SSID Authentication

While the above outlines a basic deployment scenario, in practice it is important apply strong security to each wireless network that is being accessed. To apply WPA2-Enterprise authentication with RADIUS authentication to an employee SSID, refer to the following topics.

- Replacing the default WiFi certificate
- Deploying WPA2-Enterprise SSID to FortiAP Units

To apply WPA2-Personal with a Pre-shared key or to deploy captive portal for the Guest SSID, refer to the following topics.

- Deploying WPA2-Personal SSID to FortiAP Units
- Deploying captive portal SSID to FortiAP Units

Another method is to apply a Multiple Pre-shared Key (MPSK) for your wireless access. In this method, batch PSKs can be generated and applied to groups. These groups can also have dynamic VLAN assignment to segment the users. The keys can be exported to CSV for administration. To learn more, refer to the following topic.

- Enhance MPSK functionalities for wireless controller

To configure a walled garden that allows users to access certain websites such as the company and store webpage without authentication, refer to the following topic.

- Configuring wildcard address in captive portal walled garden

# Optimization

Once authentication is configured and clients are able to connect to your wireless networks, you may want to perform some optimization to provide the best experience to your users. One optimization to consider is enabling DARRP (Distributed Automatic Radio Resource Provisioning). Through DARRP, each FortiAP unit autonomously and periodically determines the channel that is best suited for wireless communications based on various parameters including total *RSSI*, *Noise Floor*, *Channel Load*, *Spectral RSSI* and more. Refer to the following topic for more information.

- Creating a FortiAP profile with ARRP profiles

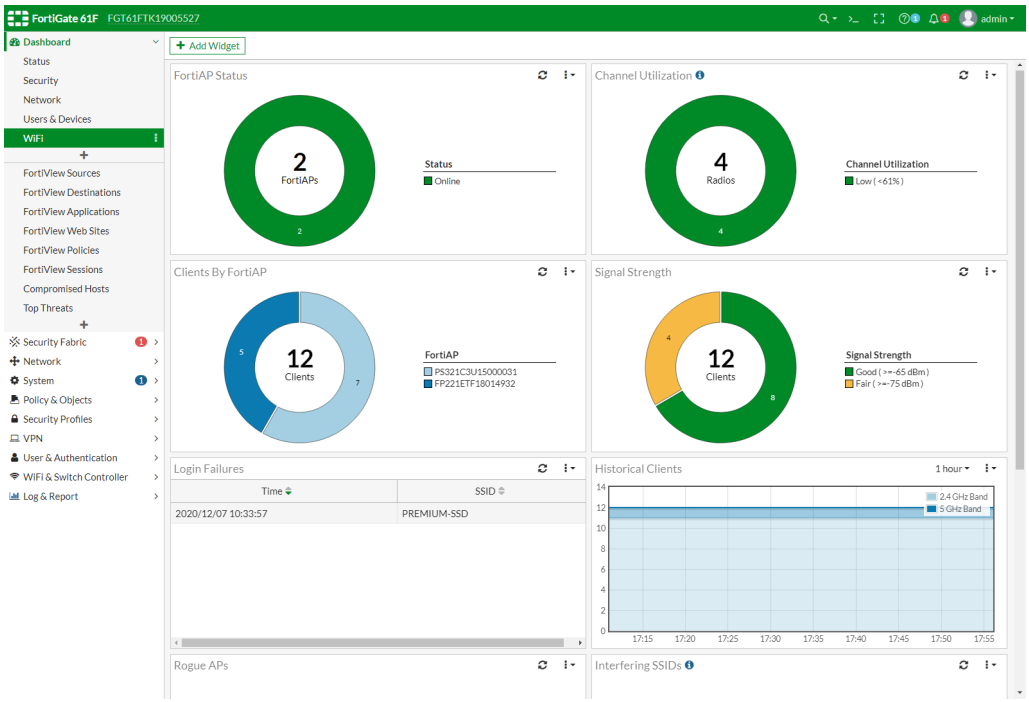
Furthermore, these additional optimizations help control the more granular settings such as ignoring weak signals, disabling low data rates, enabling frequency band load-balancing and more.

- Feature optimization for high-density deployments

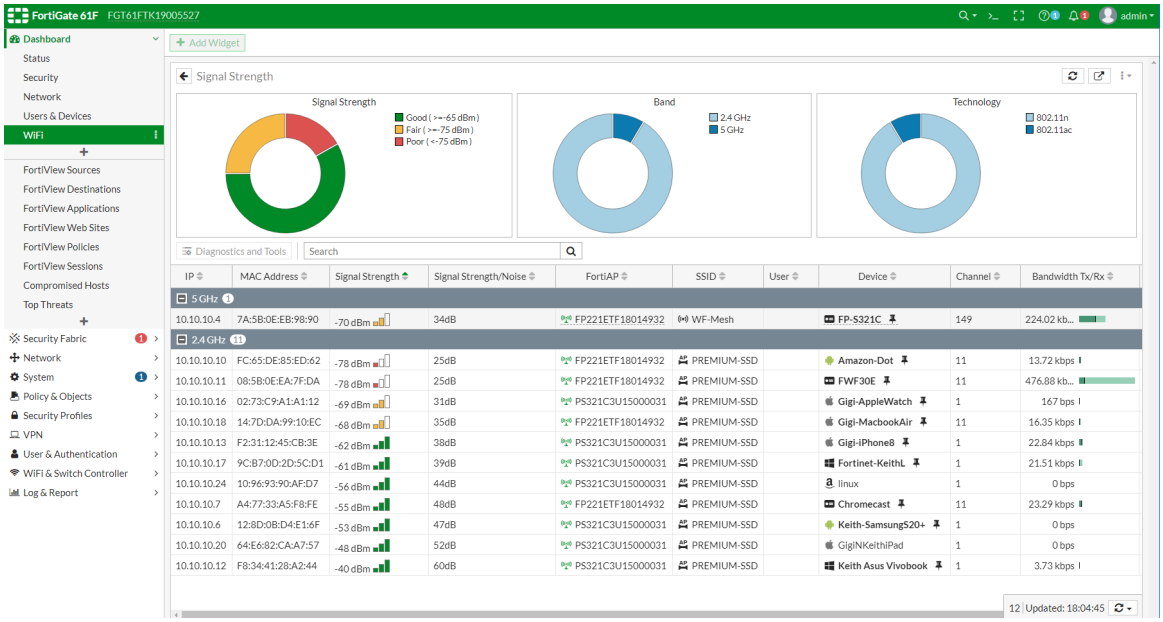
# Fortinet Security Fabric

The key advantage of a single vendor solution is the tight integration between products offered by Fortinet's Security Fabric. The fabric allows users to easily manage and log in to each device. It also enables a single pane view of the wireless network, users, and devices connected to each SSID.

To monitor the health of your wireless network, navigate to your FortiGate's *Dashboard* > *WiFi* page. This default dashboard displays a quick overview of various widgets such as *FortiAP Status*, *Channel Utilization*, *Clients By FortiAP*, *Signal Strength* and more.

