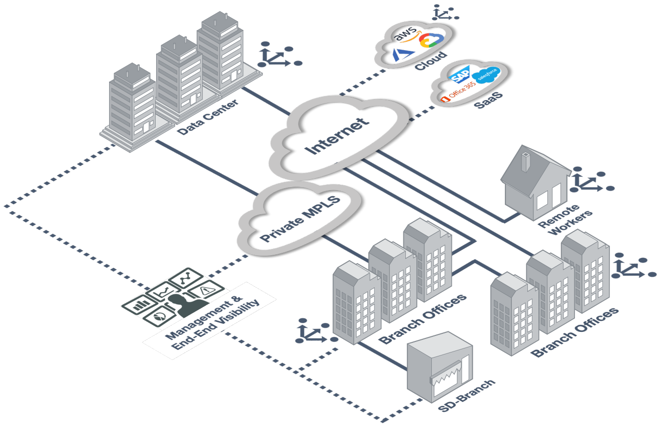
Q2 2021

DATA SHEET

Fortinet Secure SD-WAN

A Unified WAN Edge, Powered by a Single OS, to Transform and Secure the WAN



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 Security-driven 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 scheme eliminates MPLS-required traffic backhaul and delivers improved user experience without ever compromising on security. This integrated approach enables simplified, single-console management for all networking and security needs, while extending SD-WAN into wired and wireless access points of branch offices. As a result, network security and controls can be more deeply integrated, enabling consistent security enforcement into branch LAN networks.

Key Features

- World's only ASIC-accelerated SD-WAN
- 5,000+ 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

BUSINESS OUTCOMES

Improved User Experience

An application-driven approach provides broad application steering with accurate identification, advanced WAN remediation, and accelerated cloud on-ramp for optimized network and application performance

Accelerated Convergence

The industry's only organically developed, purpose-built, and ASIC-powered SD-WAN enables thin edge (SD-WAN, routing) and WAN Edge (SD-WAN, routing, NGFW) 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

Natively Integrated Security

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

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, and advanced routing 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

Fabric Management Center

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:

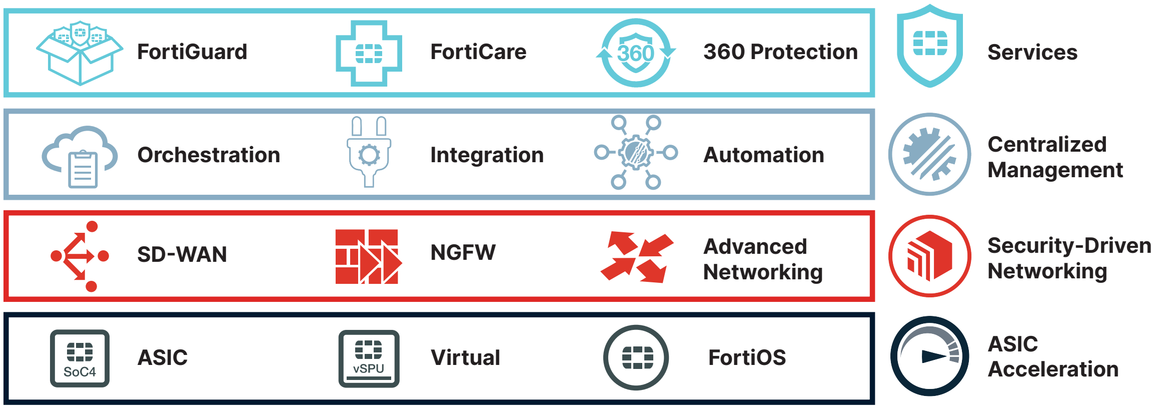
- Centrally manage 100K+ devices, including firewalls, switches, access points, and Extenders/ LTE devices from a single console
- Provision and monitor Secure SD-WAN at the application and network level across branch offices, datacenters, and cloud
- Reduce complexity by leveraging automation enabled by REST API, Ansible, and cloud connectors
- Separate and manage domains leveraging ADOMS for compliance and operational efficiency
- 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

CORE COMPONENTS



	Features	Description
FortiOS — SD-WAN	Application Identification and Control	5000+ application 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
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), MD5 and SHAT-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	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
Fabric Management Center	Centralized Management and Provisioning	FortiManager – zero touch provisioning, centralized configuration, change management, dashboard, application policies, QoS, security policies, application specific SLA, active probe configuration, RBAC, multi-tenant
	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

