FORTINET

DATA SHEET

# FortiOS™ 7.0

Available in:

Appliance | Virtual Machine | Hosted (SASE SIA) | Cloud

OS

## Fortinet's Security Operating System

The release of FortiOS 7.0 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across all networks, endpoints, and clouds with SASE and ZTNA, among others.

FortiOS 7.0 expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across the entire distributed network.

It allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

Delivering a consistent and dynamic security posture enables users and devices to access applications where they are deployed, from anywhere in the world with security that automatically asses & adjust to match the risk.

Powered by FortiOS™ 7.0, the Fortinet Security Fabric delivers:

### Security-Driven Networking

Convergence of Networking and Security into a single, integrated system that can expand to any edge

### Zero-Trust Access

Knowing and controlling every connected user and device

### Adaptive Cloud Security

Secure and control multi-cloud infrastructures and applications with agility and automation

## Highlights: What's New

### Networking

- SD-WAN advanced routing improvements

### Security

- FortiGuard Video Filtering Service
- DNS inspection enhancements ACME Support
- New Zero Trust Network Access solution
- AI-Based malware detection

### Management

- Support for Security Fabric in Multi-VDOM mode
- Fabric Devices to trigger Automation Rules
- Security Rating Overlays

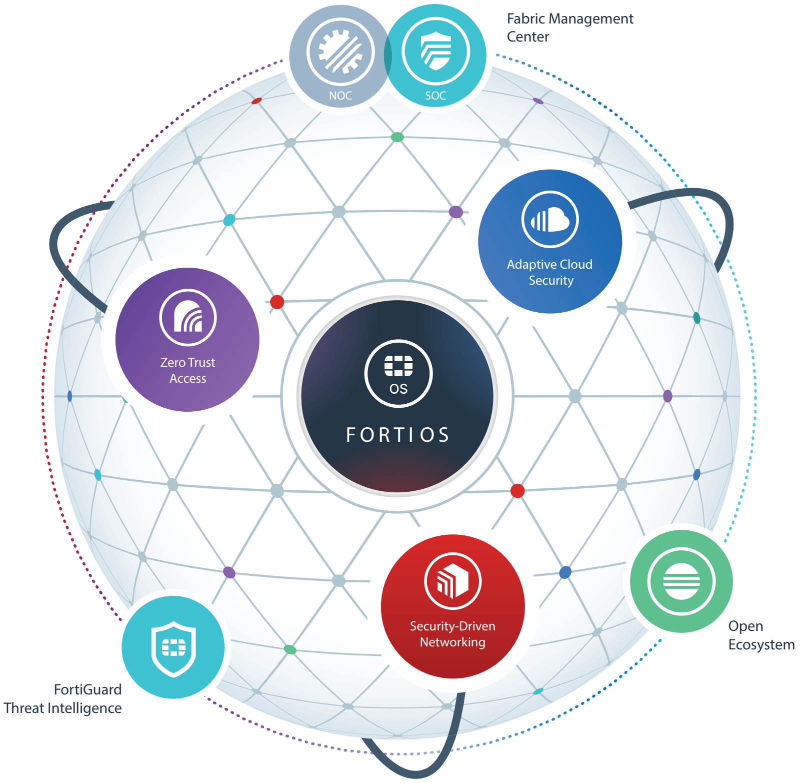
# OVERVIEW

## Introducing FortiOS™ 7.0

### Digital Innovation

As organizations accelerate their digital innovation initiatives, ensuring their security can keep up with today's complex and fast-evolving threat landscape is critical. The explosion of network edges – across data center, WAN, LAN, LTE, off-net, compute, operational technology, CASB, SASE, internet, and most recently, the home edge – has expanded and splintered the perimeter across the entire infrastructure.

The challenge with rapidly expanding the network edge is that many of the technologies needed to make things work don't work together. Much of the digital innovation progress has been piecemeal, without a unifying security strategy or framework. Most organizations have accumulated a wide variety of isolated security tools designed to protect a function or one segment of the network in isolation.



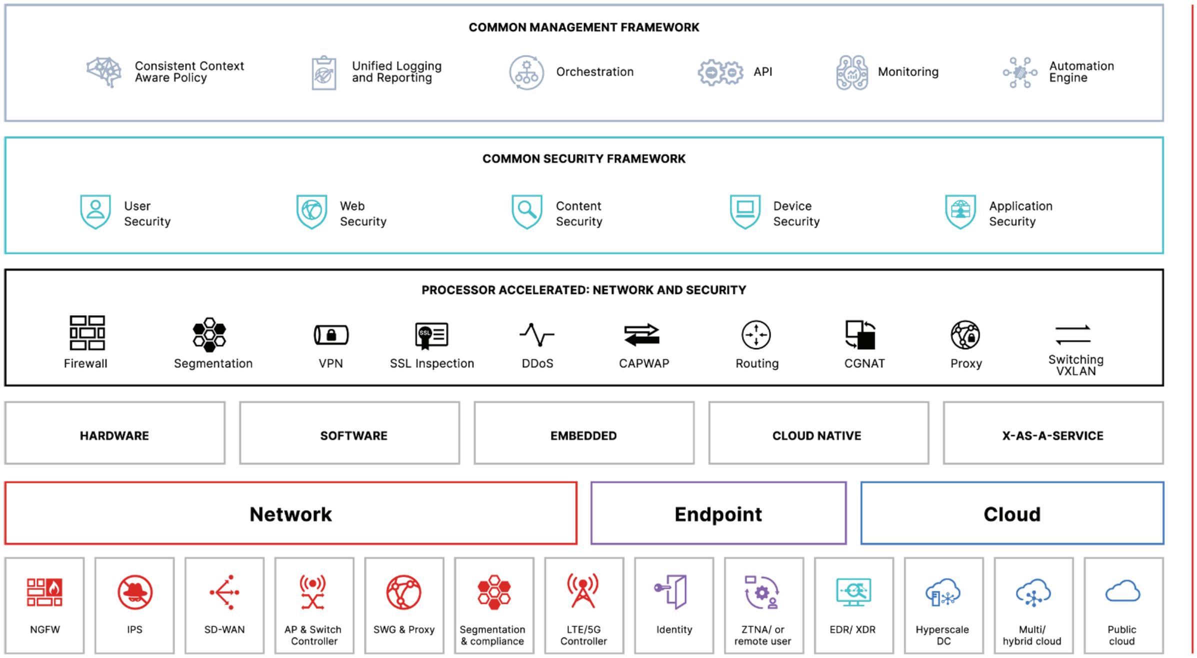
Vendor and solutions sprawl has made maintaining network-wide visibility and consistent policy enforcement next to impossible, let alone maintaining and monitoring the various security and networking solutions in place for delivering the expected high-performing user to application connection. AND keeping ahead of threats that morph, change and expand in rapid pace than ever before.