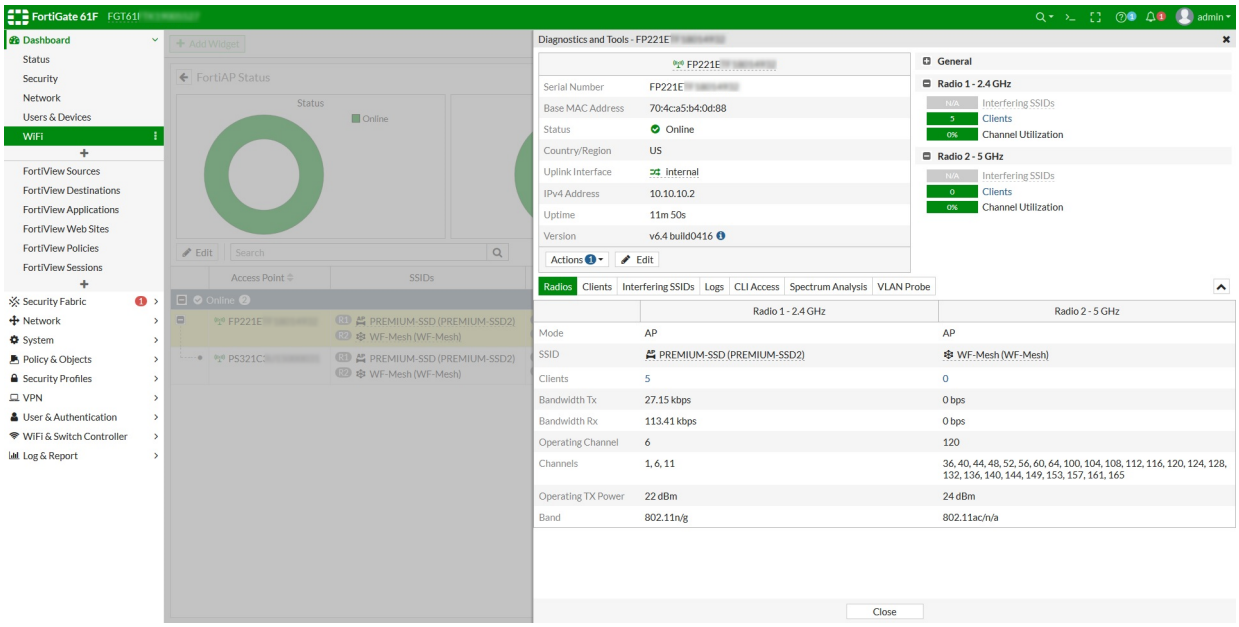



To view detailed drill-down information about the connected devices, expand a widget such as *Signal Strength*.




You can also view WiFi clients from the *WiFi & Switch Controller* > *WiFi Clients* page.

To view the health of the FortiAP and perform diagnostics, right-click a device from the *FortiAP Status* monitor, or *Managed FortiAPs* page to access the *Diagnostics and Tools* page.




To review the capabilities of different monitors on the FortiGate, and new features introduced in FortiOS 6.4., visit the following pages:

- Monitoring wireless health and clients
- Monitoring wireless clients
- Monitoring rough APs
- FortiAP status monitor
- FortiOS 6.4 Wireless new features

# Wireless Orchestration and monitoring

From an orchestration perspective, the FortiManager AP Manager allows the APs controlled by your FortiGates to be managed from the FortiManager. The AP Manager also allows you to authorize and install APs, monitor connected clients and perform spectrum analysis on the managed APs.

The *Wireless Manager (FortiWLM)* management extension further enhances the monitoring capabilities by allowing you to group together wireless controllers, access points and stations in order to view cumulative statistics for the group. This includes *Network Summary*, *AP Group Summary*, *Station Group*, *Application monitoring* and more.

To learn about these features, visit the links below.

- FortiManager AP Manager
- Getting Started with FortiWLM MEA
- Monitoring Devices and Network Traffic

# Presence analytics

FortiPresence leverages WiFi probes detected from visitor smartphones and devices to analyze user traffic and derive usage patterns within a physical store. This cloud-based presence analytics platform complements the SD-Branch setup by providing useful retail analytics formulated through data that are collected via the access points. This solution supports all Fortinet wireless access devices and controllers including FortiGate, FortiAPCloud, and FortiWLC.

The information gathered helps retailers analyze questions about:

- **Location**: Where and how many customers visit an area?
- **Time**: What time of day are customers visiting? How long did they stay?
- **Who**: Are they new visitors or recurring visitors?

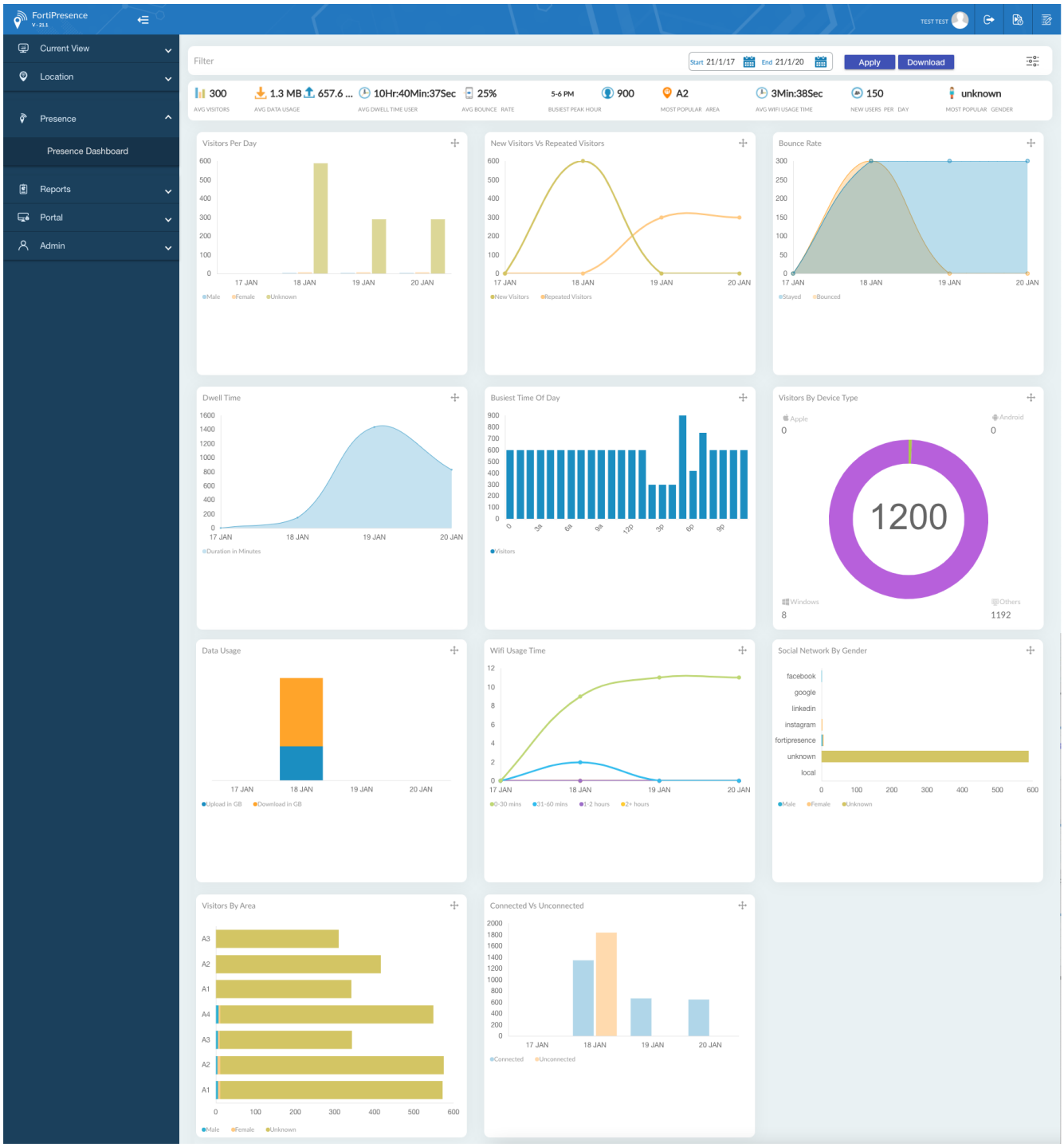
Ultimately, retailers can use the data to draw conclusions on questions such as:

- Why does a store gets more visitors?
- Why did certain visitors stay longer?
- Why did certain areas of the store have longer dwell times?

This gives retailers more power in determining how they design their stores, position products, schedule employees and more, expanding ROI in each branch.

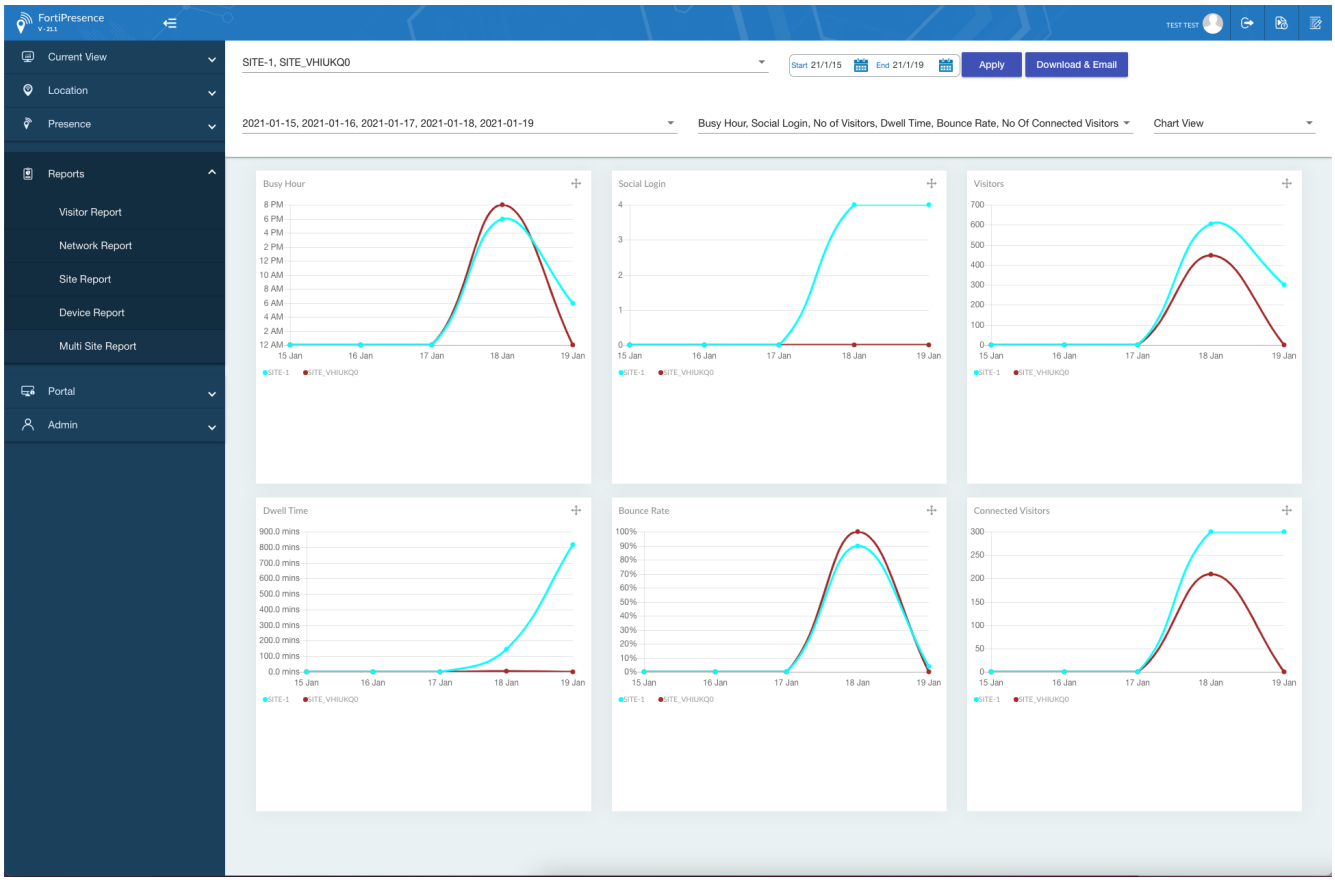
## Presence Dashboard

The *Presence Dashboard* shows a general overview of store usage based on customizable time intervals and site information, allowing you to drill-down on a site, building, floor, and even an area of a store. Average statistics help summarize important stats for a site, while *Visitor*, *Device*, and *Site Analytics* help drill-down on specific behavior.




# Reports

You can build reports to perform visitor, network, device, and site analysis for a particular time period and region. Furthermore, you can compare two sites to determine where one store is doing better than the other.

