FortiOS™ 5.6

Fortinet's Network Operating System

Control all the security and networking capabilities in all your Fortinet Security Fabric elements with one intuitive operating system. Improve your protection and visibility while reducing operating expenses and saving time with a truly consolidated next-generation enterprise firewall solution. FortiOS enables the Fortinet Security Fabric vision for enhanced protection from IoT to Cloud.

Security Fabric Integration

Deep visibility and control throughout the Security Fabric reduce the attack surface from IoT to Cloud.

Accelerated Performance

Accelerated cloud-scale and security processor-based appliances enable maximum threat protection without affecting performance, even when logging is turned on.

Efficient Operations

Security Fabric Audit with recommendations and automated actions, local and global threat intelligence sharing, and single pane of glass with NOC views help better manage your network.

Seamlessly integrates with Fortinet centralized management solution and offers robust APIs.

What's New — Highlights

- Security Fabric enhancements
- Security Fabric Audit
- Improved Dashboard
- Transparent web proxy
- NGFW policy mode
- Controlled failover between wireless controllers
- Multiple PSK for WPA Personal
- VXLAN support
- FortiView Endpoint Vulnerability chart
- FortiClient Profile updates
- CEF log support
- Adding Internet services to firewall policies
- Source and destination NAT in a single firewall policy
- NP6 Host Protection Engine

OVERVIEW

Introducing FortiOS 5.6

The transition to an evolving digital business model is one of the most challenging aspects of security today for an enterprise. As significant trends in computing and networking continue to drive changes across critical business infrastructures, architectures, and practices, organizations are looking for innovative network security solutions to help them embrace that evolution. The Fortinet Security Fabric, empowered by FortiOS 5.6, is an intelligent framework designed for scalable, interconnected security combined with high awareness, actionable threat intelligence, and open API standards for maximum flexibility and integration to protect even the most demanding enterprise environments. Fortinet's security technologies have earned the most independent certifications for security effectiveness and performance in the industry. The Fortinet Security Fabric closes gaps left by legacy point products and platforms by providing the broad, powerful, and automated protection that today's organizations require across their physical and virtual environments, from endpoint to the cloud.

FortiOS 5.6 Anatomy

Control all the security and networking capabilities in all your FortiGates across your entire network with one intuitive operating system. FortiOS offers an extensive feature set that allows organizations of all sizes to deploy the security gateway setup that best suits their environments. As requirements evolve, you can modify them with minimal disruptions and cost.

<table>
<tr><td>Configuration</td><td>Log & Report</td><td>Diagnostics</td><td>Monitoring</td><td>Operation</td><td>Systems Integration</td><td>Central Mgmt. and Provisioning</td><td>Cloud & SDN Integration</td></tr>
<tr><td colspan="4"></td><td></td><td colspan="3">Visibility</td></tr>
<tr><td>Policy Objects</td><td>Device Identification</td><td>SSL inspection</td><td>Actions</td><td>Policy and Control</td><td colspan="2">AAA</td><td>Compliance</td></tr>
<tr><td>Anti-Malware</td><td>IPS & DoS</td><td>Application Control</td><td>Web Filtering</td><td rowspan="2">Security</td><td colspan="3" rowspan="2">Advanced Threat Protection (ATP)</td></tr>
<tr><td>Firewall</td><td>VPN</td><td>DLP</td><td>Email Filtering</td></tr>
<tr><td>SD WAN</td><td>Explicit Proxy</td><td>IPv6</td><td>High Availability</td><td rowspan="2">Networking</td><td>Wireless Controller</td><td>Switch Controller</td><td>WAN Interface Manager</td></tr>
<tr><td>Routing/NAT</td><td>L2/Switching</td><td>Offline Inspection</td><td>Essential Network Services</td></tr>
<tr><td>Physical Appliance (+SPU)</td><td>Virtual System</td><td>Hypervisor</td><td>Cloud</td><td>Platform Support</td><td colspan="3">Security Fabric</td></tr>
</table>

