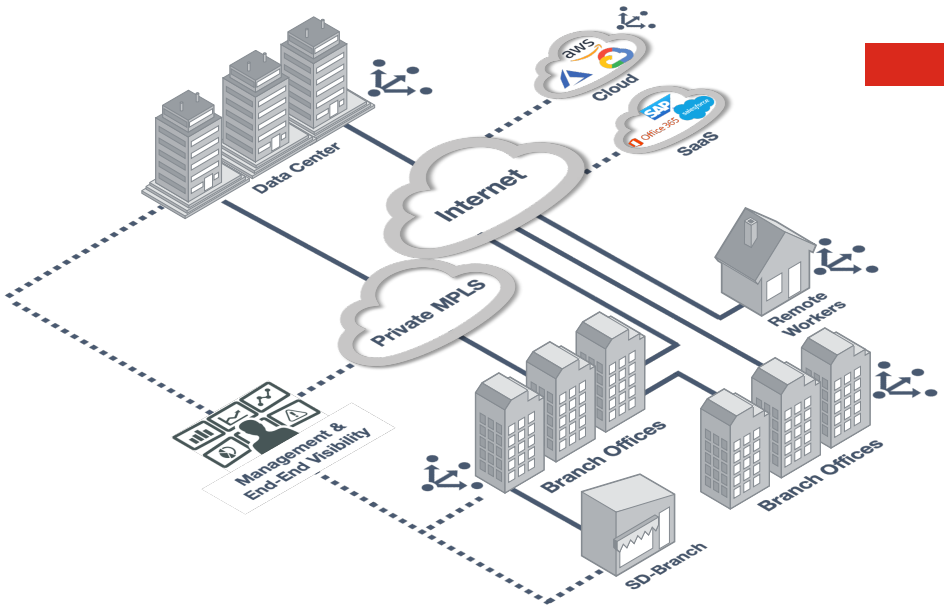
Fortinet Secure SD-WAN



Simplify Your Network Security With One Operating System

As the use of business-critical, cloud-based applications continues to increase, organizations with a distributed infrastructure of remote offices and an expanding remote workforce need to adapt. The most effective solution is to switch from static, performance-inhibited wide-area networks (WANs) to software-defined WAN (SD-WAN) architectures.

Traditional WANs may utilize SLA-backed private multiprotocol label switching (MPLS) or leased line links to an organizations' main data centers for all application and security needs. But that comes at a premium price for connectivity. While a legacy hub-and-spoke architecture may provide centralized protection, it increases latency and slows down network performance to distributed cloud services for application access and compute. The result is operational complexity and limited visibility associated with multiple point products. This scenario adds significant management overhead and difficulties, especially when trying to troubleshoot and resolve issues.

Fortinet's Secure Networking strategy tightly integrates an organization's network infrastructure and security architecture, enabling networks to transform at scale without compromising security. This next-generation approach provides consistent security enforcement across flexible perimeters by combining a next-generation firewall with advanced SD-WAN networking capabilities. This combination paves the way to Fortinet Single-Vendor SASE approach empowering organizations to consistently apply enterprise grade security and superior user experience across all edges converging networking and security across a unified operating system and agent. FortiSASE extends FortiGuard security services across Thin Edge, Secure Edge, and remote users enabling secure access to users both on and off the network. Furthermore, infrastructure networks are simplified by extending SD-WAN into wired and wireless access points of branch offices.

Key Features

- World's only ASIC-accelerated SD-WAN
- 5000+ applications identified with real-time SSL inspection
- Self-healing capabilities for enhanced user experience
- Cloud on-ramp for efficient SaaS adoption
- Simplified operations with NOC/SOC management and analytics
- Enhanced granular analytics for end-to-end visibility and control
- Foundational for a single-vendor SASE
- Gartner Magic Quadrant Leader for both SD-WAN and Network Firewalls

Business Outcomes

Improved User Experience

An application-driven approach provides broad application steering with accurate granular identification, advanced WAN remediation, and accelerated cloud on-ramp for optimized network and application performance. Furthermore, a Secure Private Access via FortiSASE to secure access to private applications for remote users.

Accelerated Convergence

The industry's only organically developed, purpose-built, and ASIC-powered SD-WAN enables Secure Edge (FortiGate SD-WAN) and thin edge (FortiExtender Wireless WAN) to transition to Fortinet Single-Vendor SASE solution to secure all applications, users, and data anywhere.

Efficient Operations

Simplify operations with centralized orchestration and enhanced analytics for SD-WAN, security, and SD-Branch at scale.

