FORTINET

WHITE PAPER

Fortinet Secure SD-WAN Reference Architecture

Executive Summary

The onset of digital transformation (DX) has introduced new technologies and solutions alongside lower-cost connectivity options for business, resulting in many organizations modernizing their legacy wide-area networks (WANs). With more and more data becoming digitized, the emergence of the public cloud, including the adoption of Software-as-a-Service (SaaS) applications, necessitates a redesign of the WAN architecture, specifically the branch, edge network, and security architecture. Software-defined WAN (SD-WAN) solutions leverage corporate WAN and multi-cloud connectivity to protect application performance at the network edge of branch sites.

This reference architecture white paper explains the evolution of WAN to SD-WAN architecture and highlights the benefits of modernizing networking infrastructure. It also provides details and security requirements with tips on what to look for when implementing a Secure SD-WAN solution from data center to branch.

Legacy WAN Architecture

Legacy WAN connectivity models, such as the one represented in Figure 1, often consisted of a single hub site, such as a data center or headquarters, with a single spoke or branch.

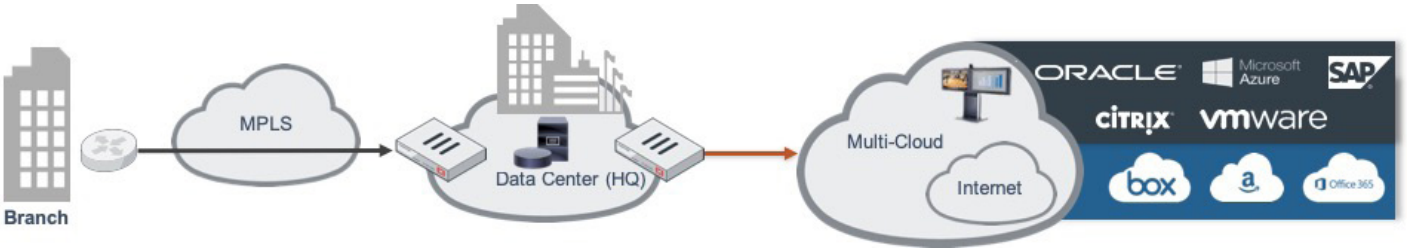

Figure 1: Legacy WAN hub-and-spoke architecture.

The routing aspect of traditional hub-and-spoke WAN architecture is simplistic in nature. Each spoke site must route all nonlocal traffic to the hub regardless of the final destination. Typically, this calls for a single static route, but adding redundant connectivity via multiple circuits can introduce higher levels of complexity. Traditional WAN architectures with legacy hardware and software solutions can still provide connectivity, performance, and security for organizations.

However, consider a branch user's legacy path to the public internet in Figure 1. To arrive at a website, packets would first need to traverse the WAN, navigate through a security stack, then proceed to the website. While this architecture traditionally minimizes branch infrastructure, it has for the most part fallen short when it comes to user experience. Users are often accustomed to broadband connectivity at their homes, something legacy WAN architecture fails to deliver for users.

Legacy security architectures deliver a centralized security stack across distributed enterprises. Figure 1a shows an example architecture where multiple functions exist within separate solutions. Branch sites might have a simple router for connectivity to an MPLS circuit, and because all traffic must first traverse the WAN, it makes sense to centralize advanced security capabilities at the data center instead of building distributed stacks at each branch. Due to the centralized stack architecture, WAN bandwidth has the propensity to become congested with traffic that ultimately will not be permitted to continue.

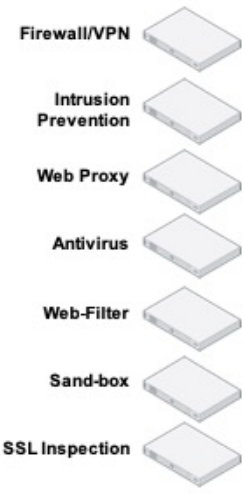

Figure 1a: Example security stack.

Fundamentals of SD-WAN

SD-WAN modernization is not just about replacing end-of-life hardware or software—it is a business solution. Organizations are adopting DX because the way business users consume technology has changed. Cloud adoption, device consolidation, and connectivity cost savings are significant drivers for infrastructure evolution. Delivering an improved user experience and increased productivity often motivate technology leaders to initiate WAN transformation projects.

SD-WAN Core Capabilities:

- Multi-path control
- Application awareness
- Dynamic application steering

Using control and data planes, SD-WAN solutions take advantage of branches with multiple points of connectivity to the internet or corporate WAN. It then decides which of these paths is most appropriate for a specific application. Data is transmitted over the optimal path to ensure performance and maximize availability.

SD-WAN protects application availability and performance across the corporate WAN or across the internet to multi-cloud environments by leveraging WAN path failover, link aggregation, link remediation, and active path performance metrics. Essentially, SD-WAN determines which path best meets performance expectations for a particular application and assigns packets or sessions to that WAN path.

Networking Improvements

A modernized WAN edge architecture with an SD-WAN solution implementation can demonstrate key improvements for an organization.

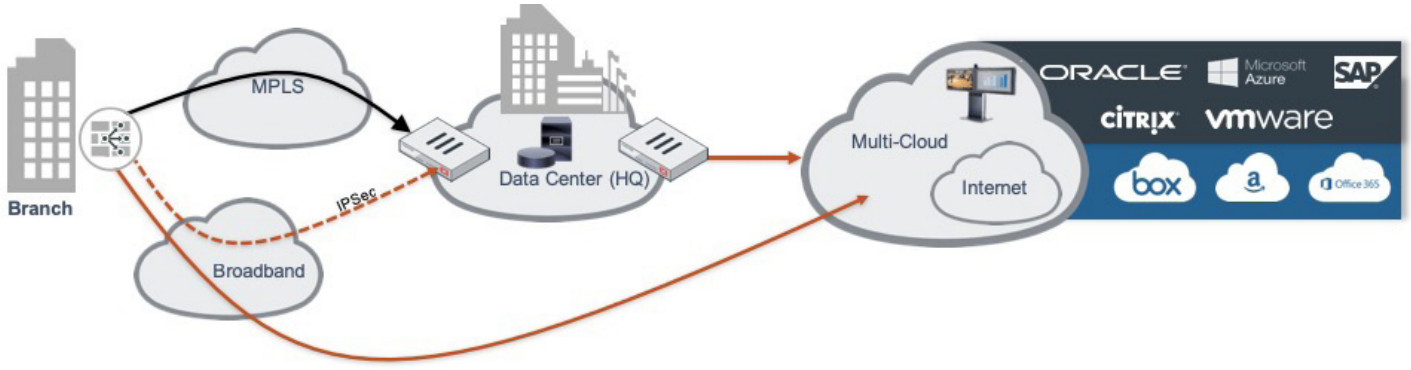

Figure 2: Modernized SD-WAN architecture.

