As the use of business critical, cloud-based applications continues to increase, organizations with a distributed infrastructure of remote offices and expanding remote workforce are switching 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 organizations' main data centers for all application and security needs that comes at a premium price for connectivity. While this legacy hub-and-spoke, architecture provides centralized protection; it increases latency and slows down network performance to distributed cloud services for application access and compute. Operational complexity and limited visibility associated with multiple point products add significant management overhead and difficulties while 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 that combines next generation firewall with advanced SD-WAN networking capabilities to eliminate MPLS required traffic backhaul and deliver improved user experience without ever compromising on security. This allows simplified single console management for all networking and security needs, while extending SD-WAN into wired and wireless access points of branch offices. This enables network security and controls for a deeper integration and consistent security enforcements into branch LAN networks.
BUSINESS OUTCOMES

**Improved User Experience**
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**
Industry’s only organically developed purpose-built SD-WAN ASIC powered enables thin edge (SD-WAN, routing) and WAN Edge (SD-WAN, routing, NGFW) securing 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**
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 performing platform to deliver the most comprehensive SD-WAN solution.

**FortiGate**
Broad product portfolio in different form factors: physical appliance and virtual appliance with the industry’s only ASIC acceleration with 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 ensures the best user experience for business critical, SaaS and UCaaS applications

**FortiOS**
Operating system that delivers Security-driven Networking strategy that secures and accelerates network and user experience. Continued innovations and enhancement enables:

- Real-time application optimization for 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 with effective support of 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**
Enables choice of SD-WAN use case with advanced protection by staying always ahead of the threats:

- Coordinated real-time detection and prevention against known and unknown protecting content, application, people, and devices
- Real-time Insights based on an extensive amount of data processed at a cloud-scale and analyzed with advanced AI, and are automatically distributed back for real-time enforcement and protection
# CORE COMPONENTS

<table>
<thead>
<tr>
<th>Features</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FortiGuard</strong></td>
<td></td>
</tr>
<tr>
<td>Application Identification &amp; Control</td>
<td>5000+ Application signatures, First packet Identification, Deep packet Inspection, Custom application signatures, SSL decryption enabled, TLS1.3 with mandated ciphers and deep inspection.</td>
</tr>
<tr>
<td>SD-WAN (Application aware traffic control)</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced SD-WAN (WAN remediation)</td>
<td>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.</td>
</tr>
<tr>
<td>SD-WAN deployment</td>
<td>Flexible deployment – hub-to-spoke (partial mesh), spoke-to-spoke (full mesh), Multi-WAN transport support.</td>
</tr>
<tr>
<td><strong>FortiOS</strong> — Networking</td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>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/Remap DSCP bits for influence traffic QoS on egress devices, Application steering based on ToS marking.</td>
</tr>
<tr>
<td>Advanced Routing (IPv4/IPv6)</td>
<td>Static routing, Internal Gateway (iBGP, OSPF v2/v3, RIP v2), External Gateway (eBGP), VRF, route redistribution, route leaking, BGP configuration, router reflectors, summarization and route-aggregation, route asymmetry.</td>
</tr>
<tr>
<td>VPN/Overlay</td>
<td>Site-to-site ADVN, Dynamic VPN tunnels, policy-based VPN, IKEv1, IKEv2, OPO, PFS 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 SHA1 based HMAC.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Multicast forwarding, PIM sparse (rfc 4601), dense mode (rfc 3973), PIM Rendezvous-Point.</td>
</tr>
<tr>
<td>Advanced Networking</td>
<td>DHCP v4/v6, DNS, NAT – source, destination, static NAT, destination NAT, PAT, NAPT, Full IPv4/v6 support.</td>
</tr>
<tr>
<td><strong>FortiOS</strong> — Security</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Fabric Management Center</strong></td>
<td></td>
</tr>
<tr>
<td>Centralized Management &amp; Provisioning</td>
<td>FortiManager – zero touch provisioning, centralized configuration, change management, dashboard, application policies, QoS, security policies, application specific SLA, active probe configuration, RBAC, multi-tenant.</td>
</tr>
<tr>
<td>Cloud Orchestration</td>
<td>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.</td>
</tr>
<tr>
<td>Enhanced Analytics</td>
<td>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.</td>
</tr>
<tr>
<td><strong>FortiGate</strong></td>
<td></td>
</tr>
<tr>
<td>Redundancy/High-availability</td>
<td>FortiGate dual device HA – primary and backup, FortiManager HA, Bypass interface, interface redundancy, redundant power supplies.</td>
</tr>
<tr>
<td>Integration</td>
<td>RESTful API/Ansible for configuration, zero touch provisioning, reporting and third-party integration.</td>
</tr>
<tr>
<td>Virtual environments</td>
<td>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 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 &amp; 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 SPl 1TS3, Nutanix AHV (AOS 5.10, Prism Central 5.10), Cisco Cloud Services Platform 2100.</td>
</tr>
<tr>
<td>Built-in Variants</td>
<td>POE, LTE, WiFi, ADSL/VDSL.</td>
</tr>
</tbody>
</table>
PRODUCT OFFERINGS