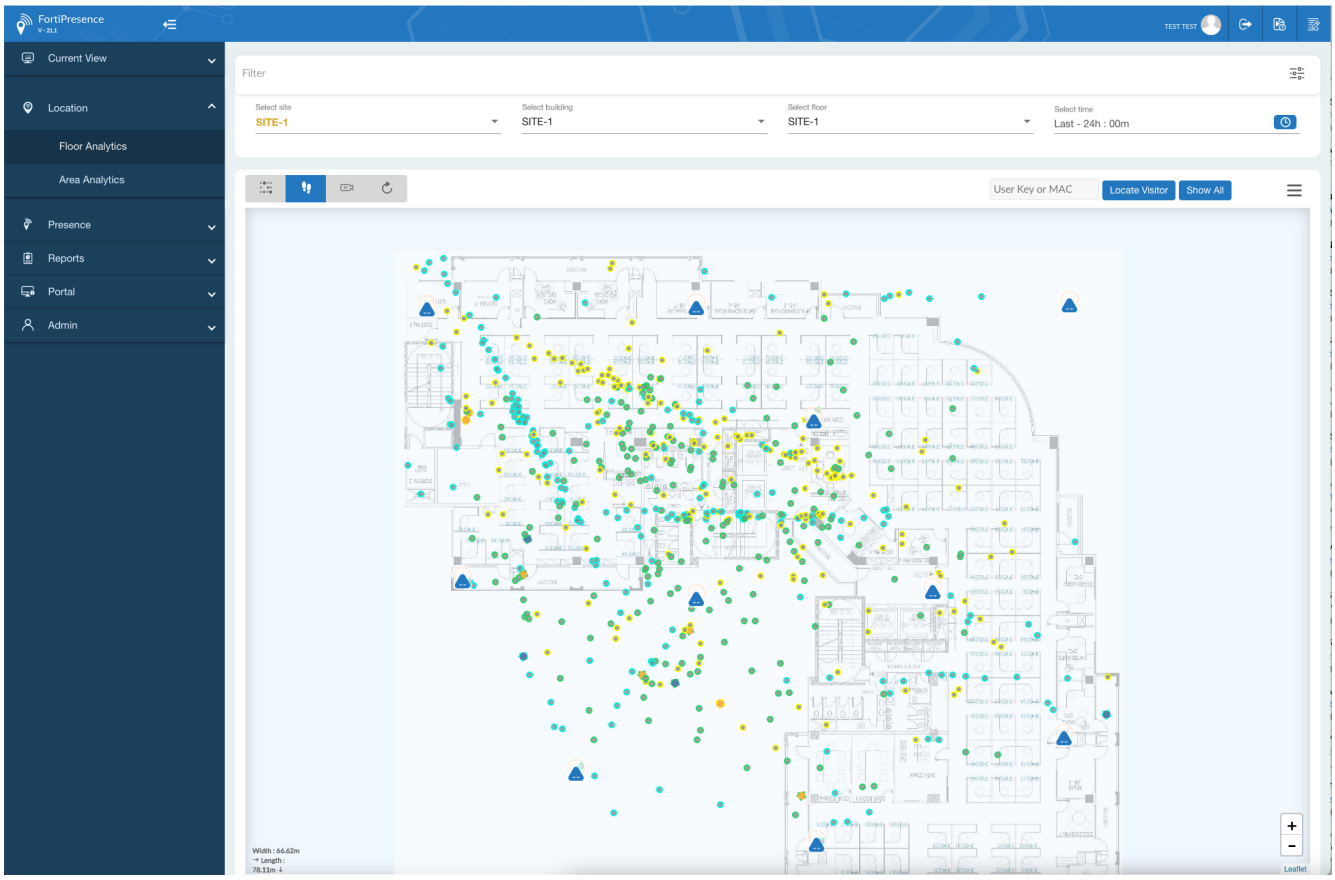



# Location Analytics

FortiPresence Location Analytics provide insights into square footage and customer traffic in a store.

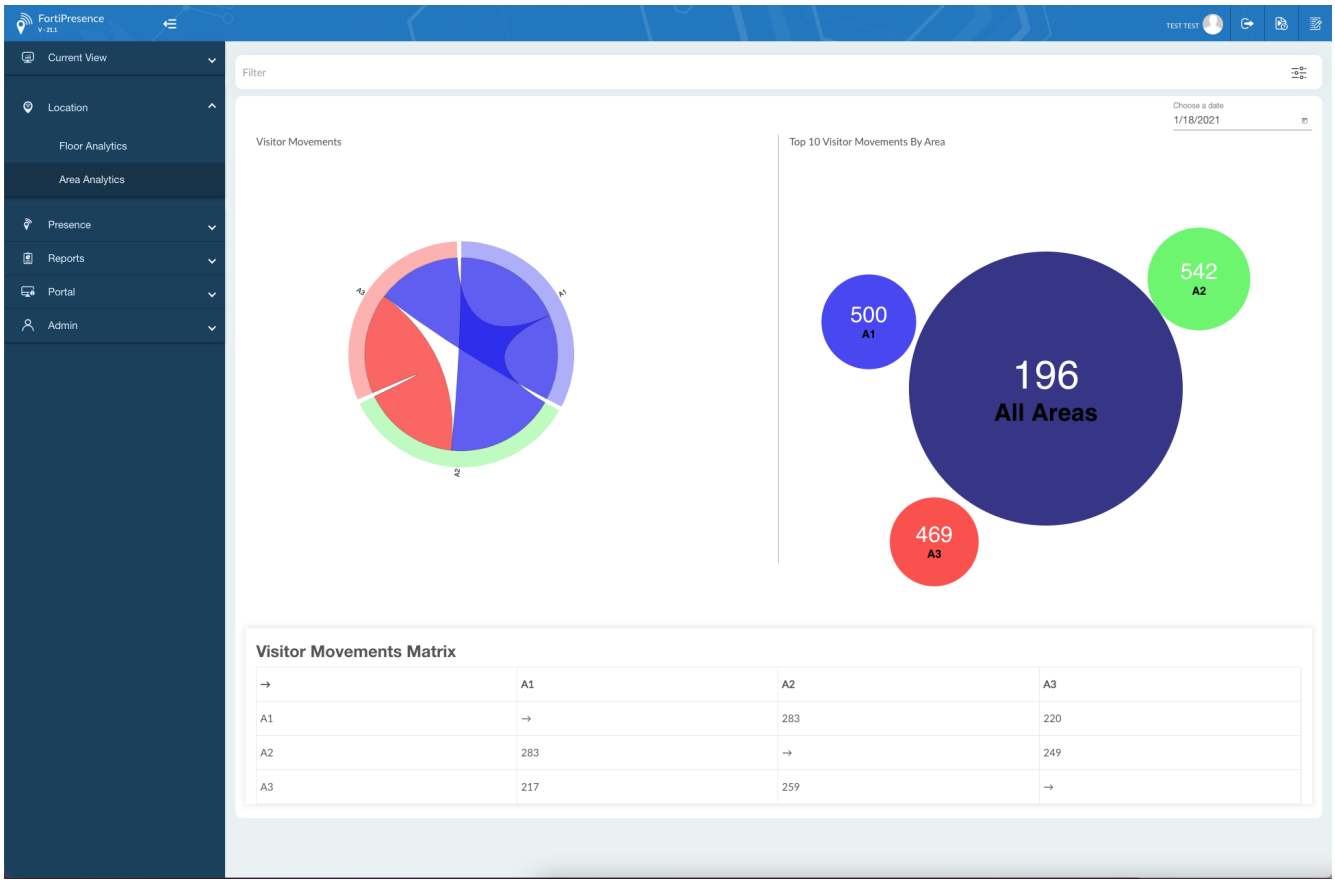
## Floor Analytics

*Floor Analytics* analyze the regions of the store where people are spending the most time. This can be represented based on client device density using heat maps, or based on individual visitor locations using footfall view.