As demonstrated by Figure 2, a branch with SD-WAN has multiple connections. In this example, the corporate WAN MPLS network remains, but the organization has introduced a single broadband connection to provide direct internet access from the branch. The organization has also established a secure IPsec tunnel to the data center over the broadband connection, creating a multi-path environment to both the data center and multi-cloud environment.

When compared to the legacy single-path architecture in Figure 3 with only one option to route traffic, it is clear why SD-WAN adoption is on the rise.

Figure 3: Legacy single path.

Secure SD-WAN

Introducing direct internet access at the branch also establishes direct connectivity to a volatile threat landscape. Branches with SD-WAN now require advanced security capabilities at the network edge. It is not enough to simply provide direct internet access with SD-WAN. Organizations need a Secure SD-WAN with built-in threat protection. Secure SD-WAN provides a security stack at the branch edge where it will provide direct services without traversing the corporate WAN.

Direct internet access applied to an MPLS-based WAN inherently provides for a redundant connectivity architecture. In terms of data-center connectivity, broadband delivers an alternative path for critical applications that will normally only traverse the MPLS network. In the same way, the MPLS network will continue to provide its path to the internet but is now superseded by the internet broadband connection.

Multi-path Control

The aforementioned core SD-WAN functionality demonstrated in Figure 2 highlights the need for multi-path control. There are three members that comprise the SD-WAN virtual link: an MPLS connection (blue), a broadband connection (solid orange), and an IPsec tunnel (broken orange). The Secure SD-WAN solution must be able to distinguish between applications to leverage the full functionality of the solution. By distinguishing applications and controlling multi-path environments, Secure SD-WAN provides dynamic application steering via packets or sessions to traverse available paths to the corporate WAN or multi-cloud environments.

Figure 4: SD-WAN virtual link.

Fortinet presents two main strategies for organizations to steer applications: best quality and minimum quality service-level agreement (SLA). Best quality determines which path is outperforming based on chosen metrics, by at least 10%. If the difference between the identified members is within the defined threshold, Secure SD-WAN selects the higher-priority link.

Alternatively, an organization may opt for an SLA strategy. FortiGate evaluates metrics defined within a performance SLA with respect to each member in the SD-WAN policy. If the primary path does not meet the SLA for the defined threshold(s), FortiGate will move the traffic to an alternate path. If no path meets the threshold(s), FortiGate chooses the path with the highest priority. To aid application steering, the Secure SD-WAN solution provides active path metrics. In conjunction with customer-defined SLAs, the SD-WAN policy engine determines which paths are viable transports for each application.

While SD-WAN routing is more complex than the legacy architecture, this implementation can continue to leverage static routes. Yet, Secure SD-WAN functionality controls route or path selection based on the dynamic application steering policy.

WAN Architecture Requirements

This section defines key high-level requirements for a WAN architecture modernization project. Noted requirements may be familiar to the reader, but all should not come solely from an organization's IT leadership or team members.

Improving Branch User Experience

It is important to understand how the branch business operates to measure and improve end-user experience. Though there are numerous IT/security considerations, there are also key business drivers that define a Secure SD-WAN design. It is beneficial for IT/security project leaders to meet with business leaders and end-users to gain the full scope of impact for new technology efforts.

For Secure SD-WAN projects, it is key to identify the applications branches use and where application servers reside (e.g., data center, multi-cloud, etc.). Once an organization has developed a relational diagram or map, the next step is to measure and determine performance baseline metrics for each application, then have the business prioritize these applications. Voice and video applications often take priority due to real-time communications requirements, but others that serve specific business objectives may fall into the critical category. Supporting the case with metrics to demonstrate gain goes a long way toward validating modernized WAN architecture.

Reduce Operating Expenses (OpEx)

Updating organizational contracts, agreements, or simple acquisition of WAN connectivity should reduce monthly OpEx. Organizations are able to take advantage of lower-cost, higher-bandwidth broadband connectivity in place of MPLS circuits.

Another means of reducing OpEx and potentially capital expenses (CapEx) is through device consolidation. Organizations with existing direct internet access may still be undergoing modernization with SD-WAN adoption. Some organizations have a costly infrastructure approach with multiple network and security vendors and disparate solutions at the branch edge. A Secure SD-WAN device is able to consolidate vendors and solutions, which reduces OpEx.

10X

The amount of potential savings by migrating from MPLS to SD-WAN.[1]

WAN Architecture Requires Security

Anything short of a fully integrated next-generation firewall (NGFW) is not delivering a Secure SD-WAN branch solution. Security services handoffs to third parties fall short of OpEx reduction regardless of whether the solution is on-premises or in the cloud. Further, the security architecture at the edge is not the same as the security architecture at the core. While unified threat management (UTM) devices have been protecting small and medium businesses (SMBs) for decades, they are also capable of serving enterprises.