This approach can't scale, slowing business down, introducing more risk and complexity. It needs to evolve.

Fortinet addresses this challenge with the Fortinet Security Fabric, an integrated cybersecurity platform with a rich ecosystem designed to span the extended digital attack surface to enable broad, integrated, and automated security protecting devices, data, and applications.

With over 300 new features spanning the full portfolio and pillars, we keep organizations ahead of the threats by providing continuous protection for data, users, devices, and applications transition across networks, endpoints, and multi-clouds leveraging our Fabric, AI-powered FortiGuard Security Services, and automated response capabilities. Our Fabric Management Center provides organizations of any size to secure and simplify their SOC, NOC, and IT infrastructure. And our new SOCaaS and best practice services help ensure that the organization's overarching security posture is optimized.

# HIGHLIGHTS



Organically Built On A Common Management And Security Framework

Powering The Highest Performing Network And Security Fabric

Consistent For Hybrid Deployment

Across The Full Attack Surface

Optimized For Leading Use Cases

## Security Fabric

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **System Integration** | ▪ Native integration with Fortinet products via quick setup GUI connectors<br>▪ Standard-based data exchange APIs support with third-party solutions<br>▪ Standard-based monitoring output – SNMP Netflow/Sflow and Syslog support to external/ third-party SIEM, SOAR and logging systems<br>▪ Endpoint/Identity infrastructure integrations<br>▪ External threat feeds integrations<br>▪ **New:** Security Fabric support in multi-virtual domain environments | ▪ Ability to reuse organization's existing systems to lower TCO and streamline processes<br>▪ Expand security and operational capabilities by seamlessly integrating with external solutions |
| **Central Management and provisioning** | ▪ Fortinet/third-party automation and portal services support via APIs and CLI scripts<br>▪ Rapid deployment features including cloud-based provisioning solutions<br>▪ Developer community platform access and professional service options for complex integrations<br>▪ Extensive integration resources for Ansible and Terraform | ▪ Extensive APIs and CLI commands offering feature-rich service enhancements<br>▪ Comprehensive rapid deployment options to save time and costs<br>▪ Fortinet Developer Network (FNDN) empowers large service providers and enterprises with shared implementation/customization/ integration knowledge |
| **Cloud and SDN Integration** | ▪ Multi-cloud support using Cloud and SDN connectors for AWS, Microsoft Azure, GCP, OCI, AliCloud, VMware ESXi, NSX, OpenStack, Cisco ACI and Nuage Virtualized Service Platforms<br>▪ Kubernetes connectors for private and public clouds<br>▪ **NEW:** Show the REST API commands behind a particular GUI action | ▪ Robust and comprehensive SDN integration capabilities that allow organizations to implement cloud solutions securely without compromising agility |

# HIGHLIGHTS

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **Visibility** | ▪ Interactive drill-down and topology viewers that illustrate real-time and historical threat status and network usage with comprehensive contextual information<br>▪ Aggregated data views provided by fabric devices | ▪ One-click remediation that offers accurate and quick protection against threats and abuses<br>▪ Unique threat score system, correlating weighted threats with particular users to prioritize investigations<br>▪ Fabric-wide views expand visibility beyond a single security entity, allowing organizations to quickly spot problems and address them |
| **Automation** | ▪ Wizard-based automation workflow that performs appropriate actions based on triggers defined, across the Fortinet Security Fabric<br>▪ Automatically quarantine compromised hosts using FortiClient via EMS or connections via FortiSwitch and FortiAP<br>▪ **NEW:** Fabric Devices to trigger Automation Rules | ▪ Reducing risk exposure and replacing manual security processes with automation to help address the organizational challenges of tighter budgets and a skilled staffing shortage |
| **NAC** | ▪ Interface with FortiAuthenticator and a wide variety of external identity management systems to facilitate user authentication processes<br>▪ Wide-ranging single sign-on identity acquisition methods, including Windows AD, terminal servers, access portals, and mail services<br>▪ Built-in token server to manage both physical and mobile tokens for use with various FortiOS authentication requirements such as VPN access and FortiGate administration<br>▪ **NEW:** Improved ZTNA (Zero Trust Network Access)  framework for mobile endpoints | ▪ FortiOS integrates with a wide variety of AAA services to facilitate user admission control from various entry points, giving users a simplified experience while implementing greater security<br>▪ Easily implement two-factor authentication for user and administrator access at little cost<br>▪ Simplified mobile user security enforcement by easily distributing and updating clients' security profiles that are consistent with gateway protection |
| **Compliance & Security Rating** | ▪ Periodic system configuration checks on fabric devices using a pre-defined checklist to reveal security posture status updates; the data is kept to produce historical trending charts<br>▪ Audit setups against PCI compliance requirements<br>▪ Security rating ranking are benchmarked against peers | ▪ Automates compliance auditing, which frees up administration resources<br>▪ Quickly verify the status and health of your setup and connected devices within the Fabric and identify any gaps that can potentially leave you at greater risk |
| **Advance Threat Protection (ATP)** | ▪ Local file quarantine (for models with storage)<br>▪ Receive dynamic remediation (malicious file checksum and URLs) DB updates and detail analysis reports from external Fortinet file analysis solutions (FortiSandbox)<br>▪ Endpoint vulnerability views that present ranked vulnerable clients with details<br>▪ IOC service integration displays IOC detection data from FortiAnalyzer onto FortiView and topology maps | ▪ Supported by proven and industry-validated AV research services.<br>▪ Ability to adopt a robust ATP framework that reaches mobile users and branch offices, detecting and preventing advanced attacks that may bypass traditional defenses by examining files from various vectors, including encrypted files<br>▪ Easily identify vulnerable hosts across the fabric<br>▪ Administrators can easily identify suspicious hosts and quickly or automatically quarantine them |

