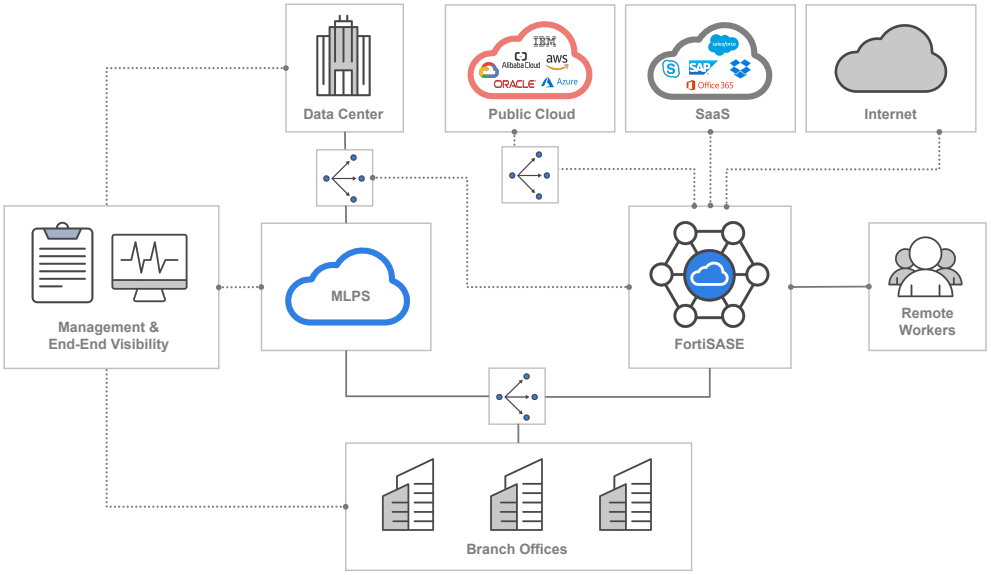
Fortinet Secure SD-WAN



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

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.

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.

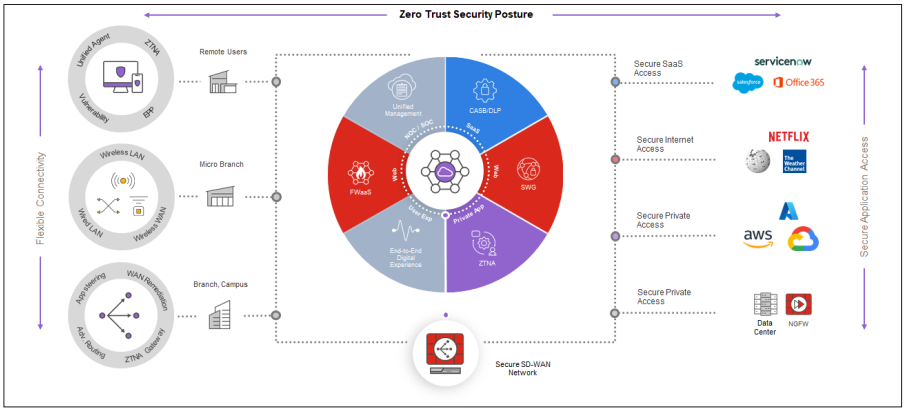
Comprehensive Security On-prem and in the Cloud

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

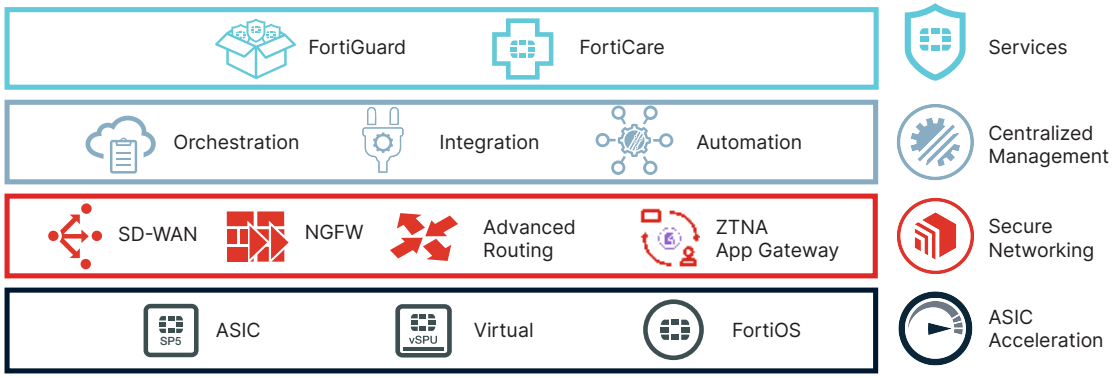
Provides a broad portfolio available in different form factors: physical appliance and virtual appliances, with the industry's only ASIC acceleration using the SOC4 SPU or vSPU.