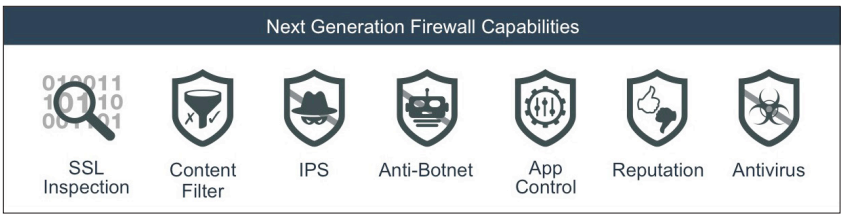

Figure 5: Security requirements.

UTMs can deliver sufficient security for distributed enterprise branch locations and provide services, including NGFWs, intrusion prevention systems (IPS), secure sockets layer (SSL) inspection, web content filtering, anti-malware gateways, and advanced routing compatibility. Device consolidation to a single, comprehensive Secure SD-WAN solution tackles the requirements listed in Figure 5.

Key Requirements Summary:

- Know the existing WAN architecture and how it serves business objectives
- List desired business outcomes of a WAN architecture refresh
- Understand security implications of the WAN architecture redesign
- Determine how much the organization spends on existing WAN architecture
- Establish a performance baseline to plan and achieve improvements

A Reflection of Existing WAN Architecture

While having accurate documentation and diagrams of an existing architecture may seem like an obvious step, it can be overlooked. Security architects can become burdened with remediation drills, resulting in a lack of detailed, accurate documentation of WAN architecture. An organization must understand its current WAN architecture to adequately propose a modernization project.

Fortinet Secure SD-WAN Solution Architecture

The Fortinet Secure SD-WAN solution is comprised of multiple components. Overall, the components that make up the Fortinet Secure SD-WAN solution are: FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy.

FortiGate runs FortiOS, the core of the Secure SD-WAN solution. **FortiManager** drives orchestration and management. **FortiAnalyzer** and **FortiDeploy** help the whole solution come together, delivering a solution that is unmatched by other vendors.

Figure 5a: Secure SD-WAN architecture components.

Secure SD-WAN must satisfy business outcomes with regard to the architecture and how they serve different roles within an organization (e.g., CIO, CISO, et al). It is also important to understand how other Fortinet solutions such as FortiExtender and FortiAuthenticator extend beyond SD-WAN, providing complete coverage across the branch to further build out the Fortinet Security Fabric.

Management, Control, and Data Planes

In organizations with small deployments of one to three sites, each FortiGate may act as a management, control, and data plane. More commonly, distributed deployments will utilize the full spectrum of Secure SD-WAN components. Such a deployment will divide the same roles, as shown in Figure 6.

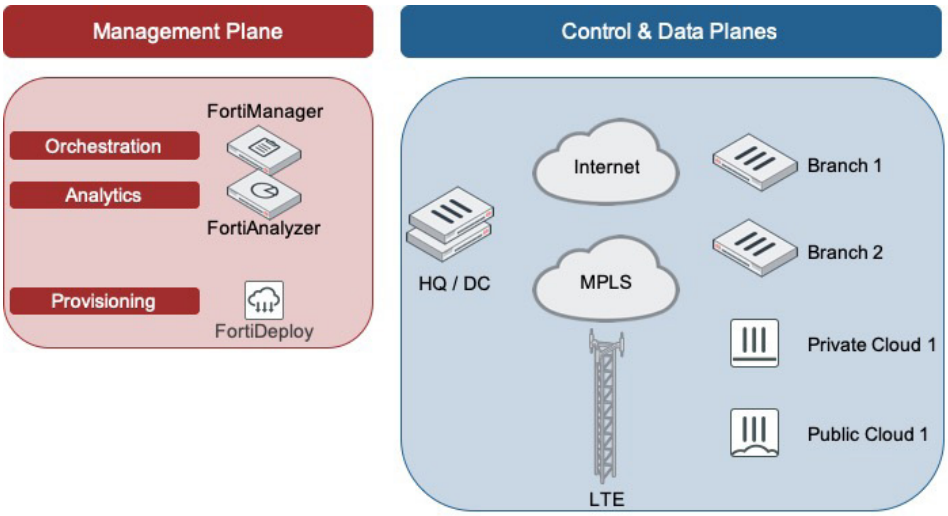

Figure 6: Secure SD-WAN architecture components.

The FortiGate, with its underlying operating system FortiOS, is the basic component of the Secure SD-WAN solution. It is able to stand alone and provide full functionality including NGFW, advanced security features, and SD-WAN capabilities. Acting in all roles, FortiGate easily consolidates WAN edge solutions into one comprehensive device. FortiGate also delivers routing protocol support (e.g., RIP, BGP, OSPF, etc.) and VPN pairing as a spoke or hub, enables WAN optimization via protocol optimization, byte, and object caching, and even acts as an access layer controller. In addition, the FortiGate supports packet priority to ensure those business-critical applications take precedence in times of congestion.

FortiGate Form Factors

With respect to distributed deployments and FortiGate models, typical edge devices range from the edge models 30E to 200E on the physical appliance implementation to VM01 to VM16 on the virtual machine implementation. Several small branch appliances come with Wi-Fi, 3G, 4G, and LTE options to further consolidate branch solutions.

The most popular FortiGate branch device is the 60E model. See an overview of the FortiGate 60E specifications in Figure 7.

Secure SD-WAN now supports IPv6.

It supports all load balance modes, health checking, and service rules for source address, source user and group, and destination address.

Newly released FortiOS 6.2 adds new capabilities and improves existing SD-WAN functionality.

New Features:

- Overlay controller VPN
- Bandwidth monitoring service
- Forward error correction
- BGP additional path support
- SLA logging
- Multiple IPsec tunnels as a single interface

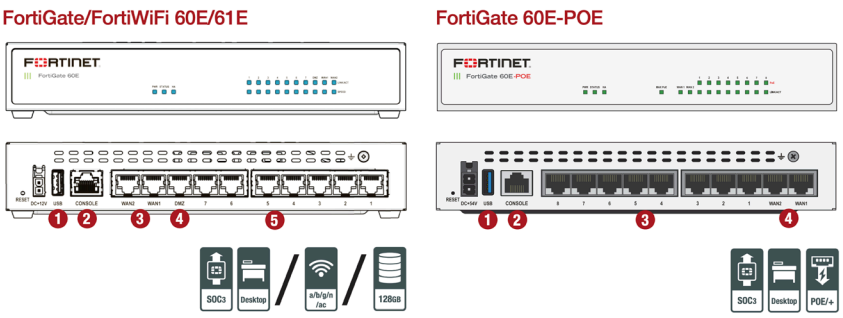

Figure 7: FortiGate 60E specifications.

