FORTINET

Concept Guide

SD-WAN / SD-Branch

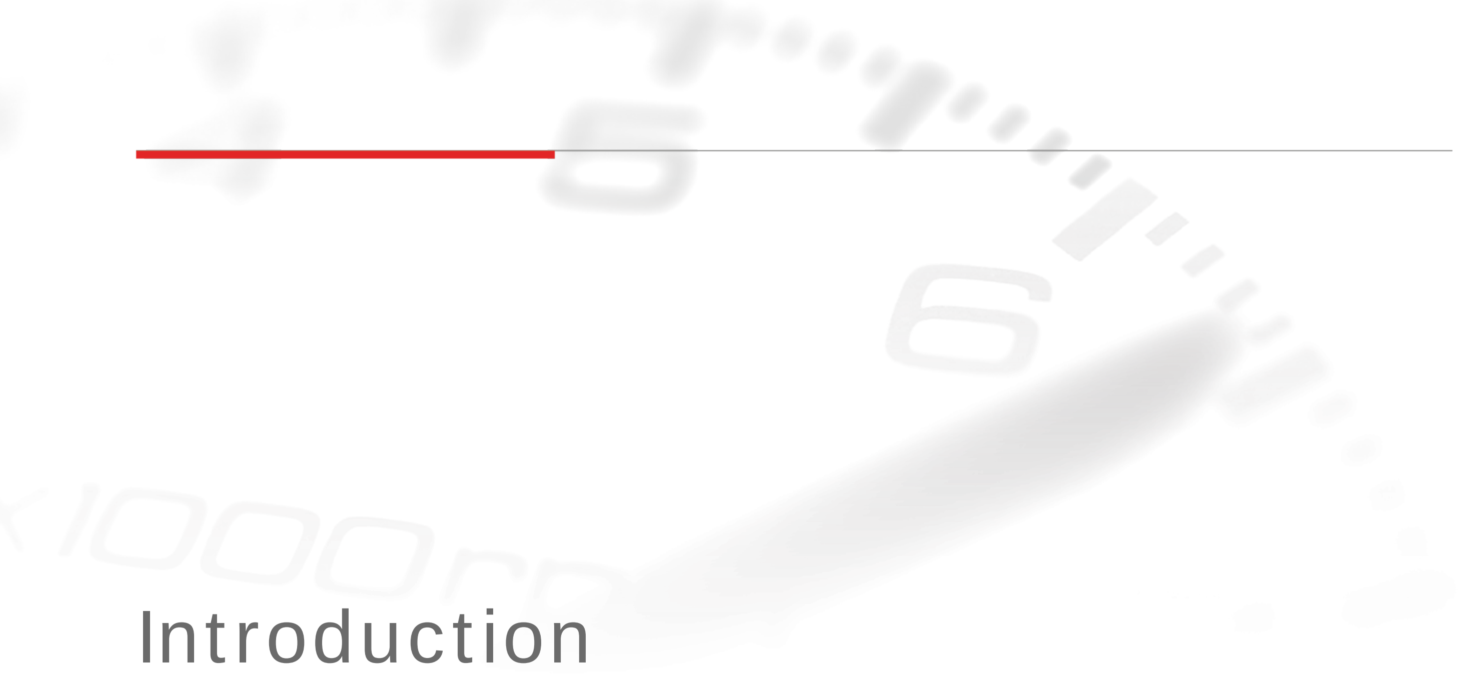
4D

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change Log

Date	Change Description
2022-04-04	Initial release.
2022-07-13	Added SD-WAN definitions on page 7.



Introduction

The intention of this document is to define some of the common concepts, use cases, and terminology in the Fortinet Secure SD-WAN solution. Once we have defined what we aim to solve with SD-WAN, our next step is to design our network. The design portion is covered in the Fortinet SD-WAN Reference Architecture Guide, which covers the Fortinet technology involved in deploying various types of SD-WAN designs, along with considerations and best practices. Once we have defined and designed our network, our next step is to deploy. Fortinet's SD-WAN Deployment Guide will cover the how-to configuration for some of the common architectures and designs covered in the Reference Architecture.

