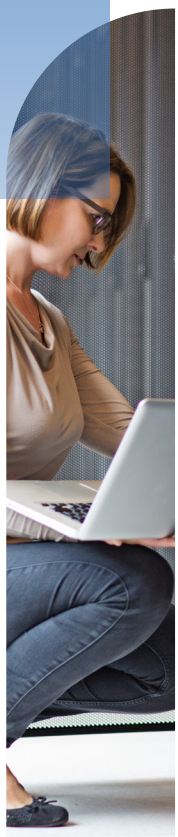
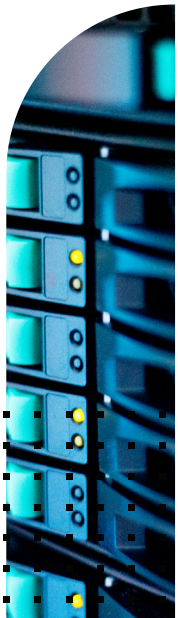
DEPLOYMENT GUIDE

# Fortinet Secure SD-WAN

## Solution Overview and Architecture Guide





# Table of Contents

## Executive Summary

Many organizations are still connecting their wide area networks (WANs) with very old technology. For decades, the hub-and-spoke network architecture portrayed in Figure 1 has been commonplace. All network traffic flows through the central corporate data center—including traffic moving from branch locations to the internet. Branch traffic travels to the data center using dedicated connections, usually multiprotocol label switching (MPLS) circuits.

But a set of forces collectively known as digital transformation (DX) is quickly changing that model. These trends include the digitization of virtually everything in business, the emergence and growth of cloud-based services like Software-as-a-Service (SaaS), and the proliferation of Internet-of-Things (IoT) devices at the network edge. Together, these revolutionary changes necessitate new approaches to networking.

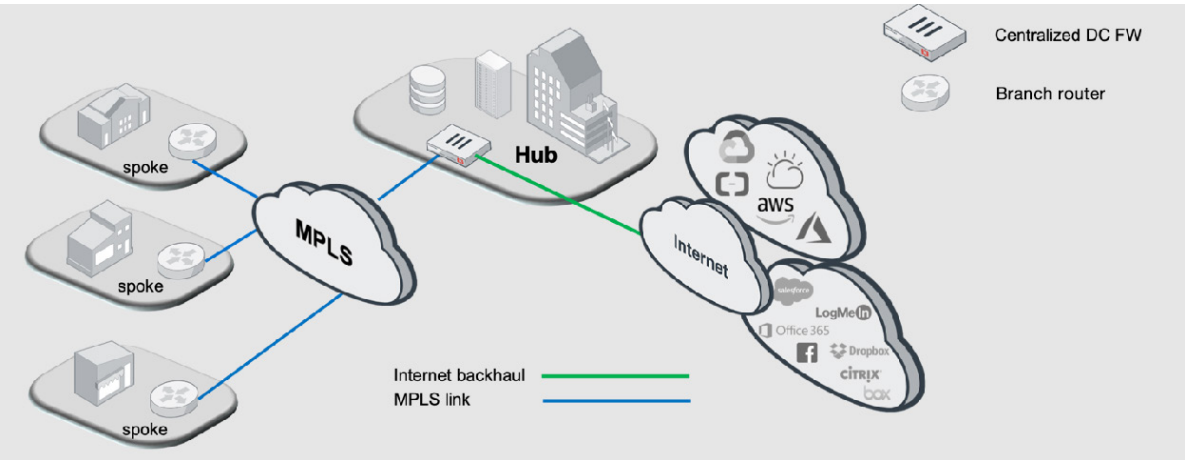



Figure 1. Legacy WAN hub-and-spoke architecture.

To address the needs of such a widely distributed network, many businesses have embraced solutions such as a software-defined WAN (SD-WAN) alongside lower-cost connectivity options for businesses. As a result, many organizations have undertaken major WAN edge transformation projects in recent years.

To support these goals, Fortinet Secure SD-WAN leverages:

- WAN path remediation
- Path failover (moving flows from an underperforming transport to a better performing transport)
- Link aggregation (taking advantage of multiple WAN transports)
- Active path performance metrics

Logically speaking, Fortinet SD-WAN determines which path best meets performance expectations or service-level agreements (SLAs) for a particular application and assigns application flows to that WAN path.

## Legacy WAN Architecture: Simple but Inadequate

The simplicity of the legacy WAN architecture in Figure 1 is evident, specifically with routing. Its hub-and-spoke design requires each remote site to route all non-local traffic to the hub, regardless of the final destination. Typically, this calls for a single, static route. Legacy WAN architectures consisting of aging hardware and software solutions continue to provide network connectivity and a consistent level of performance and security, and some organizations continue to be satisfied with them.

However, if an organization needs to add redundancy or additional bandwidth to a legacy WAN infrastructure, complexity can increase quickly. Leveraging private connectivity in a full-mesh approach, for example, would require either multiple static routes or the introduction of a dynamic routing protocol such as Border Gateway Protocol (BGP) or equal-cost multi-path (ECMP) routing.

### Inefficient routing, inferior performance

Even if an organization avoids this complexity, its network traffic is extremely inefficient. Consider a branch user's legacy path to the internet in Figure 1. In order to arrive at Google's search engine website for a simple search, for example, the application flow would need to:

- Cross the branch WAN edge
- Navigate across the MPLS circuit
- Enter the data center
- Negotiate its way through a centralized security stack—firewall, intrusion prevention system (IPS), antivirus/anti-malware (AV/AM), data loss prevention (DLP), web filter, etc.
- Travel to the Google website through the data center internet edge

The minimal infrastructure required at the branch was traditionally seen as a key benefit of legacy WAN architecture. However, it has largely fallen short of expectations concerning user experience. At a time when consumers have almost universally been using broadband connections at home for more than a decade, legacy WANs do not generally reflect typical broadband speeds. As more and more of employees' work days are spent using cloud-based services, performance has only declined.

### Security gaps and bottlenecks

The ability to centralize the security stack was also previously seen as a benefit of legacy WAN architecture. Branch sites typically have a simple router for connectivity to an MPLS or other private WAN circuit. Because all flows must first traverse the WAN, it made sense to centralize advanced security capabilities at the core instead of building distributed stacks at each branch. Unfortunately, flows failing security policy must traverse the WAN before they are inspected. As a result, infected hosts are often permitted to freely communicate throughout the enterprise network because security only exists within the data center, and site-to-site traffic therefore passes without inspection.

Another issue with the centralized security stack is performance. As traffic increases—especially traffic bound for the internet and cloud-based resources—security inspections can become a bottleneck, with legitimate traffic waiting in line behind traffic that may not be permitted to continue.

## Transforming the WAN Edge

Modernization of a WAN infrastructure is not just about replacing end-of-life hardware or software. WAN edge redesign is a business solution, not simply a technology requirement. Budgets are growing to accommodate DX not because organizations prefer to consume cutting-edge technology, but because their customers are demanding this technology. The hope of improved user experience and increased productivity loosens purse strings and provides necessary budgetary resources for technology leaders to initiate WAN transformation projects.

SD-WAN is one of the primary innovations behind WAN edge modernization. Its core capabilities include multi-path control, application awareness (such as with SaaS solutions), and the resultant dynamic application steering. These capabilities enable network traffic to be routed over the public internet or over private infrastructure—whatever is most efficient for application performance and availability in a multi-cloud environment.

### SD-WAN offers advantages

Figure 2 illustrates a modernized SD-WAN branch edge solution that manages a hybrid architecture inclusive of both private WAN (MPLS) and broadband internet connectivity. This model offers several advantages over the legacy architecture shown in Figure 1.

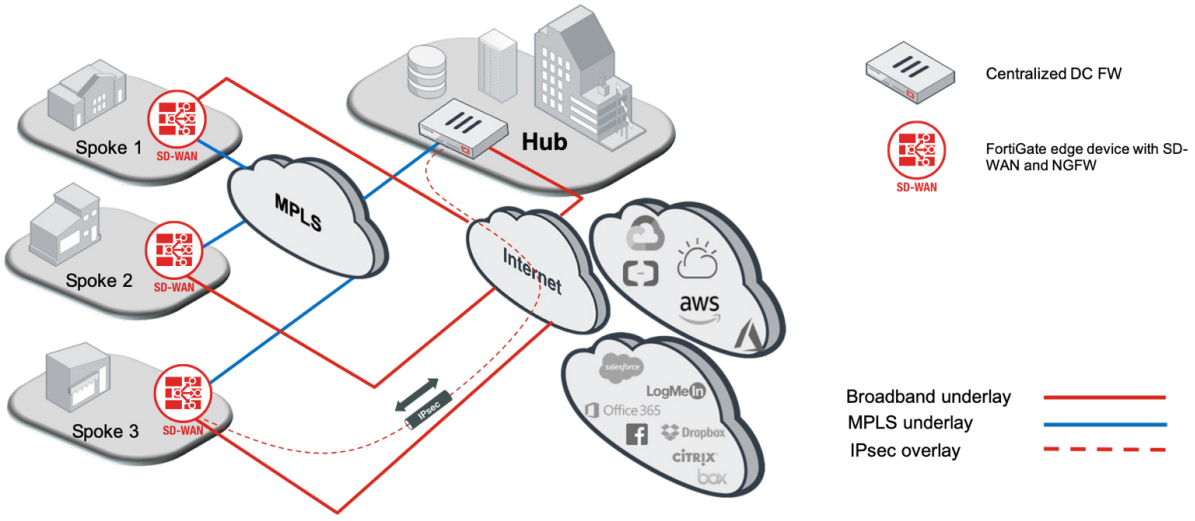



Figure 2. Modernized SD-WAN architecture.

First, the branch has multiple transports, or connectivity options. In this example, the corporate WAN MPLS network remains, but this organization has introduced a single broadband connection to provide direct internet access (DIA) from the branch. In addition, the organization has established an overlay network using Internet Protocol security (IPsec) tunnels between branches and the data center over the broadband internet transport. The result is that multiple paths are possible from the branch to both the data center and a multi-cloud environment.

Compare this with legacy single-path architecture in, a switch connected to a simple router with one connection to a private WAN. Essentially, there is only one option for egress traffic. But introducing DIA inherently provides for a redundant connectivity architecture. In terms of data center connectivity, the overlay network (IPsec tunnel) delivers an alternative path for critical applications that would normally traverse the MPLS. In the same way, the private WAN path will continue to provide its path to the internet but is now superseded by the DIA connection.

## Secure SD-WAN reduces risk

Secure SD-WAN adds the advanced security capabilities of a next-generation firewall (NGFW) to the networking solution. It is no accident that the icon in Figure 2 representing the SD-WAN device at the branch edge looks like a firewall. This is because introducing DIA at the branch also establishes direct connectivity to a volatile threat landscape. Such connectivity did not exist in the legacy architecture, which routed all traffic through a centralized security stack. The DIA necessitates that the centralized security stack give way to a more distributed security architecture.

In a multi-cloud environment with many SaaS solutions, it is especially important that the secure SD-WAN solution be able to distinguish between applications to leverage the full functionality of the solution. In addition to distinguishing applications and controlling a multi-path environment, a secure SD-WAN solution provides dynamic application steering (packets or sessions) to traverse available paths to the corporate WAN or the multi-cloud environment. To aid application steering, it provides active path metrics. In conjunction with customer-defined SLAs, the SD-WAN policy engine determines which paths are viable transports for each application, choosing the best path or balancing traffic between multiple viable paths.

## Supporting DX initiatives

In summary, for this high-level secure SD-WAN architecture example, DX is the driver for branch edge modernization. Organizations are spinning up projects to address WAN connectivity models (MPLS, broadband, Long-Term Evolution [LTE]), edge device consolidation (router, firewall, advanced security, etc.) and adding SD-WAN functionality in order to improve branch-user experience, maintain application performance, and sustain application availability.

## Modern WAN Architecture Requirements

This section addresses defining a few key business requirements for WAN architecture modernization projects at most companies. Organization-specific requirements should be developed with input from stakeholders across the organization—not just IT leadership.

### Improving branch user experience

Most employees go home at the end of the workday to broadband access with speeds of 50 Mbps, 100 Mbps, or even as much as 1 Gbps. In most cases, these employees are not experiencing similar transfer rates at their office location. To help improve user experience at the office, there is a need to understand where application servers reside and the path that requests traverse to these destinations. Essentially, improving user experience means reducing latency between branch edge and application servicer location. With the increase in cloud adoption, many organizations achieve this simply by adding a DIA path that does not have to traverse a private WAN prior to navigating the internet. Figure 3 lists the digital branch requirements for the organization in terms of accessing resources over the WAN.

| | |
|---|---|
| 1 | Business-critical applications located in the data center shall prefer the existing MPLS path(s) and alternatively via the internet overlay if the MPLS link is unavailable or in SLA brownout status. |
| 2 | Traffic between branches and the data center shall always be encrypted using IPsec (overlay network required). |
| 3 | Dynamic and direct branch-to-branch communication shall be enabled to avoid complex full-mesh topologies. |
| 4 | Cloud-based critical applications (SaaS) shall prefer a DIA path to benefit from lower latency and higher performances, and alternatively backhauled through the hub via the MPLS overlay in the event of ISP underlay issues.<br>If cloud on-ramp is available, SaaS applications shall be steered over the closest cloud POP for maximum acceleration. |
| 5 | Noncritical applications (i.e., generic internet browsing) shall utilize only a DIA path. |
| 6 | Branches shall be protected from malware, viruses, and internet attacks. |

Figure 3. Typical digital branch WAN requirements.

### Reducing operating expenses

Without question, WAN transformation projects can help organizations realize significant savings in operating expenses (OpEx). Of course, firms are often able to take advantage of low-cost, high-bandwidth broadband connectivity to replace expensive private circuits—or at least avoid adding additional circuits.

But the savings may not stop there. Another means of reducing OpEx (and potentially capital expenses [CapEx]) is through device consolidation. A secure SD-WAN device can potentially consolidate up to five network and security vendors and up to seven distinct solutions at the branch edge. The contract with each vendor includes licensing, training, and support costs, so this consolidation saves both monetary and staff resources.

Admittedly, some organizations desire a defense-in-depth approach or possess a multivendor strategy. However, more customers today are willing to forego these preferences to achieve significant cost reduction.

## Guaranteeing edge security

WAN edge solutions that deliver anything short of a fully integrated NGFW are not delivering a secure SD-WAN edge solution. Security services handoffs to third parties often fall short of OpEx reduction whether the solution is on-premises or in the cloud. Further, security architecture at the edge is different from security architecture at the core. Since the early 2000s, unified threat management (UTM) devices have protected many small and midsize businesses (SMBs) and small enterprises with the set of capabilities depicted in Figure 4.

These same devices are capable of providing sufficient security for distributed enterprise branch locations and provide services including NGFW, IPS, secure sockets layer (SSL) inspection, web content filtering, anti-malware gateways, and advanced routing (protocol) compatibility. Device consolidation reduces solutions into a single, comprehensive secure SD-WAN solution, and addresses the aforementioned two requirements.

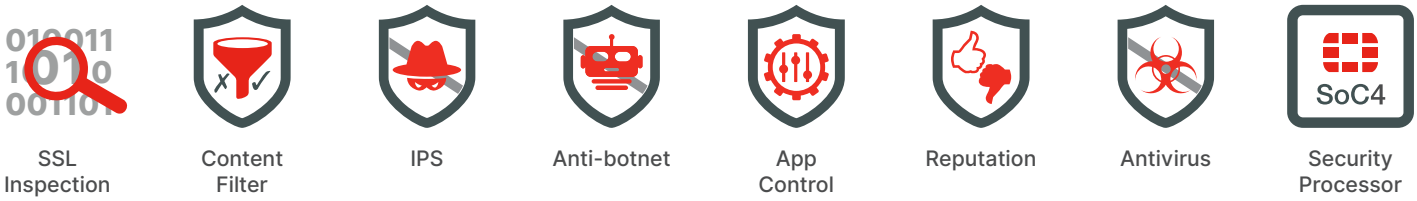



Figure 4. Security requirements.

## Simplifying branch architecture through consolidation

While introducing an intelligent WAN edge device allows for branch modernization with DIA capabilities, network administrators should look for solutions that avoid increased complexity in branch architecture. They should seek SD-WAN vendors whose solutions allow for functional consolidation of network and security so that the branch equipment footprint can be kept at a minimum. Functions such as intelligent WAN path selection, advanced routing, and security should run in an integrated manner in the WAN edge device, while guaranteeing the maximum level of scalability and performance.

To draw a comparison with the gaming and artificial intelligence (AI) world where graphics processing units (GPUs) are designed to offload graphics rendering compute from the central processing unit (CPU), WAN edge devices should be designed so that CPU-intensive networking and security processes are offloaded to specialized hardware such as application-specific integrated circuits (ASICs) and security processing units (SPUs), as illustrated in Figure 5.

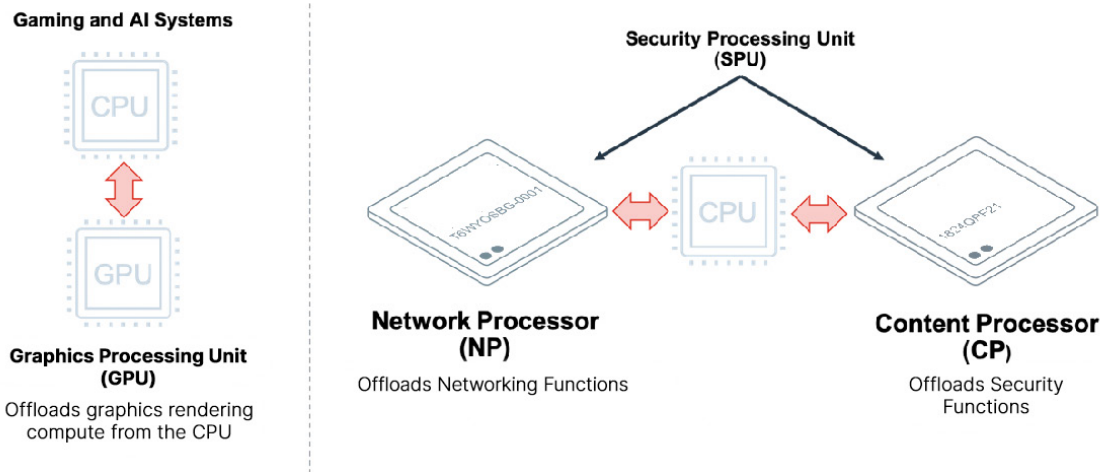



Figure 5. Modern System-on-a-Chip (SoC) architecture.

## Fortinet Secure SD-WAN Architecture

Fortinet Secure SD-WAN consists of several components:

- FortiGate NGFW, which runs FortiOS, the core of Secure SD-WAN
- FortiManager, for the orchestration and management plane
- Fortinet SD-WAN Orchestrator to further simplify and automate the deployment
- FortiAnalyzer for advanced analytics and automation
- FortiDeploy for zero-touch provisioning (ZTP)

No other vendor provides such a comprehensive secure SD-WAN solution. Figure 6 shows the components of the Fortinet Secure SD-WAN architecture, including the items mentioned above, along with additional Fortinet solutions that extend beyond SD-WAN. This provides complete coverage across the branch to further build out the Fortinet Security Fabric, providing broad visibility, integration, and automation for organizations.

