FORTINET

5.4

FortiOS™ 5.4

One Operating System to Protect Your Entire Network

FortiOS 5.4 is an intuitive operative system that can manage all your FortiGate platforms, including the capabilities and services. FortiOS 5.4 provides industry-leading protection, superior visibility and control, and extensive networking capabilities at very high throughput speeds.

More Prevention, Faster Mitigation

No matter how large or small your organization, you are at risk: 80% of organizations reported two or more data breaches between 2014 and 2015. Protect your organization better with a full range of industry-leading next generation security services from FortiGuard Labs, plus automated advanced threat protection through integration with the Fortinet Advanced Threat Protection framework. FortiGate-based solutions are certified and validated by NSS Labs, ICSA, Virus Bulletin, and AV Comparatives for superior security effectiveness.

Faster Resolution, More Visibility

Satisfy the need to keep current on your network environment and usage patterns, while quickly identifying any active security threats with 360° visibility provided by FortiOS. React quickly to new information provided through intuitive one-click shortcuts within FortiOS in order to stay relevant with today's persistent and ever-changing threat landscape. FortiOS seamlessly integrates with centralized management from Fortinet and offers robust SDN and SIEM APIs for extended centralized management and orchestration.

Faster Infrastructure

FortiOS leverages a performance optimized security engine architecture and custom FortiASICs in the FortiGate platform to deliver faster throughput performance — often 5x or 10x faster than equivalent platforms from other vendors.

Highlights

- A consolidated platform with one OS for all security and networking services, for all FortiGate platforms

- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance

- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings

- Swiftly detect, contain, and block advanced attacks automatically with an integrated advanced threat protection framework

- Solve your networking needs with extensive routing, switching, WiFi, LAN, and WAN capabilities

- Activate all the ASIC-boosted capabilities you need on the fastest firewall platform available

FortiCare Worldwide 24x7 Support
support.fortinet.com

FortiGuard Security Services
www.fortiguard.com

FEATURES

Visibility and Control

Organizations need extensive visibility into network traffic based on identification of threats, applications, users, and specific activity characteristics, combined with the ability to efficiently set granular policy controls specific to different network segments in a way that maintains consistency across the entire organization.
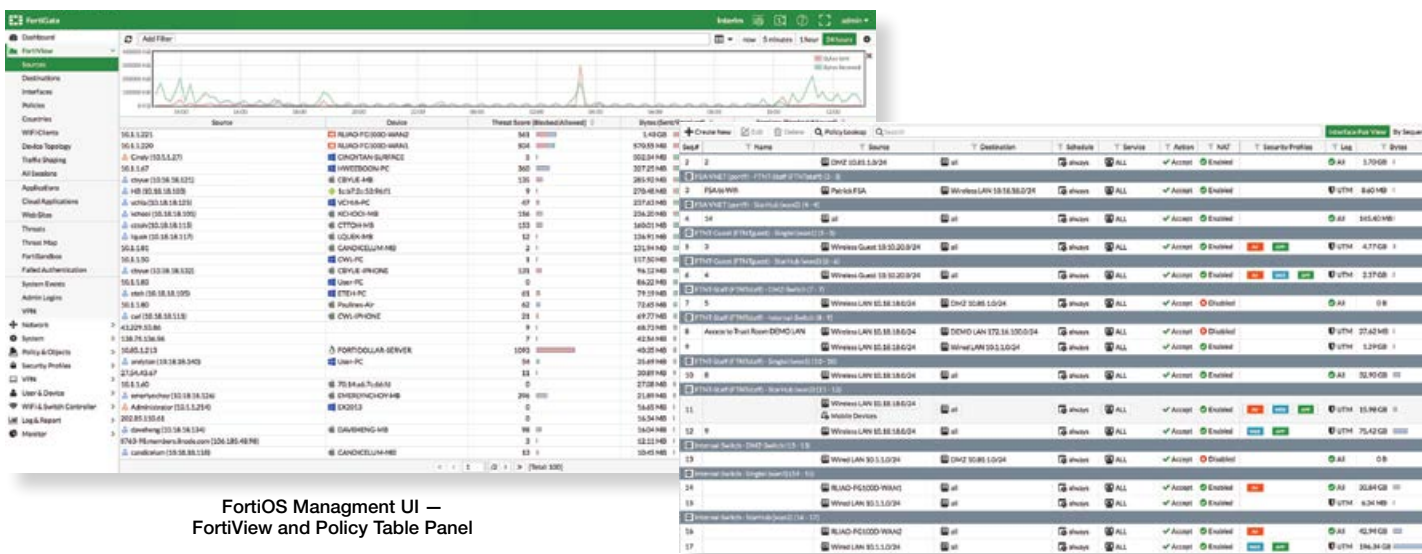
FortiOS Managment UI —
FortiView and Policy Table Panel

Visibility

The redesigned and simplified modern user interface in FortiOS 5.4 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, allow you to identify issues quickly and intuitively.