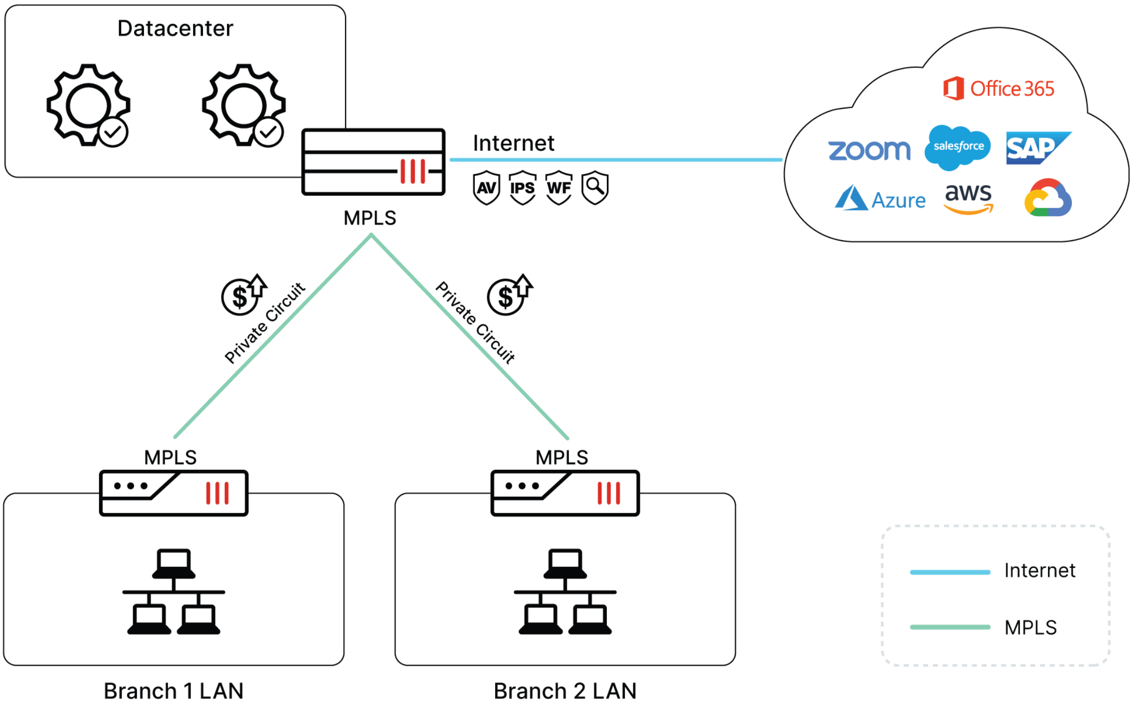
For more information and documentation about the topics covered in this document, please see the Fortinet Document Library at https://docs.fortinet.com.

This section includes the following topics:

Legacy WAN edge

For decades, the hub-and-spoke network architecture portrayed in the following image has been commonplace. All network traffic flows through the central corporate datacenter—including traffic moving from branch locations to the internet. Branch traffic travels to the datacenter 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.



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:

- Path failover
  Moving flows from an under-performing transport to a transport that performs better
- Remote destination monitoring and steering
  Detecting issues at a remote location and re-routing traffic through optimal paths
- Link aggregation
  Taking advantage of multiple WAN transports
- Active path performance metrics
  Viewing WAN underlay metrics and trends
- Application performance improvement
  Improving user experience by using a variety of techniques, such as Forward Error Correction, Packet Duplication, QoS, and WAN Optimization

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.

Transforming the WAN edge

The simplicity of the legacy WAN architecture 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. Legacy WAN architectures that consist of aging hardware and software solutions continue to provide network connectivity as well as a consistent level of performance and security, and they continue to satisfy some organizations.

However, if an organization needs to add redundancy or additional bandwidth to a legacy WAN infrastructure, complexity can quickly increase. 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.

For a diagram of the legacy WAN architecture, see Legacy WAN edge on page 4.

Improving inefficient routing and inferior performance

Even if an organization avoids the complexity of multiple static routes or a dynamic routing protocol, its network traffic is extremely inefficient. Consider a branch user’s legacy path to the internet in a legacy WAN architecture. 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 datacenter
- Negotiate its way through a centralized security stack that includes a firewall, intrusion prevention system (IPS), antivirus/anti-malware (AV/AM), data loss prevention (DLP), web filter, and so on
- Travel to the Google website through the datacenter 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 employees use cloud-based services that require more bandwidth, performance has only declined.

For a diagram of the legacy WAN architecture, see Legacy WAN edge on page 4.

Fixing 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 datacenter, 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.

Modernizing WAN

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 digital transformation (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.

Reducing risk with Secure SD-WAN

Secure SD-WAN adds the advanced security capabilities of a next-generation firewall (NGFW) to the networking solution. It's no accident that the icon in the modernized SD-WAN branch edge solution that represents 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.

For a diagram of the modernized SD-WAN branch edge solution, see the *Introduction* in SD-WAN Architecture for Enterprise.