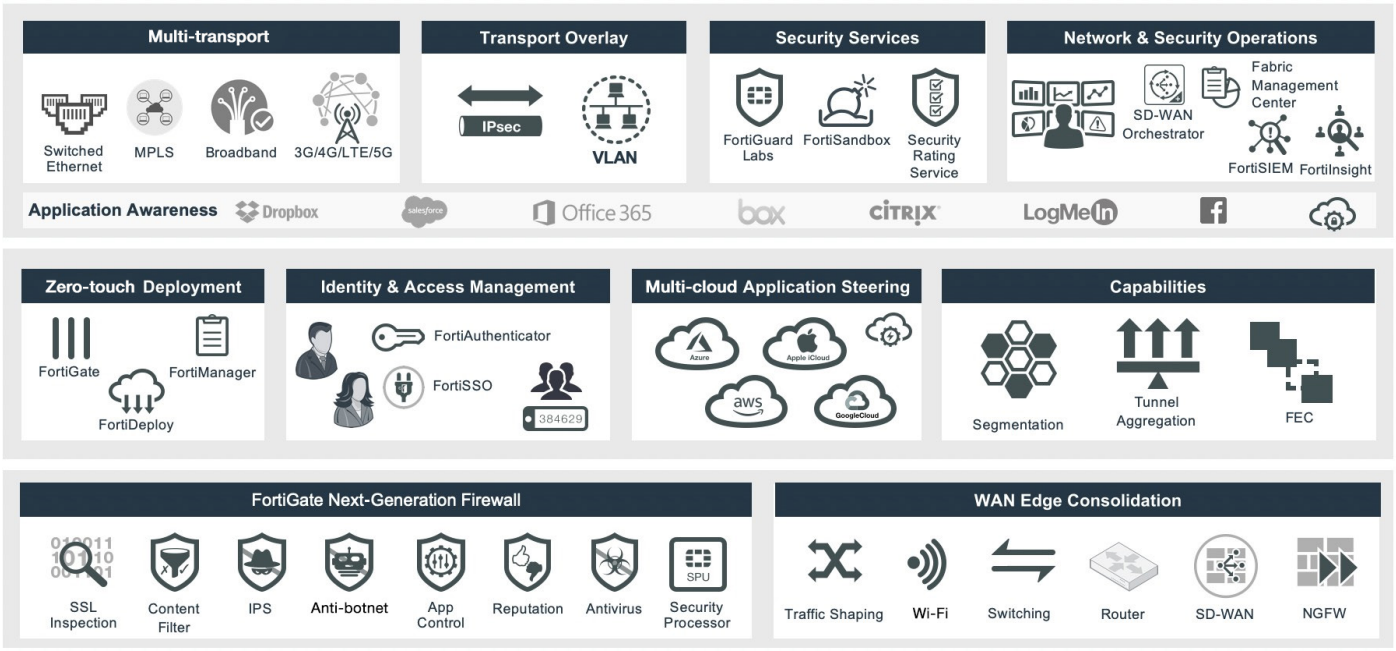



Figure 6. Fortinet Secure SD-WAN architecture components.

The FortiGate device, with its underlying firmware FortiOS, is the basic component of the Secure SD-WAN solution. Acting in all roles (the management, control, and data planes), FortiGate is a proven solution that easily consolidates WAN edge solutions into one comprehensive device. In addition to NGFW, advanced security features, and SD-WAN, FortiGate also:

- Delivers advanced routing support (RIP, BGP, OSPF, and more)
- Participates in virtual private network (VPN) pairing as a spoke or hub (concentrator)
- Brings WAN optimization via protocol optimization and byte and object caching
- Supports traffic shaping and packet priority to ensure that business-critical applications take precedence

## The benefits of a controllerless-based architecture

A major differentiator from other SD-WAN vendors, Fortinet Secure SD-WAN offers a controllerless-based architecture where each FortiGate device maintains control-plane autonomy at the branch edge. What this means is that the solution does not require a centralized or cloud-based controller to provide control-plane operations for application steering. Instead, each FortiGate edge device operates independently to evaluate available path efficacy and choose the most appropriate path for applications to traverse the WAN, whether the selected link be an overlay interface (IPsec) or an underlay interface (MPLS, DIA).

## A unique, unbeatable design

At the same time, this architecture maintains a centralized approach for full monitoring, management, analytics, and reporting capabilities over the entire enterprise deployment. To achieve this, FortiManager acts as a single pane of glass to simplify operations. Figure 7 demonstrates how each FortiGate edge device communicates with centralized components, but maintains all control-plane functionality at the edge. Transport-agnostic link support, SD-WAN core capabilities and services, and NGFW services are all delivered throughout the enterprise without dependency for control-plane input from an external device.

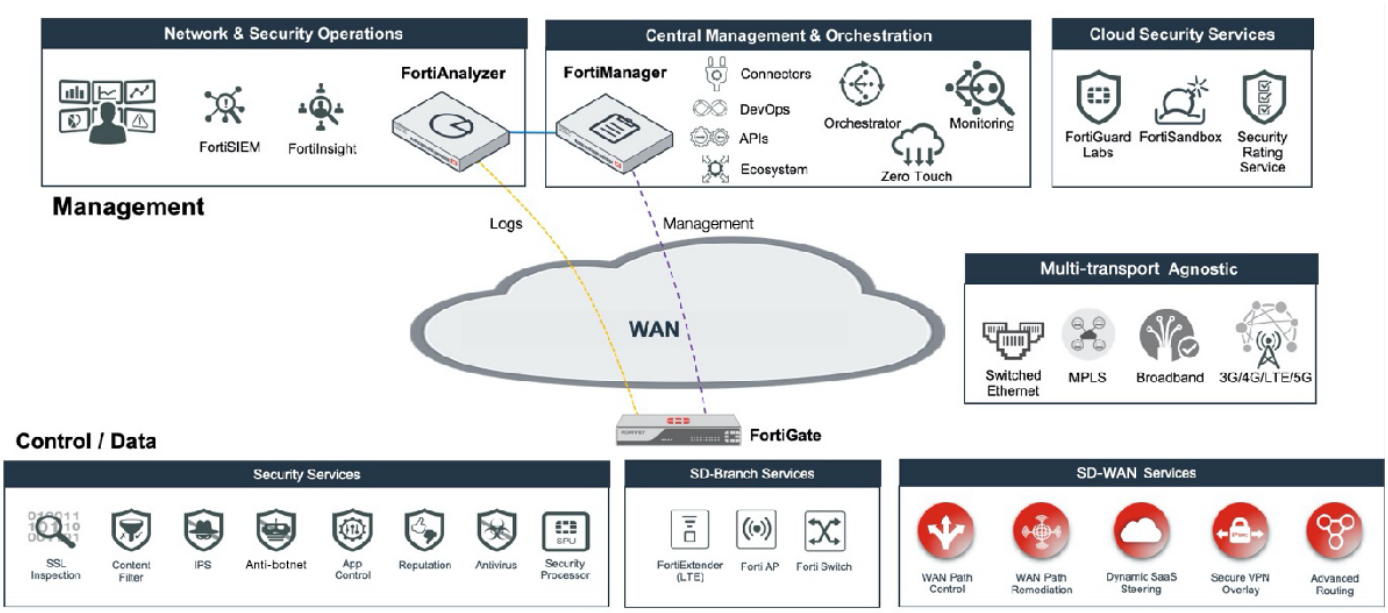



Figure 7. Fortinet Secure SD-WAN Controllerless Architecture.

This unique design has the merit of providing support for large-scale deployments with over 15,000 endpoints. This, combined with a purpose-built SPU system architecture and the world's first SD-WAN ASIC embedded into Fortinet F-Series branch device models, makes Fortinet Secure SD-WAN unbeatable when it comes to performance and scalability.

To justify this bold statement, consider how this approach allows organizations to implement a future-proof secure SD-WAN solution at scale and at the pace of their business. Figure 8 depicts a common secure SD-WAN deployment scenario. This implementation constitutes a hub-and-spoke topology with several branches, each provided with an MPLS link to the hub and a broadband link via a local internet service provider (ISP).

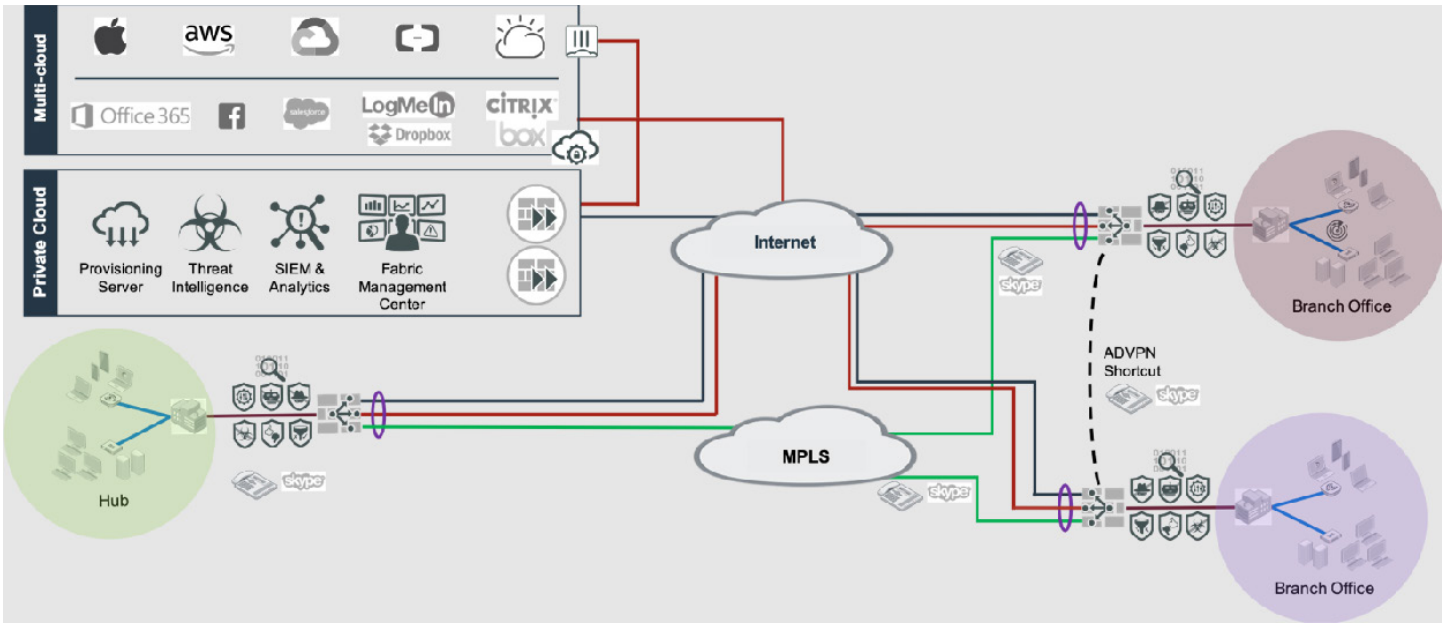



Figure 8. Secure SD-WAN topology with direct branch-to-branch communication (dynamic shortcuts).

## Design principles

Fortinet proposes a unique Secure SD-WAN design approach to overcome limitations imposed by the controller-based solutions typically offered by pure-play SD-WAN vendors, as shown in Figure 9.

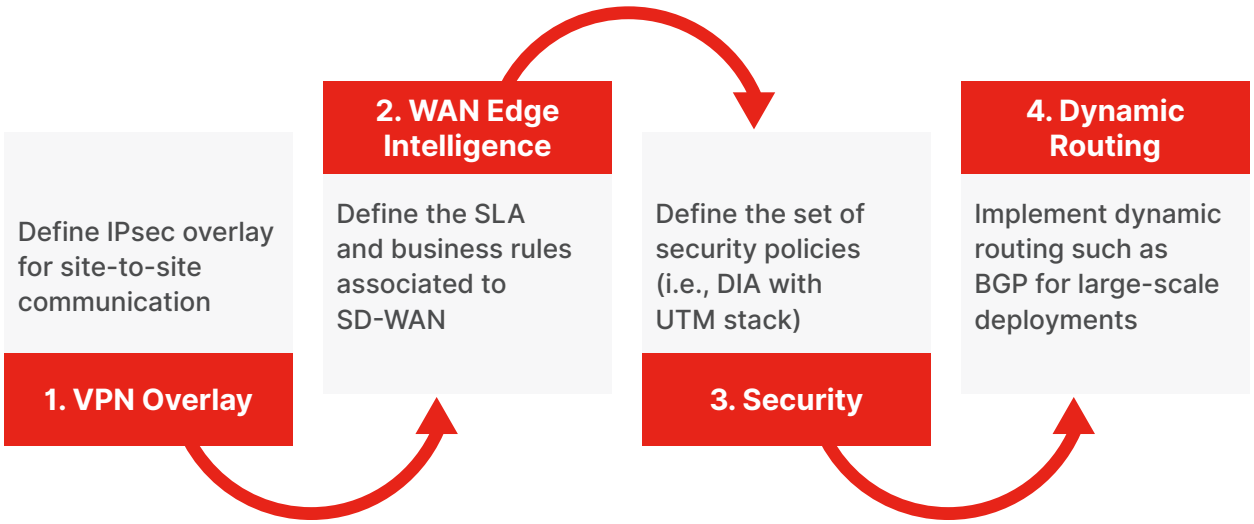



Figure 9. Fortinet Secure SD-WAN design principles.

This approach is based on the following key design principles:

1. **Establish an internet overlay network.** Building an overlay network between the hub(s) and spokes not only provides necessary traffic protection required to address requirement 2 below but also simplifies overall routing of the solution as described later in requirement 4. Fortinet delivers the highest level of IPsec scalability in the market, offering support from 200 to 40,000 IPsec tunnels in a single platform. Additionally, to enable branch-to-branch communications without the complexity of a full-mesh topology (requirement 3), Fortinet Secure SD-WAN employs an auto-discovery VPN to establish dynamic shortcut tunnels.

2. **Enable edge intelligence with SD-WAN.** As mentioned above, the intelligence in Fortinet Secure SD-WAN (i.e., the control plane) is embedded in each FortiGate edge device and does not require a centralized controller. All SD-WAN core capabilities and related processes are handled directly at each branch edge on the FortiGate device, including:
   - WAN path control (application identification, WAN path metrics, dynamic steering)
   - WAN path remediation (forward error correction and packet-based distribution)
   - Cloud optimization (Infrastructure-as-a-Service [IaaS]/Saas application steering)
   - WAN optimization

   This approach ensures that implementing a sophisticated SD-WAN policy for networks consisting of thousands of sites will not hit a limit imposed by a centralized controller. In terms of scalability, this means that the limit is effectively imposed by the maximum number of IPsec tunnels supported by the hub rather than in the control-plane capacity. The difference in numbers presents to Fortinet a significant advantage compared to other pure-play SD-WAN vendors.
3. **Security policies.** The third key design aspect involves security policies and how the implementation of security, to address customer requirement 6, may affect scalability for large networks. Typically, companies have addressed security independently from networking, deploying multiple point solutions at the edge. This siloed approach not only increases complexity in the overall architecture and solution management but results in poor scalability and higher costs. Additionally, scalability is dictated by the lowest common denominator device, which becomes the bottleneck for the whole chain. Companies looking at implementing security and SD-WAN at scale should consider this factor carefully and look for solutions with built-in advanced security capabilities like Fortinet Secure SD-WAN.

   Fortinet Secure SD-WAN security policies constitute an essential part of the SD-WAN configuration, ensuring that all outgoing and incoming traffic is adequately inspected at Layer 7 and compliant with corporate security policy prior to egressing the branch edge. In addition, the same application detection and deep packet inspection (DPI) engine used for security purposes is used to set up SD-WAN application steering rules, therefore ensuring a deep and consistent level of visibility across all applications. Recall the distributed nature of Fortinet Secure SD-WAN concerning scalability to perform DPI at the edge (for a single branch) in comparison with a centralized security stack that must perform similar services for all branches.
4. **Dynamic routing.** Setting up appropriate routing relationships and policies is key to ensuring that a secure SD-WAN solution scales without increasing complexity. This is why dynamic routing is the fourth key design principle for deploying Fortinet Secure SD-WAN. The routing approach separates the underlay network from the overlay network. While the underlay network can still be configured using dynamic or static routes, mainly for the purpose of establishing the Internet Key Exchange (IKE) traffic for the IPsec tunnels, all the internal hub and branch prefixes are advertised using internal BGP (iBGP) across this overlay network.

   Using this approach, new branches can be easily added to the network. By using a specific BGP configuration with neighbor groups and neighbor ranges, branches will dynamically join the BGP network neighborhood without having to configure each neighbor separately, therefore eliminating the need to update the hub with specific settings for each one any time a new branch is turned up or decommissioned. A later section of this document provides a sample routing configuration for a dual hub-and-spoke scenario.

   With the introduction of SD-WAN Orchestrator starting in FortiManager 6.4.1, the implementation of the VPN overlay and associated BGP routing configuration is completely automated, further simplifying large-scale SD-WAN deployments.

Last but not least, for a network that needs to scale to thousands of sites, having VPN, SD-WAN, firewall policies, and routing embedded in the same device provides a huge benefit from a cost consolidation perspective. Additionally, with central management for the entire scope of functionality, Fabric Management Center (FortiManager and FortiAnalyzer) eliminates complexity and greatly reduces the risk of manual configuration errors commonly associated with having to manage service-chained environments or those with numerous point products.

# Fortinet Secure SD-WAN: A Closer Look

Based on the fundamental design pillars of an SD-WAN deployment described in the previous section and illustrated in Figure 3, this section delves more deeply into each pillar.

## VPN overlay construction

As mentioned above, IPsec (VPN) connections are instrumental in Fortinet Secure SD-WAN deployments. As an overlay interface, IPsec tunnels sometimes exist in some level of multiplier of the underlay interfaces. For instance, Figure 10 depicts an enterprise utilizing multiple ISPs for both the branch and the data center.

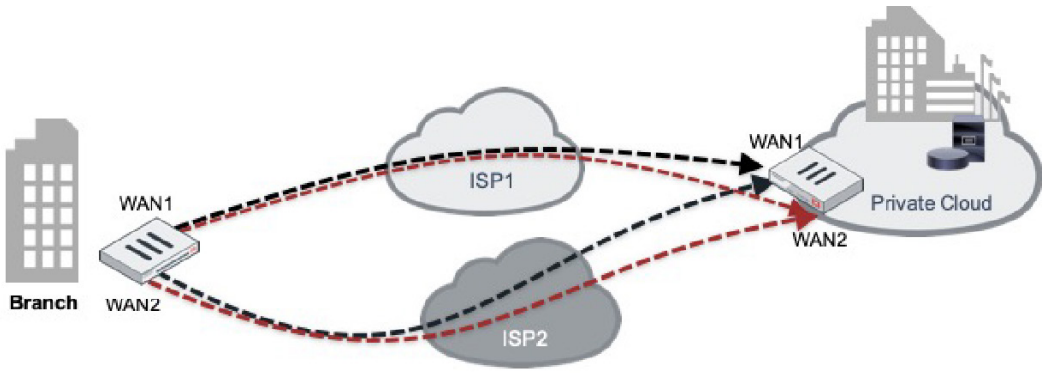



Figure 10. IPsec overlay interfaces.

For simplicity, the diagram omits the underlay transports, but there are two underlay interfaces on each side labeled WAN1 and WAN2. From these two interfaces, this organization has created four overlay interfaces on the branch FortiGate. Essentially, there is full mesh of connectivity between the underlay interfaces using IPsec tunnels. In total, this organization may choose (if it is consistent with design requirements) to add six interfaces to the SD-WAN virtual WAN (vWAN) link. That would consist of the two underlay interfaces and the four overlay interfaces.

As an aside, FortiOS also supports aggregate IPsec interfaces with SD-WAN. As a result, an organization could leverage multiple unique IPsec tunnels between two FortiGate devices in an aggregate interface and distribute application flow packets across both tunnels (presumably riding different underlay interfaces) to maximize throughput.

FortiGate supports numerous connections for IPsec tunnels and architectures, from hub-and-spoke to partial-mesh to full-mesh VPN architecture. Figure 11 depicts the overall WAN architecture with a typical hub-and-spoke architecture.