# HIGHLIGHTS

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **Wireless Controller** | ▪ Integrated wireless controller for Fortinet's wide range of AP form factors, including indoor, outdoor, and remote models, with no additional license or component fees<br>▪ Enterprise-class wireless management functionality, including rogue AP protection, wireless security, monitoring, and reporting<br>▪ Supports 802.3ax APs | ▪ The wireless controller integrates into the FortiGate console providing a true single-pane-of-glass management for ease-of-use and lower TCO |
| **Switch Controller** | ▪ Integrated switch controller for Fortinet access switches with no additional license or component fees<br>▪ Simplifies NAC deployment | ▪ Expands security to the access level to stop threats and protect terminals from one another |
| **WAN Interface Manager** | ▪ Supports LTE connectivity via integrated modem, USB port or the FortiExtender | ▪ Allows organizations to use or add 3G/4G connectivity for WAN connections while maintaining access control and defining the usage for those links |

## Operations

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **Configuration** | ▪ Wide variety of configuration tools — iOS app, Web UI and CLI<br>▪ Ease of use with intuitive, state-of-the-art GUI and wizards<br>▪ One-click access and actions between log viewers, dashboard widgets, policy tables, and more<br>▪ Intelligent object panel for policy setups and edits | ▪ Unique FortiExplorer configuration tool allows administrators to quickly access configurations, including via mobile phones and tablets<br>▪ VPN wizards facilitate easy setup, including popular mobile clients and other vendors' VPN gateways<br>▪ Useful one-click access and actions bring administrators to the next steps quickly and accurately to swiftly mitigate threats or resolve problems |
| **Log & Reports** | ▪ Detailed logs and out-of-the-box reports that are essential for compliance, audits, and diagnostic purposes<br>▪ Real-time logging to FortiAnalyzer, FortiAnalyzer Cloud, and FortiGate Cloud<br>▪ Common Event Format (CEF) support<br>▪ Logging consolidation within Security Fabric | ▪ Includes deep contextual information, including source device details and strong audit trail<br>▪ GUI Report Editor offering highly customizable reports<br>▪ Managing logs holistically simplifies configuration and guarantees that critical information from every FortiGate is centrally collected and available for analysis. This closes any gaps in intelligence |
| **Diagnostics** | ▪ Diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues<br>▪ Hardware testing suite on CLI<br>▪ Policy and routing GUI tracer | ▪ Comprehensive diagnostic tools help organizations quickly remediate problems and investigate abnormal situations |

# HIGHLIGHTS

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **Monitoring** | ▪ Real-time monitors<br>▪ NOC Dashboard<br>▪ IOS push notification via FortiExplorer app | ▪ Dashboard NOC view allows you to keep mission-critical information in view at all times. Interactive and drill-down widgets avoid dead-ends during your investigations, keeping analysis moving quickly and smoothly |

## Policy & Control

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **Policy Modes** | ▪ Easy-to-use policy management with unique Section or Global view options<br>▪ NGFW Policy-based and Policy-based modes<br>▪ Consolidated IPv4 and IPv6 policies | ▪ Flexible policy setup with various control systems assist organizations in implementing effective network security that is relevant to their networks |
| **Device Identification** | ▪ Identification of different types of devices present on the network<br>▪ MAC address policy source objects<br>▪ IoT security service allowing FortiGates to query FortiGuard servers for more information about a device | ▪ Empowers organizations to add critical security to today's BYOD environment by identifying personal devices |
| **SSL Inspection** | ▪ Effectively examine SSL-encrypted traffic with various security controls, such as AV and content filtering<br>▪ High-performance SSL inspection with content processors<br>▪ Reputable sites database for exemptions | ▪ Identify and block threats hidden within encrypted traffic without significantly impacting performance |

## Security

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **Firewall** | ▪ High-performance firewall within a SPU-powered appliance<br>▪ Implement security policies that use a combination of source objects, IPs, users, and/or devices<br>▪ Automatically or manually quarantine users/attackers<br>▪ Directs registered FortiClient to host quarantines | ▪ Industry's top firewall appliance with a superior cost-performance ratio |
| **VPN** | ▪ Comprehensive enterprise-class features for various types of VPN setups<br>▪ SSL and IPsec VPN wizards<br>▪ Cloud-assisted Overlay Controller VPN that supports, Full Mesh, Hub & Spoke topology with ADVPN options | ▪ The FortiGate's unmatched performance for VPN allows organizations to establish secure communications and data privacy between multiple networks and hosts by leveraging custom security processors (SPUs) to accelerate encryption and decryption of network traffic |

# HIGHLIGHTS

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **IPS & DoS** | ▪ Regular and rate-based signatures, supported by zero-day threat protection and research for effective, IPS implementation<br>▪ Integrated DoS protection defends against abnormal traffic behaviors<br>▪ CVE reference for IPS signatures | ▪ Proven quality protection with "NSS Recommended" award for superior coverage and cost/performance<br>▪ Adapts to enterprise needs with full IPS features and NGIPS capabilities, such as contextual visibility<br>▪ Supports various network deployment requirements, such as sniffer mode, and compatible with active-bypass bridging device or built-in bypass ports for a selected model |
| **Web & Video Filtering** | ▪ Enterprise-class URL filtering solution that includes quotas, user overrides, transparent safe search, and search engine keyword logging<br>▪ Superior coverage with URL ratings of over 70 languages and identifies redirected (cached and translated) sites<br>▪ **New:** Video Filtering using FortiGuard category based filter and/or YouTube APIs and parameters | ▪ Multi-layered anti-proxy avoidance capabilities with integrated application control and IPS allow organizations to implement air-tight web usage controls |
| **Email Filtering** | ▪ Highly effective, multilayered spam filters with low false positives | ▪ Cost-efficient anti-spam solution for small organizations or branch offices without requiring investment in an additional system |
| **Application Control** | ▪ Detects and acts against traffic-based on applications while providing visibility on network usage<br>▪ Fine-grained control on popular cloud applications, such as SalesForce, Google Docs, and Dropbox | ▪ Superior coverage, including both desktop and mobile applications, enabling better management of network access policies<br>▪ Applies deeper application inspections for better control and visibility as more enterprises rely on public cloud services |
| **Anti-Malware** | ▪ Flow- and proxy-based AV options for choices between protection and performance<br>▪ Anti-bot capability using IP reputation DB to terminates botnet communication to C&C servers<br>▪ Receive dynamic remediation (malicious file checksum and URLs) DB updates and detail analysis reports from external Fortinet file analysis solutions (FortiSandbox)<br>▪ Virus Outbreak Protection as an additional layer of proactive protection targeted at new malware; comparing and detecting threats using a real-time FortiGuard checksum database<br>▪ Content Disarm and Reconstruction (CDR) removes exploitable content before reaching users<br>▪ **NEW:** AI-powered heuristics detection engine | ▪ Supported by proven and industry-validated AV research services<br>▪ Ability to adopt robust ATP framework that reaches mobile users and branch offices, detecting and preventing advanced attacks that may bypass traditional defenses by examining files from various vectors, including encrypted files |
| **Protective DNS** | ▪ Uses existing DNS protocols and architecture to analyze DNS queries and mitigate threats | ▪ Defenses in various points of the network exploitation lifecycle, addressing phishing, malware distribution, command and control, domain generation algorithms, and content filtering. |