Supporting DX initiatives

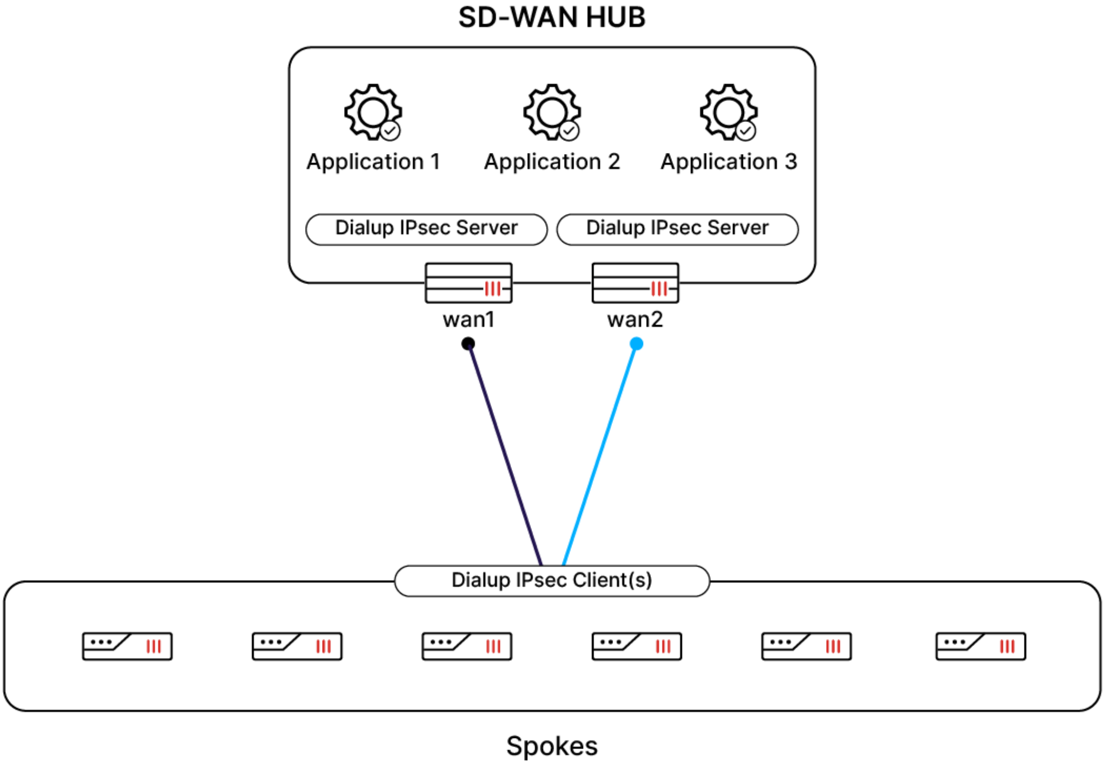
In summary, for this high-level secure SD-WAN architecture example, digital transformation (DX) is the driver for branch edge modernization. Organizations are creating projects to address WAN connectivity models (such as MPLS, Long-Term Evolution (LTE), and broadband) and edge device consolidation (such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

SD-WAN definitions

SD-WAN hub

In a hub and spoke topology, the hub is the central termination point for devices in a corporate region. In the Fortinet Secure SD-WAN Solution, the hub serves two main purposes:

- Inter-site connectivity (IPsec server): Front-end connections from spoke devices to private resources
- Routing (BGP and/or P2 selectors): Centralize routing and facilitate ADVPN connections for spoke-to-spoke traffic