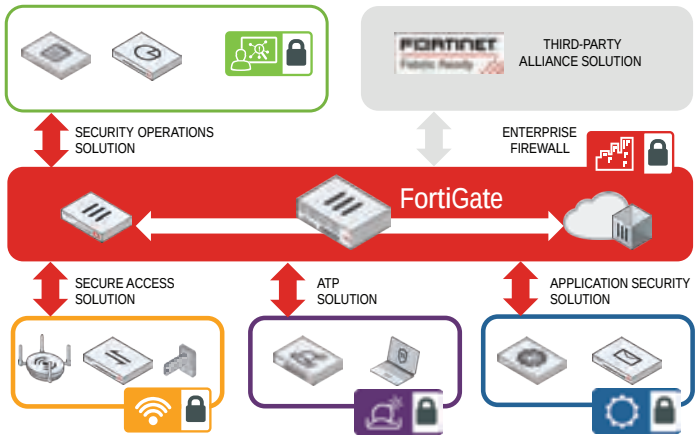
HIGHLIGHTS

Security Fabric

FortiGate Integration

The Security Fabric allows security to dynamically expand and adapt as more and more workloads and data are added, and at the same time, seamlessly follow and protect data, users, and applications as they move back and forth between IoT, smart devices, and cloud environments throughout the network.

A FortiGate firewall may be deployed at the heart of the Security Fabric, expanding its security reach via visibility and control, by tightly integrating with other FortiGates and Fortinet products, plus Fabric-Ready solutions.



FortiView

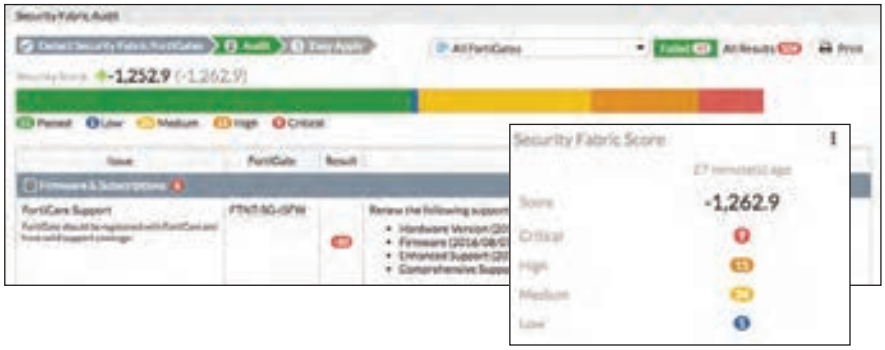
Visibility

FortiView, in FortiOS 5.6, provides you with 360° visibility into your network traffic. With a single click you can view traffic by source, destination, application, threat, interface, device, policy, and country. Graphical visualizations, such as country and topology maps and volume-based bubble charts are available in addition to comprehensive table views. These allow you to identify issues quickly and intuitively.