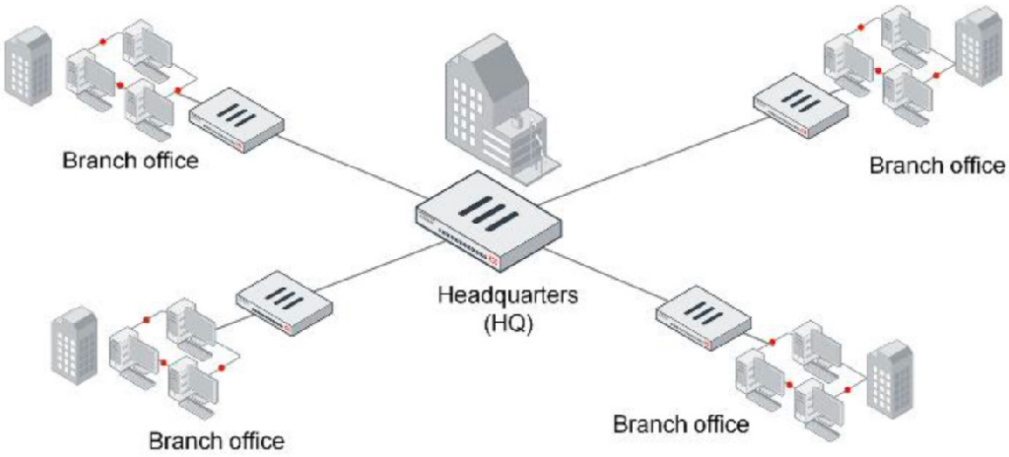



Figure 11. Hub-and-spoke WAN (VPN) architecture.

In this architecture, a path between branches must first traverse the hub. Further, in a legacy WAN environment, all traffic (internet, multi-cloud, WAN) would also pass through the hub. However, with WAN edge modernization, each of these branch sites would likely be improved with a DIA path, allowing Fortinet Secure SD-WAN to optimize path selection and protect application performance and availability. This occurs whether the application resides in the corporate data center or in a multi-cloud environment.

FortiOS provides Auto-Discovery VPN (ADVPN), a means to dynamically negotiate on-demand IPsec (shortcut) tunnels between spoke sites with the assistance of the hub site. This capability requires the use of routing protocols so that spokes can learn routes from one another (via the hub, configured as a route reflector).

Once IPsec tunnels are configured, these interface(s) can be added as members of the SD-WAN vWAN link. This will allow organizations to leverage performance SLAs, SD-WAN policy, security policy, and prioritization for this interface, as part of the SD-WAN vWAN link.

**Note: SD-WAN Orchestrator simplifies construction of the overlay network and reduces management associated with building templates for configuration and policy. SD-WAN Orchestrator also includes a self-contained environment for monitoring and analytics for applications and WAN links. For more about SD-WAN Orchestrator visit https://docs.fortinet.com/sdwan.**

## WAN edge intelligence

FortiGate Secure SD-WAN is largely made up of autonomous underlay and overlay interfaces aggregated into a single vWAN link. The digital branch requirements depicted in the previous section can be implemented using Fortinet Secure SD-WAN as shown in Figure 12 and via FortiManager screen captures (below).

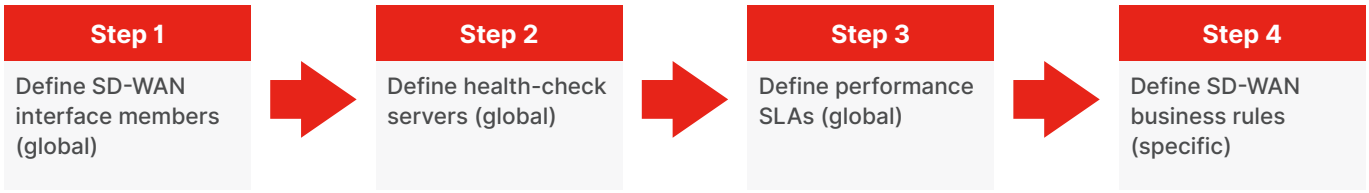
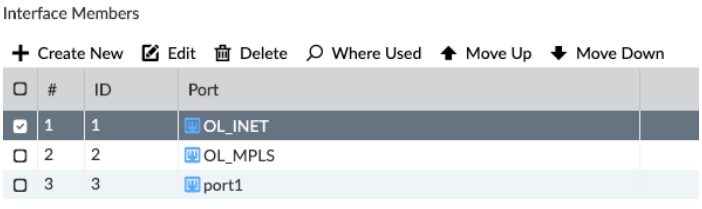


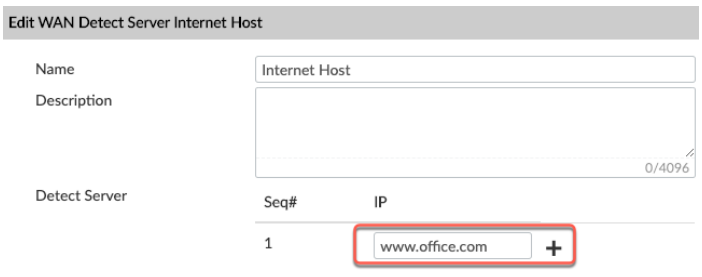

Figure 12. SD-WAN edge intelligence process flow.

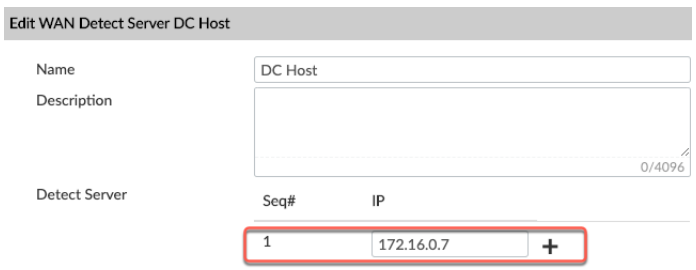
### SD-WAN application steering policy

**Step 1 (global setting): Define SD-WAN interface members.** In the picture to the right we can see how both underlay and overlay interfaces can be added as members of the SD-WAN virtual link.

**Step 2 (global setting): Define health-check servers that will be used for validating the performance SLAs.** For example, an internet host based on office.com (right) or a data center host (below).

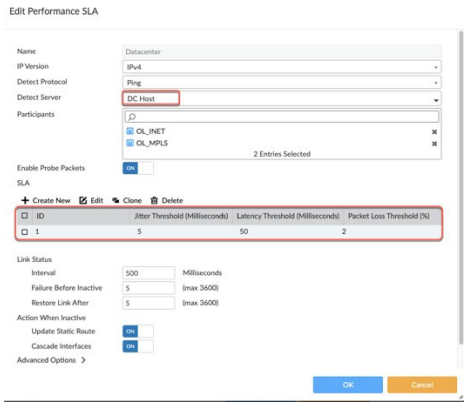


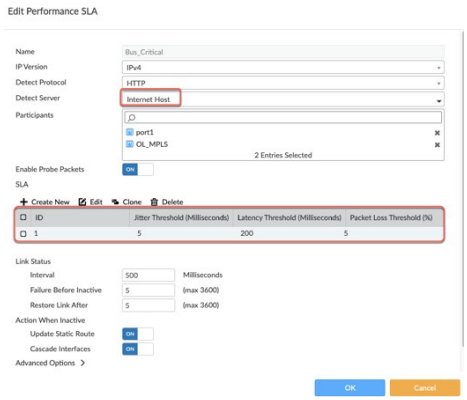
**Step 3 (global setting): Define performance SLAs based on probing the health-check servers defined in step 2,** either in the corporate data center or the internet. Different methods such as ping, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP) echo, Two-Way Active Management Protocol (TWAMP), User Datagram Protocol (UDP) echo, and Domain Name System (DNS) are available. An example of an SLA (right) is based on a data center server that will be validated only if the following conditions are met:

- Jitter less than 5ms
- Latency less than 50ms
- Packet loss less than 2%




**Step 4: Define SD-WAN rules according to the business policies set out by the organization.** An example of an SLA (right) is based on a Fully Qualified Domain Name (FQDN) server that will be validated only if the following conditions are met:

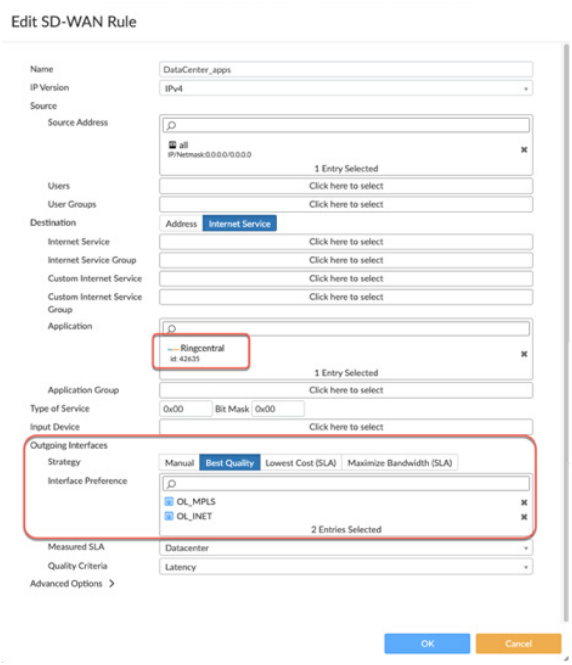
- Jitter less than 5ms
- Latency less than 500ms
- Packet loss less than 2%




Looking at digital branch requirements described in Figure 3, below is how the SD-WAN rules would look from an implementation standpoint.

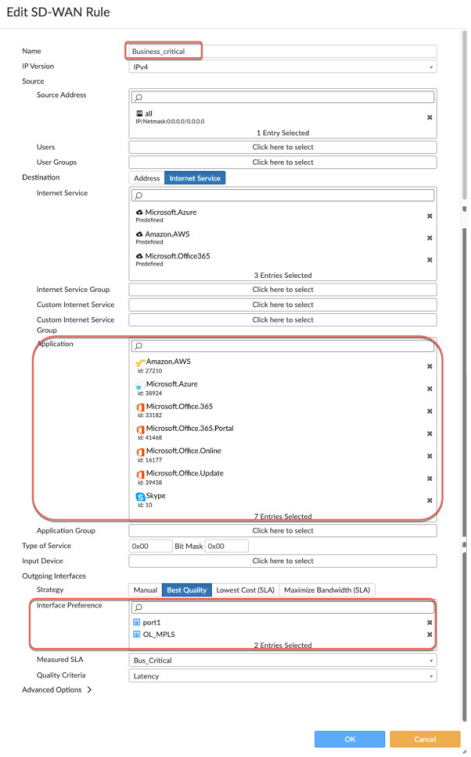
### Business-critical applications are located in the data center

Strategy: Select the MPLS overlay as long as the SLA is met and fall back to the broadband overlay if performance declines below the threshold. In this case we assume the critical app is RingCentral, a VoIP application. (Strategy: Best Quality)



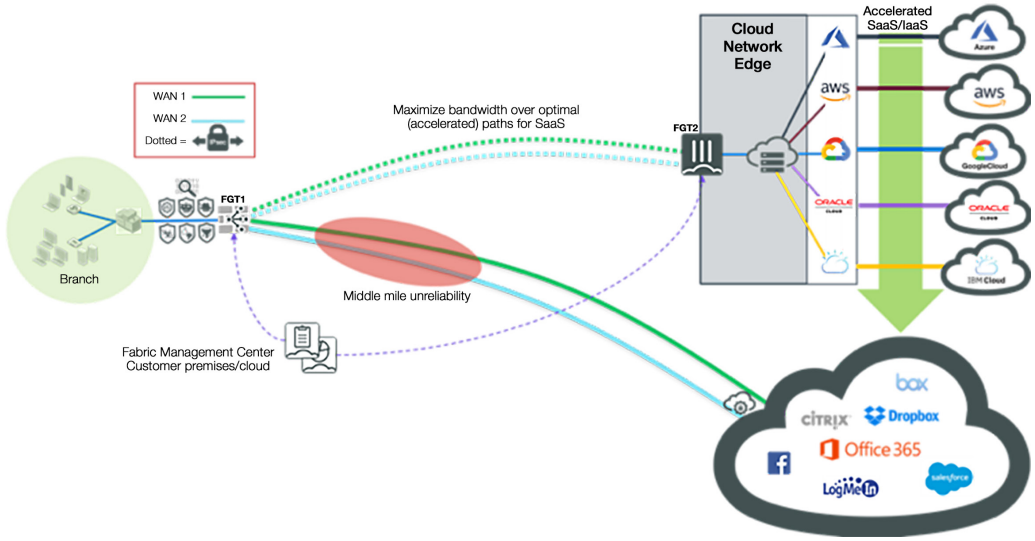

### Cloud-based critical applications (SaaS/IaaS)

Strategy: Prefer a DIA path to benefit from lower latency and higher performance, and alternatively backhaul through the hub via the MPLS overlay in the event of ISP underlay issues.

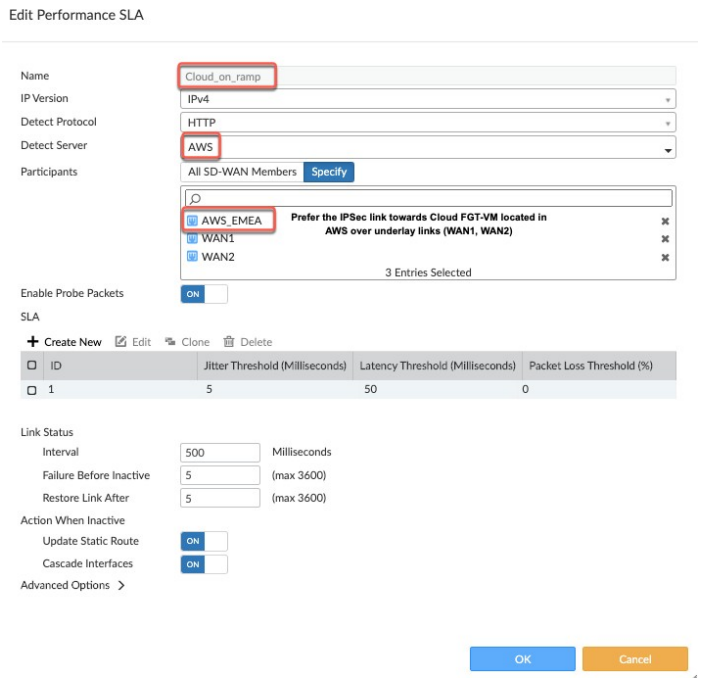


### Cloud on-ramp for SaaS/IaaS acceleration

If a connection to a FortiGate located in private or public clouds is available (see diagram below), SaaS applications should be steered over the closest cloud point of presence (POP) for maximum acceleration.

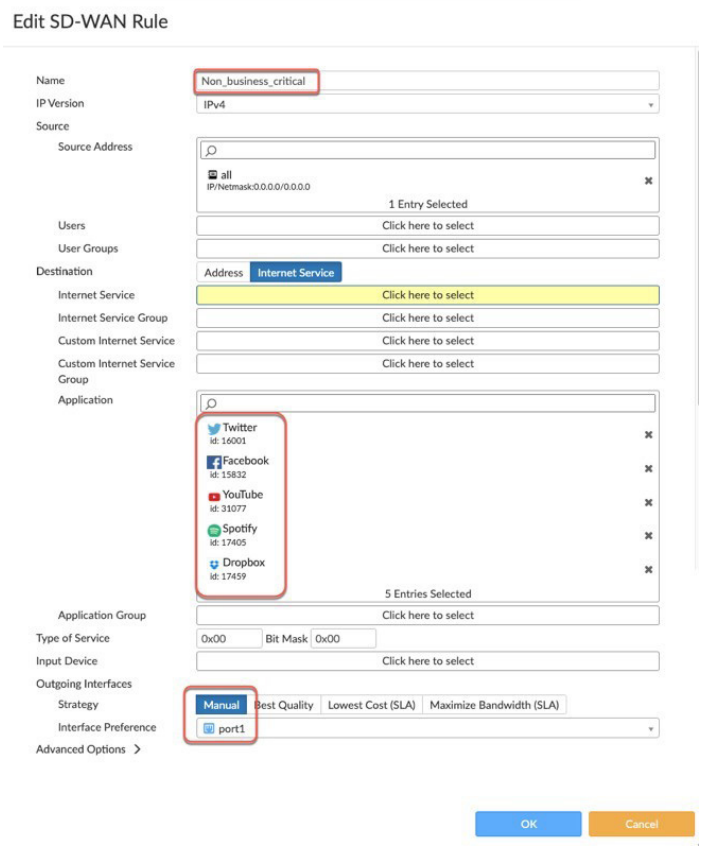



Strategy (below): Select the IPsec overlay toward the FortiGate VM located in AWS as long as the SLA is met and fall back to the broadband underlay otherwise. The direct connection to the cloud network edge alleviates the middle mile unreliability of a direct internet connection.



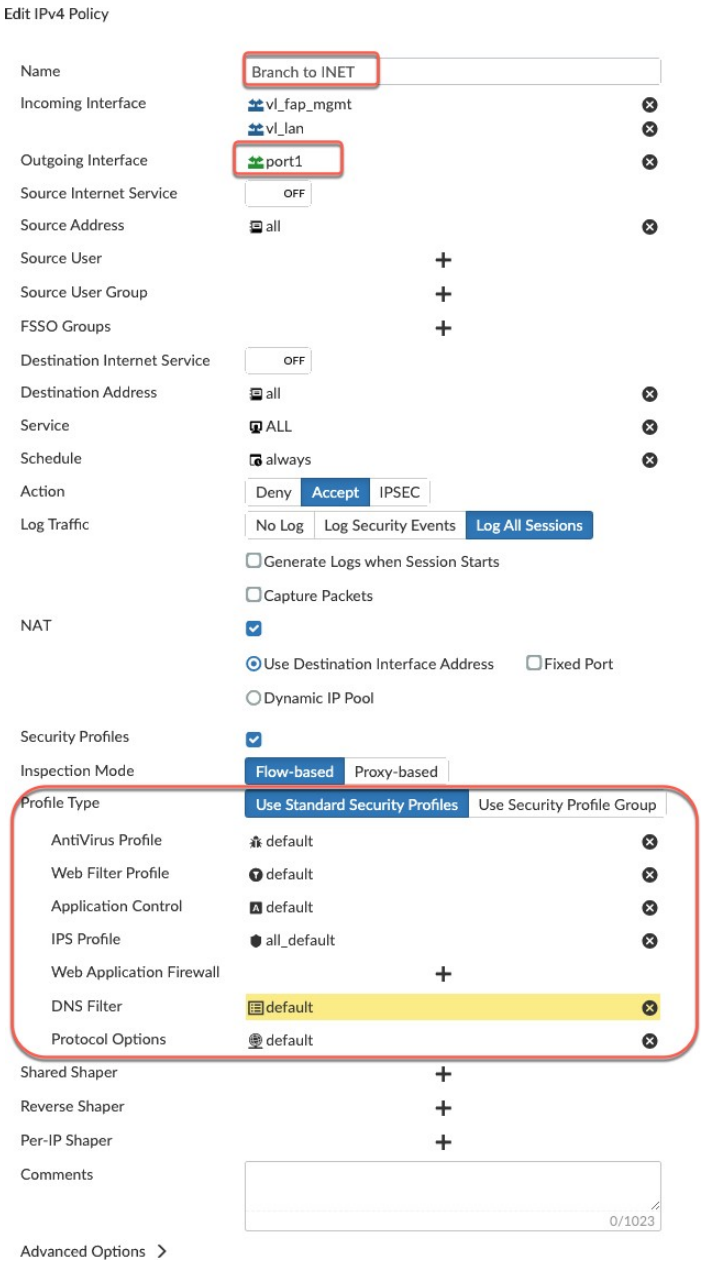

### Noncritical applications

Strategy (below): Noncritical apps should utilize the underlay link only to preserve resources and bandwidth. That is, no SLA defined and in case of congestion on the broadband link, it is acceptable if those applications suffer from lesser performances.