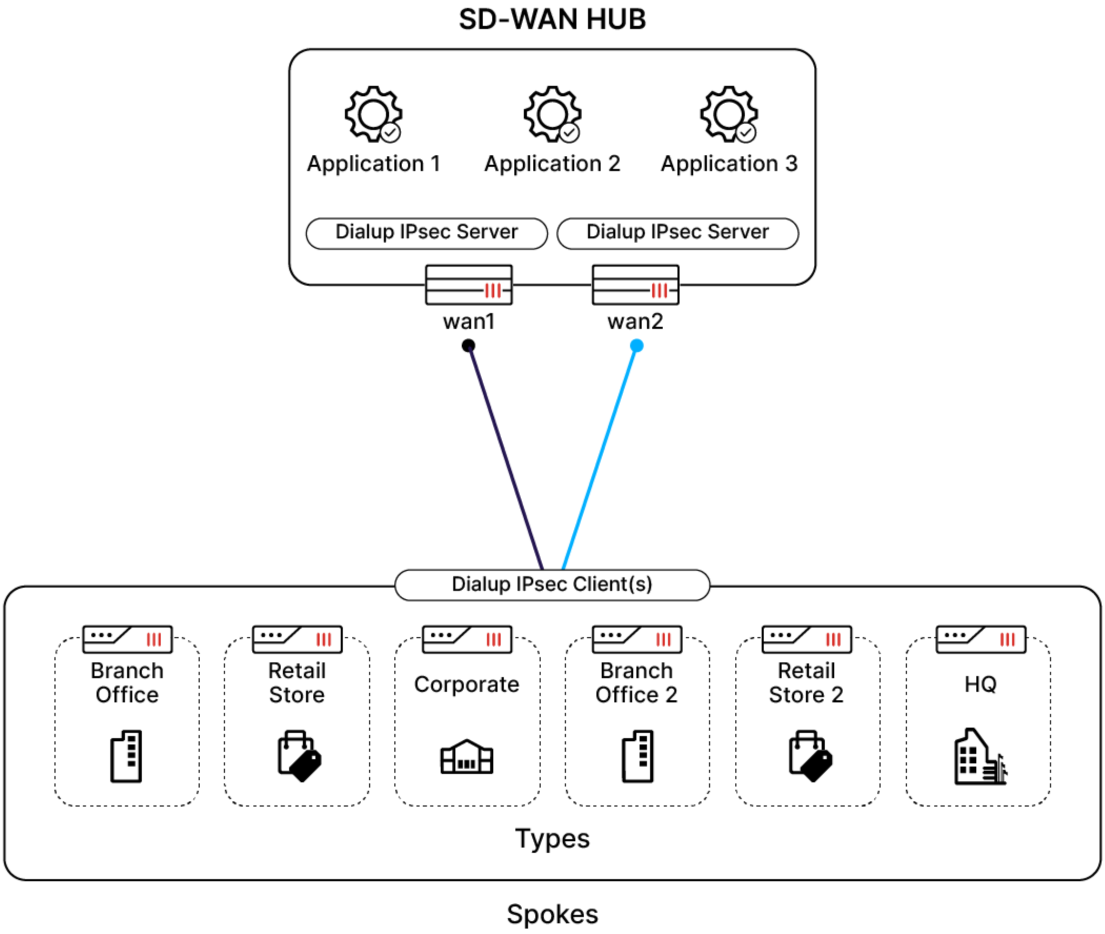


The SD-WAN hub is traditionally hosted near private resources or services that other locations need to access. Examples include:

- Headquarter (HQ) locations
- Datacenters
- Large campuses
- Public cloud providers

SD-WAN spoke

A spoke can be defined as any device in a corporate region that initiates an IPsec connection to a central location (hub). Traditionally, spokes are corporate locations that require access to a resource hosted at the hub location. Spokes connect to the hub as the IPsec initiator and peer with the hub by using BGP for routing between the SD-WAN region.



Spokes are often called *branch* locations, but can be any remote location that needs to connect to a corporate resource behind the hub. Common examples of spoke locations include:

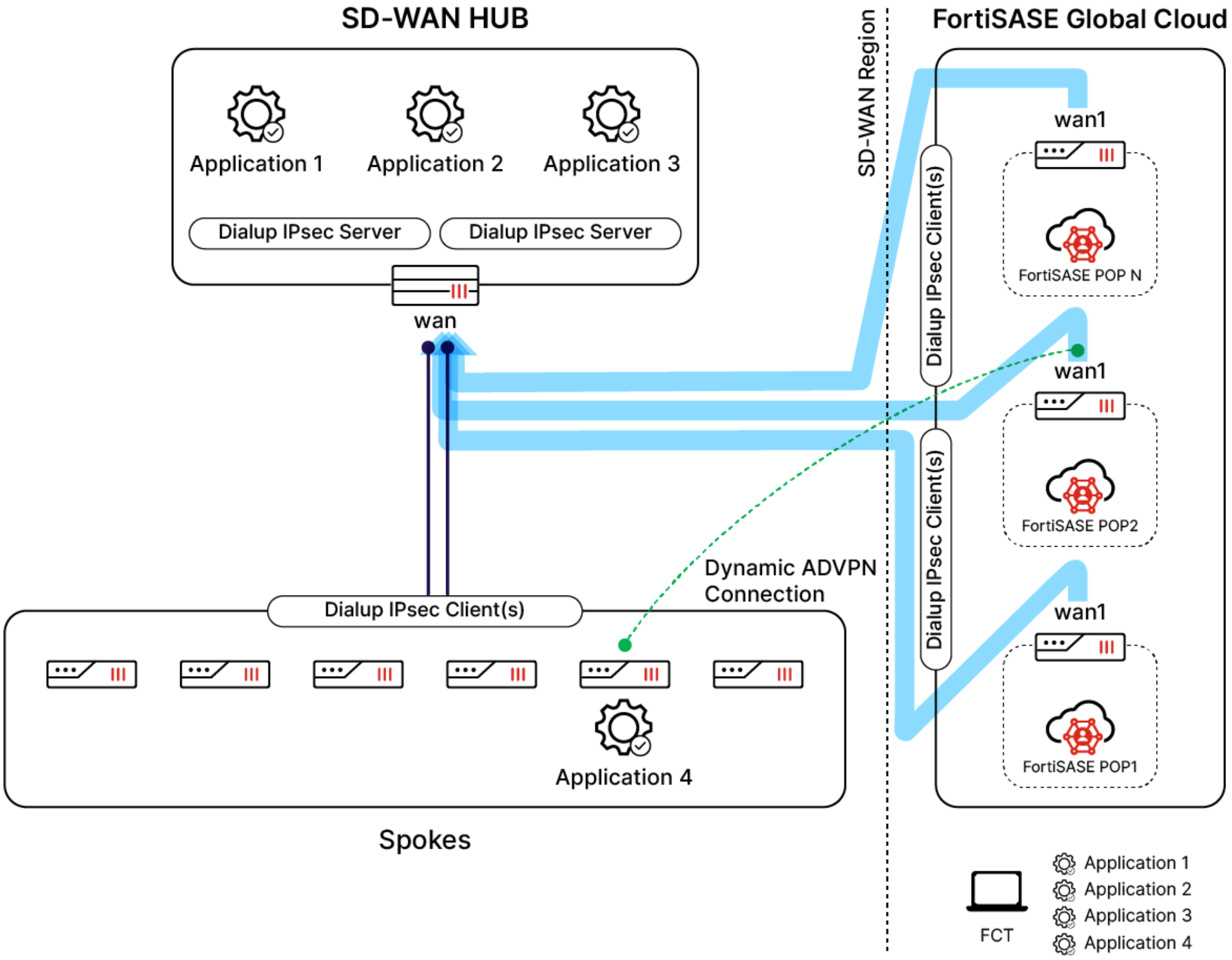
- Branch offices
- Retail locations
- Gas stations
- Other corporate locations

Spoke locations that need access to private resources behind the hub(s) may access it directly. When resources are located at another spoke location, they may connect directly through a dynamic ADVPN connection.

SASE spoke

There may be use cases where FortiSASE users require access to corporate resources inside the SD-WAN region. Customers that need to integrate FortiSASE with their corporate network may configure their SD-WAN region settings from the SASE portal.

In this scenario, the customer instance at each FortiSASE POP location initiates an IPsec connection to one or multiple hubs. This effectively makes it another *spoke* in the region, and may access resources behind the hub or at another spoke location.

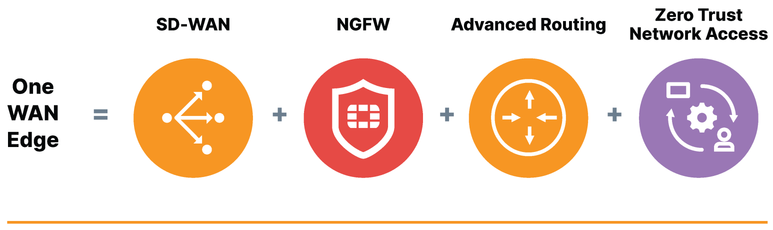


Users behind FortiSASE may access private resources directly through FortiSASE to hub(s) IPsec connections. If resources are behind another spoke device, they may connect directly to that resource through a dynamic ADVPN connection.

Why Fortinet

Fortinet offers a broad portfolio of integrated and automated security tools covering network security, cloud security, application security, access security, network operations center (NOC), and security operations center (SOC) functions.

The Fortinet Secure SD-WAN solution accelerates network and security convergence with enterprise-grade SD-WAN, advanced routing, Next-Generation Firewall, and recently added access proxy for Zero Trust Network Access (ZTNA) support. This simplifies the LAN and WAN architecture to provide a unified Fortinet WAN edge—powered by a single OS and controlled with a single management solution. Not only are we providing the best-in-class SD-WAN solution, but the technology is also integrated with network access to deliver the most secure and manageable remote branch in the industry.