Control

FortiGate provides a valuable policy enforcement point in your network where you can control your network traffic and apply security technologies. With FortiOS 5.4, 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
System Integration	▪ Standard-based monitoring output – SNMP, Netflow/Sflow ▪ Syslog support to external (3rd party) SIEM and logging system ▪ Technology alliance with specialized vendors in heterogeneous environment ▪ **NEW:** 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 existing systems lowers TCO and streamlines processes.
Central Management and Provisioning	▪ Fortinet/3rd 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 that results in cost and time savings. ▪ FNDN developer support network option empowers large service providers and enterprises with shared implementation/customization/integration knowledge.

FEATURES

| Feature	Highlights	The Fortinet Advantage
Cloud and SDN Integration	• **NEW:** 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.
Configuration	• Wide variety of configuration tools — Client software, Web UI, and CLI. • Ease-of-use with intuitive, state-of-the-art GUI and wizards. • **NEW:** One-click access and actions between log viewers, FortiView, policy tables, and more. • **NEW:** Intelligent object panel for policy setups and edits.	• Unique FortiExplorer configuration tool allows administrators to quickly access configurations, including via mobile phone & 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 resolves problems.
Visibility	• Drill-down viewers that illustrate real-time and historical threat status and network usage with comprehensive contextual information. • **NEW:** Visualization options; bubble chart and country map. • **NEW:** Additional Viewers, including Threat Map and Device Topology.	• One-click remediation against listed source(s)/destination(s) offers accurate yet quick protection against threats and abuses. • Unique threat score system correlates weighted threats with particular user(s) to prioritize investigations.
Log & Report	• Detailed logs and out-of-the-box reports that are essential for compliance, audits, and diagnostics purposes.	• Deep contextual information, including source device details and strong audit trail. • Unique security event associations per session. • GUI Report Editor offering highly customizable reports.
Diagnostics	• Diagnostic CLI commands, session tracer, and packet capture for troubleshooting hardware, system, and network issues. • **NEW:** Hardware testing suite on CLI. • **NEW:** Policy and routing GUI tracer.	• Comprehensive diagnostic tools help organizations quickly remediate problems and investigate for abnormal situations.
Virtual Systems	• Virtual Domains (VDOMs): Virtualized FOS components to multiple logical systems on a single virtual or physical appliance. • **NEW:** Proxy and Flow-based VDOMs options to simplify security profile settings. • **NEW:** Stackable VDOM Licenses.	• 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.
Policy Objects	• GeoIP and FQDN defined address objects to intelligently tracks dynamic IP/IP ranges. • **NEW:** Internet Service DB: Dynamically updated DB that provides a list of popular cloud applications with their vital information that can be used for routing and link load-balacing configurations.	• Comprehensive range of object types that facilitate today's dynamic and granular network requirements.
User Authentication	• 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. • **NEW:** Single-Sign-On Integration with Exchange Server. • **NEW:** Radius service integration improvements with third-party wireless solutions.	• FortiOS integrates with a wide variety of AAA services to facilitate user admission control from various entry points, allowing users with a simplified experience while implementing greater security.
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 for various security implementation, such as AV and DLP. • High performance SSL inspection with Content Processors. • **NEW:** SSl MITM Mirroring. • **NEW:** 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 when user activities are not allowed. • Automatic or manual quarantine of users/attackers. • **NEW:** Direct 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.