HIGHLIGHTS

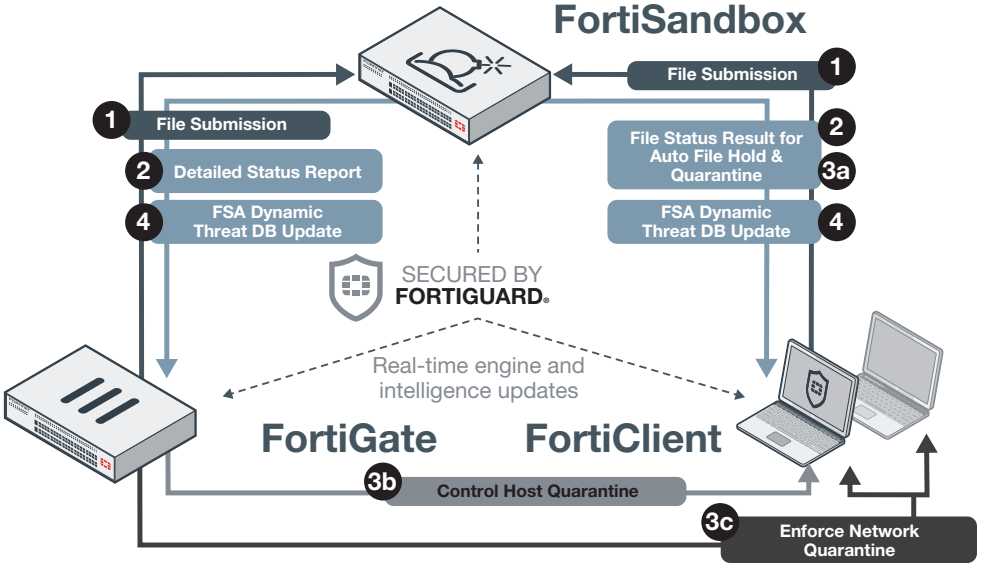
Compliance

The Security Fabric Audit is a feature that allows you to analyze your Security Fabric deployment to identify potential vulnerabilities and highlight best practices that could be used to improve your network's overall security and performance. Also, by checking your Security Fabric Score, which is determined based on how many checks your network passes/fails during the Audit, you can be confident that your network is getting more secure over time.



Advanced Threat Protection

Fortinet offers the most integrated and automated Advanced Threat Protection (ATP) solution available today through an ATP framework that includes FortiGate, FortiSandbox, FortiMail, FortiClient, and FortiWeb. These products easily work together to provide closed loop protection across all of the most common attack vectors. All products in the ATP framework are NSS Labs Recommended for both security effectiveness and performance value.



Query

1. File submission for analysis
2. Respective analysis results are returned

Remediation

- 3a Auto File Quarantine on host with option to hold file until result
- 3b Manual Host Quarantine by administrator
- 3c Manual Source IP Quarantine using firewall

Protection

4. Proactive dynamic Threat DB update to gateway and host

FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
System Integration	▪ Standard-based monitoring output – SNMP Netflow/Sflow ▪ Syslog support to external (third-party) SIEM and logging system ▪ Technology alliance with specialized vendors in heterogeneous environment ▪ Native Integration with Fortinet Products — FortiMail, FortiCache, and FortiWeb	▪ Detailed logs and SNMP output provide more insights so that organizations can accurately and quickly identify and resolve incidents or problems. ▪ Ability to reuse organization's existing systems lowers TCO and streamlines processes.