One WAN Edge Powered by **One** OS, **One** Management

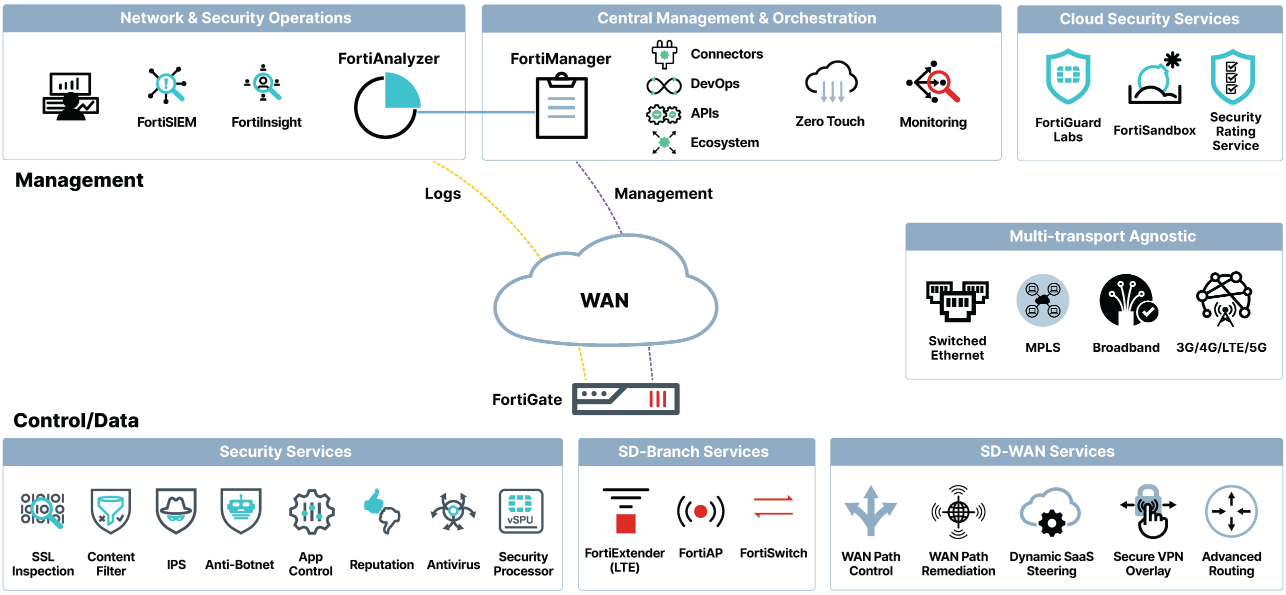
The Fortinet Secure SD-WAN goes beyond traditional SD-WAN requirements to provide a flexible and scalable fit for all enterprise sizes and requirements. The FortiGate device, with its underlying firmware FortiOS, is the basic component of the Secure SD-WAN solution. It offers self-healing capabilities without the bottleneck or single point of failure a centralized orchestrator would provide.

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. In other words, 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).

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. The following image 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.



Industry leader

Fortinet is recognized as a Gartner Leader and positioned highest for Ability to Execute in WAN Edge Infrastructure. It is also ranked number one in three out of five Critical Capabilities use cases, which is higher than any other vendor.

Fortinet is also amongst the earliest SD-WAN technology vendors to be certified by the Metro Ethernet Forum (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 them 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 for developing security standards for secure connections between separate SD-WAN devices, and for ensuring application security for SD-WAN services.

Intended Audience

This guide has primarily been created for a technical audience, including system architects and design engineers who want to deploy Fortinet Secure SD-WAN or Secure SD-Branch in a managed offering capacity.

It assumes the reader is familiar with the basic concepts of applications, networking, routing, security, and high availability, and has a basic understanding of network and datacenter architectures. For implementation, a working knowledge of FortiOS networking and policy configuration is ideal.

Uses cases

FortiGate SD-WAN is a flexible solution that can be used to cover a broad range of different use cases. This section covers some of the most common use cases.

Use case	Description
Dynamic application steering across multiple WAN links	Dynamic application steering across multiple WAN transports based on the business intent.
Redundant connectivity for enterprise branch	Leveraging multiple WAN transports to provide branch redundancy from failures and reduced performance. WAN links may include private circuits, public internet, LTE/5G, or satellite connectivity.
Reduce WAN OPEX with direct internet access	Secure, local internet breakout of SaaS applications and internet traffic without the need to offload to a remote location.
Secure and automated intra-site connectivity	Secure transport and connectivity of corporate traffic between branch, head quarters, datacenter, and other locations.
Multi-cloud connectivity and cloud on-ramp	Connectivity and intelligent steering of network traffic between one or more cloud locations.
Application performance improvement	Improving application and network performance by using various methodologies, including steering between best performing links, QoS, WAN remediation, WAN optimization, and more.
Work from anywhere	Remote workers connecting to corporate resources from any location.

This section includes the following topics:

Dynamic application steering across multiple WAN links

One of the most common SD-WAN use cases is to leverage multiple WAN transports to dynamically steer network traffic based on the business intent. The FortiGate SD-WAN's 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.