**Branches having a DIA should be protected from malware, viruses, and internet attacks**

Strategy (below): Apply critical security inspection points such as AV filtering, IPS, DNS filtering, and associated internet security policies.




It should be noted that with FortiGate, any defined interface (underlay or overlay) may be included as a member of the vWAN link. Additionally, in FortiOS v6.4.1 and above, each virtual domain (VDOM) may have one vWAN link, but is able to define SD-WAN zones to group member interfaces together to simplify use in policy. If an organization is considering introducing VDOMs at a branch, the team will need to consider inter-VDOM routing to ensure that they are taking advantage of more than one external WAN path.

Starting from FortiOS v6.4.1, SD-WAN is divided into zones. SD-WAN member interfaces are assigned to zones, and zones are used in policies as source and destination interfaces. Administrators may define multiple zones to group SD-WAN interfaces together, allowing logical groupings for overlay and underlay interfaces. The zones are used in firewall policies to allow for more granular control. With the introduction of zones, SD-WAN members cannot be used directly in policies any longer. Static routes use the entire SD-WAN, not just individual zones or members.

## Integrated without compromising performance

SD-WAN technology in FortiGate devices comes embedded in FortiOS. Customers wishing to enable SD-WAN on their existing FortiGate appliances do NOT need to purchase any additional product licensing to leverage SD-WAN capabilities.

One of the unique differentiators of Fortinet Secure SD-WAN is the integrated NGFW capabilities. Other solution architectures (offloading to third parties, tunneling to the cloud, etc.) are viable, but SD-WAN is primarily about WAN edge control, optimization, and consolidation. Because of this, it makes logical sense to perform as much functionality at the edge as is feasible—without extending budgetary constraints.

Fortinet Secure SD-WAN meets, and frankly exceeds, both of these requirements. It provides a full suite of SD-WAN and security functionality at the branch edge, prior to consuming sometimes costly bandwidth. Fortinet Secure SD-WAN is also unrivaled in both price and performance, routinely validated in third-party testing. Figure 13 highlights the architecture of the key features of the FortiGate NGFW with respect to SD-WAN and WAN edge modernization.


Figure 13. FortiGate NGFW capabilities.

FortiGate WAN edge devices deliver this NGFW functionality without compromising on performance thanks to the purpose-built security processor or System-on-a-Chip (SoC).

Smaller form factors of FortiGate come with the SoC while larger models come with both the network processor (NP) and the content processor (CP). To accelerate processing of security and networking functions, Fortinet designs unique security processors. These purpose-built security processors radically boost performance and scalability to enable the fastest network security appliance available. This propels organizations to stay ahead of rapidly growing bandwidth requirements by preventing security from impacting network performance. Fortinet security processors accelerate specific parts of packet processing and content scanning functions. All this customized technology enables organizations to run multiple security applications without performance degradation. That is the reason that organizations can run both SD-WAN and advanced security features on the same appliance (consolidation) and at the same cost (OpEx savings)—without sacrificing performance.

SoC4

**Fortinet delivered the world's first SD-WAN ASIC in February 2019 with its 4th generation SoC, the SoC4. Today, Fortinet has three branch models that leverage the SoC4: the 40F, 60F, and 100F appliances.**

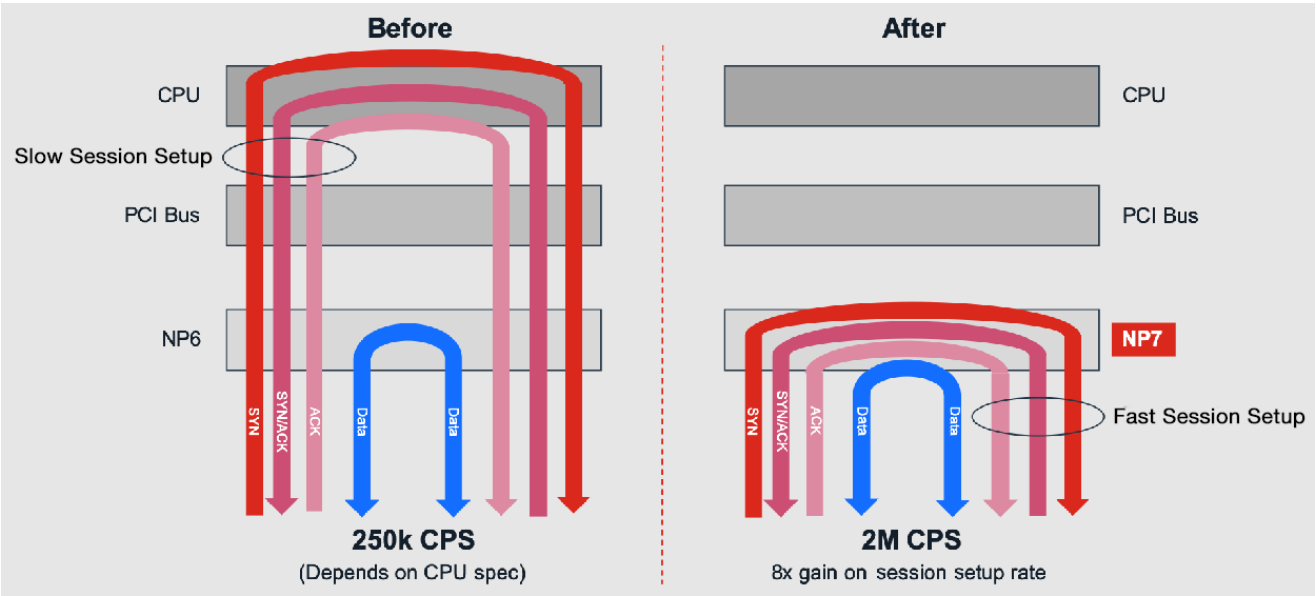



Figure 14. FortiGate parallel path processing (PPP).

To illustrate the benefit of Fortinet SPUs, Figure 14 depicts FortiGate's parallel path processing (PPP) architecture. These security processors are used to scale from 1 Gbps to 1 Tbps of firewall throughput—independent of packet size. This architecture optimizes the high-performance hardware and software resources available in packet flow to deliver ultralow latency and maximum throughput.

Having already introduced the VPN capabilities on the FortiGate, consider the firewall capabilities in Figure 13. Of course, the FortiGate is a stateful packet filter (firewall) at its core, ensuring secure session-based connectivity from the branch edge. But that is just the beginning. Built into the FortiGate solution are application control, intrusion prevention, anti-malware, Uniform Resource Locator (URL) filtering, and SSL inspection capabilities. FortiGate provides a comprehensive Secure SD-WAN solution providing security and WAN path control at the branch edge.

Firewall policy is a well-established capability to provide identity-based granular security policy. For SD-WAN deployments, FortiGate's security policy is simplified in that instead of providing rules for individual vWAN link members, one only needs to identify the SD-WAN zone within security policy (as of FortiOS v6.4.1). Such policy will apply to all member interfaces, making it easier for organizations to combine SD-WAN and security capabilities in one user interface (UI), whether FortiGate or FortiManager for typical SD-WAN deployments. Not only does this provide granular authorization and access control but it also provides a mechanism to introduce advanced security features at the branch edge.

While application control is fully necessary for SD-WAN dynamic application steering, it also plays a role in security. Most organizations maintain corporate security policy. As an example, some may permit downloading files from cloud repositories such as Dropbox.

However, these same organizations may not permit users to upload files to these same repositories. In that case, the organization requires a combination of SSL inspection, application control, and security policy features for the SD-WAN zone. Without SSL inspection, any device would be incapable of determining the operation of the session (download versus upload). Without application control, the edge device would not be able to quickly determine the application (destination), therefore allocating the session to subsequent (implicit) rules. Further, even if we could identify the application and operation, we could not introduce granular identity-based security policy without a firewall rulebase. These combined features not only allow for precise WAN path control but also the introduction of advanced security features including IPS, anti-malware, and URL filtering.

In addition, the FortiGate supports offloading file samples to FortiSandbox (cloud or on-premises) for zero-day malware protection. Bottom line, FortiGate enables a single, integrated security stack (architecture). Figure 15 shows the relation of the FortiGate architecture versus an alternative standalone (multivendor) strategy.

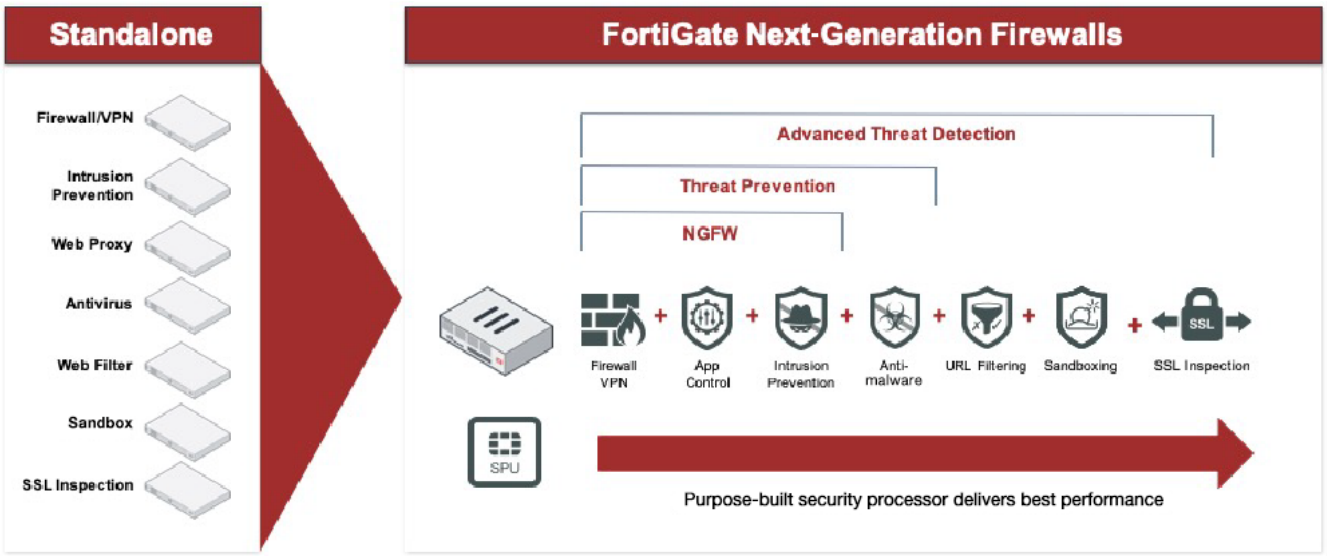



Figure 15. Standalone vs. FortiGate security architecture.

Clearly, a standalone (multivendor) branch edge strategy is costly. Highlighted are seven individual key security capabilities, and numerous vendors have focused solutions for these technologies. However, as a global cybersecurity leader, Fortinet packs all these capabilities into FortiGate form factors with unrivaled performance (due to the SPUs) and with regular threat intelligence updates driven through the FortiGuard Labs Global Threat Research and Response Team (fortiguard.com).

## FortiGate performance

When it comes to NGFW scalability and performance, no other security vendor in the market delivers near Fortinet's capability, let alone pure-play SD-WAN vendors.

Just to highlight an example illustrated in Figure 16, the FortiGate 100F model, which is a midrange model suitable for midrange enterprises, can reach impressive performance metrics in terms of VPN security and advanced security capabilities compared to other major vendors in the SD-WAN market. These impressive performance attributes are due to the parallel processing design of FortiOS and the utilization of purpose-built ASIC processors to offload computationally intensive networking and security functions.

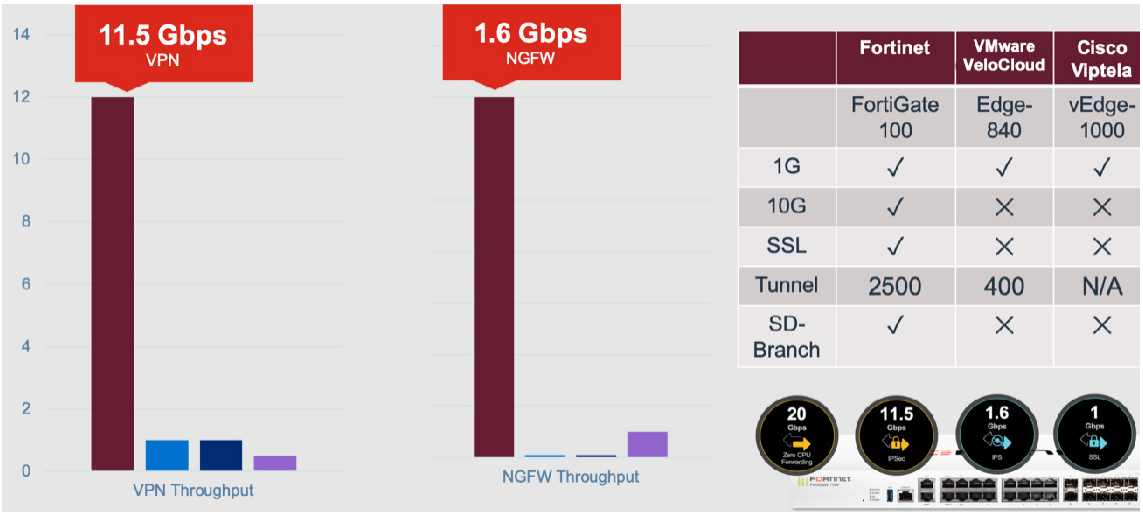



Figure 16. FortiGate 100F performance capabilities versus competitors' equivalent solutions (according to vendor data sheets).

With respect to distributed deployments and FortiGate models, typical edge devices range from models 30E, 40F, and 60F to 100F or 200E for physical appliances, and models VM01 through VM16 for virtual machines. It is noteworthy that several small branch appliances come with integrated Wi-Fi options to further consolidate branch solutions. The specifications of the most popular FortiGate branch device, the 60F, demonstrate its superiority. (The latest specifications of all models can be found at fortinet.com.)

Figure 17 provides a visual depiction of the front and rear of the 60F/61F appliance. It also gives high-level hardware specifications for connectivity. Figure 18 on the next page lays out detailed performance specifications for this device.

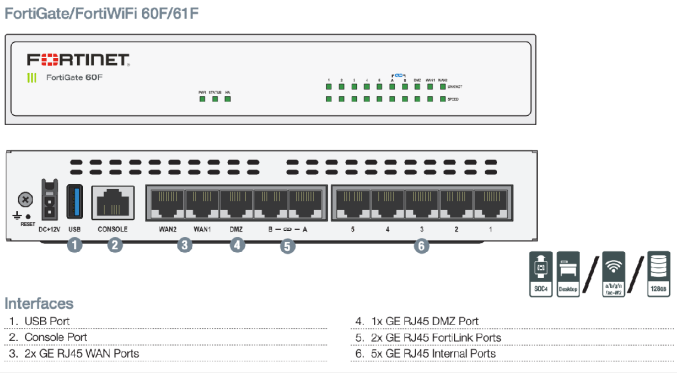



Figure 17. FortiGate 60F/61F specifications.

| System Performance | |
|---|---|
| Firewall Throughput (1518 / 512 / 64 byte UDP packets) | 10/10/6 Gbps |
| Firewall Latency (64 byte UDP packets) | 4 µs |
| Firewall Throughput (Packets Per Second) | 9 Mpps |
| Concurrent Sessions (TCP) | 700,000 |
| New Sessions/Second (TCP) | 35,000 |
| Firewall Policies | 5,000 |
| IPsec VPN Throughput (512 byte) | 6.5 Gbps |
| Gateway-to-Gateway IPsec VPN Tunnels | 200 |
| Client-to-Gateway IPsec VPN Tunnels | 500 |
| SSL-VPN Throughput | 900 Mbps |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | 200 |
| SSL Inspection Throughput (IPS, avg. HTTPS) | 750 Mbps |
| SSL Inspection CPS (IPS, avg. HTTPS) | 400 |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) | 55,000 |
| Application Control Throughput (HTTP 64K) | 1.8 Gbps |
| CAPWAP Throughput (HTTP 64K) | 8 Gbps |
| Virtual Domains (Default / Maximum) | 10 / 10 |
| Maximum Number of FortiSwitches Supported | 16 |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | 64 / 32 |
| Maximum Number of FortiTokens | 500 |
| High Availability Configurations | Active / Active, Active / Passive, Clustering |

Figure 18. FortiGate 60F Series performance specifications.

Most notable for secure SD-WAN are VPN, SSL inspection, and application control performance. Most, if not all, secure SD-WAN branch deployments will implement an overlay network via IPsec tunnels to securely transport packets between branch sites, to the data center, or outbound to cloud destinations (perhaps a FortiGate VM deployed in a public cloud).

Considering typical branch deployment requirements, 6.5 Gbps of VPN throughput is without question more bandwidth than a high percentage of branches require. Enabling application control, which evaluates application traffic, decreases throughput only to 1.8 Gbps, still far exceeding what most branches expect for overall throughput. Enabling full SSL DPI and enabling IPS, as expected, costs a bit more and provides for 750 Mbps. Again, where most branches currently enjoy 10 Mbps throughput or less via MPLS to the internet (backhauled through the data center), 750 Mpbs of secure throughput is more than sufficient. Many other solutions have trouble producing such throughput—even without advanced security features.

The reason the FortiGate 60F/61F Series appliance boasts such performance is because of Fortinet's SoC4. The SoC4 more than doubles the secure networking performance over the enterprise-class CPUs found in competing security solutions and propels the new FortiGate 60F Series distributed enterprise firewalls to unprecedented levels of security and performance. Figure 19 highlights the FortiGate 60F/61F against competition in the security and SD-WAN markets.

| Specification | FortiGate 60F (SoC4 ASIC) | Industry Average | Security Compute Rating | Palo Alto Networks PA-220 | Check Point SG-1550 | Cisco Meraki MX67 | VMware VeloCloud 520 | Juniper SRX 340 | Versa CSG 700 |
|---|---|---|---|---|---|---|---|---|---|
| Firewall | 10 Gbps | 1.23 Gbps | 8x | 0.5 Gbps | 1 Gbps | 0.45 Gbps | Not Published | 3 Gbps | Not Published |
| IPsec VPN | 6.5 Gbps | 0.48 Gbps | 13x | 0.1 Gbps | 1.3 Gbps | 0.2 Gbps | 0.2 Gbps | 0.6 Gbps | Not Published |
| Threat Prevention | 0.70 Gbps | 0.18 Gbps | 4x | 0.15 Gbps | 0.45 Gbps | 0.3 Gbps | Not Published | Not Published | Not Published |
| SSL Inspection | 0.75 Gbps | 0.065 Gbps | 11x | 0.065 Gbps | Not Published | Not Published | Not Published | Not Published | Not Published |
| Concurrent Sessions | 700,000 | 273333 | 3x | 64,000 | 500,000 | Not Published | Not Published | 256,000 | Not Published |
| Connections per Second | 35,000 | 7650 | 4x | 4200 | 14,000 | Not Published | 2400 | 10,000 | Not Published |

Figure 19. FortiGate 60F/61F industry comparison (according to vendor data sheets).

In short, Fortinet has a multitude of options to choose from to accommodate any set of branch edge requirements.

For all FortiGate models, the numeric differentiation denotes a larger amount of storage within the appliance.