HIGHLIGHTS

FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
Central Management and Provisioning	▪ Fortinet/third-party automation and portal services support via APIs and CLI scripts ▪ Rapid deployment features including cloud-based provisioning solutions ▪ Developer community platform and professional service options for complex integrations	▪ Comprehensive APIs and CLI commands offer feature-rich service enablement. ▪ Comprehensive rapid deployment options save time and costs. ▪ Fortinet Developer Network (FNDN) empowers large service providers and enterprises with shared implementation/customization/ integration knowledge.
Cloud and SDN Integration	▪ Integration with Openstack, VMware NSX, and Cisco ACI infrastructure	▪ Robust and comprehensive SDN integration capabilities allow organizations to implement cloud solutions securely without compromising agility.
Visibility	▪ Drill-down and topology viewers that illustrate real-time and historical threat status and network usage with comprehensive contextual information ▪ **NEW:** Aggregated data views with remote control of downstream FortiGates ▪ **NEW:** Endpoint vulnerability views that present ranked vulnerable clients with details	▪ One-click remediation against listed sources/destinations offers accurate and quick protection against threats and abuses. ▪ Unique threat score system correlates weighted threats with particular users to prioritize investigations. ▪ Fabric-wide views expand visibility beyond a single security entity, including endpoint vulnerabilities.
Authentication Authorization and Accounting (AAA)	▪ Interface with FortiAuthenticator and a wide variety of external identity management systems to facilitate user authentication processes. ▪ Wide-ranging single sign-on identity acquisition methods, including Windows AD, terminal servers, access portals, and mail services ▪ Built-in token server that manages both physical and mobile tokens for use with various FortiOS authentication requirements such as VPN access and FortiGate administration.	▪ 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. ▪ Easily implement two-factor authentication for user and administrator access at little cost.
Compliance	▪ Periodic system configuration check using a pre-defined PCI-compliance checklist ▪ Endpoint enforcement: posture checking profile assignment based on device/user groups ▪ NEW: Fabric-wide FortiGate security configuration and client vulnerability status audits	▪ Automates compliance auditing which frees up administration resources ▪ Simplified mobile user security enforcement by easily distributing and updating clients' security profiles that are consistent with gateway protection ▪ Quickly verify the status and health of your connected devices within the Fabric and identify any gaps that can potentially leave you at greater risk
Advance Threat Protection (ATP)	▪ Flow- and proxy-based AV options for choice between protection and performance ▪ Local file quarantine (for models with storage) ▪ Anti-bot capability using IP reputation DB terminates botnet communication to C&C servers ▪ Receive dynamic remediation (malicious file checksum and URLs) DB updates and detail analysis reports from external Fortinet file analysis solution (FortiSandbox)	▪ Supported by proven and industry-validated AV research services ▪ 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
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 ▪ Enterprise-class wireless management functionality, including rogue AP protection, wireless security, monitoring, and reporting ▪ **NEW:** 802.3az support on WAVE2 WiFi APs ▪ **NEW:** Manage distirbuted cloud-based FortiAPs	▪ The wireless controller integrated into the FortiGate console provides 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 ▪ **NEW:** Improved GUI configuration support	▪ Expands security to access level to stop threats and protect terminals from one another
WAN Interface Manager	▪ Supports the use of 3G/4G modems via USB port or FortiExtender	▪ Allows organizations to use or add 3G/4G connectivity for WAN connections while maintaining access control and defining usage for those links

HIGHLIGHTS

Operation

FortiOS provides a broad set of operation tools that make identification and response to security and network issues effective. Security operations is further optimized with automations which contribute to faster and more accurate problem resolutions.

FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
Configuration	▪ Wide variety of configuration tools — Client software, Web UI, and CLI ▪ Ease of use with intuitive, state-of-the-art GUI and wizards ▪ One-click access and actions between log viewers, FortiView, policy tables, and more ▪ Intelligent object panel for policy setups and edits	▪ Unique FortiExplorer configuration tool allows administrators to quickly access configurations, including via mobile phones and tablets. ▪ VPN wizards facilitate easy setup, including to popular mobile clients and other vendors' VPN gateways. ▪ Useful one-click access and actions bring administrators to next steps quickly and accurately to swiftly mitigate threats or resolve problems.
Log & Report	▪ Detailed logs and out-of-the-box reports that are essential for compliance, audits, and diagnostic purposes ▪ **NEW:** Real-time logging to FortiAnalyzer and FortiCloud ▪ **NEW:** Common Event Format (CEF) support ▪ **NEW:** Logging consolidation within Security Fabric	▪ Includes deep contextual information, including source device details and strong audit trail ▪ GUI Report Editor offering highly customizable reports ▪ 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 ▪ Hardware testing suite on CLI ▪ Policy and routing GUI tracer	▪ Comprehensive diagnostic tools help organizations quickly remediate problems and investigate abnormal situations.
Monitoring	▪ Real-time monitors ▪ **NEW:** NOC Dashboard	▪ 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 and Control

FortiGate provides a valuable policy enforcement point in your network where you can control your network traffic and apply security technologies. With FortiOS, you can set consolidated policies that include granular security controls. Every security service is managed through a similar paradigm of control and can be easily plugged into a consolidated policy. Intuitive drag-and-drop controls allow you to easily create policies and one-click navigation shortcuts allow you to more quickly quarantine end points or make policy edits.

FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
Policy Objects	▪ GeoIP and FQDN defined address objects to intelligently track dynamic IP/IP ranges ▪ 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.	▪ Comprehensive range of object types that facilitate today's dynamic and granular network requirements
Device Identification	▪ Identification and control of network access for different types of devices present on the network ▪ **NEW:** Improved device identification and management	▪ Empowers organizations to add critical security to today's BYOD environment by identifying and controlling personal devices
SSL Inspection	▪ Effectively examine SSL-encrypted traffic with various security controls, such as AV and DLP ▪ High-performance SSL inspection with content processors ▪ Reputable sites database for exemptions	▪ Identify and block threats hidden within encrypted traffic without significantly impacting performance.
Actions	▪ Implements security policies that use a combination of source objects, IPs, users, and/or devices. ▪ Highly customizable notifications are sent when user activities are not allowed. ▪ Automatically or manually quarantine users/attackers. ▪ Directs registered FortiClient to host quarantine.	▪ Flexible policy setup using additional identified elements and active user notifications assist organizations in implementing effective network security, while robust quarantining features helps to mitigate threats.

HIGHLIGHTS

Security

FortiGuard Labs provides the industry-leading security services and threat intelligence delivered through Fortinet solutions. FortiOS manages the broad range of FortiGuard services available for the FortiGate platform, including application control, intrusion prevention, web filtering, antivirus, advanced threat protection, SSL inspection, and mobile security. Services can be licensed a la carte or in a cost-effective bundle for maximum flexibility of deployment.

Industry-leading security effectiveness

Fortinet solutions are consistently validated for industry-leading security effectiveness in industry tests by NSS Labs for IPS and application control, by Virus Bulletin in the VB100 comparative anti-malware industry tests, and by AV Comparatives.

- Recommended Next Generation Firewall with near perfect, 99.6% security effectiveness rating. (2016 NSS Labs NGFW Test of FortiGate 3200D)
- Recommended Breach Detection Systems with 99%+ overall detection. (2016 NSS Breach Detection Systems Test of FortiGate 500D with FortiSandbox Cloud)
- Recommended Data Center Intrusion Prevention Systems with 99.9% exploit block rate, highest in test. (2016 NSS Data Center Intrusion Prevention Test with FortiGate 3000D)
- Highest antivirus security effectiveness of any vendor offering a next generation firewall and 2nd highest security effectiveness of all business antivirus solutions tested. (Oct 2014–April 2015 Virus Bulletin Reactive and Proactive Test average results)
- ICSA Certified network firewalls, network IPS, IPsec, SSL-TLS VPN, antivirus.

FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
Anti-Malware	▪ Flow- and proxy-based AV options for choice between protection and performance. ▪ Anti-bot capability using IP reputation DB terminates botnet communication to C&C servers. ▪ Receive dynamic remediation (malicious file checksum and URLs) DB updates and detail analysis reports from external Fortinet file analysis solution (FortiSandbox).	▪ Supported by proven and industry-validated AV research services. ▪ 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.
IPS and DoS	▪ Regular and rate-based signatures, supported by zero-day threat protection and research for effective. IPS implementation. ▪ Integrated DoS protection defends against abnormal traffic behaviors. ▪ CVE reference for IPS signatures.	▪ Proven quality protection with "NSS Recommended" award for superior coverage and cost/performance. ▪ Adapts to enterprise needs with full IPS features and NGIPS capabilities, such as contextual visibility. ▪ Supports various network deployment requirements, such as sniffer mode, and compatible with active-bypass FortiBridge or built-in bypass ports for selected model.
Application Control	▪ Detects and acts against traffic based on applications while providing visibility on network usage. ▪ 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. ▪ Applies deeper application inspections for better control and visibility as more enterprises rely on public cloud services.
Web Filtering	▪ Enterprise-class URL filtering solution that includes quotas, user overrides, transparent safe search, and search engine keyword logging. ▪ Superior coverage with URL ratings of over 70 languages and identifies redirected (cached and translated) sites.	▪ Multi-layered anti-proxy avoidance capabilities with integrated application control and IPS allow organizations to implement air-tight web usage controls.