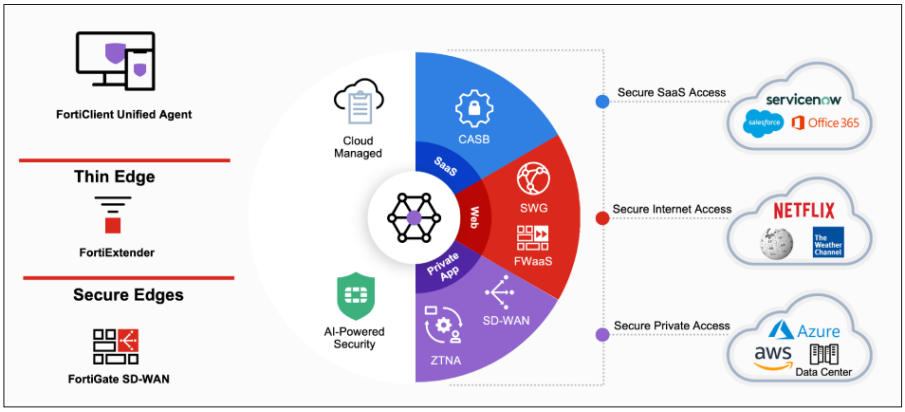
Comprehensive Security On-prem and in the Cloud

A built-in next-generation firewall (NGFW) combines SD-WAN and security capabilities in a unified solution to preserve the security and availability of the network. In addition, cloud-delivered security (SASE) can also be leveraged by the branches and remote users.

Fortinet Secure SD-WAN Is Foundational for a Seamless Transition to SASE

Fortinet Secure SD-WAN enables organizations to transition to a single-vendor SASE by extending secure access and high-performance connectivity to users regardless of their geographic locations. FortiSASE delivers a full set of networking and security capabilities including secure web gateway (SWG), universal zero-trust network access (ZTNA), next-generation dual-mode cloud access security broker (CASB), Firewall-as-a-Service (FWaaS), and secure SD-WAN integration. With a unified solution, you can:

- Overcome security gaps
- Simplify operations and enhance security and networking analytics
- Shift to an OPEX business model with simple user-based tiered licensing



Core Components

Fortinet Secure SD-WAN consists of the industry's only organically developed software complemented by an ASIC-accelerated platform to deliver the most comprehensive SD-WAN solution.

FortiGate

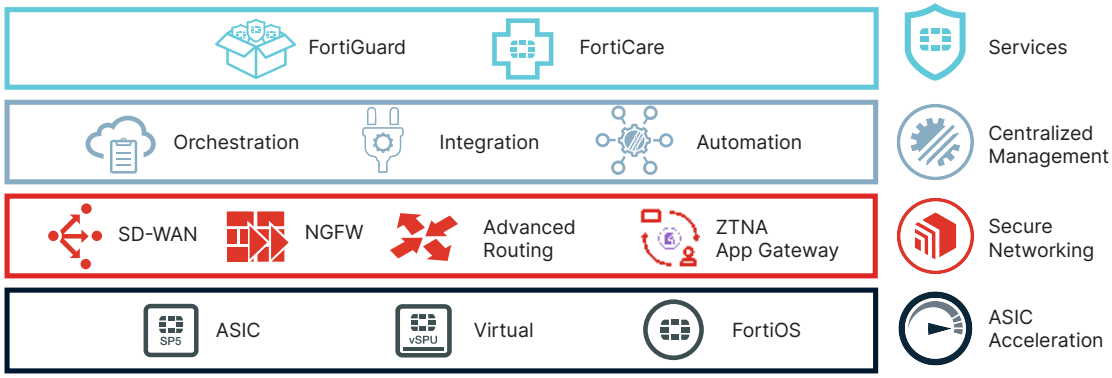
Provides a broad portfolio available in different form factors: physical appliance and virtual appliances, with the industry's only ASIC acceleration using the SOC4 SPU or vSPU.

- Reduce cost and complexity with next generation firewall, SD-WAN, advanced routing, and ZTNA application gateway on a unified platform that allows customers to eliminate multiple point products at the WAN edge
- ASIC acceleration of SD-WAN overlay tunnels, application identification, steering, remediation, and prioritization ensure the best user experience for business-critical, SaaS, and UCaaS applications

FortiOS

Fortinet's unified operating system delivers a security-driven strategy to secure and accelerate network and user experience. Continued innovation and enhancement enable:

- Real-time application optimization for a consistent and resilient application experience
- Advanced next generation firewall protection and prevention from internal and external threats while providing visibility across entire attack surface
- Dynamic Cloud connectivity and security are enabled through effective cloud integration and automation