PRODUCT OFFERINGS

FortiGate

BRANCHES

COMMON DEPLOYMENTS	SMALL RETAIL/ HOME OFFICE	BRANCH/ SMB	BIG RETAIL/ SMB	MEDIUM BRANCH	LARGE BRANCH/ CAMPUS
RECOMMENDED # OF USERS & RANGE	UP TO 10 USERS	UP TO 20 USERS	UP TO 50 USERS	UP TO 250 USERS	UP TO 500 USERS
Appliances	**40F**	**60F**	**80F**	**100F**	**200F**
IPsec VPN Throughput	4.4 Gbps	6.5 Gbps	7.5 Gbps	11.5 Gbps	13 Gbps
Max IPsec Tunnels	200	200	200	2500	2500
Threat Protection	600 Mbps	700 Mbps	900 Mbps	1 Gbps	3 Gbps
Application Control Throughput	990 Mbps	1.8 Gbps	1.8 Gbps	2.2 Gbps	13 Gbps
SSL Inspection Throughput	310 Mbps	630 Mbps	715 Mbps	1 Gbps	4 Gbps
Unrestricted Bandwidth	✓	✓	✓	✓	✓
Zero Trust Network Access (ZTNA)	✓	✓	✓	✓	✓
Connectivity					
Interfaces	5 x GE RJ45	10 x GE RJ45	8 x GE RJ45 2 x 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	WiFi, Bypass, POE, Storage	Storage	Storage
Extensibility	Supports FortiAP, FortiSwitch, and FortiExtender				
Form Factor	Desktop	Desktop	Desktop	1RU	1RU
Power Supply	Single AC PS	Single AC PS	Single AC PS, dual inputs	Dual AC PS	Dual AC PS

Use Case	Offering Name	Support	Content Security - IPS	Content Security - Anti-Malware	Content Security - Cloud Sandbox	Web Security: Web and Video Filtering	Web Security: DNS Filtering
WAN Edge	Unified Threat Protection	24 × 7	✓	✓	✓	✓	✓

HUBS

Appliances	**400E**	**600E**	**1100E**	**1800F**	**2600F**	**3400E**	**3600E**	**4200F**	**4400F**
IPsec VPN Throughput	20 Gbps	20 Gbps	48 Gbps	55 Gbps	55 Gbps	140 Gbps	140 Gbps	210 Gbps	310 Gbps
Max IPsec Tunnels	50,000	50,000	100,000	100,000	100,000	200,000	200,000	200,000	200,000
Threat Protection	5 Gbps	7 Gbps	7.1 Gbps	9.1 Gbps	17 Gbps	25 Gbps	30 Gbps	45 Gbps	75 Gbps
SSL Inspection Throughput (IPS, avg. HTTPS)	4.8 Gbps	8 Gbps	10 Gbps	17 Gbps	20 Gbps	30 Gbps	34 Gbps	50 Gbps	86 Gbps
Connectivity									
100GE QSFP28					✓	✓	✓	✓	✓
40GE QSFP+			✓	✓	✓	✓	✓	✓	✓
25GE SFP28			✓	✓	✓	✓	✓	✓	✓
10GE SFP+		✓	✓	✓	✓	✓	✓	✓	✓
1GE SFP/RJ45	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hardware Variants									
Built-in Storage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bypass	✓								
Redundant Hot-Swap PSUs	Optional	Optional	✓	✓	✓	✓	✓	✓	2 + 2
DC Power			✓			✓	3600E Only	✓	

Use Case	Offering Name	Support	Content Security - IPS	Content Security - Anti-Malware	Content Security - Cloud Sandbox	Web Security: Web and Video Filtering	Web Security: DNS Filtering
HUB	Unified Threat Protection	24 × 7	✓	✓	✓	✓	✓

PRODUCT OFFERINGS

FortiGate-VM Support Matrix

	Private Cloud						Public Cloud				
	VMware VSphere	Citrix Xen	Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Amazon AWS	Microsoft Azure	Oracle OCI / OPC	Google GCP	Ailbaba AliCloud
FG-VM **	✓	✓	✓	✓	✓	✓	✓ / #	✓ / #	✓ / #	✓ / #	✓ / #

** Available as FortiGate-VMX solution for VMware NSX environment, AzureStack and RackSpace (PAYG)
# on-demand

FORTIMANAGER: CENTRALIZED MANAGEMENT PLATFORM							
FortiManager	200G	300F	1000F	2000E	3000G	3700F	FMG-BASE to FMG-VM-UL-UG
Devices/VDOMs (Maximum)	30	100	1000	1200	4000	10.000+	10 to Unlimited
Sustained Log Rates	50	50	50	50	150	150	Hardware dependent
GB/Day	2	2	2	2	10	10	1-50
Total Interfaces	4 x GE RJ45	4 x GE RJ45, 2 x SFP	2 × 10G RJ45 2 x SFP+	4 x GE 2 × 10 GE SFP+	2 x GE RJ45 2 × 25 GE SFP28	2 x GE RJ45 2× 10 GE SFP28	1 / 4 (vNIC Min / Max)
Storage Capacity	2 × 4 TB	4 × 4 TB	8 × 4 TB	12 × 3 TB	16 × 4 TB	60 × 4 TB	80 GB / 16 TB (Min / Max)
Zero Touch Provisioning	Order FortiDeploy at the time of Purchase						
Third Party Automation	✓	✓	✓	✓	✓	✓	✓

www.fortinet.com