# HIGHLIGHTS

## Security

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **SD-WAN** | ▪ Intelligent WAN path control with the ability to direct traffic among WAN links based on over 3,000 applications and users/user groups<br>▪ Measure application transactions such as latency, jitter, and packet-loss plus built-in automatic fail-over to determine preferred paths and maintain the optimal application performance of business-critical applications<br>▪ Use QoS, Traffic Shaping and policy routing for bandwidth management<br>▪ Peer to peer and remote user WAN optimization and byte caching technologies<br>▪ **New:** Passive WAN health measurement | ▪ Broad coverage of application visibility and first packet classification for efficient<br>SD-WAN adoption<br>▪ Integrated NGFW and SD-WAN on the same appliance further reduces TCO and complexity<br>▪ WAN Path Controller automation continues to provide high application performance<br>▪ Industry's highest IPsec VPN performance<br>▪ Zero Touch Deployment of SD-WAN Edge |
| **Explicit Proxy** | ▪ Explicit HTTP and HTTPS, FTP over HTTP, or SOCKS proxying of IPv4 and IPv6 traffic on one or more interfaces<br>▪ Transparent web proxy | ▪ Integrated, enterprise-class explicit web proxy provides HTTP and HTTPS proxying with the added benefits of UTM security and user identity |
| **IPv6** | ▪ Comprehensive IPv6 support for routing, NAT, security policies, and more | ▪ Operating mode options provide flexibility when deploying into existing or new networks, reducing network change requirements |
| **High Availability** | ▪ Support for industry-standard VRRP and various proprietary solutions, with ability to combine more than one high availability solution into a single configuration | ▪ Flexible high availability offerings allow organizations to pick the most suitable solutions based on their network environments and SLA requirements |
| **Routing/NAT** | ▪ Comprehensive routing protocols and NAT support<br>▪ Traffic redirection with ICAP and WCCP support | ▪ Wide-ranging routing features that meet carrier and enterprise resilience networking requirements |
| **L2/Switching** | ▪ Ability to craft software switches or emulate VLAN switches from interfaces<br>▪ Support SPAN ports and port aggregation with multiple interfaces.<br>▪ Implement admission control modes on interfaces such as 802.1x or captive portal<br>▪ Comprehensive WiFi and WAN interface configuration options<br>▪ VXLAN and EMAC VLAN Support | ▪ Flexible interface configurations offer various setup possibilities that best suit an organization's network requirements while providing optional access security |
| **Offline Inspection** | ▪ Sniffer mode allows threat and usage monitoring of network activities offline | ▪ Wide-ranging routing features that meet carrier and enterprise resilience networking requirements |
| **Essential Network Services** | ▪ A wealth of networking services such as DHCP, DNS server, NTP server and more | ▪ Built-in, out-of-the-box capabilities let organizations quickly provide necessary network services to internal terminals or to integrate with other network devices |

# HIGHLIGHTS

## Platform Support

| FEATURE | HIGHLIGHTS | FORTINET ADVANTAGE |
|---|---|---|
| **Physical Appliance (+SPU)** | ▪ Integration with proprietary hardware architecture that includes acceleration components (SPU) and multicore processors | ▪ Superior software and hardware integration ensures the optimal use of hardware components, yielding the highest cost/performance for customers |
| **Virtual System** | ▪ Virtual Domains (VDOMs): Virtualized FortiOS components to multiple logical systems on a single virtual or physical appliance.<br>▪ Global security profiles<br>▪ Support Virtual routing and forwarding (VRF) that allows multiple instances of a routing table to exist and work simultaneously<br>▪ Support for Split-Task VDOM | ▪ Built-in, out-of-the-box capabilities let organizations quickly provide necessary network services to internal terminals or to integrate with other network devices |
| **Hypervisor** | ▪ Support for popular hypervisor platforms, including VMware vSphere, Citrix and open source Xen, KVM, and MS Hyper-V | ▪ Consistent management and features between physical and virtual appliances reduces management cost and simplifies deployments |
| **Cloud** | ▪ Support for public cloud services: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI) and AliCloud | ▪ Consistent management and features between on-premises and cloud platforms reduces management cost and simplifies deployments |
| **Hosted (FortiSASE SIA)** | ▪ **New:** Powering FWaaS and hosted SWG components of FortiSASE SIA offering | ▪ SASE extends networking and security capabilities beyond where they have typically been available, allowing users, regardless of location, to take advantage of firewall-as-a-service (FWaaS), secure web gateway (SWG), zero-trust network access (ZTNA), and a medley of other threat detection functions. |

# SPECIFICATIONS

## Security Fabric

### SYSTEM INTEGRATION

Security Fabric Logging:
- Synchronized logging to FortiAnalyzer configurations among FortiGates
- Data exchange (information such as topology and device asset tags) with FortiAnalyzer

Technology ecosystem encompasses leading partners in the Firewall and Network Risk Management, SDN and Virtualization, Security Information and Event Management (SIEM), Systems Integration, Testing and Training, and Wireless markets