F⊕RTINET

FEATURES

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 96.3% NGFW security effectiveness rating (2014 NSS Labs NGFW Test of FortiGate 3600C)
- 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)
- 2nd highest security effectiveness of all anti-phishing solutions tested (August 2015, AV Comparatives Anti-Phishing Test)
- 99.6% file detection rates (March 2015, AV Comparatives File Detection Test)
- 98.7% antivirus effectiveness (July 2015, AV Comparatives Real World Protection Test)
- ICSA Certified network firewalls, network IPS, IPsec, SSL-TLS VPN, antivirus
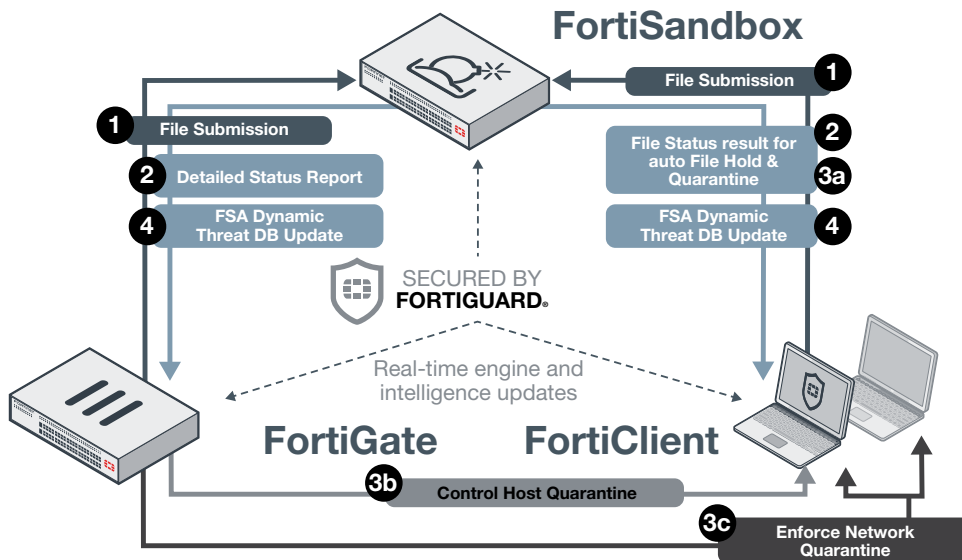
Advanced Threat Protection

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.

FEATURES

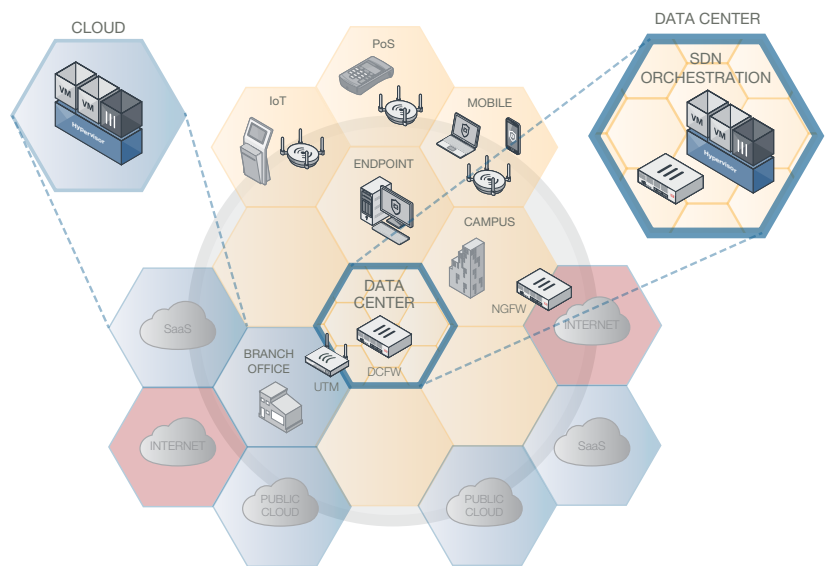| Feature	Highlights	The Fortinet Advantage
Anti-Malware / ATP	▪ Flow and proxy based AV options for choice between protection and performance. ▪ Local File Quarantine (for models with storage). ▪ Anti-bot capability using IP reputation DB, terminates botnet communication to C&C servers. ▪ **NEW:** Receive 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	▪ Over 7,000+ regular and rate based signatures, supported by zero-day threat protection and research for effective IPS implementation. ▪ Integrated DOS protection protects against abnormal traffic behaviors. ▪ **NEW:** DSRI option for specific deployment scenarios while increasing throughput performance. ▪ **NEW:** 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 in-built bypass ports for selected model.
Application Control	▪ Detects and acts against traffic based on applications while providing visibility on network usage.	▪ Superior coverage, including both desktop and mobile applications, enabling better management of network access policies.
Cloud Access Security Inspection	▪ **NEW:** Fine-grained control on popular cloud applications, such as SalesForce, Google Docs, and Dropbox.	▪ Applies deeper application inspections for better control and visbility 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 ratings that covers URLs 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.
Anti-Spam	▪ Highly effective, multilayered spam filters with low false positives.	▪ Cost-efficient anti-spam solution for small organizations or branch offices without requiring investment on additional system.
Firewall	▪ High performance firewall with FortiASIC-powered appliance. ▪ Easy-to-use policy management with unique Section or Global View options.	▪ Industry's top firewall appliance with superior cost-performance ratio.
VPN	▪ Comprehensive enterprise-class features for various type of VPN setups. ▪ **NEW:** Group-based SSL VPN bookmark. ▪ **NEW:** Improved 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 FortiASIC™ Network Processors 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. ▪ FortiExplorer Watermark Tool allows organizers to apply document marking for DLP.	▪ Prevents sensitive information from transiting out of the network easily with low TCO.
Compliance	▪ **NEW:** Periodical system configuration check using a pre-defined PCI compliance checklist.	▪ Automates compliance auditing which frees up precious administration resources.