HIGHLIGHTS

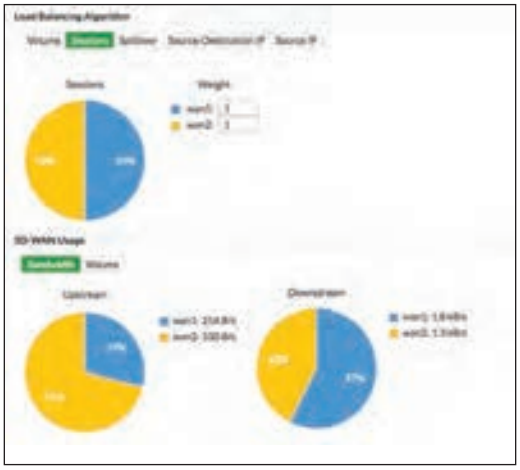
FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
Firewall	▪ High-performance firewall with SPU-powered appliance ▪ Easy-to-use policy management with unique Section or Global View options ▪ **NEW:** NGFW Policy-Based Mode	▪ Industry's top firewall appliance with superior cost-performance ratio
VPN	▪ Comprehensive enterprise-class features for various types of VPN setups ▪ SSL and IPsec VPN wizards	▪ 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.
DLP	▪ Monitor network traffic and stop sensitive information from leaving the network by matching against file format and content definitions. ▪ The FortiExplorer Watermark Tool allows organizers to apply document marking for DLP.	▪ Prevent sensitive information from leaving the network, easily and cost-effectively.
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

Networking

With FortiOS you can manage your networking and security in one consistent native OS on the FortiGate. FortiOS delivers a wide range of networking capabilities, including extensive routing, NAT, switching, Wi-Fi, WAN, load balancing, and high availability, making the FortiGate a popular choice for organizations wanting to consolidate their networking and security functions.

SD WAN

Fortinet's Distributed Enterprise Firewall enables software-defined WAN (SD-WAN). It essentially links network and security paths across the world through the Internet or private WAN links, making it a truly borderless infrastructure for the enterprise. In addition, it provides application visibility and intelligent load balancing. Consolidation and control of network security features in a centralized environment simplifies administration.



FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
Routing / NAT	▪ Comprehensive routing protocols and NAT support ▪ 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 ▪ Support SPAN ports and port aggregation with multiple interfaces. ▪ Implement admission control modes on interfaces such as 802.1x or captive portal. ▪ Comprehensive WiFi and WAN interface configuration options ▪ **NEW:** VXLAN 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.	▪ Offline mode provides flexibility when deploying into existing critical networks where in-line security solution is not yet appropriate.

HIGHLIGHTS

FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
SD WAN	▪ Comprehensive WAN Link LB algorithm, link status, plus quality checks, and policy routing support ▪ Direct traffic among WAN links based on applications and users/ user groups ▪ Manage the level of service and preference given to the various types and sources of traffic using traffic policing, traffic shaping, and queuing. ▪ Peer-to-peer and remote user WAN optimization for protocol optimization and byte caching technologies ▪ Web cached storage of remote files and web pages on local devices for easy local access to commonly accessed objects	▪ Robust multi-link feature aids organizations in SD-WAN implementation. ▪ QoS capabilities adjust allocation of bandwidth to different traffic types, improving the performance and stability of latency-sensitive or bandwidth-intensive network applications. ▪ Built-in WAN optimization capabilities reduce network overhead, resulting in more efficient use of bandwidth and better application performance, without the need for costly WAN link upgrades.
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.
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.
Explicit Proxy	▪ Explicit HTTP and HTTPS, FTP over HTTP, or SOCKS proxying of IPv4 and IPV6 traffic on one or more interfaces ▪ **NEW:** Transparent web proxy	▪ Integrated, enterprise-class explicit web proxy provides HTTP and HTTPS proxying with the added benefits of UTM security and user identity.
Essential Network Services	▪ A wealth of networking services such as DHCP, DNS server, NTP server etc.	▪ Built-in, out-of-the-box capabilities let organizations quickly provide necessary network services to internal terminals or to integrate with other network devices.