Native integration with FortiSandbox, FortiSandbox Cloud, FortiMail, FortiNAC, FortiMail Cloud, FortiProxy, FortiAI, FortiDeceptor, FortiTester and FortiWeb

### CENTRAL MANAGEMENT AND PROVISIONING

Central management support: FortiManager, FortiCloud hosted service, web service APIs

Rapid deployment: Install wizards, USB auto-install, local and remote script execution

### CLOUD AND SDN INTEGRATION

Integration via connectors with:
- Public Cloud: AWS, MS Azure, GCP, OCI, AliCloud and IBM Cloud
- Private SDN: Kubernetes, VMware ESXi and NSX, OpenStack, Cisco ACI, Nuage Networks and Nutanix Prism

API Preview: view all REST API requests being used on a particular GUI page

### VISIBILITY

Interactive and graphical visualizer for user, device, network, and security activities (FortiView):
- A variety of GUI consoles that display current and historical status using different perspectives such as
  'sources', 'destinations', 'applications', and 'threats' etc.
- Threat and VPN map
- Data view options: Table, bubble chart, or world map if applicable
- Statistics and system information about the connected fabric device
- Accelerated session indication
- WHOIS Lookup for Public IP addresses within FortiView and log tables

Physical and logical topology viewers that illustrate:
- location of hosts within the security fabric network
- one-click access to quarantine, IP ban, or access detailed contextual information of hosts
- connections between security fabric entities
- SD-WAN related information such as link usage

Aggregated data views with downstream FortiGates within a Security Fabric
- presented on FortiView, topology maps, and monitors

### AUTOMATION

Define automation within the Security Fabric using simple if-then setup:
- Triggers: Compromised host detection, system status, configuration changes, FortiAnalyzer event handler, Incoming Webhook and schedule
- Actions: CLI scripts, email, iOS, MS Teams and Slack notification, public cloud functions, API calls/webhooks

Quarantine remote host automatically at the access layer with FortiAP and/or FortiSwitch, or FortiClient via EMS

### NETWORK ACCESS CONTROL (NAC)

Local user database and remote user authentication service support: LDAP, Radius and TACACS+, native FortiClient and FortiNAC user integration and two-factor authentication

Single-sign-on: Integration with Windows AD, Microsoft Exchange Server, Novell eDirectory, FortiClient, Citrix and Terminal Server Agent, Radius (accounting message), POP3/POP3S, user access (802.1x, captive portal) authentication

SAML SSO support within a fabric network allows an administrator to move between fabric devices without logging in again

PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support

Integrated token server that provisions and manages physical, SMS, and Soft One Time Password (OTP) tokens

ZTNA Framework: FortiClient EMS uses zero-trust tagging rules to automatically tag managed endpoints based on various attributes detected by the FortiClient. These tags are synchronized as dynamic address objects on the FortiGate

NAC with integrated Wireless and Switch Controller:
- supports NAC profiles that onboard clients into the default VLAN, NAC policies match clients based on device properties, user groups, or ZTNA tags, and then assign the clients to specific VLANs

### COMPLIANCE AND SECURITY RATING

Run a series of system configuration compliance check against PCI requirements

Security Fabric Rating: audit components within the fabric against best practices, provide results and recommendations, then allow users to easily apply remediations for some items

Manages network devices compliance via dynamic access control with tags provided by external client management systems

### ADVANCE THREAT PROTECTION (ATP)

Display list of vulnerable hosts and their vulnerabilities via telemetry with FortiClient

Display list of compromised hosts via information provided by FortiAnalyzer

External cloud-based or on-premise file analysis (OS sandbox) integration:
- File submission (with option to select types)
- Receive file analysis reports
- Receive dynamic signature updates from file analysis system (file checksum and malicious URL DB)

Support for external block lists for domain names, web filtering URLs, IP addresses and malware hashes

### WIRELESS CONTROLLER

Manages and provisions settings for local and remote access points

SSID Authentication:
- WPA2-Personal, WPA2-Enterprise
- WPA3 (SAE, SAE transition, Enterprise
- Open

Supports integrated or external captive portal, 802.1x, preshared keys

Client limiting, MAC filtering, broadcast disabling, block intra-traffic and host quarantine on SSID

Multiple PSK for WPA Personal

Dynamic user VLAN assignment:
- with RADIUS attributes
- with VLAN Pooling (Round-Robin/Hash Load balancing)

Airtime fairness: improve the overall network performance by managing downlink link traffic toward different clients with balanced airtime

CAPWAP data channel security: DTLS and IPsec VPN option

WiFi Security: Rogue AP suppression, wireless IDS, monitor and suppress phishing SSID

WiFi troubleshooting tools, spectrum analysis and location map

Extended logging information in key areas to help WiFi troubleshooting:
- association, authentication, DHCP, and DNS

Wireless topology support: Fast roaming, AP load balancing, Wireless Mesh and bridging

WiFi QoS WMM marking: preserve the WiFi Multi-Media (WMM) QoS marking of packets by translating them to DSCP values when forwarding upstream (For 802.11ac-W2 APs only)

Wi-Fi Alliance Agile Multiband Operation (MBO) support: enables better use of Wi-Fi network resources in roaming decisions and improves overall performance

Controlled failover between wireless controllers

### SWITCH CONTROLLER

Extends access control and security to wired devices by managing Fortinet switches (FortSwitch) via CAPWAP-like communication known as FortiLink

Automatic provisioning of switch firmware upon authorization

Switch Topologies:
- single/stack of switch units
- HA-mode FortiGate with single/Stack of switch units
- HA-mode FortiGate with two-tier switch units (Optional: with access rings)
- Dual-homed servers connected to a pair of switch units using an MCLAG
- Standalone/HA-mode FortiGate unit with dual-homed FortiSwitch access
- Multi-tiered MCLAG with HA-mode FortiGate units

Switch port Features:
- PoE settings
- DHCP blocking and IGMP snooping
- STP (status, BPDU, root guard)
- LLDP, IGMP, sFlow and Dynamic ARP inspection (DAI)
- Port mirroring

Port security policies:
- 802.1x Port-based and MAC-based mode
- Restrict the type of frames allowed through IEEE 802.1Q ports
- RADIUS accounting support
- MAC authentication bypass
- EAP pass-through