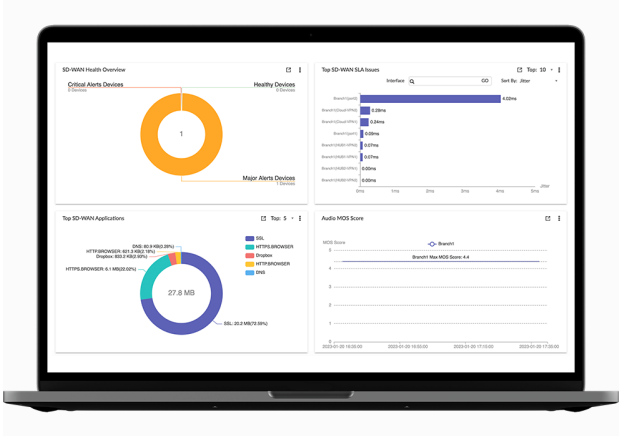


Core Components

NOC Operations

Simplify centralized management, deployment, and automation to save time and respond quickly to business demands with end-to-end visibility. With a single pane of glass management that offers deployment at scale, customers can:

- Centrally manage 100K+ devices, including firewalls, switches, access points, and LTE/5G extenders from a single console
- Provision and monitor Secure SD-WAN at the application and network level across branch offices, datacenters, and cloud
- Reduce complexity by leveraging automation enabled by REST APIs, scripting tools such as Ansible/Terraform, and fabric connectors
- Separate and manage domains leveraging ADOMS for compliance and operational efficiency
- Accelerate troubleshooting and enhance user experience with Digital Experience Monitoring (DEM) and AIOps
- Role-based access control to provide management flexibility and separation



FortiGuard Security Services

Enhances SD-WAN security with advanced protection to help organizations stay ahead of today's sophisticated threats:

- Coordinated real-time detection and prevention against known and unknown protecting content, application, people, and devices
- Real-time insights are achieved by processing extensive amounts of data at cloud-scale, analyzing that data with advanced AI, and then automatically distributing the resulting intelligence back for enforcement and protection