By leveraging a variety of different methods described in this documentation, the FortiGate SD-WAN chooses the optimal path based on the business requirements and protects the application as it traverses the WAN.

Redundant connectivity for enterprise branch

Modern branch locations require maximum availability and uptime for business-critical services. A combination of private circuits (MPLS), public internet, LTE/5G wireless connectivity or satellite WAN transports may be required to achieve redundancy from WAN failures and impairments. The SD-WAN solution needs to manage a hybrid of public and private WAN connections, while also providing intelligent steering across multiple, diverse connections.

FortiGate SD-WAN provides sub-second detection of issues across all available WAN paths to provide failover based on user configuration SLA's. Using the techniques we'll review in this document, SD-WAN rules may be configured to take advantage of all available paths based on the business requirements.

Reduce WAN OPEX with direct internet access

The traditional WAN model consisted of using expensive private circuits for all connectivity to business services. This model involved sending all packets to a central location where security inspection would take place, and policies would control traffic flow. As businesses move their workloads to SaaS and cloud, the need for more bandwidth and intelligent steering is required.

In the modern WAN edge model, it is now common for branch locations to share multiple WAN links of varying transport dependencies. Secure DIA (direct internet access) provides intelligent and secure steering of network traffic based on business requirements. Applications destined to a SaaS or cloud provider can be sent directly to the internet using a public internet connection without the need of backhauling to a central location. This allows for a much more efficient use of WAN bandwidth and improved user experience. Because FortiGate SD-WAN is also a Next-Generation Firewall, internet traffic can be locally inspected and controlled without needing to offload inspection to another location.

An important consideration for this use case is that edge locations may consist of many different WAN types. The FortiGate SD-WAN solution is transport agnostic, and can be mixed and matched with several different WAN types, including MPLS through Ethernet handoff, internet, and LTE.

Secure and automated intra-site connectivity

As businesses look towards supplementing or replacing their traditional MPLS or private links, the need for secure transport connectivity over public internet becomes essential. For customers that have business applications in a datacenter or HQ location, branch locations require remote connectivity to access these resources. For redundancy, there may be multiple WAN transports and multiple gateways across geo-redundant locations that could be used to access the resource. This leads to many potential paths from the edge that must be evaluated and steered accordingly.

The Fortinet SD-WAN solution can be used to automatically set up dynamic, site-to-site connections across all corporate resources and locations. This may include branch offices, HQ sites, datacenters, or public cloud providers. FortiGate SD-WAN appliances can be configured at any location as a physical or virtual device to provide connectivity and intelligent steering across all available WAN links.

FortiManager is our central management solution that can provide *light touch* or *zero touch* provisioning to onboard new locations, and provide centralized management and monitoring. This means you can choose how much to automate during the onboarding process.

Multi-cloud connectivity and cloud on-ramp

Multi-cloud connectivity refers to the ability of the edge location to steer traffic to one or multiple cloud environments. This could span across workloads within a single cloud provider or multiple cloud providers. As business requirements evolve and cloud providers continue to offer differentiating services, a flexible solution with broad support is critical.

Because of the dynamic nature of cloud environments, the edge device needs to know in real-time where the application is hosted. SaaS or IaaS applications and services should be available via redundant paths, with appropriates routes automatically added or removed as services in the cloud change. Then all available paths should be measured and steered according to the business intent.

Application performance improvement

Application performance can be impacted for a variety of issues. Congestion, WAN link performance (such as, high latency, jitter, or packet loss), server issues, routing changes, and other network issues could all be detrimental to performance and user experience. The FortiGate SD-WAN solution incorporates a number of techniques and capabilities to improve application performance for a variety of deployment methods.