NAC policy enforcement: use user or detected device information, such as device type or OS, to put traffic into a specific VLAN or apply specific port settings
- Device attributes conditions: MAC address, hardware vendor, device type, operating system
- User-based conditions
- Actions: assignment to VLAN and application of port specific settings

Provision of guest, authentication-fail and quarantined VLANs

### WAN INTERFACE MANAGER

Support USB 3G/4G Wireless WAN modems and modem extender (FortiExtender)

3G/4G modem settings:
- Support standalone and as redundant WAN interface mode
- “Always connect” and “On demand” dial mode
- Configurable redial limit

Some hardware variants support in-built DSL and/or 3G/4G modems

## Operations

### CONFIGURATION

Management access: HTTPS via web browser, SSH, telnet, console

Administrator login:
- ACME certificate support
- Password policy enforcement

FortiExplorer:
- Management client on IOS platforms
- Ease-of-use by using USB connectivity
- Provides mobile notification (as part of automation feature)

Feature Store: Toggle GUI component displays

GUI configuration:
- ‘One-click’ access that quickly transfer administrators to next step panels
- Dynamic object selectors and predictive search queries

Web UI administration language support: English, Spanish, French, Portuguese, Japanese, Simplified Chinese, Traditional Chinese, Korean

### LOG & REPORT

Logging facilities support: Local memory & storage (if available), multiple syslog servers, multiple FortiAnalyzers, WebTrends servers, FortiCloud hosted service

Reliable syslog based on RFC 3195/RFC6587

Encrypted logging & log Integrity with FortiAnalyzer

Scheduled batch log uploading, real-time logging or queue locally until external system is available

Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets

Comprehensive event logs: systems & administrators activity audits, routing & networking, VPN, user authentications, WiFi related events

Brief traffic log format option

Sending logs to syslog servers in Common Event Format (CEF)

IP and service port name resolution option

### DIAGNOSTICS

Diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues.

Policy and routing GUI tracer

Packet flow CLI tracer

Hardware testing suite on CLI

### MONITORING

SNMP System Monitoring:
- SNMP v1 and v2c support
- SNMP v3 implementation includes support for queries, traps, authentication, and privacy
- SNMP traps alerting to events such as a full log disk or a detected virus

Traffic Monitoring:
- sFlow version 5
- Netflow 9.0 and IPFIX, may be extended to managed FortiSwitches

Graphical Monitors: Real-time system, network service, and user status viewers

Dashboard: customized widgets and layout

## Policy & Control

### POLICY MODES

Policy objects: predefined, custom and object grouping

Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN, Dynamic (based on received tags from external systems) and MAC address

Internet Service DB: Dynamically updated DB that provides a list of popular cloud applications with their vital information that can be used for policy setup, routing and link load-balancing configurations.

NGFW policy mode: setup policies with applications and URLs as objects

User notifications: customizable replacement message for block sites and attachments

User quarantine:
- Manually assigned with perpetual or customizable duration
- Automatically when triggered by automation configuration

### DEVICE IDENTIFICATION

Device Identification: Cloud-based query DB service, device and OS fingerprinting, automatic classification, inventory management

Device inventory for visibility

Switch controller LLDP-MED Voice detection

### SSL INSPECTION

Inspect SSL encrypted traffic option for IPS, application control, antivirus, web filtering, and DLP

SSL MITM Mirroring

SSL Inspection Method options: SSL certificate inspection or full SSL inspection

SSL inspection exemption by site reputation DB, web categories, and/or policy addresses

## Security

### ANTI-MALWARE

Botnet server IP blocking with global IP reputation database

Antivirus database type selection depending on the network and security needs

Virus Outbreak Prevention Database query: uses real-time checksums DB of newly detected threats before AV signatures are available

Content Disarm and Reconstruction option:
- AV Engine removes all active content in real time before passing to user
- Forward original file to sandbox for further analysis, quarantine or discarded

AI-based malware detection: module is trained by FortiGuard AV against many malware samples to identify file features that make up the malware

AV Inspected protocols and file types:
- Support for HTTP, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS and SSH
- Scan encrypted traffic with SSL inspection
- (Password-protected) archive files
- Grayware and mobile malware

Option to treat Windows executables in email attachments as viruses

File quarantine (local storage required) and infected host ban

### IPS AND DOS

IPS engine: 11,000+ up-to-date signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration

IPS Actions: Default, monitor, block, reset, or quarantine attackers IP with expiry time

Filter-Based Selection: Severity, target, OS, application, and/or protocol

Packet logging option

IP(s) exemption from specified IPS signatures

IPv4 and IPv6 rate-based DOS protection (available on most models) with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)

IDS sniffer mode

### PROTECTIVE DNS

DNS Filter: DNS-based web category filtering and botnet protection
- Support DNS translation, external block list and static domain filter

### APPLICATION CONTROL

Detects thousands of applications in 18 categories: Business, Cloud IT, Collaboration, Email, Game, General Interest, Mobile, Network Service, P2P, Proxy, Remote Access, Social Media, Storage/Backup, Update, Video/Audio, VoIP, Web Chat and Industrial.

Custom application signature support

Multiple parameter support on some signatures

Supports detection for traffic using HTTP/2 protocol and able to block QUIC traffic so that browser automatically falls back to HTTP/2 + TLS 1.2

Filter-based overrides by: behavior, category, popularity, technology, risk, vendor, and/or protocol

Actions: Allow, block, reset session (CLI only), monitor only and attacker quarantine

Port enforcement check: block applications detected on non-default ports

Protocol enforcement: set networking services to defined ports. A violation can be set to block

SSH Inspection

Deep application control over popular public cloud services, such as SalesForce, Google Docs, and Dropbox

### WEB & VIDEO FILTERING

Web filtering inspection mode support: Proxy-based, flow-based, and DNS

Manually-defined web filtering based on URL, web content and MIME header

Dynamic web filtering with cloud-based real-time categorization database:
- Over 250 million URLs rated into 78 categories, in 70 languages

Pre-configured category-based filter: "G", 'PG-13", "R" and custom

Safe Search enforcement: transparently inserts Safe Search parameter to queries. Supports Google, Yahoo!, Bing and Yandex, definable YouTube Education Filter