Platform Support

Performance

The FortiGate appliances deliver up to 5 times the next generation firewall performance and 10 times the firewall performance of equivalently priced platforms from other vendors. The high performance levels in the FortiGate are based on a Parallel Path Processing architecture in FortiOS that leverages performance, optimized security engines, and custom developed network and content processors. Thus, FortiGate achieved the best cost per Mbps performance value results.

Ultimate deployment flexibility

Protect your entire network inside and out through a policy-driven network segmentation strategy using the Fortinet solution. It is easy to deploy segment optimized firewalls, leveraging the wide range of FortiGate platforms and the flexibility of FortiOS to protect internal network segments, the network perimeter, distributed locations, public and private clouds, and the data center — making sure you have the right mix of capabilities and performance for each deployment mode.

FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
Physical Appliance (+SPU)	▪ Integration with proprietary hardware architecture that includes acceleration components (SPU) and multicore processors.	▪ Superior software and hardware integration ensures most optimal use of hardware components, yielding best cost/performance for customers.
Virtual Systems	▪ Virtual Domains (VDOMs): Virtualized FOS components to multiple logical systems on a single virtual or physical appliance. ▪ Proxy and Flow-based VDOM options to simplify security profile settings	▪ Offers MSSPs and large organizations the ability to run separate instances of FOS for multi-tenant environment or to consolidate various security gateways for lower TCO.
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) and Microsoft Azure.	▪ Consistent management and features between on-premises and cloud platforms reduces management cost and simplifies deployments.

SPECIFICATIONS

Security Fabric

SYSTEM INTEGRATION

SNMP System Monitoring:
- SNMP v1and 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 virus detected

Traffic Monitoring:
- sFlow version 5 and Netflow V9.0

External Logging:
- Syslog
- Reliable syslog (RAW Profile) based on RFC 3195
- WebTrends WELF compatible

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 FortiMail, FortiCache, and FortiWeb

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

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 with Openstack, VMWare NSX, and Cisco ACI infrastructure

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', 'interfaces', 'applications', 'threats' etc.
- Phyiscal and logical topology views
- Threat and VPN map
- Data views options: Table, bubble chart, or world map if applicable
- File analysis/sandbox result view (FortiSandbox integration required)
- Endpoint Vulnerbility view (FortiClient integration required)
- Accelerated session indication on 'All sessions' FortiView Console
- WHOIS Lookup for Public IP addresses within FortiView and log tables

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

AUTHENTICATION AUTHORIZATION AND ACCOUNTING (AAA)

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

Single-sign-on: Intergation 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

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

COMPLIANCE

Run a series of system configuration compliance check and log results periodically or on-demand

Security Fabric Audit: Audit FortiGate within the fabric, provide results and recommendation, then allow users to easily apply remediations for some items.

Manages network devices compliance via client software:
- Posture checking: Enforce client software installation and desired settings accordingly to device type/group and/or user/usergroup and/or locations (IPs)
- Quarantine clients if hit vulnerability level threshold

ADVANCE THREAT PROTECTION (ATP)

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)

WIRELESS CONTROLLER

Manages and provisions settings for local and remote Thin Access points or switches (selected models)

Set up access and authentication methods for SSIDs and VLANs, supports integrated or external captive portal, 802.1x, preshared keys

Multiple PSK for WPA Personal

WiFi Security: Rogue AP suppression, wireless IDS

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

Controlled failover between wireless controllers

SWITCH CONTROLLER

Extends access control and security to wired devices by managing Fortinet switches (FortiSwitch) via CAPWAP-like communication.