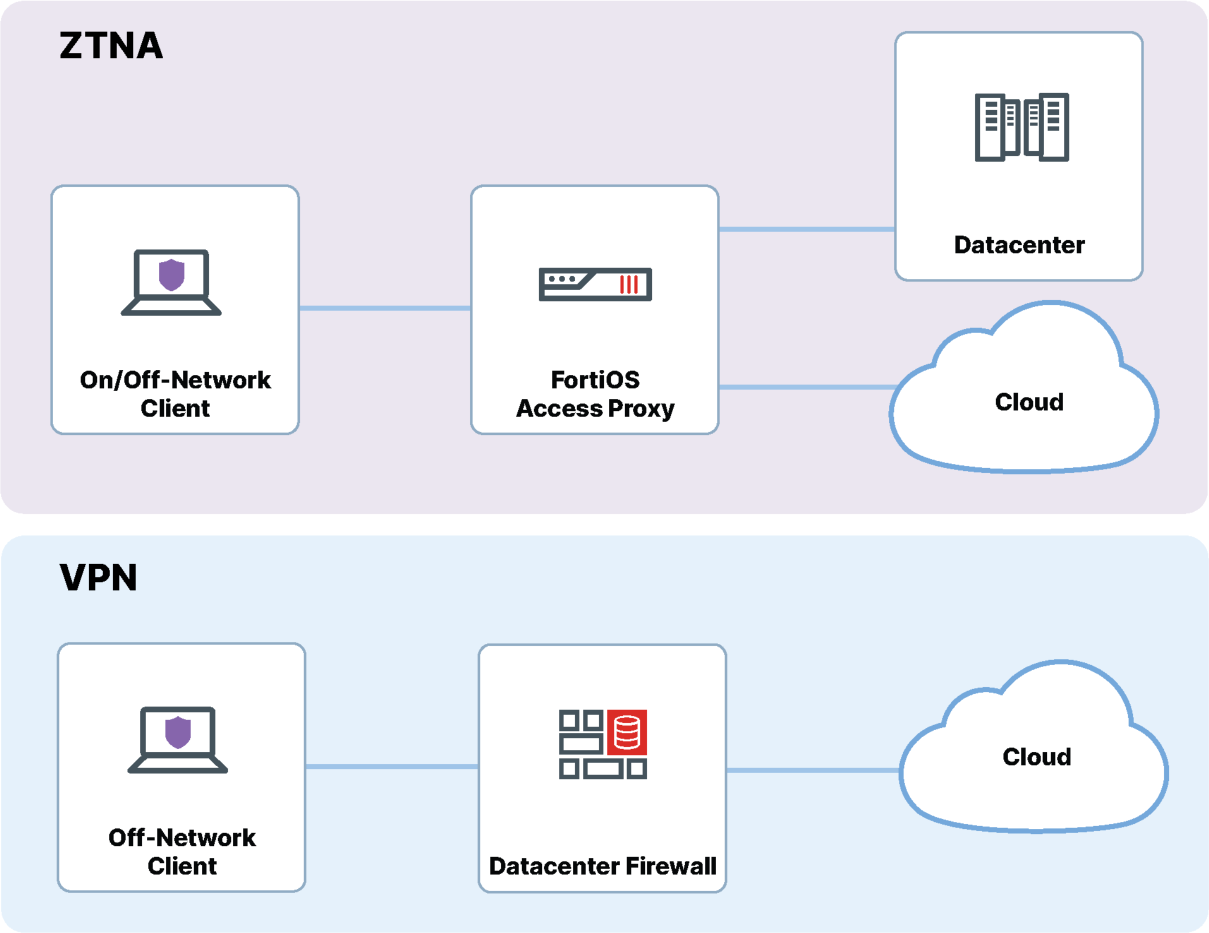
- **Application identification and steering**: Performance SLAs check all available paths to the application to determine the best performing link. Potential network issues can be detected in sub-second speed and steered to a better performing link based on the business requirement.
- **WAN Remediation (Packet loss correction)**: There are situations were protecting the application from packet loss is crucial to business continuity. WAN remediation refers to a series of techniques to fix packet loss on a WAN link. Forward Error Correction (FEC) and Packet Duplication are WAN remediation techniques that can be used to protect a link from various types of impairments.
- **QoS (Quality of Service)**: Because bandwidth is finite, sometimes it is necessary to prioritize how traffic is distributed based on business needs. FortiGate SD-WAN allows you to police, shape, and queue network traffic at each location. Adjustments can be made automatically, depending on available bandwidth at certain times of the day.

- **WAN Optimization**: WAN optimization is a comprehensive solution that maximizes your WAN bandwidth and improves user experience. Some techniques include protocol optimization, web caching, explicit proxy, byte caching, and more.

Work from anywhere

Remote users requiring access to corporate resources is more important than ever. Today's workers require secure, remote access to corporate resources from wherever they are located, as easily as they would inside the corporate network. Work from anywhere (WFA) solutions should be integrated into the SD-WAN device to provide consistent security policy enforcement from anywhere the user is located.

Fortinet SD-WAN devices include support for Virtual Private Network (VPNs) and Zero Trust Network Access (ZTNA) . The FortiGate SD-WAN device can act as a VPN server or access proxy, depending on your desired WFA deployment.



Appendix A - Documentation references

Feature documentation:

- SD-WAN 7.0 New Features
- 7.0 FortiOS 7.0 Administration Guide
- SD-WAN overview
- SD-WAN zones
- Performance SLA
- SD-WAN Rules
- FortiManager 7.0 Administration Guide
- SD-WAN templates
- SD-WAN device database

Solution hub:

- Secure SD-WAN 7.0 solution hub

www.fortinet.com