## Dynamic routing

Each FortiGate deployed across an enterprise, whether the organization is small or large, serves as its own control plane at the edge due to its controllerless architecture. Before an organization can properly introduce Fortinet Secure SD-WAN at the WAN edge, it first must gain an understanding of the various paths application flows may choose to traverse the WAN when going from one site to another. In legacy networks (MPLS, virtual private local-area network service [VPLS], etc.) organizations might leverage static routes for a low number of sites or dynamic routing protocols such as Open Shortest Path First (OSPF) and BGP for a larger number of sites. In an SD-WAN scenario utilizing FortiGate at the edge, BGP is the preferred dynamic routing protocol due to its flexibility. While this document is not meant to serve as a volume on BGP, refer to the SD-WAN document repository (https://docs.fortinet.com/sdwan) for guidance about how FortiGate and FortiOS support BGP.

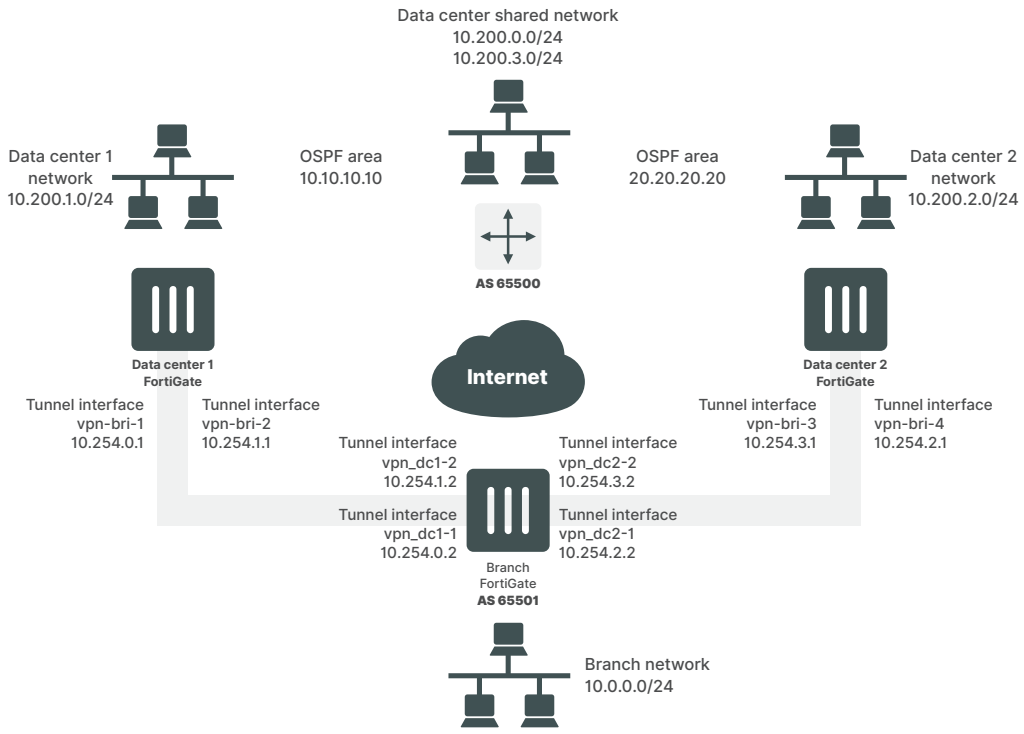



Figure 20. Client-side Fortinet Secure SD-WAN with IPsec VPN.

In Figure 20, the BGP routing environment is all within private address space. In this case, the customer has established an overlay network using IPsec tunnels via the internet underlay interface(s) to connect its WAN. At the data center, the AS is 65500 and at the branch, the AS is 65501. Data center FortiGate devices will advertise protected network subnets across the WAN to the branch site(s). For example, DCFW 1 (the upper left FortiGate in the diagram) will advertise routes to 10.200.1.0/24, 10.200.0.0/24, and 10.200.3.0/24. On DC 2's FortiGate, it too will advertise the 10.200.0.0/24 and 10.200.3.0/24 networks. However, it will not advertise the 10.200.1.0/24, but instead advertise the 10.200.2.0/24 network. Not to state the obvious, but each network will advertise its own back end without advertising the other. However, advertising both is possible and will work in some scenarios.

There is one caution when it comes to BGP and dynamic routing. Sometimes, as is the case here, the same networks are advertised from more than one hop (router). In these routing architectures, asynchronous routing, especially in a secure SD-WAN environment where firewall functionality enforces sessions (reverse path forwarding, or anti-spoofing), is something to look out for and ensure it be adequately addressed in the overall design and implementation.

From the branch side, the FortiGate advertises the 10.0.0.0/24 subnet. In addition to advertising their own subnets, the data center FortiGate devices will also act as route reflectors, letting all other overlay network participating members (branches) know about route updates from individual branch devices. This reduces the necessity for every participant to communicate with one another as is the case with a full-mesh route advertising scenario. There are other cautions with regard to very large networks concerning convergence times and memory consumption. However, most enterprises will likely not encounter these challenges with such a hub-and-spoke topology using dynamic routing.

While OSPF is noted in the diagram, the FortiGate devices are not participating in this back-end DC-to-DC routing scheme (though FortiOS does support OSPF). This is a simple example of BGP routing, but understand that BGP can become quite complex. To that end, be sure to engage network architecture team members or Fortinet consulting resources when spinning up a Fortinet Secure SD-WAN project to ensure that the routing scheme is both supported and properly designed.

Even though routes must be first configured using the SD-WAN vWAN link, FortiGate installs individual routes for member interfaces into the actual routing table. These routes are each active and share similar attributes (destination address and subnet, distance, and priority). This action allows FortiGate to remove individual routes in the event of an interface outage or SLA failure, and redirect all traffic to the remaining member interfaces (defined in the policy/rule), without affecting application performance or availability.

**Note: It is a best practice to create static black hole routes with destinations set to each branch network (or a small enough mask to cover all branches). If the data center FortiGate devices temporarily lose connectivity with a branch network, traffic destined to that network is sent to the black hole until connectivity has been restored and routes have converged through BGP.**

## SD-WAN packet prioritization

Legacy WAN architecture includes quality of service, or QoS. Where MPLS networks live, so does low-bandwidth connectivity. Some branches still leverage incredibly low bandwidth such as 1.5 to 3 Mbps. While this may be more than sufficient for said branches, they also beg for QoS features. This is because organizations need to protect critical business applications. Typically, these applications include voice (VoIP) and video, and are marked at an edge device (router) so they receive priority transmission over the WAN. In addition to security and SD-WAN, FortiOS also provides traffic shaping capabilities including default priority buckets and differentiated services (DiffServ) marking. In the same way, priority allows for critical business applications to receive preferential ordering (and transmission) across a specified vWAN link member interface if congestion begins to impact overall interface performance. Figure 21 on the next page shows how to apply shaping policy to traffic matching DiffServ code 100010.

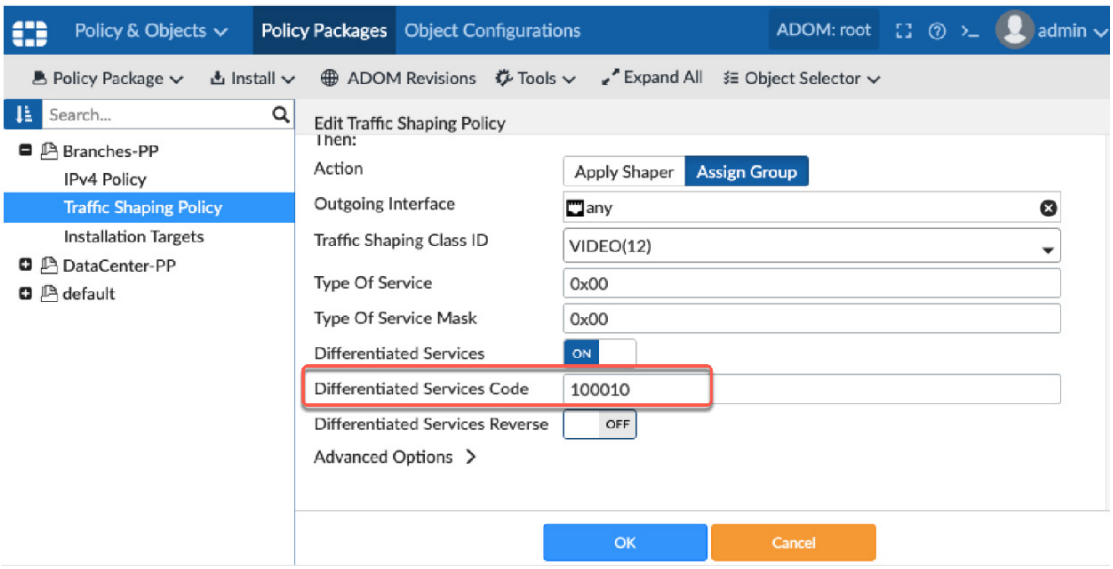



Figure 21. Traffic shaping policy with differentiated services.

## Application detection and classification

**First packet identification.** At the foundation of any robust SD-WAN solution is the capability to correctly identify and classify application traffic—including encrypted flows, which constitute more than 75% of total internet traffic. Failing to do so would not only prevent solutions from providing a granular traffic steering decision but also would expose the branch to security threats that are more and more conveyed across encrypted channels.

Commonly the techniques to classify applications utilize a combination of IP address, TCP/UDP port, and DPI. DPI is useful when applications use ports unpredictably, or when one must distinguish applications that share the same HTTP or Hypertext Transfer Protocol Secure (HTTPS) port. However, DPI is not sufficient to granularly steer traffic to a specific destination based on the application because it cannot identify the application on the first packet. DPI relies on a library of application signatures and heuristics, requiring two to six packets to identify an HTTP application and 10 packets or more to identify an HTTPS application.

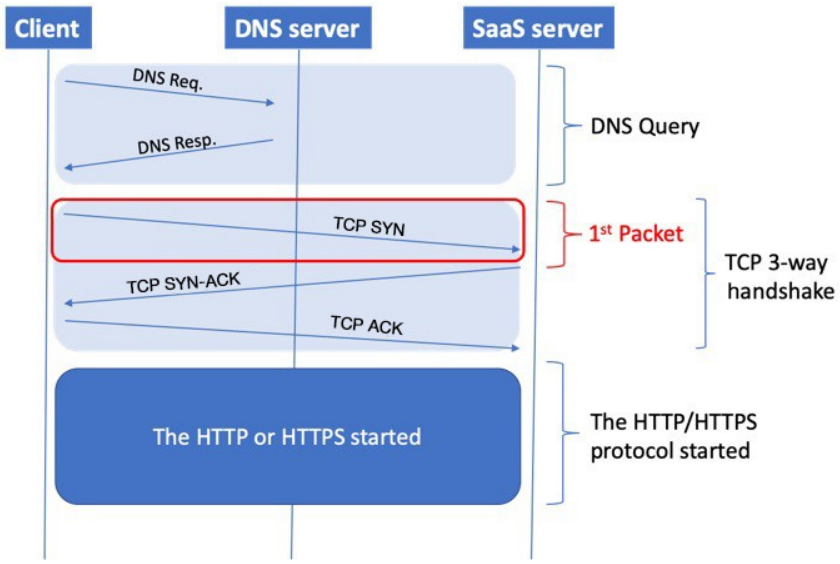



Figure 22. Packet identification.

**Fortinet Internet Service Database (ISDB).** URL filtering and DPI will work after the HTTP/HTTPS traffic begins and it will not be able to identify the first packet. Blocking/allowing user access based on public IP address is not an easy task. There will be dozens of IP addresses, such as Microsoft 365 or Facebook, and it is not easy to manage the IP database, since new IP addresses may always get added or changed on this list.

Internet Service Database, or ISDB, is a FortiGuard Labs service introduced in FortiOS 5.4. It consists of a comprehensive public IP address database that combines IP address range, IP owner, service port number, and IP security credibility. The data comes from the FortiGuard Labs service system. Information is regularly added to this database—for example, geographic location, IP reputation, popularity, DNS, and more. All this information helps organizations define internet security more effectively.

Administrators may use the contents of the database as criteria for inclusion or exclusion in a security policy or SD-WAN business rule.

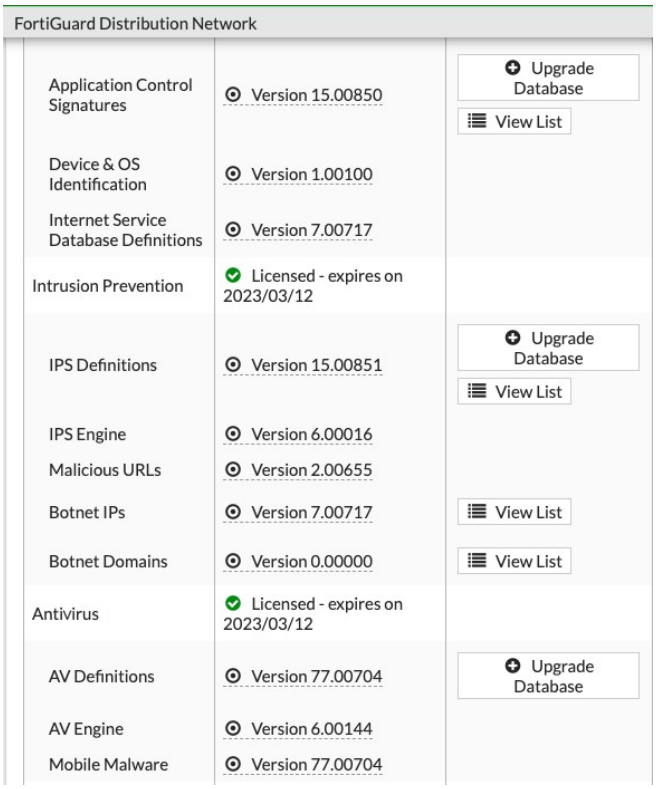



Figure 23. FortiGuard Distribution Network.

The ISDB is consistently up to date, including the list of IP addresses that are associated with common SaaS applications. As a result, when a client sends a TCP-SYN packet to a SaaS application server, the FortiGate device with ISDB enabled will identify the packet as part of appropriate SaaS application traffic and act according to the defined policies.

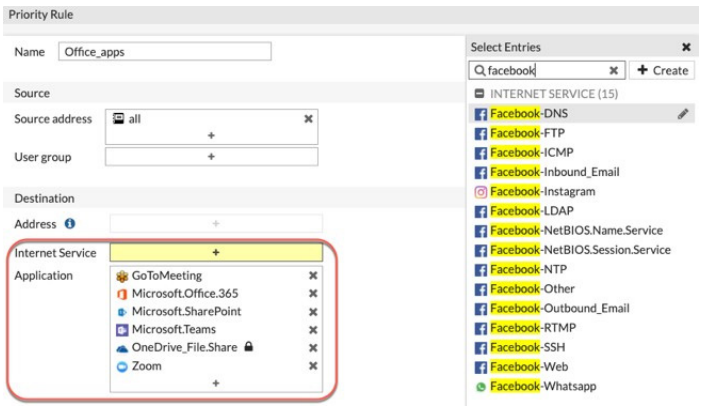



Figure 24. Priority Rule.

## Management and orchestration with FortiManager

FortiManager (in multiple form factors) is the device that provides for centralized management and orchestration of the Fortinet Secure SD-WAN branch edge and data center devices. An organization's FortiManager may reside on-premises, in a private cloud, or in public clouds such as AWS and Microsoft Azure. Regardless of the deployment location, FortiManager maintains connectivity to each FortiGate device, monitors performance SLAs for each device, and presents a single-pane-of-glass view into global connectivity. FortiManager also provides templates for security policy configuration, SD-WAN policy configuration, performance SLA definitions, and much more.

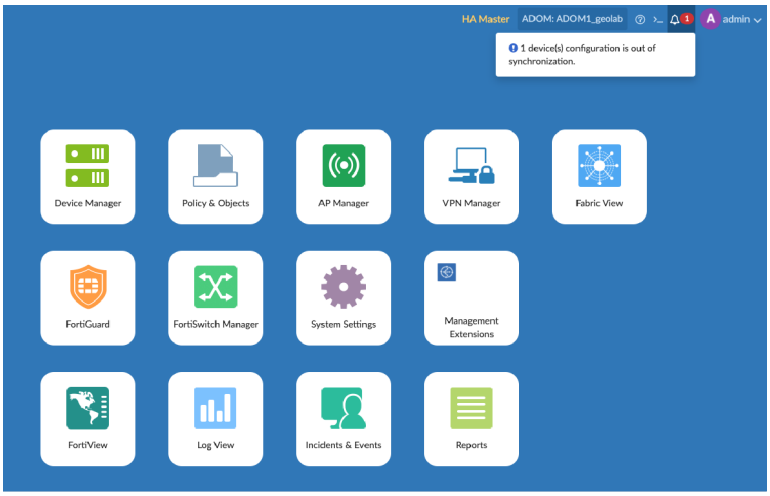



Figure 25. FortiManager single-pane-of-glass management and reporting console.

With flexibility to support application programming interfaces (APIs) and Security Fabric Connectors, FortiManager seamlessly integrates into the greater workflow within an organization. Figure 26 displays the geographical representation and highlights the granularity of the monitoring capabilities FortiManager provides for Fortinet Secure SD-WAN deployments.

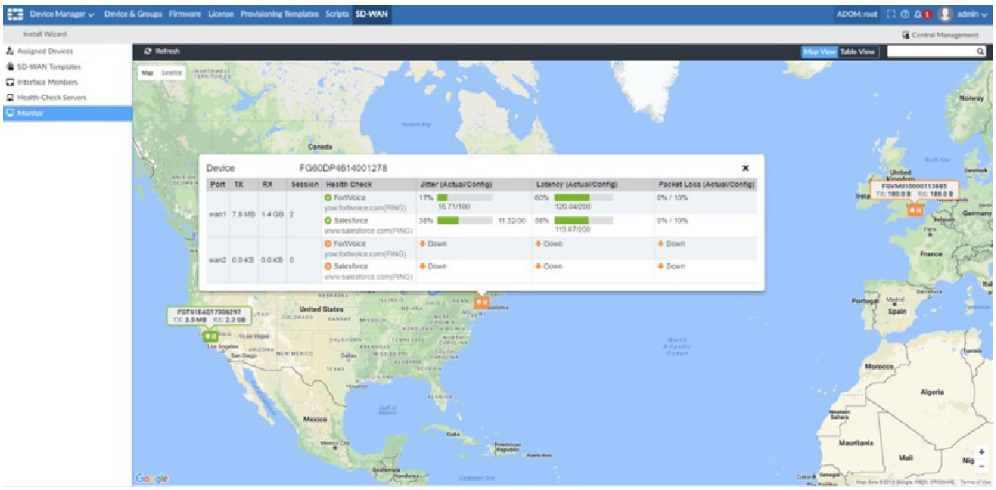



Figure 26. FortiManager geographical monitoring.

**Fortinet ISDB service is available with an active FortiCare support contract.**

**Secure SD-WAN administrators can use FortiManager to control their entire deployment.**

The **Fabric View** module enables organizations to view Security Fabric ratings of configurations for FortiGate Security Fabric groups. Administrators can view the results for multiple FortiGate Security Fabric groups here.