## Area Analytics

*Area Analytics* determine how the foot traffic flows from one area to another.




# Captive Portals and Authentication

FortiPresence provides the means to define portals, a form of customized login pages for visitors to connect to your WiFi network. Portals can be mapped to multiple sites, and multiple portals can be created per site.

Supported authentication methods include Portal Login, Social Login and SMS Login. Each FortiGate, FortiAPCloud or FortiWLC controller must be configured as a RADIUS client on FortiPresence, and point to `radius.presence.fortinet.com` as the RADIUS server. Users will be redirected to the FortiPresence Captive Portal once they connect to the store's available wireless SSID.

# Resources

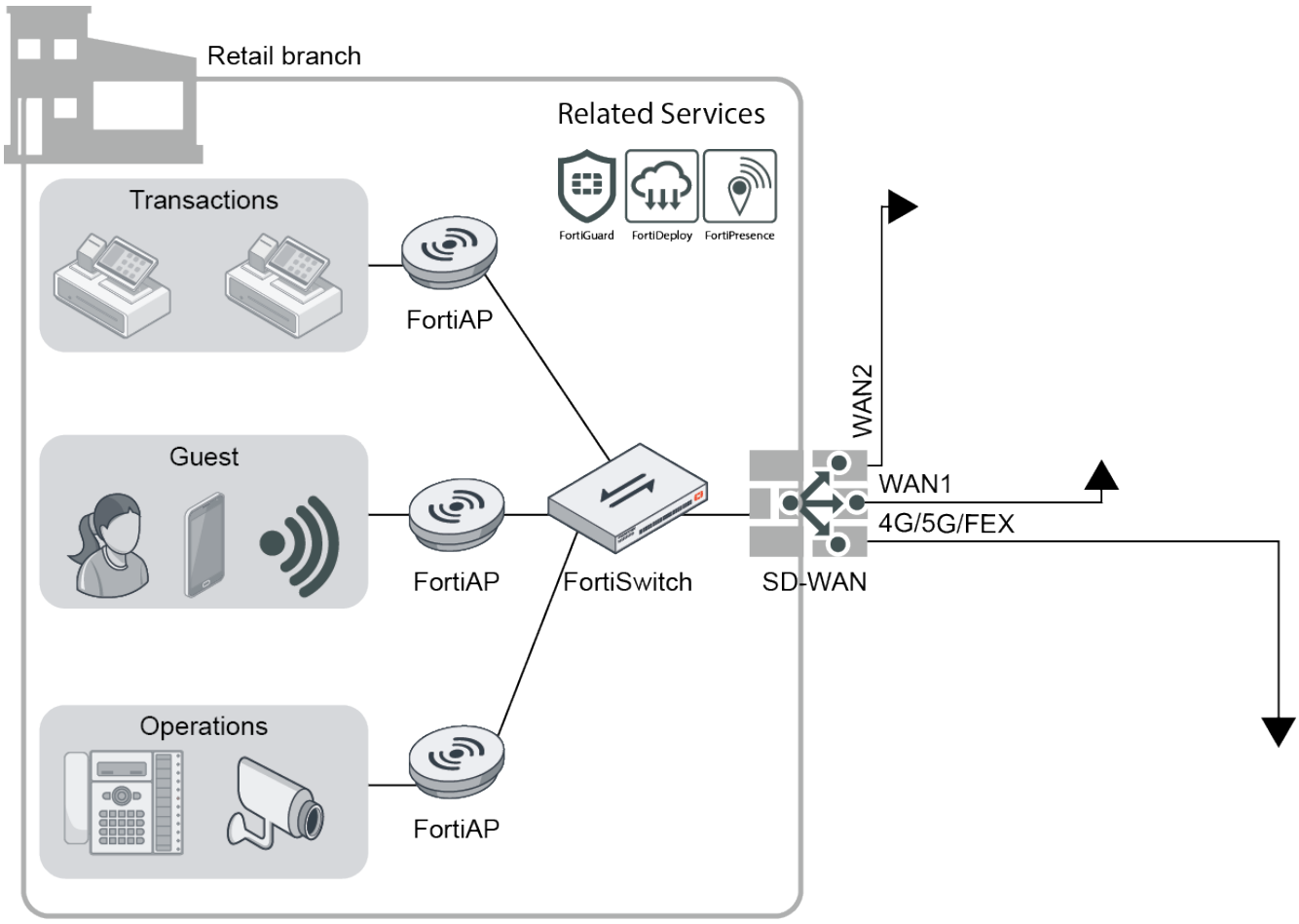
| Topic | Description |
|---|---|
| Presence Dashboard | Filter on time intervals and sites, and drill-down on usage patterns through analytic widgets |
| Reports | Discover the different reports available from FortiPresence |

| Topic | Description |
| --- | --- |
| Location Analytics | Utilize location data to understand your foot traffic |
| Portal Management | Create new portals for logging into your wireless network |
| Configuring Captive Portal | Connect your wireless controller to FortiPresence for Captive Portal authentication |

# Integrated Segmentation

In the previous chapter, we explored the advantages of the single vendor solution in terms of integrating Wireless into the Fortinet Security Fabric. Here, we will explore integrated segmentation through the FortiGate switch controller.

Let's review our Retail branch topology:




While many users will connect to your network over WiFi, there may be devices that still require wired connections such as VoIP phones, POS terminals, security cameras, printers, TVs and desktops. With the variety of devices and security needs, it is necessary to segment these devices in different subnets and VLANs. This can be accomplished with the built-in NAC features on the FortiGate switch controller, allowing you to define rules for segmenting your devices at a very granular level.

# Default VLANs

When you first connect a FortiSwitch to the FortiGate on a designated FortiLink port, the switch automatically recognizes the switch controller and the FortiGate begins to configure the FortiSwitch using its default VLAN template. This template can be customized to define VLANs that are needed for your network. You can also customize the IPs for your subnets used in each VLAN.

Default VLANs include: *default*, *quarantine*, *voice*, *video*, *rspan*, and *onboarding*.

To learn more, visit the following page:

- VLAN interface templates for FortiSwitch units

# Network Access Control (NAC)

With VLANs defined you can group devices into the VLANs by defining NAC policies. NAC policies allow you to specify device matching criterion based on *Device info*, *User logon info*, or FortiClient *EMS Tag*.

**Device Info**: Information recognized by the FortiSwitch and the FortiGate such as *MAC address*, *Hardware vendor*, *Device Family*, *Type*, *OS*, and *User*.

**User logon info**: The firewall user identified by the FortiGate via firewall authentication

**EMS Tag**: If FortiClient is installed on the device and is managed by EMS, the EMS tags can be shared with the FortiGate to identify a user group, device group, or other categories

Once the device is matched, the NAC policy can either assign the port to a specific VLAN, or apply various profiles or policy to the port.

Based on your VLANs and NAC policies, you can define firewall policies to apply the appropriate UTM profiles and allow traffic only to appropriate networks, thereby securely segmenting your devices.