Features

	FEATURES	DESCRIPTION
FortiOS — SD-WAN	Application Identification and Control	5000+ application signatures, 3000+ industrial signatures, first packet Identification, deep packet inspection, custom application signatures, SSL decryption, TLS1.3 with mandated ciphers, and deep inspection
	SD-WAN (Application aware traffic control)	Granular application policies, application SLA based path selection, dynamic bandwidth measurement of SD-WAN paths, active/active and active/standby forwarding, overlay support for encrypted transport, Application session-based steering, probe-based SLA measurements
	Advanced SD-WAN (WAN remediation)	Forward Error Correction (FEC) for packet loss compensation, packet duplication for best real-time application performance, Active Directory integration for user based SD-WAN steering policies, per packet link aggregation with packet distribution across aggregate members
	SD-WAN deployment	Flexible deployment – hub-to-spoke (partial mesh), spoke-to-spoke (full mesh), multi-WAN transport support
	SASE	Secure remote users/branches to private applications (Secure Private Access) by establishing IPSec tunnels from SASE PoP to multiple SD-WAN Hubs
FortiOS — Networking	QoS	Traffic shaping based on bandwidth limits per application and WAN link, rate limits per application and WAN link, prioritize application traffic per WAN link, mark/remark DSCP bits for influencing traffic QoS on egress devices, application steering based on ToS marking
	Advanced Routing (IPv4/IPv6)	Static routing, Internal Gateway (iBGP, OSPF v2/v3 , RIP v2), External Gateway(eBGP), VRF, route redistribution, route leaking, BGP confederation, router reflectors, summarization and route-aggregation, route asymmetry
	VPN/Overlay	Site-to-site ADVPN – dynamic VPN tunnels, policy-based VPN, IKEv1, IKEv2, DPD, PFS, ESP and ESP-HMAC support, symmetric cipher support (IKE/ESP): AES-128 and AES-256 modes: CBC, CNTR, XCBC, GCM, Pre-shared and PKI authentication with RSA certificates, Diffie-Hellman key exchange (Group 1, 2, 5, 14 through 21 and 27 through 32), MD5, and SHA-based HMAC
	Multicast	Multicast forwarding, PIM spare (rfc 4601), dense mode (rfc 3973), PIM rendezvous point
	Advanced Networking	DHCP v4/v6, DNS, NAT – source, destination, static NAT, destination NAT, PAT, NAPT, Full IPv4/v6 support
FortiOS — Security	On-prem Security	Next Generation Firewall with FortiGuard threat intelligence – SSL inspection, application control, Intrusion prevention, antivirus, web filtering, DLP, and advanced threat protection. Segmentation – micro, macro, single task VDOM, multi VDOM, ZTNA application gateway
	Cloud-delivered Security	Universal zero-trust network access (ZTNA), next-generation dual-mode cloud access security broker (CASB), Firewall-as-a-Service (FWaaS), secure SD-WAN integration, and hollistic visibility (apps, threats, sessions, policies)
NOC Operations	Centralized Management and Provisioning	FortiManager provides zero touch provisioning, centralized configuration, change management, dashboard, application policies, QoS, security policies, application specific SLA, active probe configuration, RBAC, multi-tenant. Fabric Overlay Orchestrator capability is built directly into FortiOS allowing automatic connectivity between devices without FortiManager. Overlay-as-a-Service is a SaaS offering that delivers efficient setup and management of new SD-WAN regions via the easy-to-use FortiCloud portal.
	Cloud Orchestration	FortiManager Cloud through FortiCloud, Single Sign-on portal to manage Fortinet NGFW and SD-WAN, Cloud-based network management to streamline FortiGate provisioning and management, extensive automation-enabled management of Fortinet devices
	Enhanced Analytics	Bandwidth consumption, SLA metrics – jitter, packet loss, and latency, real-time monitoring, filter based on time slot, WAN link SLA reports, per-application session usage, threat information - malware signature, malware domain or URL, infected host, threat level, malware category, indicator of compromise
	Cloud On-ramp	Cloud integration – AWS, Azure, Alibaba, Oracle, Google. AWS – transit, direct and VPC connectivity, transit gateways, Azure – Virtual WAN connectivity, Oracle – OCI connectivity
FortiGate	Redundancy/High-availability	FortiGate dual device HA – primary and backup, FortiManager HA, bypass interface, interface redundancy, redundant power supplies
	Integration	RESTful API/Ansible for configuration, zero touch provisioning, reporting, and third-party integration
	Virtual environments	VMware ESXi v5.5 / v6.0 / v6.5/ v6.7, VMware NSX-T v2.3 Microsoft Hyper-V Server 2008 R2 / 2012 / 2012 R2 / 2016 Citrix Xen XenServer v5.6 sp2, v6.0, v6.2 and later Open source Xen v3.4.3, v4.1 and later KVM qemu 0.12.1 & libvirt 0.10.2 and later for Red Hat Enterprise Linux / CentOS 6.4 and later / Ubuntu 16.04 LTS (generic kernel) ,KVM qemu 2.3.1 for SuSE Linux Enterprise Server 12 SP1 LTSS Nutanix AHV (AOS 5.10, Prisim Central 5.10) Cisco Cloud Services Platform 2100
	Built-in Variants	POE, LTE, WiFi, ADSL/VDSL

BRANCHES	SMALL RETAIL/OFFICE		MEDIUM RETAIL/BRANCH/SMB			LARGE BRANCH/CAMPUS	
Appliances	**40F**	**60F**	**70F**	**80F**	**90G**	**100F**	**200F**
IPsec VPN Throughput[1]	4.4 Gbps	6.5 Gbps	6.1 Gbps	6.5 Gbps	25 Gbps	11.5 Gbps	13 Gbps
Threat Protection[2]	600 Mbps	700 Mbps	800 Mbps	900 Mbps	2.2 Gbps	1 Gbps	3 Gbps
Application Control Throughput[3]	990 Mbps	1.8 Gbps	1.8 Gbps	1.8 Gbps	6.7 Gbps	2.2 Gbps	13 Gbps
SSL Inspection Throughput	310 Mbps	630 Mbps	700 Mbps	715 Mbps	2.6 Gbps	1 Gbps	4 Gbps
Unrestricted Bandwidth	✓	✓	✓	✓	✓	✓	✓
Zero Trust Network Access (ZTNA)	✓	✓	✓	✓	✓	✓	✓
Services							
Cloud Management and Analytics	Available with FGT Cloud Management and Analytics license						
Underlay Monitoring Services	Available with SDWAN-Underlay Monitoring Services license						
Overlay-as-a-Service	Available with Overlay-as-a-Service license						
Connectivity							
Interfaces	5 x GE RJ45	10 x GE RJ45	10 x GE RJ45	8 x GE RJ45 2 x Shared Port Pairs	8 x GE RJ45 2 × 10 GE Shared Port Pairs	18 x GE RJ45 8 x GE SFP 2 × 10 GE SFP+ 4 x Shared Port Pairs	18 x GE RJ45 8 x GE SFP 4 × 10 GE SFP+
Hardware Variants	WiFi, 3G4G	WiFi, Storage	Storage	WiFi, Bypass, POE, Storage	Storage	Storage	Storage
5G/LTE Connectivity	Supports FortiExtender						
Extensibility	Supports FortiAP, FortiSwitch						
Form Factor	Desktop	Desktop	Desktop	Desktop	Desktop	1RU	1RU
Power Supply	Single AC PS	Single AC PS	Single AC PS	Single AC PS, Dual Inputs	Single AC PS, Dual Inputs	Dual AC PS	Dual AC PS