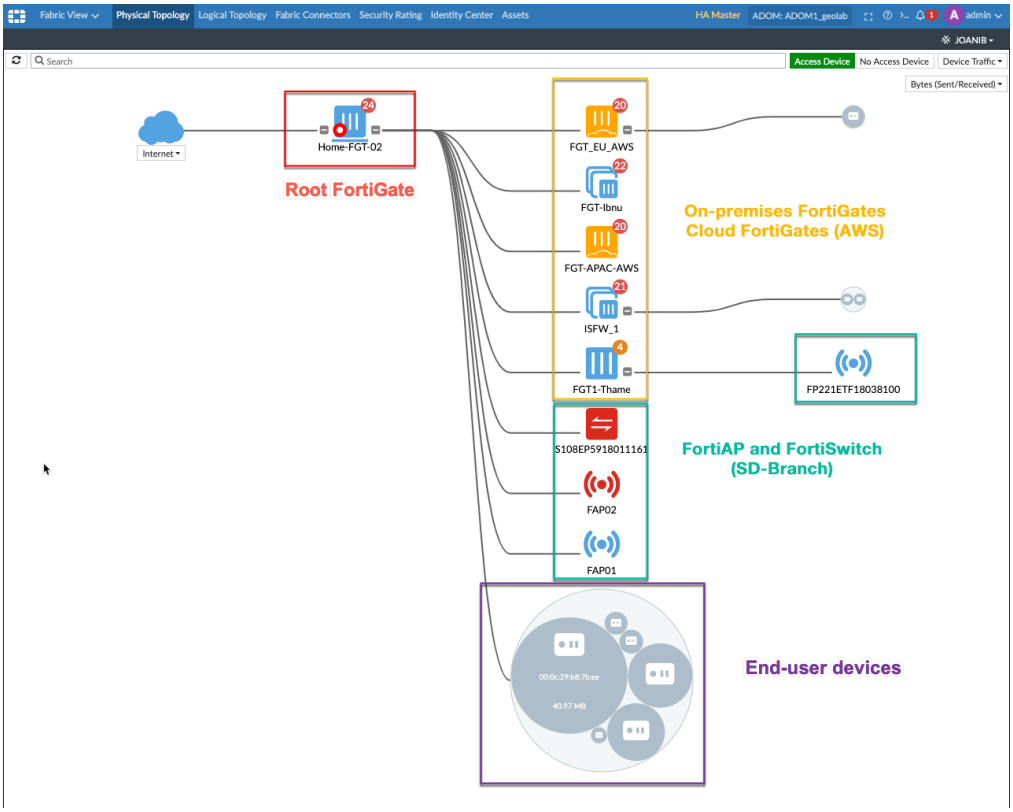



Figure 27. Holistic view of the Security Fabric across hybrid multi-clouds.

**SD-WAN Orchestrator.** SD-WAN Orchestrator, an application module running as a management extension within FortiManager, is included. SD-WAN Orchestrator automates the configuration and automation of SD-WAN networks for an enterprise deployment of SD-WAN devices.

Using container technology to deploy the Orchestrator allows for maximum independency from the rest of the FortiManager components. That is, new features added in Orchestrator can be quickly tested without impacting the rest of the FortiManager capabilities.


Figure 28. SD-WAN Orchestrator.

**Configuration automation.** Administrators can use SD-WAN Orchestrator to configure SD-WAN networks and assign configurations to FortiGate devices. When using SD-WAN Orchestrator to apply the configuration to FortiGate devices, SD-WAN Orchestrator uses the following method:

1. SD-WAN Orchestrator automatically generates command-line interface (CLI) scripts of the configuration. There is an option to view these scripts in FortiManager on the **Device Manager > Scripts** pane.
2. SD-WAN Orchestrator installs the CLI scripts to the **Device Manager** database in FortiManager.
3. FortiManager receives the CLI scripts, and FortiManager installs the configurations to all managed devices.

When the configuration is installed to managed devices, the overlay and underlay links between all devices in the SD-WAN network are automatically created.

SD-WAN Orchestrator creates the dynamic interfaces for generated-tunnel interfaces. The dynamic interfaces use per-device interface mappings, and administrators can select them in FortiManager when creating policies.

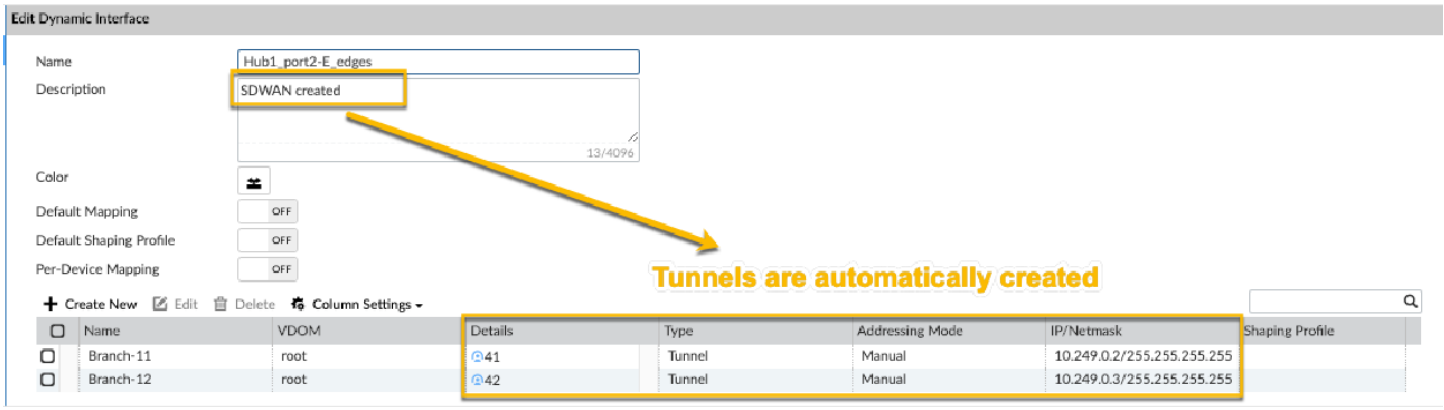



Figure 29. SD-WAN Orchestrator: tunnel creation automation.

SD-WAN Orchestrator also creates two policy blocks in FortiManager: one for hub devices and one for edge devices. The policy blocks include the necessary firewall policies to allow health check probes through the VPN tunnels. Administrators can view the policy blocks in FortiManager by going to **Policy & Objects > Policy Packages.**

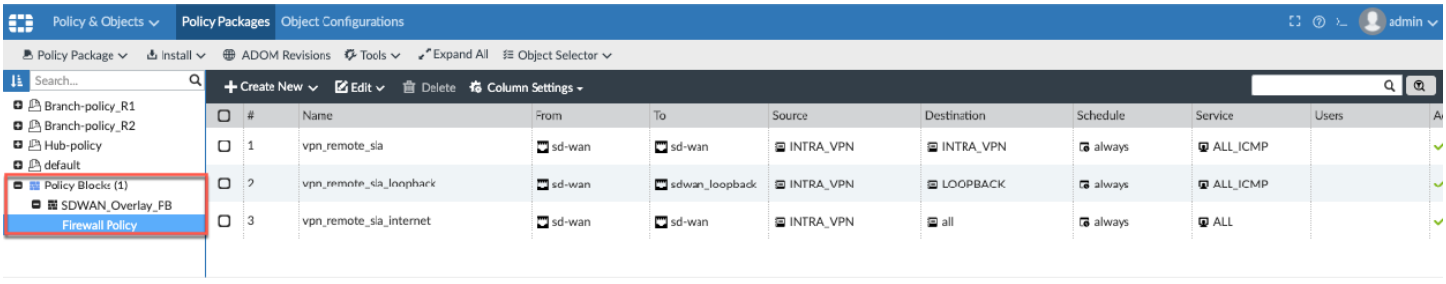



Figure 30. SD-WAN Orchestrator automatic policy block for health checks.

Organizations should use SD-WAN Orchestrator for all configuration and monitoring of SD-WAN networks. In combination with FortiManager, SD-WAN Orchestrator provides a feature-rich, granular central management solution for SD-WAN deployments.

**Note: SD-WAN Orchestrator completely automates two of the most complex and error-prone design pillars of a large-scale SD-WAN deployment: the VPN overlay and dynamic routing. The other two pillars, SD-WAN edge intelligence and integrated security, are left to an administrator to be manually configured according to the company WAN edge and security strategy.**

For more information, please refer to the SD-WAN Orchestrator Administrator Guide.

**Monitoring and reporting.** After administrators have configured an SD-WAN network, they can monitor the global network as well as individual devices in the network by using the Monitor tree menu.

The following example shows a deployment with two hubs in two different regions, each handling two branches.

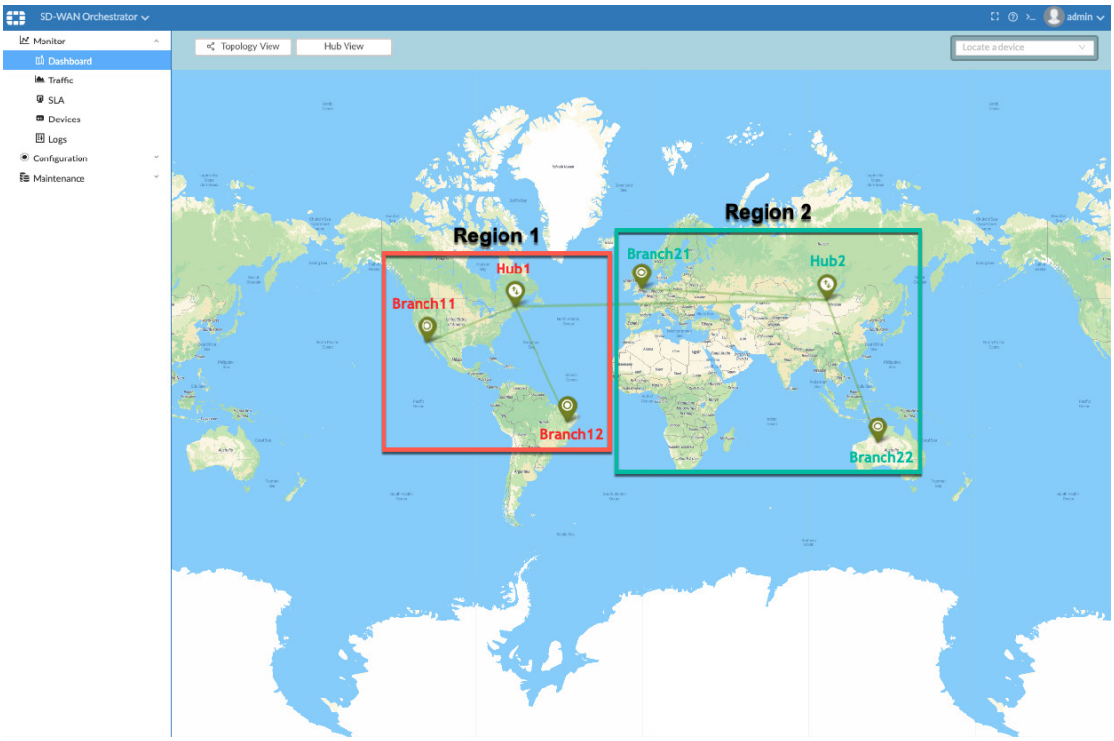



Figure 31. SD-WAN Orchestrator Monitor dashboard.

The SD-WAN Orchestrator Monitor provides the ability to view granular information about link quality for both underlay and overlay (static and dynamic), device status and application usage, and SLA performance, therefore allowing for faster resolution of most typical problems. The figures below report some device views and what is presented to an administrator in case of a potential link failure/congestion. The device in consideration is Branch 11 located in region 1.

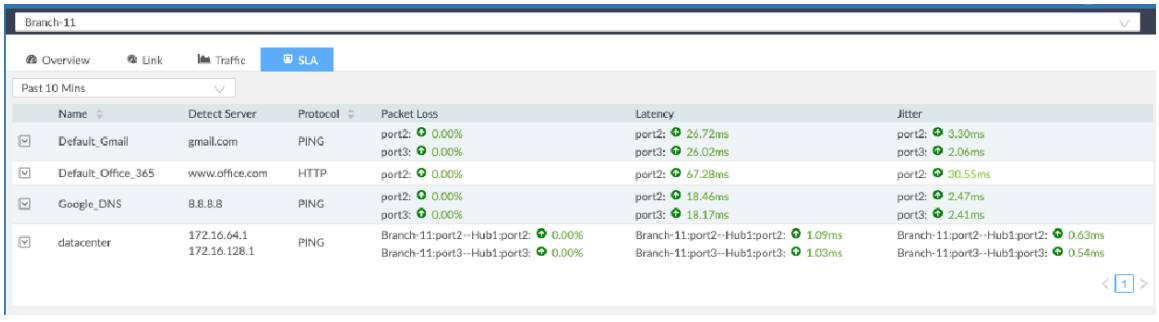



Figure 32. Device SLA status, normal operation.

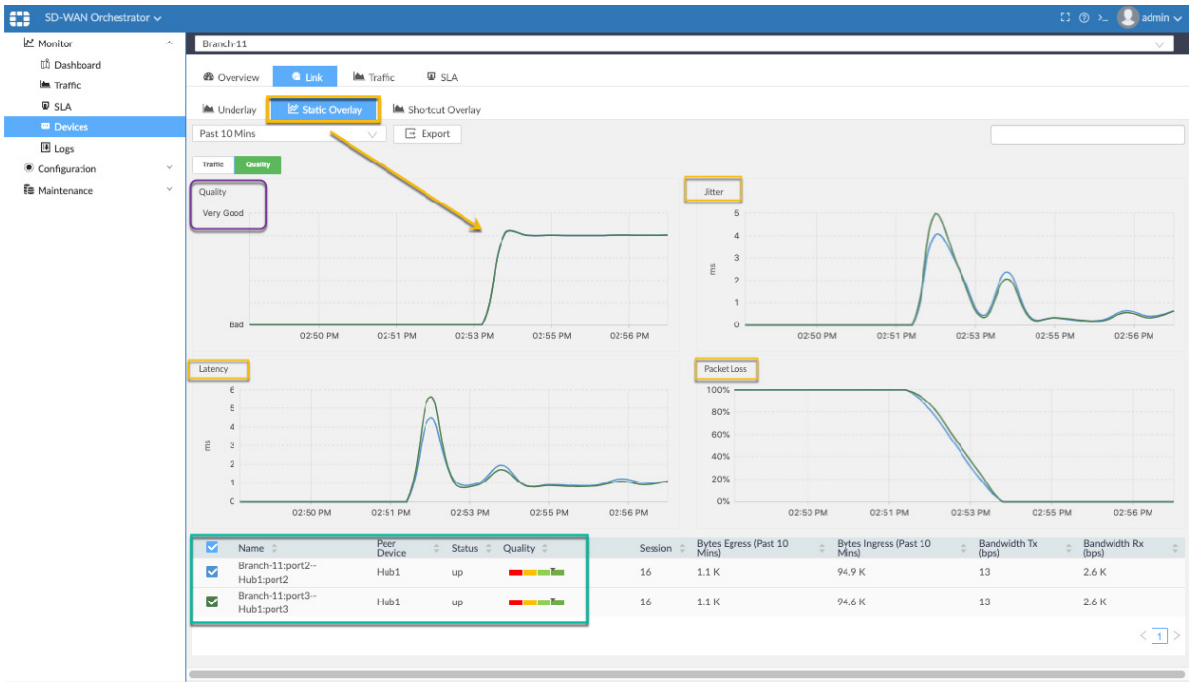



Figure 33. Device link status (overlay), normal operation.

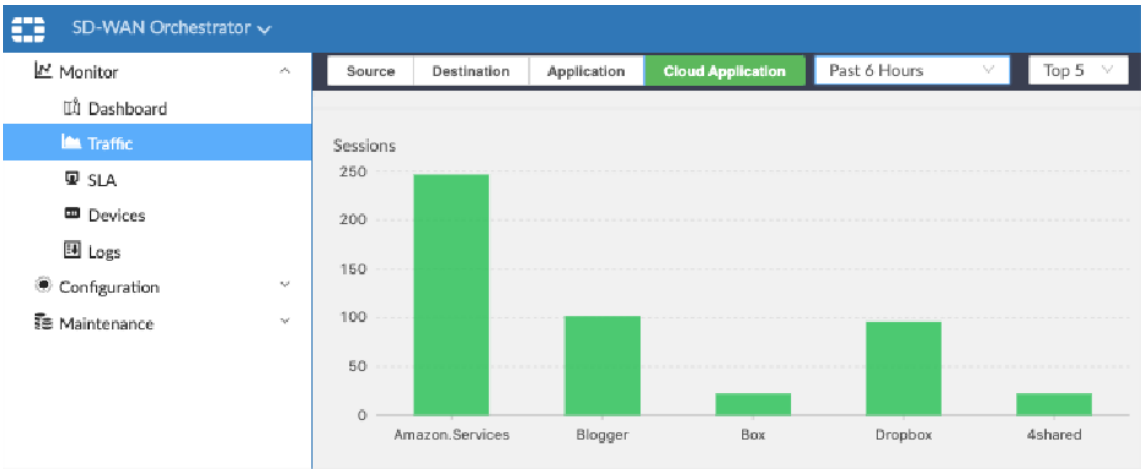



Figure 34. Device traffic, top cloud (SaaS/IaaS) apps.

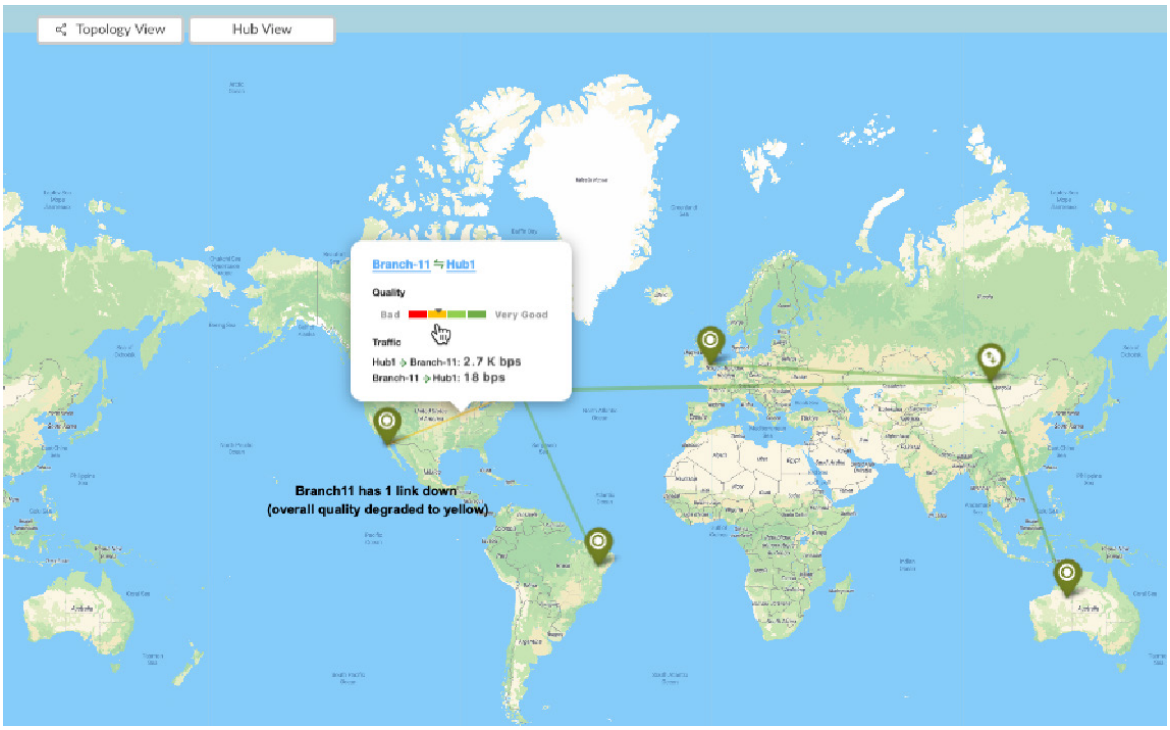



Figure 35. Main dashboard, one underlay link down.

The SD-WAN administrator may then dig down into the device-level section to find out that one of the underlays is down (packet loss 100%). Thanks to SD-WAN, traffic still flows over the remaining link(s).