For more information, see the following topics:

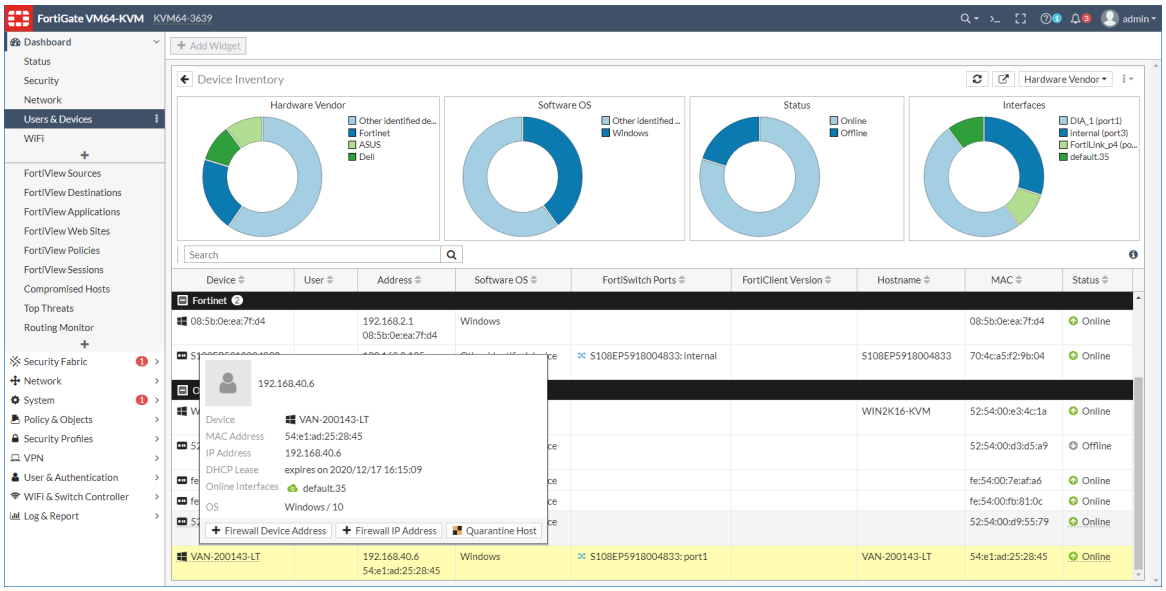
| Topic | Description |
|---|---|
| Configuring the FortiSwitch NAC settings | Configure a FortiSwitch network access control (NAC) policy within FortiOS that matches devices with the specified criteria, devices belonging to a specified user group, or devices with a specified FortiClient EMS tag. |
| Configuring the DHCP trust setting | The DHCP blocking feature monitors the DHCP traffic from untrusted sources (for example, typically host ports and unknown DHCP servers) that might initiate traffic attacks or other hostile actions. |
| FortiSwitch security policies (802.1x) | To control network access, the managed FortiSwitch unit supports IEEE 802.1x authentication. |
| Blocking intra-VLAN traffic | You can block intra-VLAN traffic by aggregating traffic using solely the FortiGate unit. |

# Quarantine

It may be necessary to quarantine a rogue device or rogue user. The FortiGate switch controller can either quarantine users by placing them into the quarantine VLAN, or by directly placing the device MAC in a quarantine address group. Administrators can define firewall policies to handle the type of access a quarantined user has.

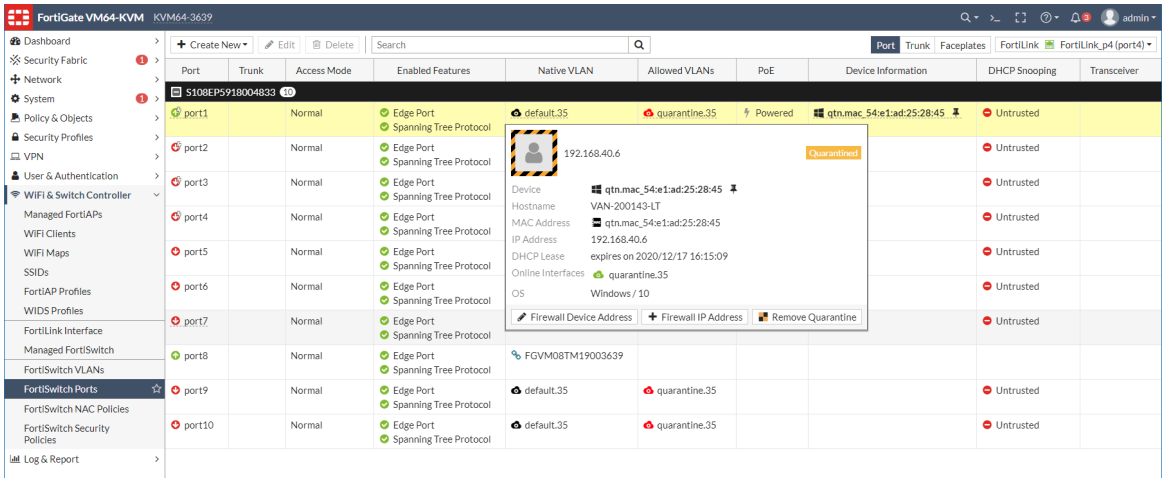
Quarantine can be triggered from several places, including the *Physical Topology* page, *Device Inventory* widget, and from the *FortiSwitch Ports* page.

The image below shows the *Device Inventory* widget, and a device that is connected to the FortiSwitch's port1.




Click the *Quarantine Host* on the device popup to quarantine the user.

The image below shows the same device which is now quarantined on port1 of the FortiSwitch.




Quarantining can also be triggered automatically, by a DDoS policy for example that detects a rogue device. To learn more about quarantining on the FortiSwitch, see:

- FortiSwitch security - Quarantine

# Device Detection

*Device Detection* allows for more granular control and understanding of devices in your network. By enabling device detection on the switches, information about detected devices can be checked against local databases or FortiGuard services to help identify information such as *device*, *vendor*, *family*, and *OS*. This information is used in NAC policies, and it also provides more insight about the devices when viewing it with the FortiGate GUI, CLI, or logs.

See the following topics for more details:

- Configuring IoT detection
- Voice device detection

# Multi-switch Topology

When your network has out-grown your FortiSwitch, you may need to expand to a multi-tiered switching architecture to support the devices in your network.

The following pages can help you determine the best network topology to use.

- Determining the network topology
- Single FortiGate managing a single FortiSwitch unit
- Single FortiGate unit managing a stack of several FortiSwitch units
- Single FortiGate unit managing multiple FortiSwitch units (using a hardware or software switch interface)
- FortiLink mode over a layer-3 network

Finally, many Switch Controller and NAC features were introduced on FortiOS 6.4, including several of the features described in this chapter. See the links below for a more complete list of new features:

- 6.4 Switch Controller features
- 6.4 NAC Features

# PCI Risk Assessment

In the retail environment, PCI compliance and risk assessment are integral to the operations of the organization. PCI auditors look for evidence of:

- Repeatable & consistency processes
- Proactive Monitoring
- Risk Awareness & Reporting

Unfortunately, many organizations are not able to meet PCI compliance due to the reasons above. Other compliance issues are:

- Failed security processes (change management, logging & monitoring)
- System not secured out of the box
- Weak user access management

These gaps may lead to identity theft, data theft and other forms of lost data. The top three reasons are symptoms of a larger problem. As digital adoption expands at a rapid pace, the balance between driving strategic growth in sales and managing regulatory risk become competing priorities. Silo teams begin to form as security decisions are decentralized and applied on different equipment and devices.