1 The IPsec VPN performance test uses AES256-SHA256.

2 SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

3 IPS, Application Control, NGFW, and Threat Protection are measured with logging enabled.

HUBS

Appliances	400F	600F	900G	1000F	1800F	2200E	2600F
IPsec VPN Throughput[1]	55 Gbps	55 Gbps	55 Gbps	55 Gbps	55 Gbps	98 Gbps	55 Gbps
Max IPsec Tunnels[1]	50 000	50 000	50 000	100 000	100 000	100 000	100 000
Threat Protection[2]	9 Gbps	10.5 Gbps	20 Gbps	13 Gbps	15 Gbps	11 Gbps	25 Gbps
SSL Inspection Throughput[3] (IPS, avg. HTTPS)	8 Gbps	9 Gbps	16.7 Gbps	10 Gbps	12 Gbps	17 Gbps	20 Gbps
Services							
Cloud Management and Analytics	Available with FGT Cloud Management and Analytics license						
Underlay Monitoring Services	Available with SDWAN-Underlay Monitoring Services license						
Overlay-as-a-Service	Available with Overlay-as-a-Service license						
Connectivity							
100GE QSFP28				✓	✓		✓
40GE QSFP+				✓	✓	✓	✓
25GE SFP28		✓	✓	✓	✓	✓	✓
10GE SFP+	✓	✓	✓	✓	✓	✓	✓
1GE SFP/RJ45	✓	✓	✓	✓	✓	✓	✓
Hardware Variants							
Built-in Storage	✓	✓	✓	✓	✓	✓	✓
Bypass							
Redundant Hot-Swap PSUs	✓	✓	✓	✓	✓	✓	✓
DC Power					✓		✓

HUBS

Appliances	3000F	3200F	3300E	3400E	3500F	3700F
IPsec VPN Throughput[1]	105 Gbps	105 Gbps	98 Gbps	140 Gbps	165 Gbps	160 Gbps
Max IPsec Tunnels[1]	200 000	200 000	200 000	200 000	200 000	200 000
Threat Protection[2]	33 Gbps	45 Gbps	17 Gbps	25 Gbps	63 Gbps	75 Gbps
SSL Inspection Throughput[3] (IPS, avg. HTTPS)	29 Gbps	29 Gbps	21 Gbps	30 Gbps	63 Gbps	55 Gbps
Services						
Cloud Management and Analytics	Available with FGT Cloud Management and Analytics license					
Underlay Monitoring Services	Available with SDWAN-Underlay Monitoring Services license					
Overlay-as-a-Service	Available with Overlay-as-a-Service license					
Connectivity						
400GE QSFP-DD						✓
200GE QSFP56						✓
100GE QSFP28	✓			✓	✓	✓
50GE SFP56						✓
40GE QSFP+	✓		✓	✓	✓	✓
25GE SFP28	✓		✓	✓	✓	✓
10GE SFP+	✓		✓	✓	✓	✓
1GE SFP/RJ45	✓		✓	✓	✓	✓
Hardware Variants						
Built-in Storage	✓		✓	✓	✓	✓
Bypass						
Redundant Hot-Swap PSUs	✓		✓	✓	✓	✓
DC Power				✓		

1 The IPsec VPN performance test uses AES256-SHA256.

2 SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

3 IPS, Application Control, NGFW, and Threat Protection are measured with logging enabled.

HUBS

Appliances	3960E	3980E	4200F	4400F	4800F
IPsec VPN Throughput[1]	280 Gbps	400 Gbps	210 Gbps	310 Gbps	800 Gbps
Max IPsec Tunnels[1]	200 000	200 000	200 000	200 000	200 000
Threat Protection[2]	13.5 Gbps	20 Gbps	45 Gbps	75 Gbps	75 Gbps
SSL Inspection Throughput[3] (IPS, avg. HTTPS)	23 Gbps	26 Gbps	50 Gbps	86 Gbps	63 Gbps
Services					
Cloud Management and Analytics	Available with FGT Cloud Management and Analytics license				
Underlay Monitoring Services	Available with SDWAN-Underlay Monitoring Services license				
Overlay-as-a-Service	Available with Overlay-as-a-Service license				
Connectivity					
400GE QSFP-DD					✓
200GE QSFP56					✓
100GE QSFP28	✓	✓	✓	✓	✓
50GE SFP56					✓
40GE QSFP+	✓	✓	✓	✓	✓
25GE SFP28			✓	✓	✓
10GE SFP+	✓	✓	✓	✓	✓
1GE SFP/RJ45	✓	✓	✓	✓	✓
Hardware Variants					
Built-in Storage			✓	✓	✓
Bypass					
Redundant Hot-Swap PSUs	✓	✓	✓	✓	✓
DC Power	✓	✓	✓	✓	