Proxy avoidance prevention: Proxy site category blocking, rate URLs by domain & IP address, block redirects from cache & translation sites, proxy avoidance application blocking (application control), proxy behavior blocking (IPS)

Web filtering local categories & category rating override

Web filtering profile override: Allows administrator to temporarily assign different profiles to user/user group/IP

Multiple, external blacklist support

Restrict access to Google Corporate Accounts only

URL certificate blacklist: useful to block botnet communication that relies on SSL

Additional features offered by proxy-based web filtering:
- Filter Java Applet, ActiveX, and/or cookie
- Block HTTP Post
- Log search keywords
- Block HTTP redirects by rating
- Exempt scanning encrypted connections on certain categories for privacy
- Web Browsing quota by categories

Video filtering:
- Dynamic video filtering with cloud-based real-time categorization database
- Filter YouTube videos by channel IDs
- Enforce "Restrict YouTube access" and "Vimeo access" settings

### FIREWALL

Operating modes: NAT/route and transparent (bridge)

Schedules: one-time, recurring

Session helpers and ALGs: DCE/RPC, DNS-TCP, DNS-UDP, FTP, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)

VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing

Protocol type support: SCTP, TCP, UDP, ICMP, IP

User and device-based policies

Policy Management: Sections or global policy management view

Consolidated IPv4 and IPv6 policy table

### VPN

Customizable SSL VPN portal: color themes, layout, bookmarks, connection tools, client download

SSL VPN realm support: enables multiple custom SSL VPN logins associated with user groups
(URL paths, design)

Single-sign-on bookmarks: reuse previous login or predefined credentials to access resources

Personal bookmarks management: allow administrators to view and maintain remote client bookmarks

Limit SSL portal concurrent users

One time login per user options: Prevents concurrent logins using same username

SSL VPN web mode: For thin remote clients equipped with a web browser only and support web application, such as HTTP/HTTPS Proxy, FTP, Telnet, SMB/CIFS, SSH. VNC, RDP, Citrix

SSL VPN tunnel mode: for remote computers that run a variety of client and server applications, SSL VPN client supports MAC OSX, Linux, Windows Vista and with 64-bit Windows operating systems

SSL VPN port forwarding mode: uses a Java Applet that listens on local ports on the user's computer. When it receives data from a client application, the port forward module encrypts and sends the data to the SSL VPN device, which then forwards the traffic to the application server.

Host integrity checking and OS check (for windows terminals only) prior to SSL tunnel mode connections

MAC host check per portal

Cache cleaning option just before the SSL VPN session ends

IPsec VPN:
- Remote peer support: IPsec-compliant dialup clients, peers with static IP/dynamic DNS
- Authentication method: Certificate, pre-shared key
- IPsec Phase 1 mode: Aggressive and main (ID protection) mode
- Peer acceptance options: Any ID, specific ID, ID in dialup user group
- Supports IKEv1, IKEv2 (RFC 4306)
- IKE mode configuration support (as server or client), DHCP over IPsec
- Configurable IKE port
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256, ARIA128, ARIA192, ARIA256, SEED
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14 to 21, 27 to 32
- Suite-B support: GCM128 and GCM256
- ChaCha20/Poly1305 PRF support: SHA1, SHA256, SHA384 and SHA512
- XAuth support as client or server mode
- XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option
- Configurable IKE encryption key expiry, NAT traversal keepalive frequency
- IP fragmentation before/after IPsec encapsulation
- Dead peer detection
- Replay detection
- Autokey keep-alive for Phase 2 SA

FQDN support for remote gateways

IPsec Configuration Wizard for termination with popular third-party devices

IPsec Aggregate tunnels: set up redundancy and traffic load-balancing
- per-packet load balancing algorithm: by IP addresses, L4 information and (weighted)-round-robin

Cloud-assisted One-Click VPN/ VPN Overlay Controller: easily configure
- hub-and-spoke VPN (with ADVPN option)
- Mesh VPN (with ADVPN option)
- SD-WAN configuration integration
- Support VPN Client connection to hub

IPsec VPN deployment modes: Gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode

IPsec VPN Configuration options: Route-based or policy-based

Auto Discovery VPN (ADVPN): Dynamically establish direct tunnels (called shortcuts) between the spokes of a traditional Hub and Spoke architecture
- UDP hole punching for spokes behind NAT

VPN monitoring: View and manage current IPsec and SSL VPN connections in details

Other VPN support: L2TP client (on selected models) and server mode, L2TP over IPsec, PPTP,
GRE over IPEC

### EMAIL FILTERING

Mail protocol support: IMAP(S), POP3(S), and SMTP(S)

Anti-Spam DB query: IP address check, URL check, and email checksum

Local Spam Filtering: HELO DNS Lookup, return email DNS check, and Black/White List

## Networking

### ROUTING / NAT

Static and policy routing

Dynamic routing protocols: RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4

Content routing: WCCP and ICAP

NAT configuration: Per policy based and central NAT Table

NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN

Multicast traffic: sparse and dense mode, PIM support

### L2 / SWITCHING

Layer-2 interface modes: Port aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software, and VLAN switches

EMAC-VLAN support: allow adding multiple Layer 2 addresses (or Ethernet MAC addresses) to a single physical interface

VXLAN support:
- interVTEP (VXLAN Tunnel End Point)
- Support for multiple remote IPs, these remote IPs can be IPv4 unicast, IPv6 unicast, IPv4 multicast,
  or IPv6 multicast

Virtual Wire Pair:
- Process traffic only between 2 assigned interfaces on the same network segment
- Available on both transparent and NAT/route Mode
- Option to implement wildcard VLANs setup

### OFFLINE INSPECTION

Sniffer Mode: Dedicate an interface exclusively where all traffic entering the interface is processed by the sniffer

Offline Security inspection: AV, Web Filtering, Application Control, IPS, and Anti-spam

### SD WAN

WAN load balancing (weighted) algorithms by: volume, sessions, source-destination IP, Source IP, and spillover

WAN link checks for SLAs:
- Ping or HTTP probes
- Monitoring criteria including latency, jitter, and packet loss
- Configurable check interval, failure and fail-back thresholds
- Cloud-based SD-WAN bandwidth monitoring service

Passive WAN health measurement: determines the health check measurements using session information that is captured on firewall policies

Multi-path intelligence using rules defined by:
- Source address and/or user group
- Destination address and/or a selection of over 3,000 applications
- path selection using particular link quality criteria or SLAs defined

Traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, interface-based traffic shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), ,Differentiated Services (DiffServ) and Forward Error Correction (FEC) for VPN support

Packet duplication:
- Packets are duplicated on other good links within the SD-WAN zone and de-duplicated on the destination FortiGate
- Can be triggered by SD-WAN rules, source, destination, and service parameters
- Support over aggregated dial-up IPsec tunnels

Option to set up traffic shaping profile by defining the percentage of interface bandwidth for each classified traffic and then bind to interfaces

Traffic Shaping Policies: Assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.