A CISO must maintain balance between the customer experience and the accountability of customer's data, ensuring that fast access to data is accompanied by a priority in securing the data in motion and at rest. Customer data needs to be secured and integrated with identity and access control, whether they are using the cloud, local wireless hotspots. or between wired networks.

Furthermore, a CISO must reduce inconsistent and decentralized management, and design a process for standardized baseline images and configurations for devices. Finally, the CISO must produce adequate stakeholder reporting and awareness to continually identify gaps and remediation plans for the system.

The steps outlined below provide the initial start to building a sustainable solution that meets the compliance requirements and strategic needs of the organization. It is not intended to be an end-to-end compliance solution. However, by leveraging the Fortinet Security Fabric and processes outlined in previous chapters, the goal is to drive more consistency and improvements through automation, centralized management, and monitoring.

Step 1. Planning on page 28: Understand what needs to be protected

Step 2. Baseline on page 30: Enable automation and continuous audits of configuration templates

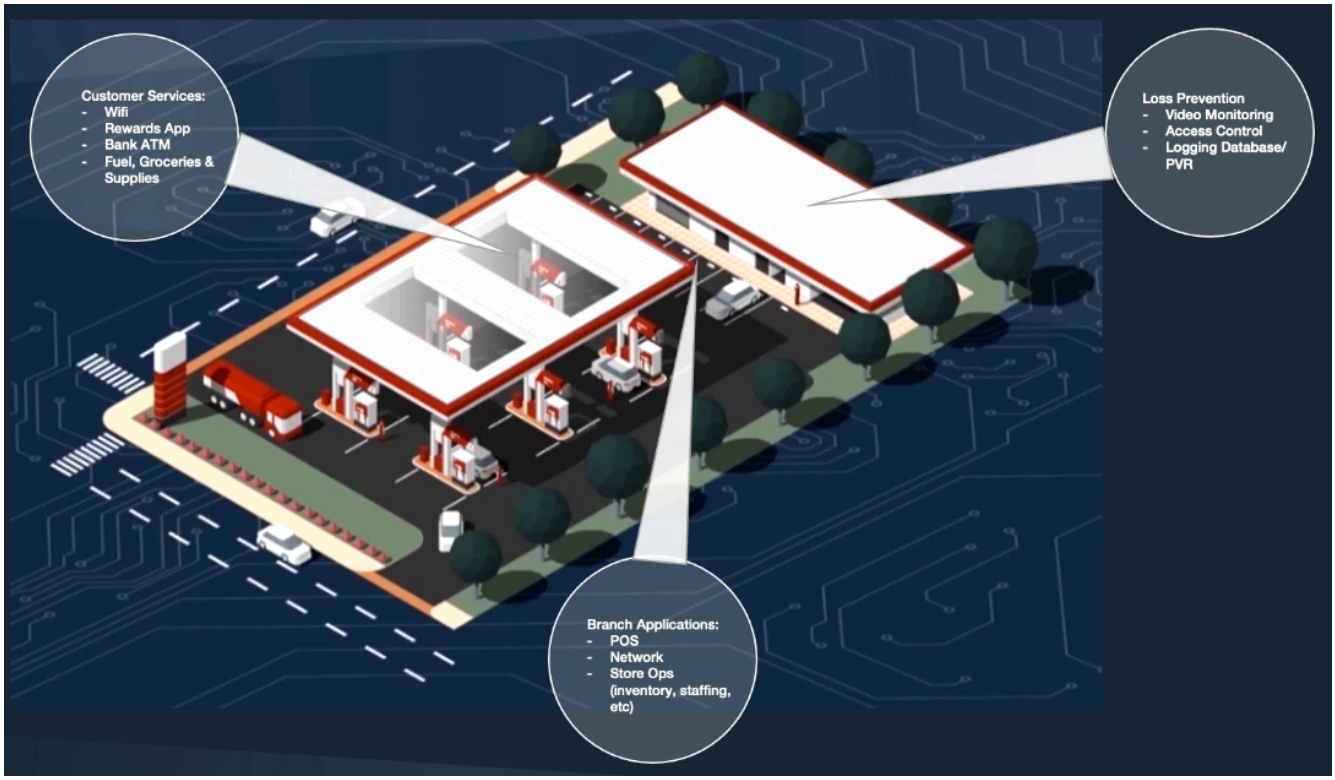
Step 3. Deploy on page 31: Centralize configurations and deployment

Step 4. Monitor on page 32: Report on risk and compliance issues

## Step 1. Planning

Using a gas station as an example, what do we need to protect?

By identifying the various devices and groups, we also identify how they need to be protected and their risk profiles. We can further segment these groups into zones, such as *Customer* zone, *Application* zone, and zone. Security controls can then be applied, limiting access between zones.




| Zone | What do we need to protect? |
|---|---|
| **Customer** | • WiFi<br>• Rewards App<br>• Bank ATM<br>• Fuel, Groceries, and Supplies |
| **Application** | • POS<br>• Network store Ops (Inventory, staffing, etc) |
| **Security** | • Video Monitoring<br>• Access control<br>• Logging Database/PVR |

A basic way to accomplish this would be using *Address Objects* and *Firewall Policies*. Group together branch assets into address groups, then apply firewall policies between zones to enforce access control.

Having an integrated WiFi and switch controller on the FortiGate also increases the granularity in which access control and segmentation can be accomplished. As introduced in the previous Integrated Wireless on page 14 and Integrated Segmentation on page 24 chapters, wireless authentication and *Guest* management help identify users connecting to your network. Furthermore, device detection provides insights into the type of devices used, and NAC policies can help automate which devices need to be placed on which VLAN on the switch for access control.

In a broader scope, each branch may access external resources in the Data center, Cloud and Internet. In the Secure SD-Branch on page 6 chapter, we reviewed how SD-WAN provides the infrastructure to dynamically and securely balance your traffic amongst multiple WAN connections.