1 The IPsec VPN performance test uses AES256-SHA256.

2 SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

3 IPS, Application Control, NGFW, and Threat Protection are measured with logging enabled.

FORTIGATE VM: PRIVATE CLOUD SUPPORT MATRIX

	VMware VSphere	Citrix Xen	Xen	KVM	Microsoft Hyper-V	Nutanix AHV
FG-VM	✓	✓	✓	✓	✓	✓

FORTIGATE VM: PUBLIC CLOUD SUPPORT MATRIX

	Amazon AWS	Microsoft Azure	Oracle OCI / OPC	Google GCP	Alibaba AliCloud
FG-VM	✓ / #	✓ / #	✓ / #	✓ / #	✓ / #

- On-demand

PROFESSIONAL SERVICES PACKAGES

	Standalone Site	Hub and Spoke (Single DC)	Hub and Spoke with ZTP (Single DC)
SDWAN FortiGate Deployment QuickStart Service	FP-10-QSSDWAN-DP1-00-00	FP-10-QSSDWAN-DP2-00-00	FP-10-QSSDWAN-DP3-00-00

The QuickStart SD-WAN service is a consulting service that provides assistance for the deployment of a pre-defined FortiGate SD-WAN configuration into a customer's environment.

FORTIMANAGER: CENTRALIZED MANAGEMENT PLATFORM							
	Hardware					Subscription	
	200G	400G	1000F	3000G	3700G	Cloud	VM
Default Devices/VDOMs	30	150	1000	4000	10 000		10
Max Devices/VDOMs with add-on license				8000	100 000	10 000	100 000
Default ADOMs	30	150	1000	4000	10 000		Add-On
Max ADOMs with add-on license				8000	12 000		1200
Management Extension Application (MEA) enabled				✓	✓		✓
Additional Services							
FortiCare Premium Contract	Subscription					✓	✓
FortiCare Elite Contract	Subscription					No	No
FortiCare Best Practice Services (BPS)	Included in hardware bundle + a la carte					✓	✓
Replacement Disks			✓	✓	✓		
How to Buy	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Hardware Bundle	Multi-Device Subscription	VM Bundle/ Subscription

FORTIMANAGER VM					
	10 Devices	100 Devices	1000 Devices		Description
Subscription Bundles	FC1-10-FMGVS-448-01-DD	FC2-10-FMGVS-448-01-DD	FC3-10-FMGVS-448-01-DD		All in one subscription bundle including FortiManager VM S-series, FortiCare Premium Contract, and FortiCare Best Practice services. Fully stackable.
	10 Devices	100 Devices	1000 Devices	5000 Devices	Description
Perpetual License	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG	Perpetual license. Purchase FortiCare Premium Contract and FortiCare Best Practices services separately. Only the number of managed devices is stackable.

FORTIMANAGER CLOUD				
	10 Devices	100 Devices	1000 Devices	
Multi-Device Subscription	FC1-10-MVCLD-227-01-DD	FC2-10-MVCLD-227-01-DD	FC3-10-MVCLD-227-01-DD	FortiManager Cloud Central Management and Orchestration Service including 24×7 FortiCare support. Fully stackable.

FORTIMANAGER VM: PRIVATE CLOUD SUPPORT							
	VMware	Citrix Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Oracle Private Cloud	OpenSource Xen
FMG-VM	✓	✓	✓	✓	✓	✓	✓

FORTIMANAGER VM: PUBLIC CLOUD SUPPORT				
	Amazon AWS	Microsoft Azure	Google GCP	Oracle OCI / OPC
FMG-VM	✓	✓	✓	✓

FORTIMONITOR: SD-WAN SYNTHETIC TRANSACTION MONITORING (STM)		
SOLUTION BUNDLE	SKU LICENSE	SD WAN STM BUNDLE
SD WAN STM Application Monitoring Retrieves NTT, SRT, DNS lookup time, HTTPS response time, and RTT against customer and OOTB applications across all SD WAN connections to measure application reachability and performance.	10-Pack	FC1-10-MNCLD-672-01-12
	25-Pack	FC2-10-MNCLD-672-01-12
	500-Pack	FC3-10-MNCLD-672-01-12
	2000-Pack	FC4-10-MNCLD-672-01-12
	10 000-Pack	FC5-10-MNCLD-672-01-12

Branch and Hub Selection

Selecting the Branch or HUB devices depends on multiple factors that are unique to each deployment. Speak with a Fortinet specialist for assistance selecting the right devices for your environment. Below are the most common selection criteria and some commonly selected Hub devices, based on deployment sizes (for reference purposes only).