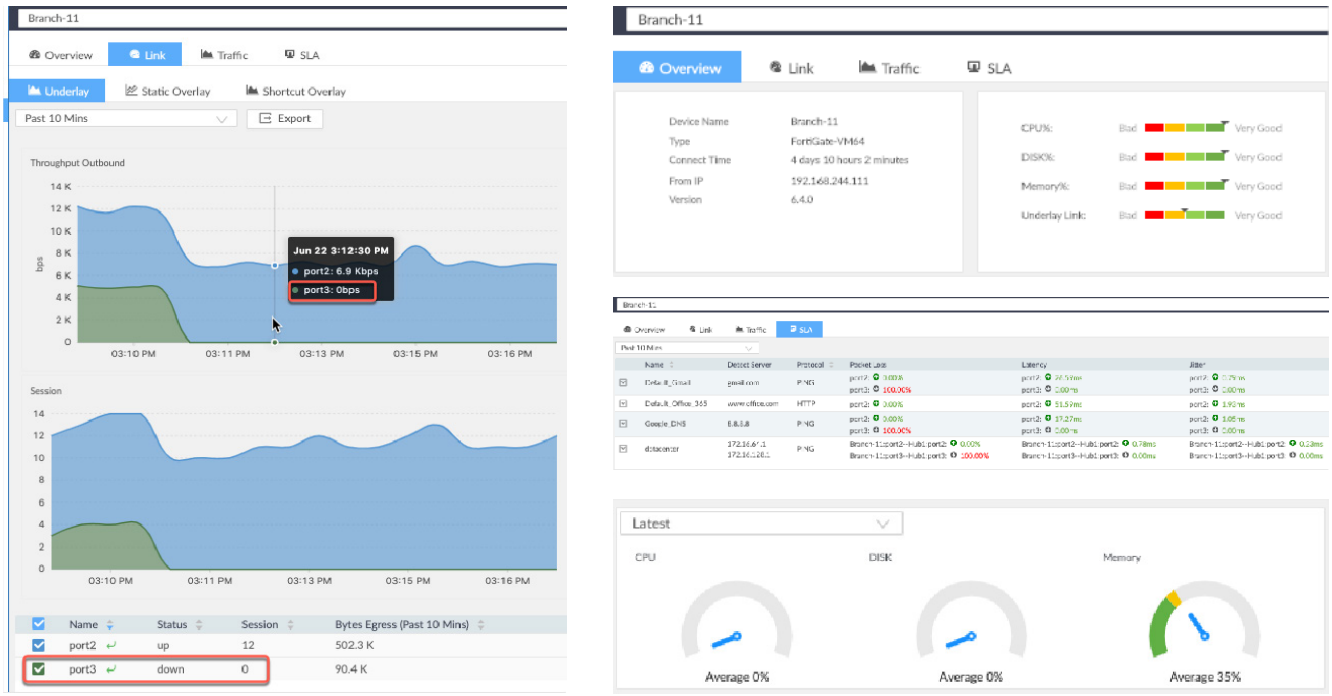



Figure 36. Monitoring device status, one underlay link down.

## FortiAnalyzer and FortiView

When FortiManager is enabled with FortiAnalyzer features, customers can take advantage of full integration with FortiView. FortiView is a comprehensive monitoring system for networks that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

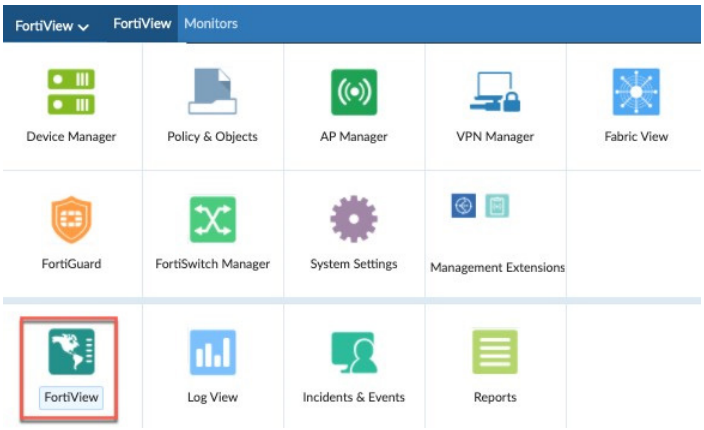



Figure 37. FortiView.

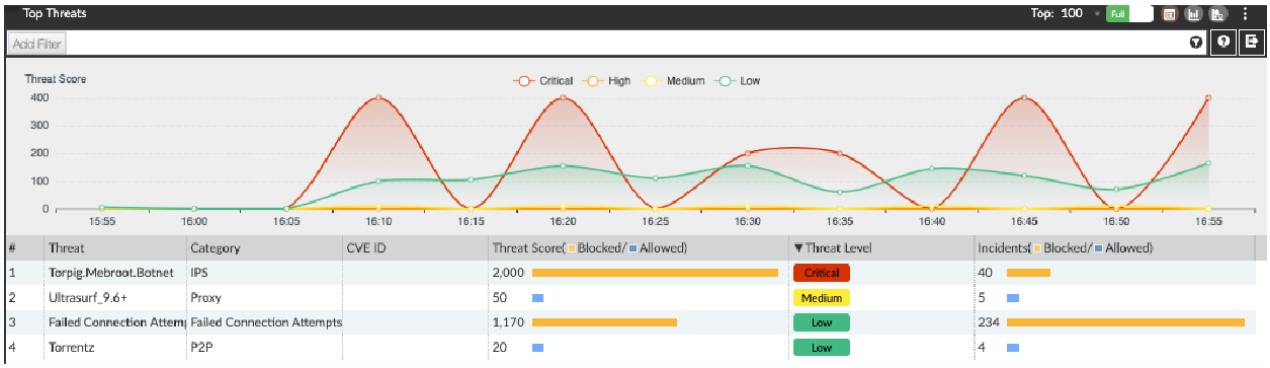



Figure 38. FortiView—top threats.

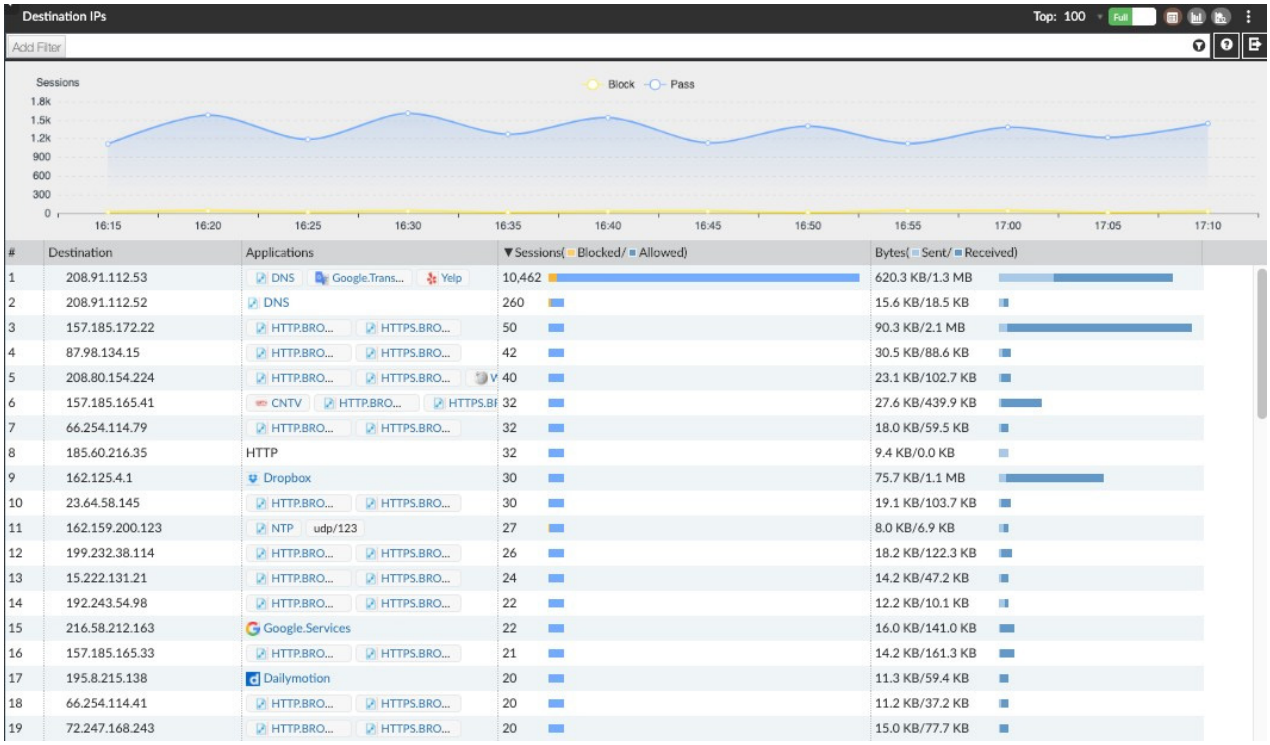
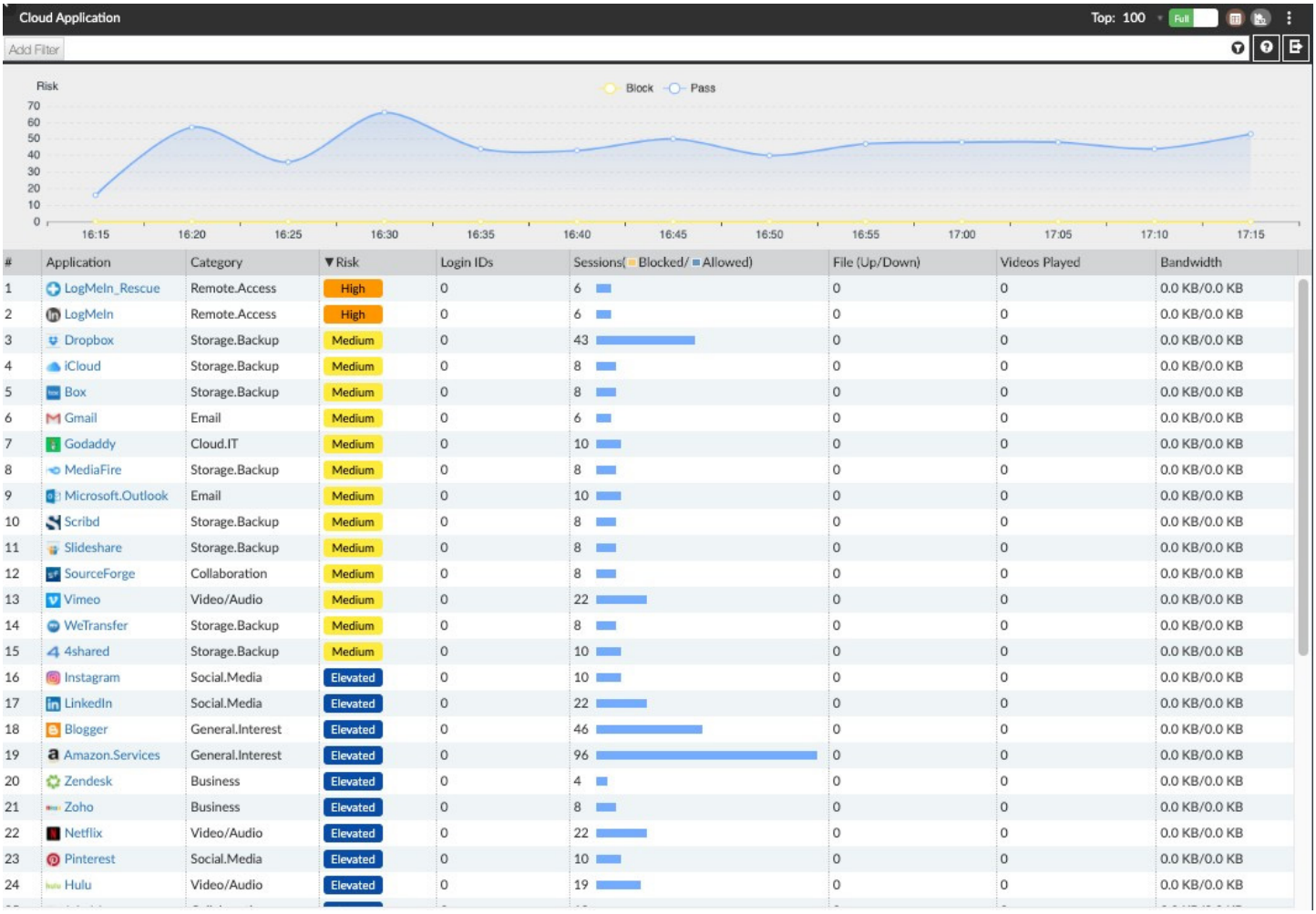



Figure 39. FortiView—top destinations.

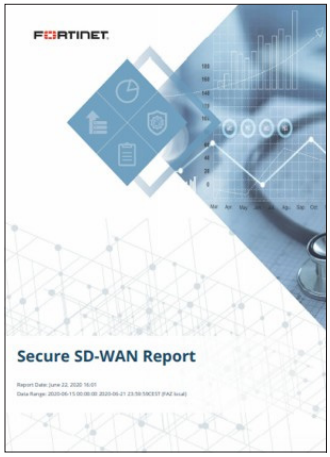


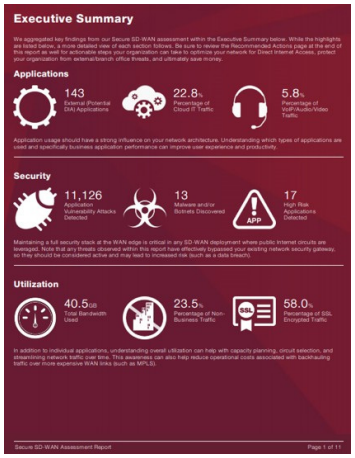

| # | Application | Category | ▼Risk | Login IDs | Sessions( Blocked/ Allowed) | File (Up/Down) | Videos Played | Bandwidth |
|---|---|---|---|---|---|---|---|---|
| 1 | LogMeIn_Rescue | Remote.Access | High | 0 | 6 | 0 | 0 | 0.0 KB/0.0 KB |
| 2 | LogMeIn | Remote.Access | High | 0 | 6 | 0 | 0 | 0.0 KB/0.0 KB |
| 3 | Dropbox | Storage.Backup | Medium | 0 | 43 | 0 | 0 | 0.0 KB/0.0 KB |
| 4 | iCloud | Storage.Backup | Medium | 0 | 8 | 0 | 0 | 0.0 KB/0.0 KB |
| 5 | Box | Storage.Backup | Medium | 0 | 8 | 0 | 0 | 0.0 KB/0.0 KB |
| 6 | Gmail | Email | Medium | 0 | 6 | 0 | 0 | 0.0 KB/0.0 KB |
| 7 | Godaddy | Cloud.IT | Medium | 0 | 10 | 0 | 0 | 0.0 KB/0.0 KB |
| 8 | MediaFire | Storage.Backup | Medium | 0 | 8 | 0 | 0 | 0.0 KB/0.0 KB |
| 9 | Microsoft.Outlook | Email | Medium | 0 | 10 | 0 | 0 | 0.0 KB/0.0 KB |
| 10 | Scribd | Storage.Backup | Medium | 0 | 8 | 0 | 0 | 0.0 KB/0.0 KB |
| 11 | Slideshare | Storage.Backup | Medium | 0 | 8 | 0 | 0 | 0.0 KB/0.0 KB |
| 12 | SourceForge | Collaboration | Medium | 0 | 8 | 0 | 0 | 0.0 KB/0.0 KB |
| 13 | Vimeo | Video/Audio | Medium | 0 | 22 | 0 | 0 | 0.0 KB/0.0 KB |
| 14 | WeTransfer | Storage.Backup | Medium | 0 | 8 | 0 | 0 | 0.0 KB/0.0 KB |
| 15 | 4shared | Storage.Backup | Medium | 0 | 10 | 0 | 0 | 0.0 KB/0.0 KB |
| 16 | Instagram | Social.Media | Elevated | 0 | 10 | 0 | 0 | 0.0 KB/0.0 KB |
| 17 | LinkedIn | Social.Media | Elevated | 0 | 22 | 0 | 0 | 0.0 KB/0.0 KB |
| 18 | Blogger | General.Interest | Elevated | 0 | 46 | 0 | 0 | 0.0 KB/0.0 KB |
| 19 | Amazon.Services | General.Interest | Elevated | 0 | 96 | 0 | 0 | 0.0 KB/0.0 KB |
| 20 | Zendesk | Business | Elevated | 0 | 4 | 0 | 0 | 0.0 KB/0.0 KB |
| 21 | Zoho | Business | Elevated | 0 | 8 | 0 | 0 | 0.0 KB/0.0 KB |
| 22 | Netflix | Video/Audio | Elevated | 0 | 22 | 0 | 0 | 0.0 KB/0.0 KB |
| 23 | Pinterest | Social.Media | Elevated | 0 | 10 | 0 | 0 | 0.0 KB/0.0 KB |
| 24 | Hulu | Video/Audio | Elevated | 0 | 19 | 0 | 0 | 0.0 KB/0.0 KB |

Figure 40. FortiView—top cloud applications.

## Automatic SD-WAN reports

FortiManager allows administrators or business owners to generate automatic SD-WAN reports, targeted to executive management. These reports provide immediate information to assess the benefits of the SD-WAN solution while at the same time aggregating critical security information. While the highlights are listed below in a convenient executive summary report, a more detailed view of each section is provided. This includes a set of recommended actions at the end of the report, plus actionable steps an organization may take to optimize their network for DIA, protect their organization from external/branch office threats, and ultimately reduce expenditures and save money.



## Zero-touch deployment

In addition to management and monitoring, FortiManager is also a key part of the zero-touch deployment (ZTD) capability. In essence, Fortinet ZTD begins in the purchasing process. By adding a ZTD bulk key to the bill of materials, organizations register devices in the FortiDeploy system as ZTD devices. Customers then identify a routable IP address for their FortiManager in the FortiDeploy system. When a new device is plugged into power and connected to the internet via Ethernet (WAN1), the FortiGate automatically calls home, receives the FortiManager IP address, and immediately requests connectivity to the FortiManager. This process is depicted in Figure 41.

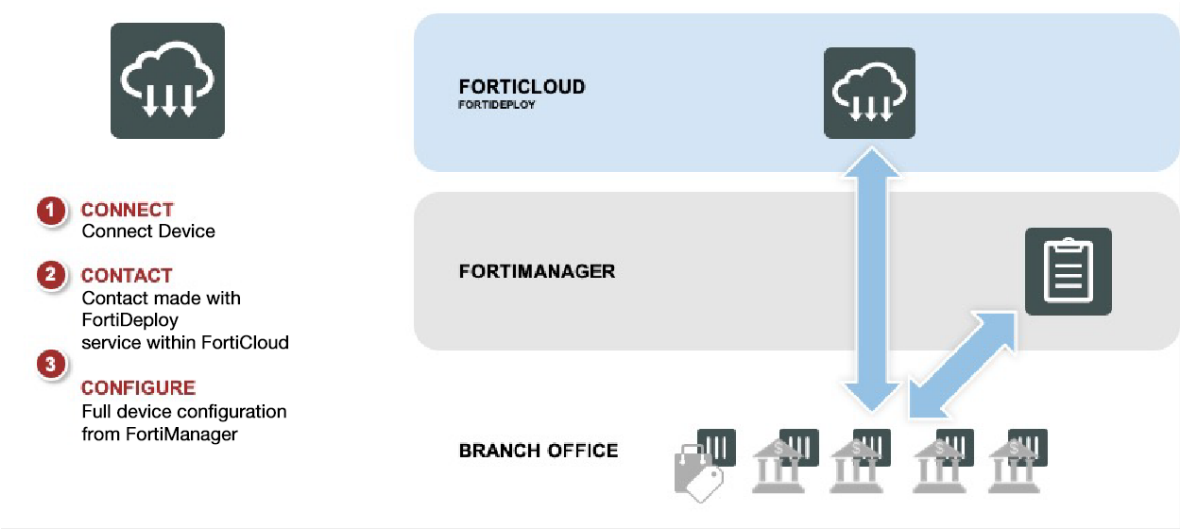



Figure 41. Fortinet zero-touch deployment process.