Figure 8 details the performance data of the FortiGate 60E series appliances.

System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	3 / 3 / 3 Gbps
Firewall Latency (64 byte UDP packets)	3 µs
Firewall Throughput (Packets Per Second)	4.5 Mpps
Concurrent Sessions (TCP)	1.3 Million
New Sessions/Second (TCP)	30,000
Firewall Policies	5,000
IPsec VPN Throughput (512 byte) [1]	2 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	500
SSL-VPN Throughput	150 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	100
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	135 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	135
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	75,000
Application Control Throughput (HTTP 64K) [2]	650 Mbps
CAPWAP Throughput (HTTP 64K)	890 Mbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of Switches Supported	8
Maximum Number of FortiAPs (Total / Tunnel Mode)	30 / 10
Maximum Number of FortiTokens	100
Maximum Number of Registered FortiClients	200
High Availability Configurations	Active / Active, Active / Passive, Clustering

Figure 8: FortiGate 60E series performance specifications.

Most Secure SD-WAN branch deployments are going to implement IPsec tunnels to securely transport packets between branch sites, to the data center, or to the cloud. Considering typical branch deployment requirements, 2 Gbps of VPN throughput offers more bandwidth than many branches require. Enabling application control, which examines the application layer of packets, decreases throughput only to 890 Mbps, still supporting branch bandwidth needs. Enabling full secure sockets layer (SSL)/transport layer security (TLS) inspection and enabling IPS provides for 135 Mbps.

The reason the FortiGate 60E series appliance boasts such performance is because of the Fortinet system-on-a-chip (SOC3) purpose-built processor and now SOC4, the only purpose-built processor designed to accelerate SD-WAN.

The Fortinet incumbent SOC3 accelerates the 60E series security appliances to further speed its best-in-class throughput with consolidated security and networking capabilities. The SOC3 more than doubles the secure networking performance over the enterprise-class CPUs found in competing security solutions and propels the FortiGate 60E series distributed enterprise firewalls to unprecedented levels of security and performance.[2]

SOC4 Release

Fortinet recently released the SOC4 processor leading with the FortiGate 100F series appliance. The SOC4 is the only purpose-built processor specifically designed to accelerate SD-WAN capabilities.

World's First SD-WAN ASIC:

- Fastest application steering
- Accelerated WAN overlay
- Best-of-breed security performance
- Security extension acceleration

Specification	FortiGate 60E (SOC3 ASIC)	Industry Average (Based on this price point)	Distributed Enterprise Advantage using FortiGate 60E
Firewall	3000 Mbps	630 Mbps	**5x** higher firewall throughput compare to industry average
IPSEC VPN (AES256 and 1400 bytes)	3000 Mbps	275 Mbps	**11x** higher VPN with AES256 encryption compare to industry average helps more users to securely access public cloud applications
IPS Throughput	1400 Mbps	300 Mbps	**5x** higher IPS throughput compare to industry average benefits higher threat prevention
SSL Inspection	340 Mbps	45 Mbps	**8x** better SSL inspection throughput compare to industry average provides complete protection against rising SSL traffic
Concurrent Sessions	1.3 Million	0.27 Million	**5x** higher sessions compare to industry average increases the productivity as more users are getting benefit of complete security
Power Consumption	5 W	15 W	**3x** lower power consumption enables high scalability

**Industry Averages Calculated By Price Point of Competing Solutions from CheckPoint, Dell, and Cisco Meraki*

Figure 9: FortiGate 60E industry comparison.

Fortinet has a multitude of options to choose from after an organization has determined its branch edge requirements.

FortiGate Routing

Before an organization can properly introduce Secure SD-WAN into its WAN architecture, it first must lay out how packets might get from one site to another. In legacy networks, organizations might use static routes or border gateway protocol (BGP) for dynamic routing between a multitude of sites. FortiGate fully supports BGP, even for Secure SD-WAN deployments.

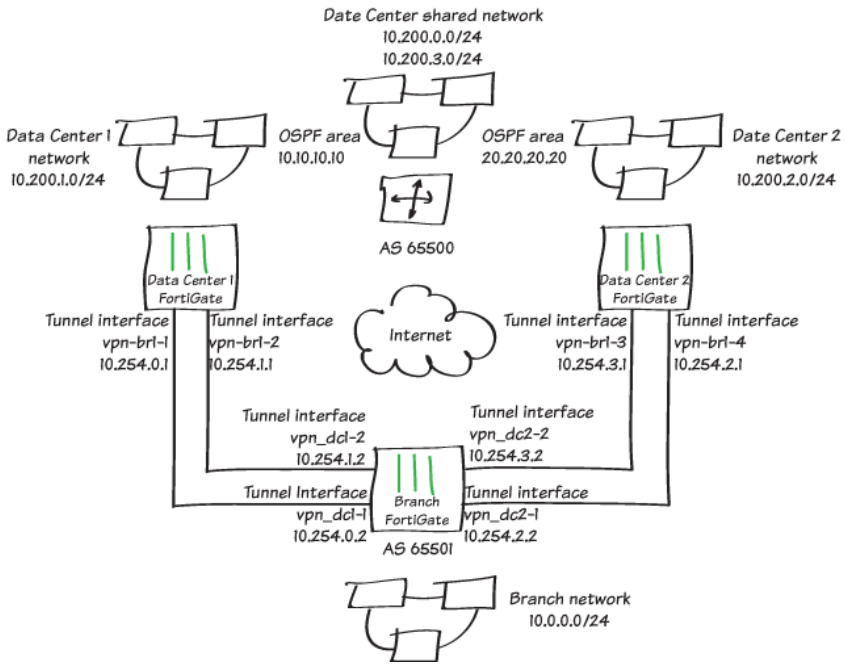

Figure 10: Client-side Secure SD-WAN with IPsec VPN.