Branch Selection

- Security requirements
- Number of users
- Throughput
- Interface connectivity
- Wireless requirements
- Redundancy (WAN, Power, IPsec Tunnels, Device)

Hub Selection

- Security requirements
- IPsec throughput
- Total IPsec Tunnels
- Interface connectivity
- Redundancy (Ports, Device, Power, Intra-site)
- AC or DC Power

Hub Sizing Examples (Reference Only)

- Up to 500 Sites (400F-600F)
- Up to 2000 Sites (1000F-1800F)
- Up to 5000 Sites (2200E-2600F)
- Up to 10 000 Sites (3000F-3700F)
- Beyond 10 000+ Sites (3960E-4800F)

NSE Training and Certification

FCSS - SD-WAN

In this course, you will learn about common SD-WAN deployment scenarios using the Fortinet Secure SD-WAN solution. You will explore different situations, from a single enterprise site to multiple data center environments, that will help you to enhance and troubleshoot SD-WAN deployments.

Ordering Information

SKU	DESCRIPTION
FT-SD-WAN	Instructor-led Training - Four days
FT-SD-WAN-LAB	On-demand Labs (self-paced)
NSE-EX-FTE2	Certification Exam

Pre-requisites

You must have an understanding of the topics covered in the following courses, or have equivalent experience.

- FCP - FortiGate Security
- FCP - FortiGate Infrastructure
- FCP - FortiManager

References

Course description

Frequently Asked Questions

Is there an extra license to use SD-WAN with FortiGate?

No, SD-WAN is a feature included in FortiOS at no additional cost. Fortinet recommends purchasing security subscription services as necessary and utilizing a FortiManager for central management.

Are there any bandwidth licensing or restrictions?

Fortinet does not charge for bandwidth usage and you are free to use as much as the box will physically support.

Which FortiGate models can be utilized as a SD-WAN Hub?

Any FortiGate model can be utilized as an SD-WAN Hub or Branch. This document provides guidance on Branch and Hub models based on common deployment use cases.

Why is "Maximum IPSec Tunnels" omitted for Branches?

IPSec phase1 interfaces have no hard limit and are only limited by system memory. Our tests have shown to support several hundred tunnels on even the smallest box but varies based on many factors.

How is Overlay-as-a-Service priced?

The licensing model is per-FortiGate device. This approach means each FortiGate that participates in the SDWAN overlay region will need an individual device entitlement and be registered to the same FortiCloud account. No other purchase or license is necessary. Upon activating the service from the OaaS portal, FortiGate HUB devices will be assigned and allocated for the SDWAN overlay region.

How is the SDWAN Underlay Monitoring service priced? Is a FortiManager license required?

SDWAN Underlay Monitoring is licensed per-FortiGate and no additional licensing is required. FortiManager allows you to execute and monitor the speed test service from a remote FortiGate device with the proper license.

How is FortiMonitor Synthetic Transaction Monitoring (STM) priced?

A Pack refers to the total number of FortiGates that will integrate with FortiMonitor OnSight agents. Agents integrate with SD-WAN to monitor all available WAN underlay links. There is no licensing limits on the number of WAN underlay links to be monitored. Example: 10-Pack includes 10 FortiGates, 25-Pack includes 25 FortiGates.

How is "Threat Protection" measured and what does it include?

Threat Protection performance is measured with Firewall, IPS, Application Control, URL Filtering and Malware Protection enabled, Enterprise Mix traffic.

What does the "Unified Threat Protection" license include?

The Unified Threat Protection license includes: IPS, Advanced Malware Protection, Application Control, Botnet DB, Mobile Malware, Outbreak Prevention, Web and Video Filtering, Cloud sandbox, Secure DNS filtering, AntiSpam Service, and 24×7 support. For more information, please see the FortiGuard Security Services datasheet here.

Where could I find the maximum values for SD-WAN components, such as rules and performance SLAs?

The maximum system values for all FortiGates can be found here.

What do I need for Zero Touch Provisioning (ZTP)?