DSCP support:
- DSCP match in SD-WAN rules
- DSCP tagging of forwarded packets based on identified applications

Inline and out-of-path WAN optimization topology, peer to peer, and remote client support

Transparent Mode option: keeps the original source address of the packets, so that servers appear to receive traffic directly from clients.

WAN optimization techniques: Protocol optimization and byte caching

WAN optimization protocols supported: CIFS, FTP, HTTP(S), MAPI, TCP

Secure Tunneling option: Use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel

Tunnel sharing option: Multiple WAN optimization sessions share the same tunnel

Web caching: Object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Supports caching of HTTP 1.0 and HTTP 1.1 web sites

SSL Offloading with Web caching:
- Full mode: performs both decryption and encryption of the HTTPS traffic
- Half mode: performs only one encryption or decryption action

Option to exempt certain web sites from web caching with URL patterns

Support advanced web caching configurations and options:
- Always revalidate, Max cache object zie, negative response duration, fresh factor, Max/Min/Default TTL, proxy FQDN, Max HTTP request/message length, ignore options, cache expired objects, revalidated
  prama-no-cache

WAN optimization and web cache monitor

### EXPLICIT PROXY

Explicit web & FTP proxy: FTP, HTTP, and HTTPS proxying on one or more interfaces

Proxy auto-config (PAC): Provide automatic proxy configurations for explicit web proxy users

Proxy chaining: Web proxy forwarding to redirect web proxy sessions to other proxy servers

Web proxy forwarding server monitoring and health checking

IP reflect capability

Load balancing for forward proxy and proxy chaining

Explicit web proxy authentication: IP-based authentication and per session authentication

Transparent web proxy

SAML user authentication support

### IPV6

IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunneling, firewall and UTM for IPv6 traffic, NAT46, NAT64, IPv6 IPsec VPN

IPv6 SD-WAN Support: Ping6 link monitor, IPv6 source and destination objects

Fully support wireless client IPv6 traffic on both from tunnel and local-bridge mode SSID

### HIGH AVAILABILITY

High availability modes: Active-passive, active-active, virtual clusters, VRRP, FG-5000 series clustering

Redundant heartbeat interfaces

HA reserved management interface

Failover:
- Port, local and remote link monitoring
- Stateful failover
- Subsecond failover
- Failure detection notification
- When memory utilization exceeds the threshold for a specific amount of time

Deployment Options:
- HA with link aggregation
- Full mesh HA
- Geographically dispersed HA

Standalone session synchronization
- Support security inspection over asymmetric traffic, TCP, UDP, ICMP sessions as well as NAT sessions
- Configuration synchronization between similar FortiGates.

### ESSENTIAL NETWORK SERVICES

Built-in DHCP, NTP, DNS Server, and DNS proxy

FortiGuard NTP, DDNS, and DNS service

## Platform Support

### PHYSICAL APPLIANCE (+SPU)

Integrates with SPU components for traffic processing acceleration.

### VIRTUAL SYSTEMS

Virtual Systems (FortiOS Virtual Domains) divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.

Configurable virtual systems resource limiting and management such as maximum/guaranteed 'active sessions' and log disk quota

VDOM operating modes: NAT/Route or Transparent

Spilt-Task VDOM: Separate VDOMs for management and data paths

Virtual routing and forwarding (VRF):
- Route leaking capabilities between locally defined VRFs (VRF-lite)
- Supports static, OSPF, IBGP and EBGP

### PRIVATE CLOUD

Support for popular hypervisor platform, including VMware vSphere, Citrix and open source Xen, KVM, Nutanix and MS hyper-V

### PUBLIC CLOUD

Amazon AWS: auto-scaling, native HA with ELB, crossing AZ HA, Guard Duty integration; IAM, topology and CVE integration

Microsoft Azure: auto-scaling, native HA (Azure LB), Azure Security Center integration
Azure Stack: Active-Passive HA

Google Cloud Platform: auto-scaling, HA between zones

Oracle Cloud Infrastructure: Native and para-virtualized modes, IAM integration

AliCloud: autoscaling, native HA

## Others

### OTHERS

Web Application Firewall:
- Signature based, URL constraints and HTTP method policy

Server load balancing: traffic can be distributed across multiple backend servers:
- Based on multiple methods including static (failover), round robin, weighted or based on round trip time, number of connections.
- Supports HTTP, HTTPS, IMAPS, POP3S, SMTPS, SSL or generic TCP/UDP or IP protocols.
- Session persistence is supported based on the SSL session ID or based on an injected HTTP cookie.

Credential Stuffing Defense: scans user names and passwords in submission traffic to external URLs against the sensitive corporate network credentials stored in the corporate domain controller

DLP message filter:
- Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Actions: Log only, block, quarantine user/IP/Interface
- Predefined filter: Credit card number, Social Security ID

DLP file filter:
- Protocols Supported: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Filter options: size, file type, watermark, content, if encrypted

DLP watermarking: Allows filter files that pass through the FortiGate unit and contain a corporate identifier
(a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark. Support Windows and Linux free watermarking tools

DLP fingerprinting: Generates a checksum fingerprint from intercepted files and compares it to those in the fingerprint database

DLP archiving: Records full content in email, FTP, IM, NNTP, and web traffic

PRP (Parallel Redundancy Protocol) support: preserves the PRP RCT (redundancy control trailer) while the packet is processed by the FortiOS.

NOTE: Feature set based on FortiOS V6.4, some features may not apply to all models. For availability, please refer to Software feature Matrix on docs.fortinet.com

FORTINET®

www.fortinet.com