Tech Tip

For all FortiGate models, the numeric differentiation denotes a larger amount of hard disk within the appliance. For instance, 61E comes with 128 GB SSD storage.

Figure 10 demonstrates the BGP routing environment within a private space. In this case, the customer is using IPsec tunnels over the internet to connect its WAN. AS 65500 is defined in the data center and AS 65501 is assigned at the branch. Data-center networks are advertised across the WAN to the branch by each of the FortiGate NGFWs at the data-center edge. 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 the right 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. Each network will advertise its own back end without advertising the other. Advertising both is possible and will work in some scenarios.

There is one note of caution when it comes to BGP and dynamic routing. Sometimes, as is the case here, we introduce networks that 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 (return path forwarding, or anti-spoofing), is something to look out for and address.

From the client side, FortiGate will advertise the 10.0.0.0/24 network. In addition to advertising their own routes, the data center FortiGate NGFWs will also act as route reflectors, letting all other participating members (branches) know about route updates from branch participants. This functionality reduces the necessity for each branch to communicate its route updates to all other branches. This can cause unnecessary overhead traffic and potential delays with updating routes across the WAN. There are other cautions for large networks concerning convergence times and memory consumption; yet, most enterprises will not likely encounter these challenges.

While Open Shortest Path First (OSPF) is noted in the diagram, FortiGate does not participate in this back-end data-center-to-data-center routing scheme (though the FortiGate does support OSPF). Engage the internal network architecture team when spinning up a Secure SD-WAN project to ensure that the routing scheme is both supported and properly designed.

Even though administrators and engineers must configure routes using the SD-WAN virtual WAN link, FortiGate installs individual routes for member interfaces into the routing table. These routes are each active and share similar attributes (e.g., destination address and subnet, distance, and priority). This action allows the FortiGate NGFW to remove individual routes in the event of an interface outage and to redirect all traffic to the remaining member interfaces without affecting SD-WAN members.

WAN Paths (SD-WAN Interfaces)

The FortiGate Secure SD-WAN solution is largely comprised of autonomous underlay and overlay interfaces aggregated into a single virtual WAN link.

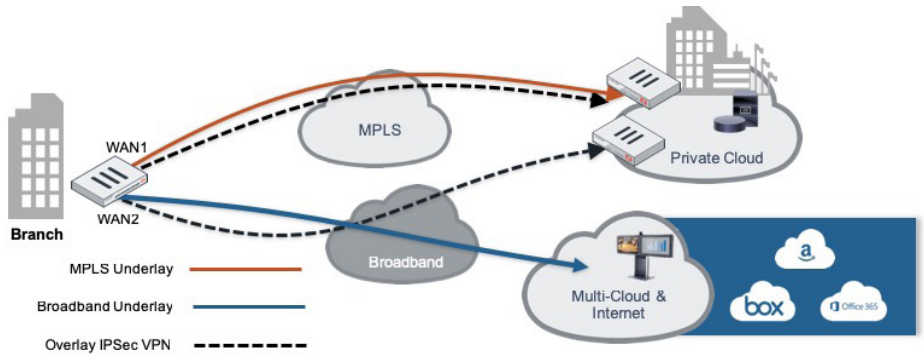

Figure 11: SD-WAN interface members (underlay and overlay).

Tech Tip

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

Terms to Know

Underlay transport
The raw transport typically associated with the wire attached to the FortiGate device. There is a one-to-one relationship between underlay interfaces and FortiGate physical interfaces. Examples include MPLS, broadband, or 4G/LTE connections over Ethernet.

Overlay transport
A virtual interface riding an underlay transport. There may be a one-to-many (physical interface to overlay interface) relationship for overlay transports. Examples include IPsec tunnel and VLAN interfaces.

In Figure 11, there are four unique interfaces defined on the branch FortiGate. From a physical perspective, there are two connections (WAN1 and WAN2)—one to the MPLS network and the other through the broadband provider. However, this organization has created two IPsec overlay interfaces—one tunneling over each physical underlay. In total, these four interfaces are all available to become members of the FortiGate virtual WAN link. This organization may choose to configure primary/secondary paths, or even aggregate multiple paths to increase bandwidth.

On the FortiGate NGFW, any defined interface, whether underlay or overlay, may be included as a member of the SD-WAN virtual WAN link. In FortiOS 6.x, each virtual domain (VDOM) may have one SD-WAN virtual WAN link or SD-WAN interface. If an organization is considering introducing VDOMs at one or more branch sites, the design team should consider inter-VDOM routing to ensure that the SD-WAN capabilities are leveraging more than one external WAN path.

Tech Tip

Not all interfaces within FortiGate must be added to the SD-WAN virtual WAN link. To exempt a nonparticipating interface, FortiGate supports the configuration of an implicit rule to address negation. This ensures SD-WAN policy-based routing rules do not match traffic unless the traffic is intended for SD-WAN interfaces.

Administrators must specify at least two virtual WAN link member interfaces. SD-WAN should be configured early during the initial setup of FortiGate because interfaces already referenced by a firewall policy or static route are not eligible to be added as a member interface.

Virtual Private Network Connections

VPN connections are instrumental in Secure SD-WAN deployments. As an overlay interface, VPN tunnels sometimes exist in some level of multiplier of the underlay interfaces.