ZTP can be accomplished a number of different ways. For most deployments, we recommend purchasing FortiDeploy (FDP-SINGLE-US) with your purchase order. FortiDeploy will link the serial numbers in your order to your FortiCloud account. A FortiManager IP address can be assigned to your devices automatically so they retrieve their configuration from the FortiManager of your choice.

Professional Services and Support

FortiGuard Bundles

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Professional Services

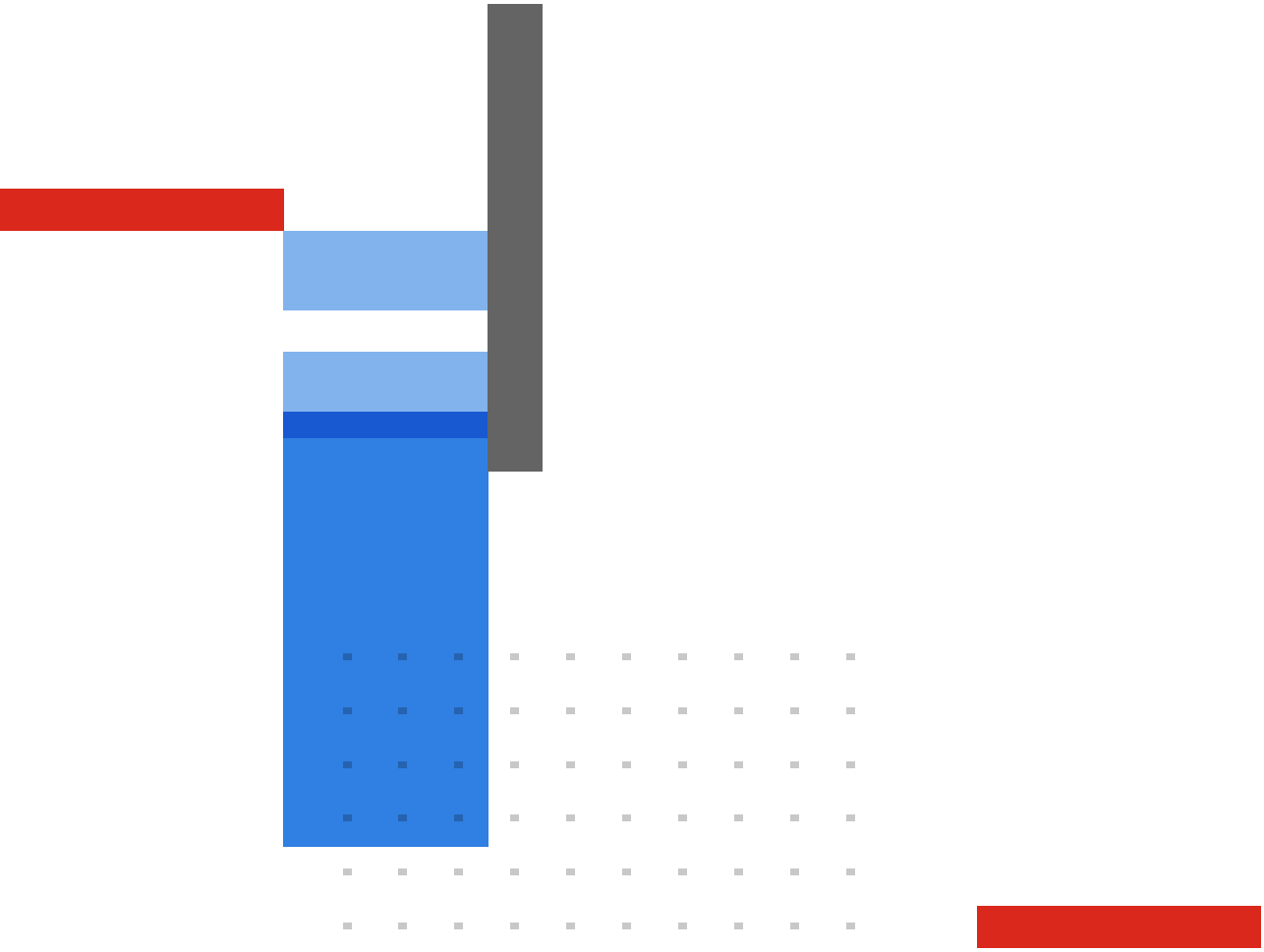
Fortinet offers QuickStart SD-WAN consulting services to help customers accelerate the time-to-value of their SD-WAN network based on predefined configurations. This best-practice-based service also includes both as-built documentation and knowledge transfer.

FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

November 27, 2023

SSD-WAN-DAT-R19-20231127