FEATURES

Platform

Performance

The FortiGate platform delivers 5x the next generation firewall performance and 10x the firewall performance of equivalently priced platforms from other vendors. The high performance levels in the FortiGate are based on an Optimum Path Processing architecture in FortiOS that leverages performance, optimized security engines and custom developed FortiASIC network and content processors. The FortiGate achieved the best cost per Mbps performance value results in the 2014 NSS Labs NGFW industry tests.

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 and the data center — making sure you have the right mix of capabilities and performance for each deployment mode.

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, WiFi, WAN, load balancing, and high availability, making the FortiGate a popular choice for organizations wanting to consolidate their networking and security functions.

Feature	Highlights	The 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. ▪ Enterprise-class wireless management functionality, including rogue AP protection, wireless security, monitoring, and reporting. ▪ **NEW:** NP6 CAPWAP acceleration.	▪ Wireless controller integrated into the FortiGate console provides true single-pane-of-glass management that benefits organization with ease-of-use and lower TCO.
Switch Controller	▪ Integrated switch controller for Fortinet access switches with no additional license or component fees. ▪ **NEW:** Extend support for more switches and FortiGate platforms. ▪ **NEW:** PoE port control, LACP FortiLink support, HA deployment support.	▪ Expands security to access level to stop threats and protect terminals from one another.
WAN Interface Manager	▪ Support the use of 3G/4G modems via USB port or FortiExtender. ▪ **NEW:** Allow FortiExtender to use VLAN interfaces.	▪ Allow organizations to use or add 3G/4G connectivity for WAN connections while maintaining access control and defining usage for those links.
Endpoint Manager	▪ Manage Multi-OS FortiClients with policy and setting provisioning. ▪ Endpoint profile assignment based on device/user groups. ▪ Posture checking that integrates with captive portal.	▪ Simplified mobile user security enforcement by easily distribute and updating clients' security profiles that are consistent with gateway protection.

FEATURES

Feature	Highlights	The Fortinet Advantage
Token Server	▪ In-built token server that manages both physical and mobile tokens for use with various FortiOS authentication requirements such as VPN access and FortiGate administration. ▪ Robust provisioning features, such as SMS activation.	▪ Easily implement with two factor authentication for user and administrator access with low cost to deploy.
Routing / NAT	▪ Comprehensive routing protocols and NAT support. ▪ Traffic redirection with ICAP and WCCP support. ▪ **NEW:** Static route definition with policy objects.	▪ 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:** Virtual wire pairs. ▪ **NEW:** Wildcard VLAN creation.	▪ Flexible interface configurations offers 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. ▪ **NEW:** More UTM components and logging support	▪ Offline mode provides flexibility when deploying into existing critical networks where in-line security solution is not yet appropriate.
Hybrid WAN	▪ Comprehensive WAN Link LB algorithm, link status, plus quality checks, and policy routing support. ▪ **NEW:** Direct traffic among WAN links based on applications and users/user groups.	▪ Robust multi-link feature supports aids organizations in hybrid WAN implementation.
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 environment and SLA requirements.
QoS	▪ Manage the level of service and preference given to the various types and sources of traffic using traffic policing, traffic shaping, and queuing.	▪ Robust QoS capabilities adjust allocation of bandwidth to different traffic types, improving the performance and stability of latency sensitive or bandwidth intensive network applications.
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.
WAN Optimization & Web Caching	▪ 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.	▪ In-built WAN optimization capabilities reduces network overhead, resulting more effcient use of bandwidth and better application performance, without the need for costly WAN link upgrades.
Explicit Proxy	▪ Explicit HTTP and HTTPS, FTP over HTTP, or SOCKS proxying of IPv4 and IPV6 traffic on one or more interfaces.	▪ Integrated, enterprise-class explicit web proxy provides HTTP and HTTPS proxying with the added benefits of UTM security and user identity..
Server Load Balancing	▪ Traffic distribution across multiple backend servers based on multiple methods that account for different sized servers, or based on the health and performance of the server.	▪ Ideal for smaller server farms, the in-built feature allows you to secure critical servers and ensure high avaibility of their services possible.
Essential Network Services	▪ A wealth of networking services such as DHCP, DNS server, NTP server etc.	▪ In-built, out-of-the-box capabilities let orgnizations quickly provide necessary network services to internal terminals or to integrate with other network devices.
Physical Appliance (+ASICs)	▪ Integration with proprietary hardware architecture that includes acceleration components (FortiASICs) and multicore processors.	▪ Superior software and hardware integration ensures most optimal use of hardware components, hence yielding best cost/performance for customers
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 appliance reduces management cost and simplifies deployments.
Cloud	▪ Support for public cloud services: Amazon AWS and Microsoft Azure.	▪ Consistent management and features between physical and cloud platforms reduces management cost and simplifies deployments.