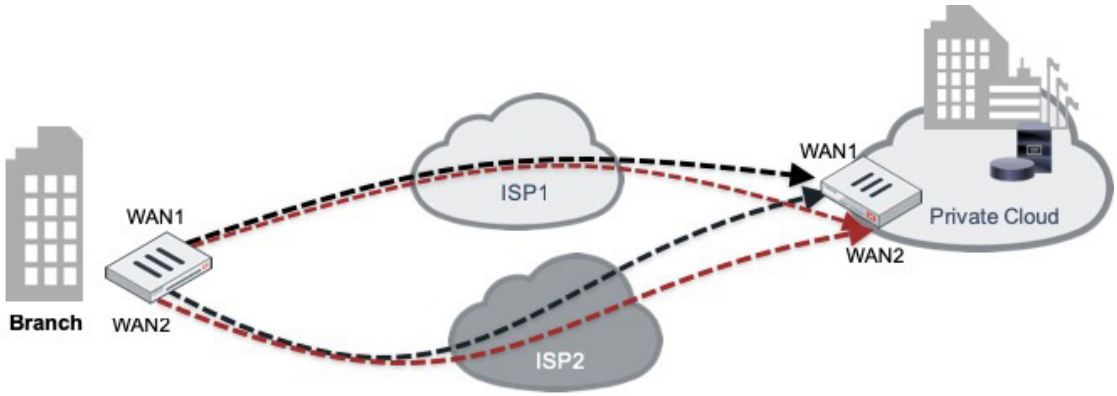

Figure 12: IPsec overlay interfaces.

There are two underlay interfaces in Figure 12 labeled WAN1 and WAN2. From these two interfaces, this organization has created four overlay interfaces on the branch FortiGate. Essentially, there is a full mesh of connectivity between the underlay interfaces using IPsec tunnels. In total, this particular organization may choose to add six interfaces to the SD-WAN virtual WAN link, consisting of the two underlay interfaces and four overlay interfaces.

FortiGate supports numerous connections for IPsec tunnels and architectures, from common hub and spoke and partial mesh, to full mesh VPN architectures. Figure 13 demonstrates a typical hub-and-spoke VPN architecture.

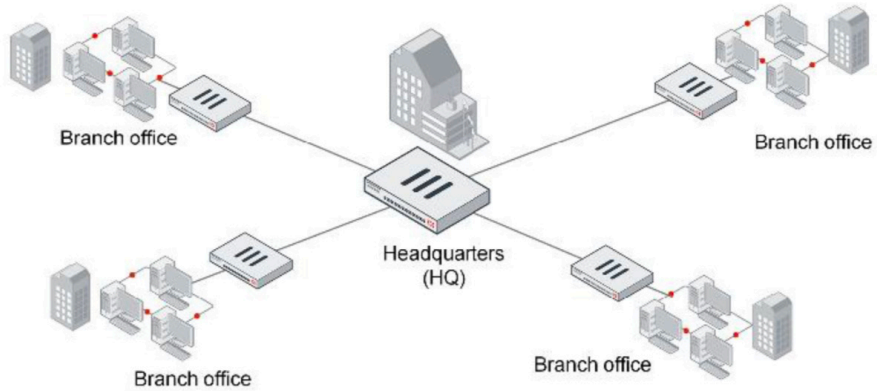

Figure 13: Hub-and-spoke WAN (VPN) architecture.

In this architecture, the path between sites passes through the hub. Further, in a legacy WAN environment, all traffic passes through the hub. However, with WAN edge modernization, each of these branch sites would receive direct internet access, allowing Secure SD-WAN to optimize path selection and protect application performance and availability, whether the application resides in the corporate data center or in a multi-cloud environment. Partial or full mesh provides branch sites with direct connectivity to one another. FortiGate includes auto-discovery VPN (ADVPN) to dynamically negotiate on-demand direct VPNs between spoke sites with the assistance of the hub site. While this capability typically requires the use of routing protocols so spokes are able to learn routes from one another, the FortiGate device serving in hub roles maintains a record of networks for each spoke and is able to communicate routes while facilitating a direct connection between two spokes.

Tech Tip

FortiOS 6.2 allows administrators to add forward error correction (FEC) to IPsec VPN members to lower packet loss ratio for critical business applications like voice and video.

Once an administrator configures the FortiGate IPsec tunnels, they can add the interface as members of the SD-WAN virtual WAN link. This allows FortiGate to leverage performance SLAs, SD-WAN policy, security policy, and prioritization as part of the SD-WAN virtual WAN link.

Integrated NGFW

The most beneficial aspect of Fortinet Secure SD-WAN are the integrated NGFW capabilities. Other solution architectures (e.g., offloading to third parties, tunneling to the cloud, etc.) are viable, but SD-WAN is primarily about WAN edge control and optimization. Therefore, it makes sense to perform as much control at the edge as possible without extending budgetary constraints. FortiGate meets and exceeds both of these requirements.

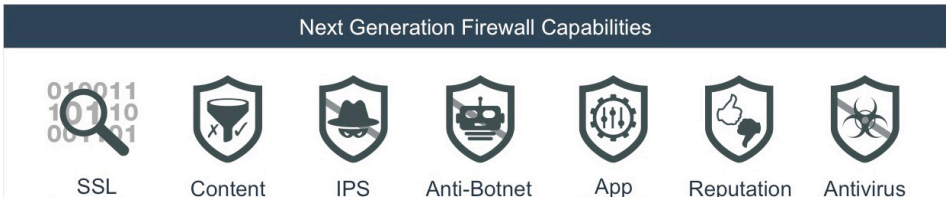

Figure 14: Security requirements.

Providing a full set of SD-WAN and security functions at the branch edge, prior to consuming costly bandwidth, FortiGate Secure SD-WAN is unrivaled in price, performance, and security effectiveness. Examine the architecture of FortiGate NGFW key features with respect to SD-WAN and WAN edge modernization.

The best value delivered in every FortiGate appliance is the SOC3. 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. This customized technology enables organizations to run multiple security applications without degradation in performance. Without performance degradation, an organization is enabled to run both SD-WAN and advanced security features on the same appliance (consolidation) and at the same cost (OpEx savings).