Once the device is authorized (manually or via automated configuration), the FortiManager pushes configuration templates to the device, fully configuring it for security and SD-WAN functionality at the branch.

## High availability

Fortinet Secure SD-WAN may be deployed in high availability (HA) from a site-level or network-level standpoint.

**Site-level HA.** A site-level HA configuration allows organizations to deploy two redundant FortiGate devices in the branch according to the following architecture:

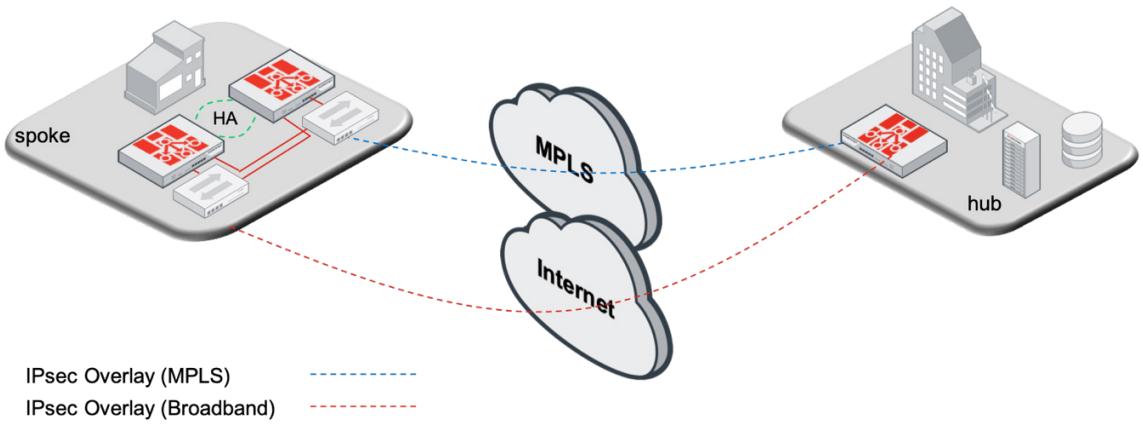



Figure 42. High availability (site level).

This SD-WAN HA configuration allows organizations to load balance internet traffic between multiple links. It also provides redundancy for the network's connection if one of the links is unavailable or if one of the FortiGate devices in the HA cluster fails.

**Network-level HA (disaster recovery).** A network-level HA configuration allows organizations to deploy a geographical redundant network with multiple hubs that can be located in different regions, according to the following architecture topology:

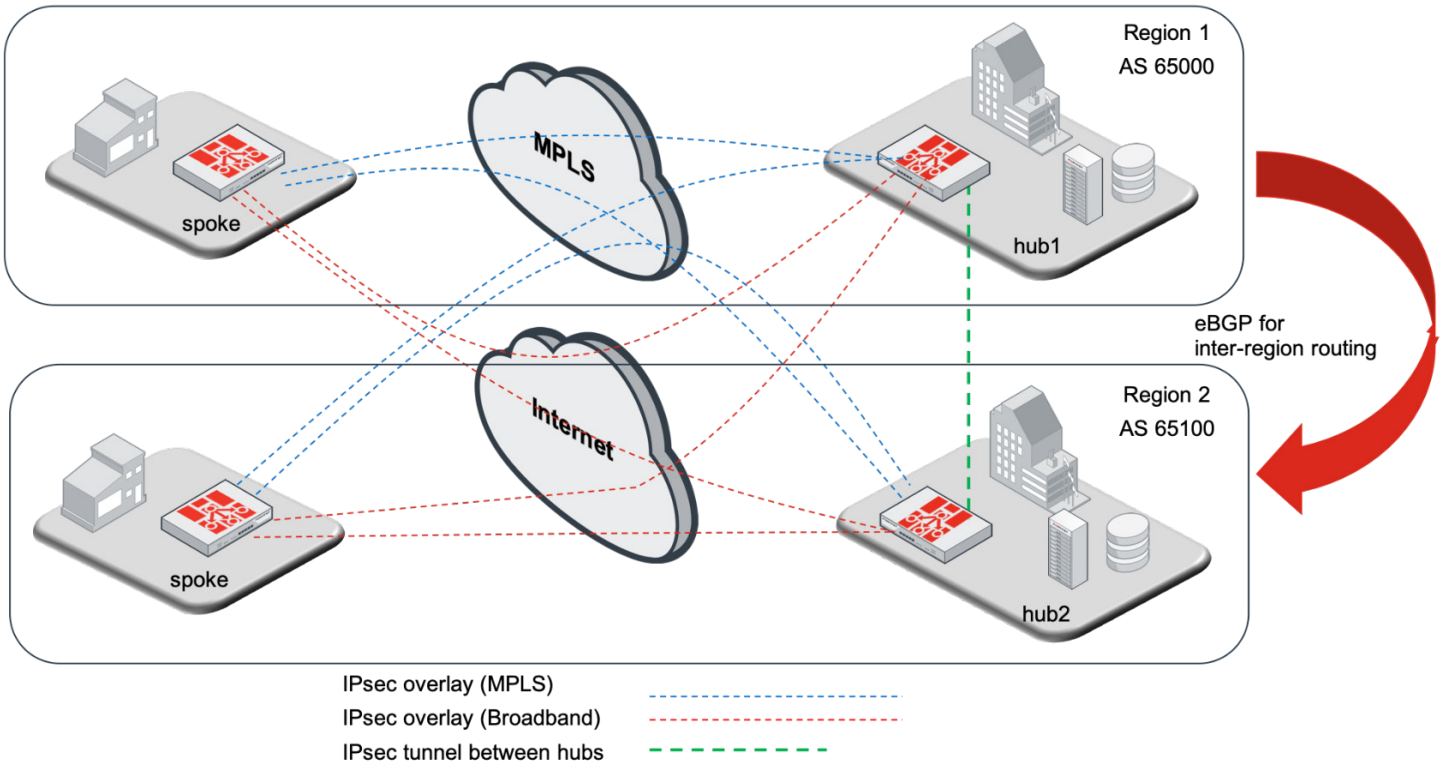



Figure 43. High availability (network level).

Each hub acts as the main destination for corporate applications during normal operations. This architecture topology provides support for disaster recovery scenarios. For example, if one hub becomes unavailable, then spokes can establish dynamic shortcuts (ADVPN) with other spokes and hubs located in the other region. Once again, BGP routing is used for maximum flexibility (iBGP for inter-region routing and external BGP [eBGP] for intra-region routing).

## Fortinet Secure SD-WAN Managed Service Support

We have described the key capabilities and advantages of Fortinet Secure SD-WAN from a product and architecture point of view. However, as demand for enterprise-level SD-WAN increases, organizations are increasingly moving from acquiring and operating their own SD-WAN equipment to using managed SD-WAN services. Therefore, it is critically important for an SD-WAN solution to provide a flexible multitenant support.

The following architecture shows the high-level architecture of Fortinet Secure SD-WAN from a managed service point of view:

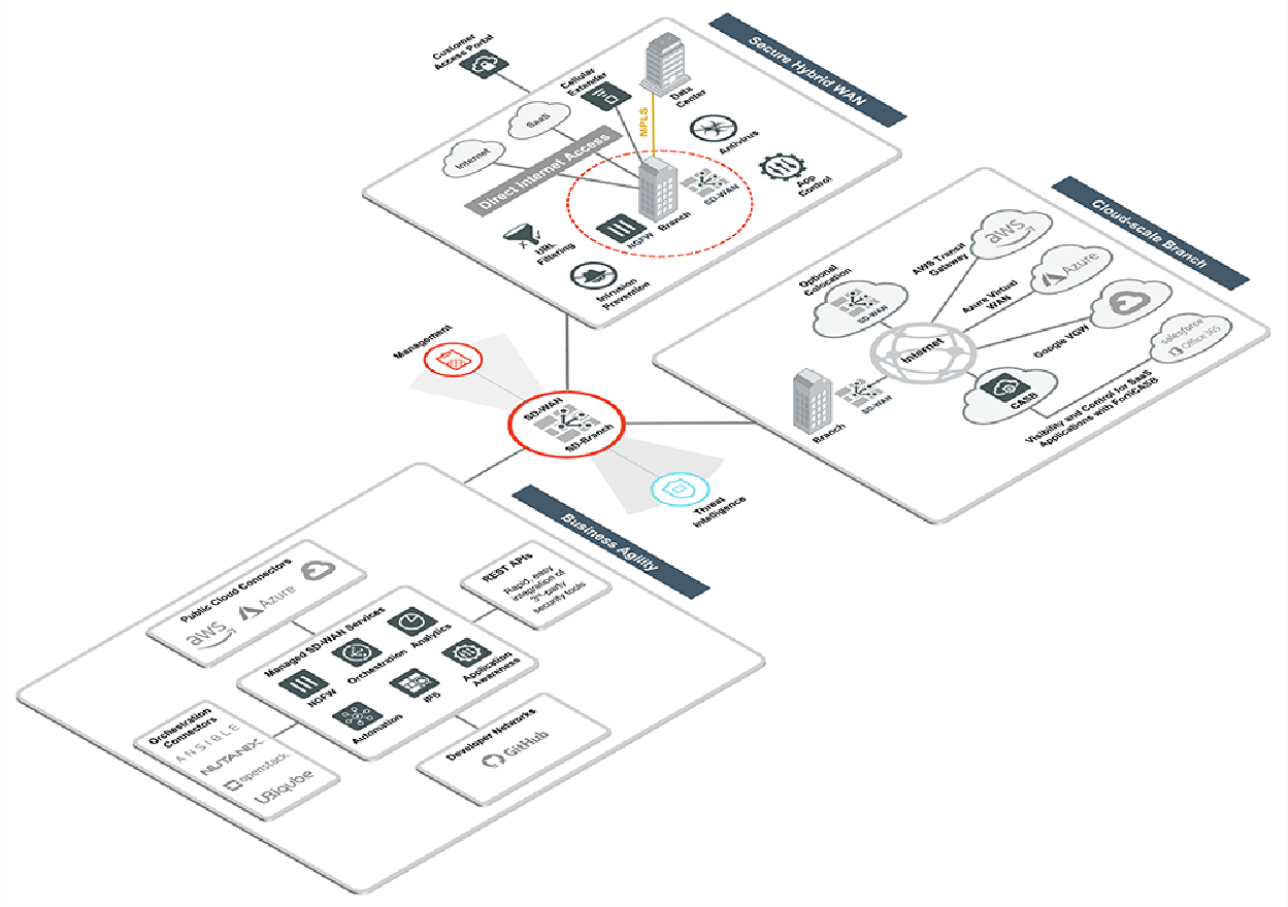



Figure 44. Fortinet Secure SD-WAN Managed Service architecture.

Fortinet Secure SD-WAN provides the following key benefits for managed service providers (MSPs) and managed security service providers (MSSPs):

### Visibility

The Fortinet Security Fabric enables:

- Out-of-the-box integration with over 250 third-party vendor products
- Single-pane-of-glass visibility and configuration management
- Real-time threat-intelligence sharing across a service provider's entire network environment

With Fortinet Secure SD-WAN, MSPs and MSSPs manage their customers' entire network infrastructure from a single pane of glass. FortiGate next-generation firewalls also support numerous administrative domains (ADOMs) and virtual domains (VDOMs), to provide management flexibility and support role-based access control (RBAC).

### Automation

MSPs and MSSPs can automate threat prevention, detection, and response, minimizing the overhead associated with securing customer environments with:

- An open-API architecture
- Out-of-the-box integration with over 250 third-party vendor products through 12 Fabric Connectors
- Over 135 third-party APIs
- Nine Fabric DevOps scripts
- Over 130 extended Security Fabric ecosystem partnerships

### Proactive, AI-driven threat intelligence

The Security Fabric orchestrates threat intelligence across and between each of the organization's security elements in real time. FortiGuard Labs leverages artificial intelligence (AI) and machine learning (ML) capabilities to pinpoint known and unknown threats and communicate actionable intelligence across the Security Fabric. Threat intelligence is enhanced through partnerships with over 30 threat-sharing organizations and integration with over 100 other vendor products. Fortinet Secure SD-WAN links a customer's entire security architecture via the Fortinet Security Fabric. This threat intelligence is communicated to all SD-WAN appliances in a customer's WAN, ensuring enterprisewide threat detection and prevention.

### Simplified operations

With FortiManager, Fortinet solutions can be easily deployed and centrally managed, allowing MSPs and MSSPs to easily roll out security infrastructure to new customers. FortiManager and FortiAnalyzer also allow MSPs and MSSPs to integrate and automate a client's security deployment via the Fortinet Security Fabric, enabling analytics and compliance reporting through FortiAnalyzer.

This integration also allows MSPs and MSSPs to break down silos that isolate security operations center (SOC) and network operations center (NOC) operations, enabling improved global visibility and more efficient operations. By deploying Fortinet Secure SD-Branch, centralized visibility and management is expanded to cover everything from the internet to the switching infrastructure in customer locations, simplifying security monitoring and management for MSPs and MSSPs.

### Zero-touch deployment

Fortinet devices are capable of touchless onboarding and provisioning with the ability to preconfigure deployment settings before sending devices to customer locations. Fortinet devices also allow a single key for supported devices on bulk orders and expose a JavaScript Object Notation/Extensible Markup Language (JSON/XML) API for device customization. This enables automated or programmatic deployment of Fortinet devices, enabling MSPs and MSSPs to eliminate truck rolls and achieve faster onboarding of new customers.

### Flexible consumption models

Multiple pricing and product consumption options offer MSPs and MSSPs and their customers the flexibility needed to optimally secure their data, infrastructure, and applications. This enables MSPs and MSSPs to scope their customers' SD-WAN deployments, and the value-added services that it supports, to meet their customers' specific needs.

### Multitenant by design

Fortinet solutions are designed to be multitenant from the ground up, enabling MSPs and MSSPs to isolate but still manage multiple customer networks from a single console. This enables MSPs and MSSPs to take advantage of cost savings by offering customers networking over shared, but isolated, SD-WAN infrastructure—increasing average revenue per user (ARPU) while improving operational efficiencies.

### MEF 3.0 certified

Fortinet is among some of the earliest SD-WAN technology vendors certified by MEF, the world's defining authority for standardized services designed to address the most demanding networking needs of today's digital transformation efforts.

Fortinet has been an active member of MEF since 2017, and is closely partnering with MEF to develop new SD-WAN security standards. Fortinet currently leads a key initiative in the MEF Applications Committee on application security for SD-WAN services (MEF 88) and has won two MEF 3.0 Proof of Concept awards, one for developing security standards for secure connections between separate SD-WAN devices, and another for ensuring application security for SD-WAN services.

This certification demonstrates Fortinet Secure SD-WAN's ability to comply with the highest industry standards required by service providers to deliver SD-WAN services. The Fortinet MEF SD-WAN product certification Test Report is available to learn more about test environment and testing methodology.

## Why Fortinet Secure SD-WAN Is the Best Choice

Fortinet simplifies necessary WAN edge architecture by providing a comprehensive Secure SD-WAN solution via FortiGate NGFWs and the Fabric Management Center (FortiManager and FortiAnalyzer) for centralized management and reporting. Consolidating numerous devices at the branch edge, FortiGate (with FortiOS) provides routing capability for support of both static and dynamic protocols. Additionally, FortiGate offers replacement of multidevice security architectures, without sacrificing performance, through the introduction of SPUs.

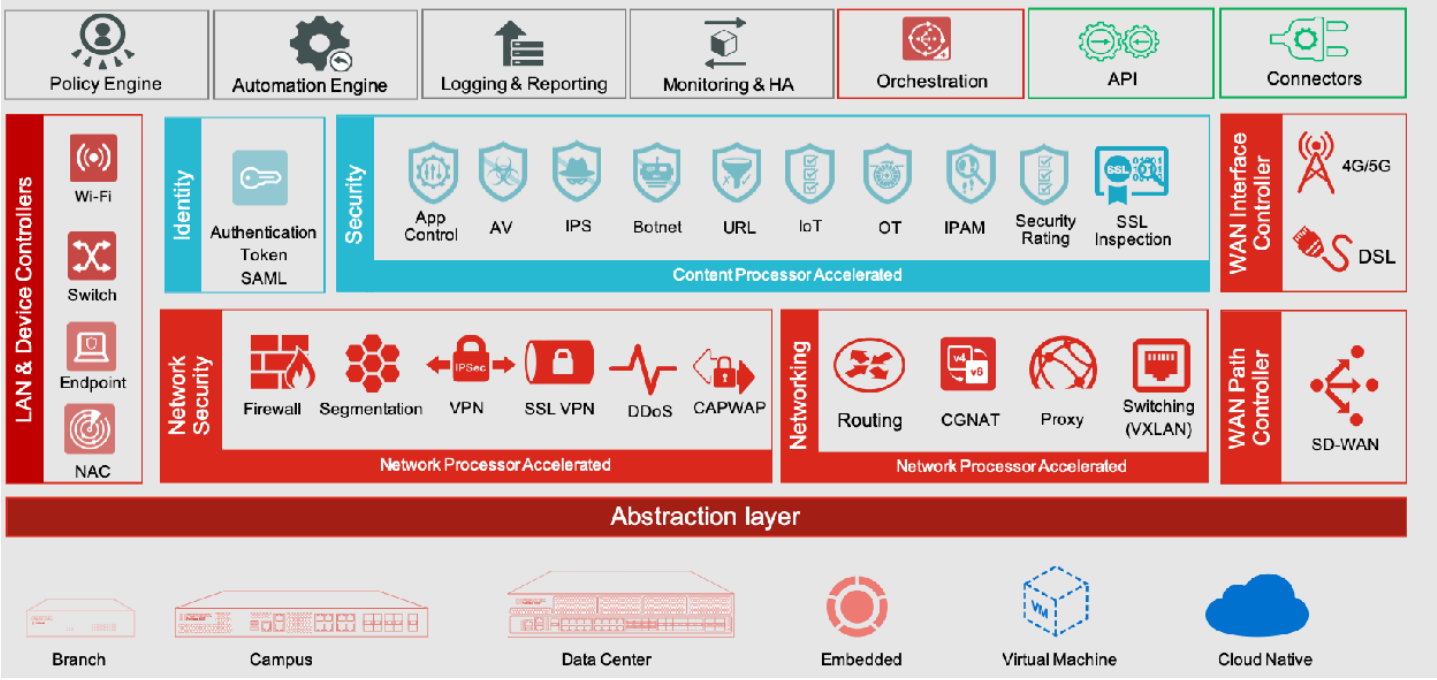



Figure 45. Secure SD-WAN system architecture: FortiOS.

FortiGate offers proven performance and manageability of SD-WAN core functionality. The FortiGate is the leading Secure SD-WAN solution delivering network and security architecture in one robust, easy-to-deploy and manage solution.

Lastly, the controllerless architecture provides maximum scalability to more than 10,000 sites without increasing overall complexity, since fundamental operations such as WAN overlay and routing are all taken care of by the SD-WAN Orchestrator running as a management extension within FortiManager.

www.fortinet.com



February 27, 2021 10:35 PM

D:\Fortinet\Work\2021\0227\wp-secure-sd-wan

888261-0-0-EN