Ability to configure switch port features such as PoE, VLAN assignment

WAN INTERFACE MANAGER

Support USB 3G/4G Wireless WAN modems

Operation

CONFIGURATION

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

FortiExplorer:
- Management client for Windows and IOS platforms
- Ease-of-use by using USB connectivity

Feature Store: Toggle GUI component displays

GUI configuration:
- 'One-Click' access that transfer administrators to next step panels quickly
- 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 logging using TCP option (RFC 3195)

Encrypted logging & log Integrity with FortiAnalyzer

Scheduled batch log uploading or real-time logging

Detailed traffic logs:fForwarded, 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

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

Dashboard: customized widgets and layout

Policy and Control

POLICY OBJECTS

Policy objects: predefined, customs, object grouping, tagging, and coloring

Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN

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-balacing configurations.

SPECIFICATIONS

Security

DEVICE IDENTIFICATION

Device Identification: Device and OS fingerprinting, automatic classification, inventory management

Support for MAC Authentication enforcement and bypass

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

ACTIONS

User notifications: customizable replacement message for block sites and attachments

Web Browser top banner insert (Fortinet Bar): shows application control violations, Endpoint control enforcement, web browsing quota etc

User quarantine:
- Manually assigned with perpetual or customizable duration
- Automatically when triggered by violated IPS signature

ANTI-MALWARE

Botnet server IP blocking with global IP reputation database

Antivirus database type selection (on selected models)

Flow-based or proxy-based AV option:
- Support for popular web, mail, and FTP protocols
- Scan encrypted traffic with SSL inspection

Option to treat Windows executables in email attachments as viruses

File quarantine (local storage required)

IPS AND DOS

IPS engine: 7,000+ 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, attackers IP and Victim IP, incoming interface) 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

Active bypass with bypass Interfaces (selected models) and FortiBridge

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

Supports detection for traffic using HTTP/2 protocol and able to block QUIC traffic so taht 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

SSH Inspection

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

WEB 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

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

Restrict access to Google Corporate Accounts only

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

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: Section or global policy management view

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

VPN

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

SSL VPN realm support: Allows 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

Virtual desktop option to isolates the SSL VPN session from the client computer's desktop environment

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
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
- 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
- Dead peer detection
- Replay detection
- Autokey keep-alive for Phase 2 SA

IPsec Configuration Wizard for termination with popular third-party devices

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

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

SPECIFICATIONS

DLP

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

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 compare it to those in the fingerprint database.

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

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

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: An interface can be dedicated to its exclusive use 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 and Source IP

Usage-based WAN link assignment: Routes new sessions to interfaces that have not reached a configured bandwidth limit

WAN link checks:
- Ping or HTTP probes
- Monitoring Criterias including latency, jitter, and packet loss
- Configurable warning, alert, and failure thresholds

Route Overrides Rules which direct specific traffic based on source/user/usergroups and cloud applications/ policy address objects.

Traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), and Differentiated Services (DiffServ) support

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

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 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: Only performs 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

IPV6

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

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

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

Standalone session synchronization

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

VDOM security inspection modes: Proxy or Flow-based

SPECIFICATIONS

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

CLOUD
Support for public cloud services: Amazon AWS and Microsoft Azure

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.

NOTE: Feature set based on FortiOS V5.4.GA, some features may not apply to all models. For availability, please refer to Software feature Matrix on docs.fortinet.com

REFERENCES

RESOURCE	URL
The FortiOS Handbook — The Complete Guide	http://docs.fortinet.com/fgt.html
Fortinet Knowledge Base	http://kb.fortinet.com/
Product Data Sheets & Matrix	http://www.fortinet.com/resource_center/datasheets.html

GLOBAL HEADQUARTERS
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

FST-PROD-DS-FOS

FOS-DAT-R4-201705