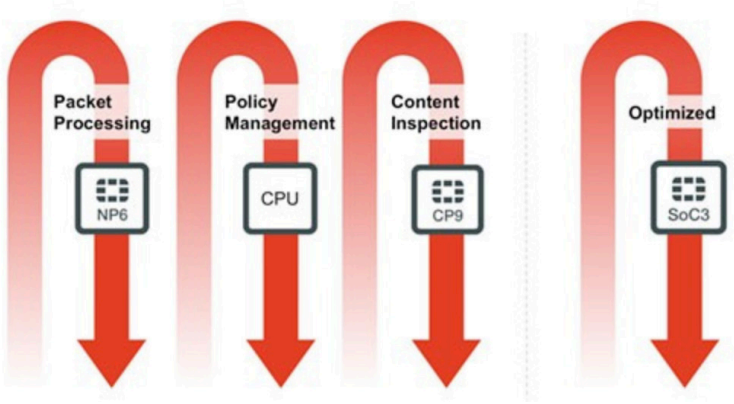

Figure 15: FortiGate parallel path processing (PPP).

The security processors in Figure 15 are used to scale from 1 Gbps to 1 Tbps of firewall throughput—independent of packet size. Fortinet parallel path processing architecture optimizes the high-performance hardware and software resources available in packet flow to deliver ultra-low latency and maximum throughput.

FortiGate is a stateful packet filter (firewall) at its core, ensuring secure session-based connectivity from the branch edge. FortiGate is 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, the FortiGate security policy is simplified. Instead of providing rules for individual virtual WAN link members, one only needs to identify the SD-WAN interface within the policy. The policy will apply to all member interfaces, making it easier for organizations to combine SD-WAN and security capabilities in one interface, whether that be the FortiGate itself or FortiManager. This provides granular authorization and access control, along with a mechanism to introduce advanced security features at the branch edge.

While application control is necessary for SD-WAN dynamic application steering, it also plays a role in security. For example, some organizations 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, organizations need a combination of SSL inspection, application control, and security policy features for the SD-WAN interface.

Without SSL inspection, any device would be incapable of determining the activity of the session. Without application control, the edge device would not be able to quickly determine the application, therefore allocating the session to subsequent rules. Even if organizations could identify application and user activity, they cannot introduce a granular identity-based security policy without a firewall rule base. These combined features allow for not only precise WAN path control but also the introduction of advanced security features, including IPS, anti-malware, and URL filtering.

In addition, FortiGate supports offloading file samples to a FortiSandbox for zero-day malware protection. FortiGate enables a single, full security stack.

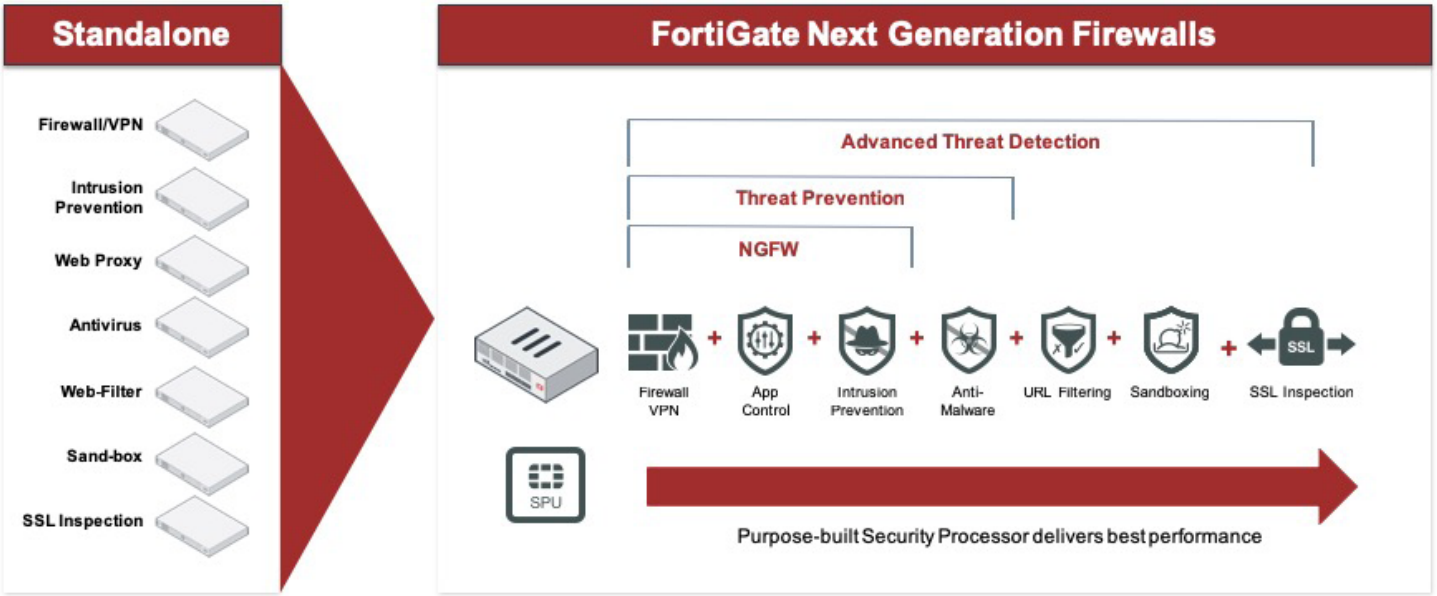

Figure 16: Standalone versus FortiGate security architecture.

A standalone branch edge strategy appears costly. Fortinet packs all seven of the featured capabilities into FortiGate form factors with unrivaled performance, with threat intelligence driven through Fortinet's own FortiGuard Labs global threat research and response team.

SD-WAN Packet Prioritization

Legacy WAN architecture typically includes quality of service (QoS). Where MPLS networks exist, so do low-bandwidth connections, leaving some branches with slow connectivity. While these may be more than sufficient for some branches, they also beg for QoS features to protect critical business applications. Typically including voice (VoIP) and video, these applications are marked at an edge device (router), so they receive priority transmission over the WAN. In addition, the FortiGate also provides packet-shaping capabilities, including default priority buckets and differentiated services marking. Priority allows critical business applications to receive preferential ordering across a specified virtual WAN link member interface if congestion begins to impact overall performance of that interface.