FortiGate

<table>
<thead>
<tr>
<th>SD-WAN Branch Offices</th>
<th>FG/FWF-40F Series</th>
<th>FG/FWF-60F Series</th>
<th>FG/FWF-80F Series</th>
<th>FG-100F Series</th>
<th>FG-200F Series</th>
</tr>
</thead>
</table>

**Use Case**
- **Type**: Remote Office/Home, Small Branch, Medium Branch, Large Branch, Large Branch

**Performance**
- **Unrestricted WAN Bandwidth**: Fortinet Secure SD-WAN offers unrestricted bandwidth unlike other SD-WAN vendors
- **Zero Touch Provisioning**: Order FortiDeploy at the time of Purchase

**WAN VPN Throughput**
- 4.4 Gbps

**Application Control Throughput**
- 990 Mbps

**Threat Protection Throughput**
- 600 Mbps

**SSL Inspection Throughput**
- 310 Mbps

**Connectivity**
- **Dedicated WAN Ports**: 1, 2, 2, 2, 2 (10GE)
- **Dedicated FortiLink Ports**: 1, 2, 2, 2 (10GE), 2 (10GE)
- **LAN / Switch Ports**: 2, 5, 6, 12

**Hardware Variants**
- **Built-in**: 3G/4G, WiFi, WiFi, Storage, WiFi, Bypass, Storage, Storage
- **Form Factor**: Desktop, Desktop, 1RU, 1RU

**Use Case Offering**
- **Name**: Priority Access, Support, Priority Access To Level 2 Support
- **Support**: To Level 2 Support
- **With AV & Cloud Sandbox**: Yes, Hot Swappable
- **Web & Application Access Protection**: Yes, Hot Swappable
- **Vuln. And Device Protection (IoT/Ot)**: Yes, Hot Swappable
- **Compliance Monitoring Tools**: Yes, Hot Swappable
- **SD-WAN Management & Orchestration**: Yes, Hot Swappable
- **Network & Security Cloud Management**: Yes, Hot Swappable

**WAN Edge**
- **360 Protection Bundle**: 24 x 7 ⃝✓ ⃝✓ ⃝✓ ⃝✓ ⃝✓ ⃝✓ ⃝✓ ⃝✓ ⃝✓ ⃝✓

**SD-WAN Hub Sites**
- FG-600E Series
- FG-1100E Series
- FG-1800F Series
- FG-2600F Series
- FG-3400E Series
- FG-3600E Series
- FG-4200F Series
- FG-4400F Series

**Use Case**
- **Type**: Campus/Small Datacenter, Campus/Small Datacenter, Large Datacenter, Large Datacenter, Large Datacenter, Large Datacenter, Hyperscale Datacenter, Hyperscale Datacenter

**Performance**
- **Unrestricted WAN Bandwidth**: Fortinet Secure SD-WAN offers unrestricted bandwidth unlike other SD-WAN vendors
- **IPSEC VPN Throughput**
- **Max Client to G/W IPSEC Tunnels**
- **Threat Protection Throughput**
- **SSL Inspection Throughput**

**Connectivity**
- **40/100GE**: - - - 4 4 6 8 12
- **10/100GE**: - 4 - - - - -
- **10/25GE**: - 4 12 - - - -
- **1/10GE**: - 4 12 - - - -

**Dual Power Supply**
- Optional, Yes, Hot Swappable

**Use Case Offering**
- **Name**: Unified Threat Protection Bundle
- **Support**: Priority Access To Level 2 Support
- **With AV & Cloud Sandbox**: Yes, Hot Swappable
- **Web & Application Access Protection**: Yes, Hot Swappable
- **Vuln. And Device Protection (IoT/Ot)**: Yes, Hot Swappable
- **Compliance Monitoring Tools**: Yes, Hot Swappable
- **SD-WAN Management & Orchestration**: Yes, Hot Swappable
- **Network & Security Cloud Management**: Yes, Hot Swappable
- **Recommended Add-on Protections / Products**: SD-WAN mgmt.
# PRODUCT OFFERINGS

## FortiGate-VM Support Matrix

<table>
<thead>
<tr>
<th></th>
<th>Private Cloud</th>
<th>Public Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMware VSphere</td>
<td>Citrix Xen</td>
</tr>
<tr>
<td>FG-VM **</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

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

---

** Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet discloses all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.