- 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

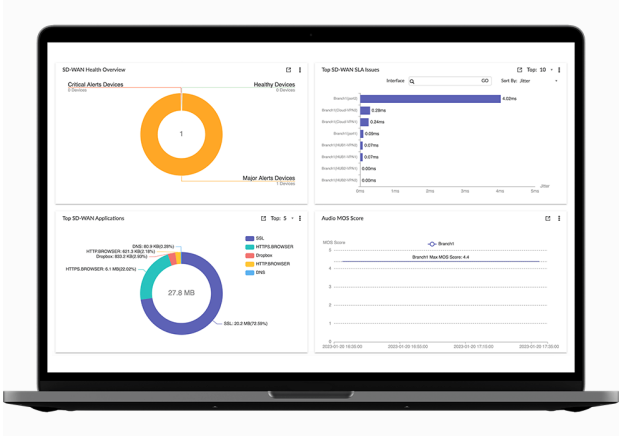


Core Components

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

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

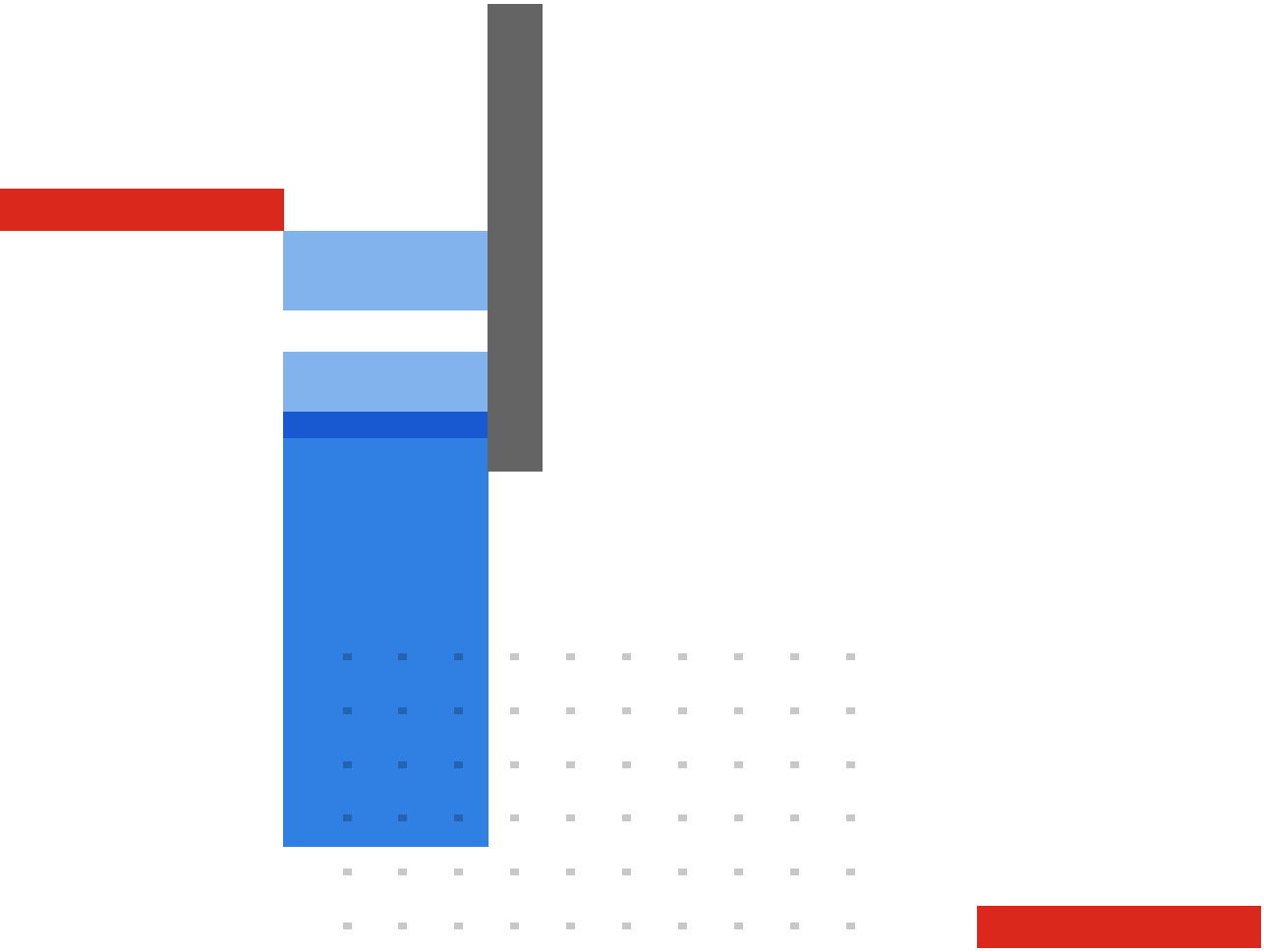
FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (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.

Ordering Guide

Please refer to the **SD WAN Ordering Guide** here.

FortiGuard Fortinet Corporate Social Responsibility 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

April 11, 2024

SSD-WAN-DAT-R20-20240411