Management and Orchestration

FortiManager provides centralized management and orchestration of Secure SD-WAN branch edge devices. An organization's FortiManager may reside on-premises, in a private cloud, or in public cloud environments. Regardless of location, FortiManager maintains connectivity to each FortiGate device, monitors performance SLAs, and presents a single-pane-of-glass view into global connectivity. It also provides templates for security policy configuration, SD-WAN policy configuration, and performance SLA definition.

Secure SD-WAN administrators only need FortiManager to control their entire deployment. With flexibility to support APIs and Security Fabric Connectors, FortiManager seamlessly integrates into the greater workflow within any organization.

Tech Tip

Use IPsec VPN templates to configure site-to-site VPN tunnels (via FortiGate or FortiManager). Because there are many options to configure when setting up tunnel negotiation, templates reduce the chance for manual mistakes.

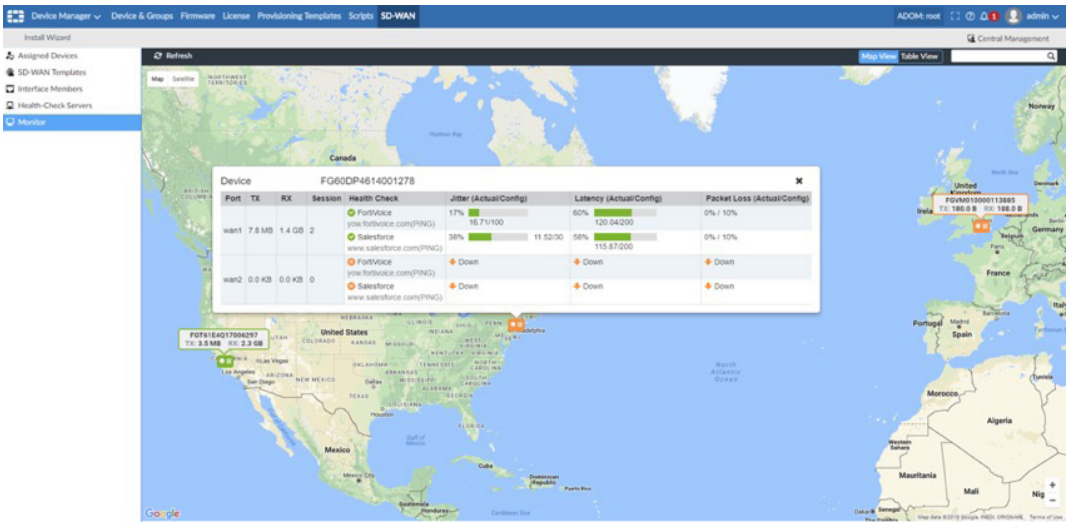

Figure 17: FortiManager geographical monitoring.

Zero-Touch Deployment

FortiManager is also a key part of enabling zero-touch deployment (ZTD). By adding a ZTD key to an order, organizations register devices in the FortiDeploy system as ZTD devices. Customers then identify a routable IP address for FortiManager in the FortiDeploy system. When a new device is simply plugged into power and connected to the internet via Ethernet, FortiGate automatically calls home, receives the FortiManager IP address, and immediately requests connectivity to FortiManager.

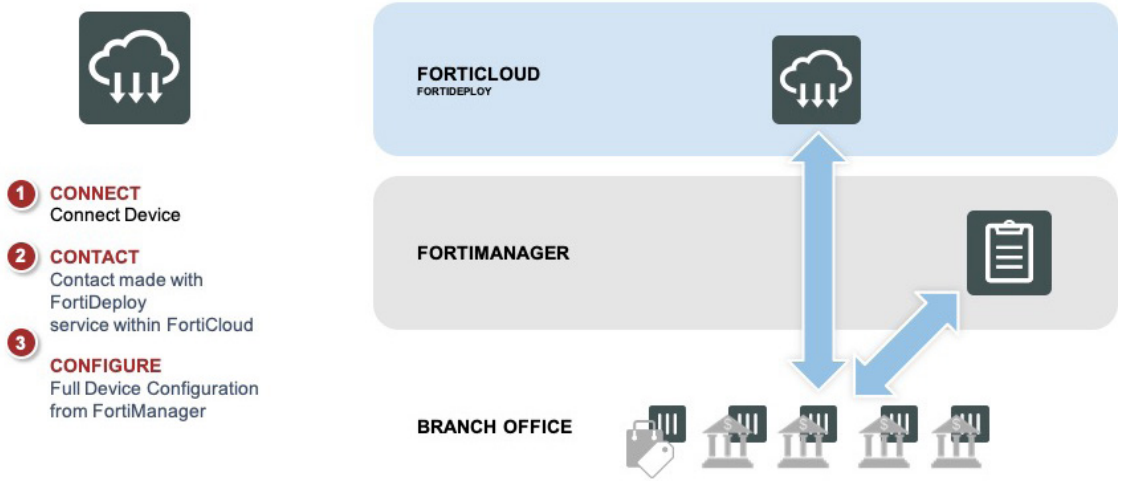

Figure 18: Fortinet zero-touch deployment process.

Once the devices are authorized, FortiManager pushes configuration templates to each device, fully configuring them for security and SD-WAN functionality at the branch.

Conclusion

Fortinet simplifies the necessary WAN edge architecture for organizations by providing a comprehensive Secure SD-WAN solution via FortiGate. 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. Finally, FortiGate offers proven performance and manageability of SD-WAN core functionality. FortiGate is the only Secure SD-WAN solution delivering network and security architecture in one robust, easy-to-deploy, and easy-to-manage solution.

[1] Based on internal Fortinet research and testing.
[2] Ibid.

April 3, 2019 8:50 AM

379990-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:WP-Fortinet-Secure-SD-WAN-Architecture:wp-fortinet-secure-sd-wan-architecture Folder:wp-fortinet-secure-sd-wan-architecture