SPECIFICATIONS

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

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.

Configuration

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

FortiExplorer:
- Management client for Windows, Mac, IOS, and Andriod 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

Visibility

Dashboard: Customizable widgets that inform administrators of crucial system, licensing threats, and network status

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.
- Device topology
- Threat map
- Data views options: Table, bubble chart, or world map if applicable
- Accelerated session indication on 'All sessions' FortiView Console
- WHOIS Lookup for Public IP addresses within FortiView and log tables.

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

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

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

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

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

Policy Objects

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

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

User Authentication

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

Single-sign-on: Intergration 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

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 / ATP

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)

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)

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

SPECIFICATIONS

Application Control

Detects over 3,000 applications in 18 Categories: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)

Custom application signature support

Supports detection for traffic using SPDY protocol

Filter-based selection: By behavior, category, popularity, technology, risk, vendor, and/or protocol

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

SSH Inspection

Cloud Access Security 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

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

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

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)

Anti-Spam

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

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

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

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

Compliance

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

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

WiFi Security: Rogue AP suppression, wireless IDS

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

Switch Controller

Extends access control and security to wired devices by managing Fortinet switches (FortSwitch) 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

SPECIFICATIONS

Endpoint Manager

Manages network devices via client software:
- Posture checking: Enforce client software installation and desired settings
- Client configuration provisioning: Push and update client configurations such as VPN and web filtering settings, accordingly to device type/group and/or user/usergroup
- "Off-net" security enforcement: Detects when not protected by security gateway, activates provisioning security settings
- Allows client activities logging implementation

Client software support: Windows, OS X, iOS, Android

Token Server

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

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

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

Hybrid 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.

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

QoS

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.

IPv6

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

WAN Optimization & Web Caching

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

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.

Essential Network Services

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

FortiGuard NTP, DDNS, and DNS service

Physical Appliance (+ASICs)

Integrates with ASIC components for traffic processing acceleration.

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

Network Vulnerability Scan: Protect network assets (servers and workstations) by scanning them for security weaknesses.
- On-demand or scheduled
- Scan Modes: Quick, standard, or full
- Authenticated scanning
- Detailed scan results are logged with direct reference on threat encyclopedia

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

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

ADDITIONAL 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

F⊙RTINET®

GLOBAL HEADQUARTERS	EMEA SALES OFFICE	APAC SALES OFFICE	LATIN AMERICA SALES OFFICE
Fortinet Inc.	120 rue Albert Caquot	300 Beach Road 20-01	Prol. Paseo de la Reforma 115 Int. 702
899 Kifer Road	06560, Sophia Antipolis,	The Concourse	Col. Lomas de Santa Fe,
Sunnyvale, CA 94086	France	Singapore 199555	C.P. 01219
United States	Tel: +33.4.8987.0510	Tel: +65.6513.3730	Del. Alvaro Obregón
Tel: +1.408.235.7700			México D.F.
www.fortinet.com/sales			Tel: 011-52-(55) 5524-8480