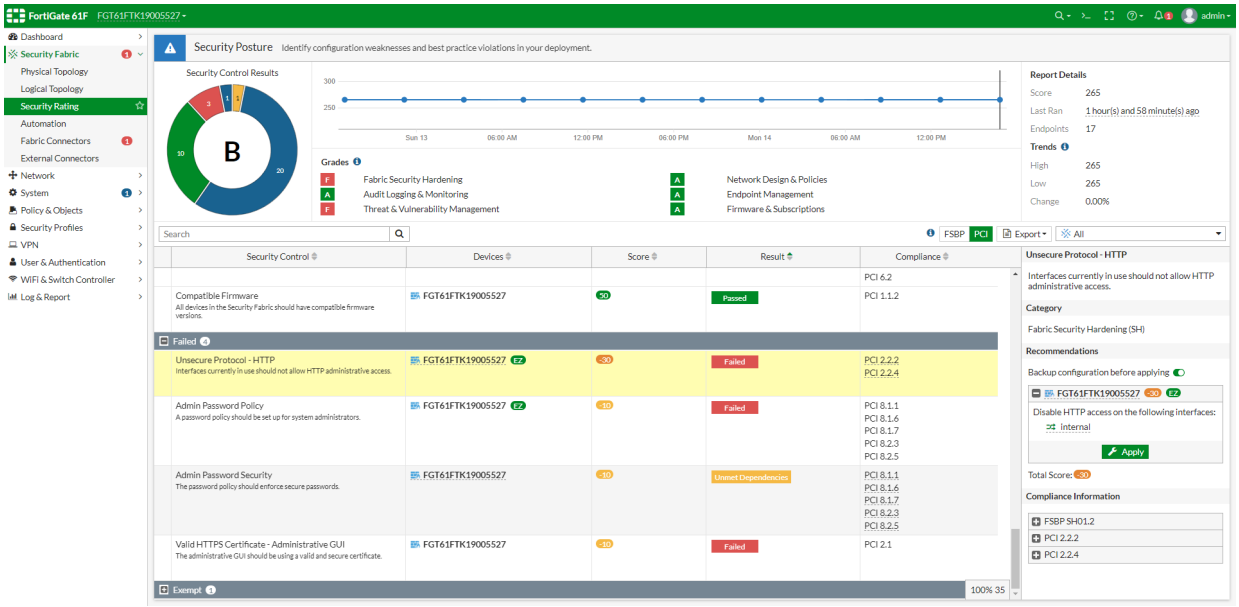
Lastly, *Identity and Access Management* can be centralized with FortiAuthenticator, providing the means to control access to sensitive data. To learn more, see the following links.

- FortiAuthenticator WiFi authentication
- Configure Captive and Self-Service Portals
- Port based Network Access Control (802.1X)

# Step 2. Baseline

Building a baseline configuration helps enable automation and continuous audits of your branches. In Step 1. Planning on page 28, we considered the business needs of an individual branch. This step addresses the need to meet compliance requirements.

Using the *Security Rating* feature on the FortiGate, we can discover any residual security and compliance gaps after the initial configuration. As part of the Security Fabric, *Security Rating* can analyze the *Security Posture* of your Fabric devices, review your Fabric coverage and suggest Optimizations to improve your deployment. The report is able to provide recommendations based on Fortinet Security Best Practices (FSBP) or in PCI terms, allowing customers to take action based on these requirements.




By taking the recommendations to harden your device, you can produce a baseline branch template that meets your compliance requirements. This baseline configuration template can be replicated on other branches to produce a consistent and repeatable process for branch configurations. The *Security report* also helps track the trend on the device, producing a score that enables you to evaluate the *Security Posture*, *Fabric Coverage*, and *Optimization* between different branches.

To learn more about *Security Rating*, and about other Best practices for hardening your FortiGate, visit the links below:

- Configuring and using Security Rating
- Hardening your FortiGate

# Step 3. Deploy

To provision the baseline configuration template, it must first be configured on the FortiManager. There may be many components to a branch configuration, including:

- System configurations
- Policy and objects
- Tunnel configurations
- SD-WAN configurations
- FortiSwitch
- FortiAP and more

Where applicable, you must decide on the proper orchestration method to provision the configurations as outlined in the SD-WAN Orchestration on page 9 chapter.

FortiManager provides the framework for change management, and provisioning configurations using a repeatable and consistent process. By adding additional 3rd party automations as explained in the Zero Touch Provisioning on page 11 chapter, the process can be streamlined to provide cost savings and reduce mistakes caused by human errors.

To learn more about how configurations can be provisioned with various templates, visit the following links.

| Topic | Description |
|---|---|
| Provisioning Templates | This section includes System, Threat Weight, Certificate, and IPsec tunnel templates. |
| Adding a model device by using device template | This section describes how to add a FortiGate model device to FortiManager by using a device template. |
| Firewall Policy and Objects | The Policy & Objects pane enables you to centrally manage and configure the devices that are managed by the FortiManager unit. |
| Central VPN Management | When central VPN management is enabled, you can use the VPN Manager pane to configure IPsec VPN settings that you can install to one or more devices. |
| Using FortiSwitch Manager for central management | This chapter describes how to connect to the GUI for FortiManager and configure FortiManager, provides an overview of adding devices to FortiManager, as well as configuring and monitoring managed device. |
| WiFi profiles for central management | The WiFi Profiles pane allows you to create and manage SSIDs, and AP, Wireless Intrusion Detection System (WIDS), Bluetooth, Quality of Service (QoS), and Bonjour profiles that can be assigned to managed FortiAP devices. |

# Step 4. Monitor

PCI requires a centralized facility to manage all devices across the network to identify any type of fault arising in any branch location and in any particular segment.

FortiManager provides these centralized monitoring capabilities and offers change management for all the security settings. Furthermore, FortiAnalyzer provides the central analysis necessary to analyze and build reports of threats, risks and indication of compromises related to devices on your network.

FortiGate's built-in security rating offers visibility into the state of the security posture on each branch as described in step Step 2. Baseline on page 30.

# Resources

For more on FortiManager and FortiAnalyzer's monitoring and reporting capabilities, visit the following links.

| Topic | Description |
|---|---|
| Monitoring managed devices | Review the different options for monitoring managed devices, inlcuding the quick status bar, device dashboard, device configurations, and more. |
| AP Manager Health Monitor | The Health Monitor displays information about *AP Status*, *Client Count Over Time*, *Top Client Count*, and *Top Wireless Interference*. |
| Monitoring Devices and Network Traffic on Wireless Manager (FortiWLM) | Monitor the network as well as individual devices in the network |
| FortiSwitch Manager Monitor | The FortiSwitch Manager Monitor pane shows a graphical representation of the connected FortiSwitch devices. |
| Monitoring SD-WAN on SD-WAN Manager | The SD-WAN Monitor evaluates whether the interface is meeting performance SLA criteria. |
| Monitoring SD-WAN on SD-WAN Orchestrator | The SD-WAN Orchestrator monitors the global network as well as individual devices in the network by using the Monitor tree menu. |
| Monitoring IPsec VPN tunnels | View the list of IPsec VPN tunnels. You can also bring the tunnels up or down. |
| FortiAnalyzer Situation Awareness Report | This *Situation Awareness Report* identifies issues on the NIST CyberSecurity framework and provides recommended actions. |
| FortiAnalyzer SOC View - FSBP Summary Dashboard | The *Best Practices Overview* monitor shows aggregated security rating results based on different geographical regions (EMEA, APAC, North America, and South/Latin America). |