FortiOS® 5.2 Network Security Operating System
For Next Generation Firewall

FortiOS is a security-hardened, purpose-built operating system that forms the foundation of all FortiGate® platforms. FortiOS 5.2 software leverages the hardware acceleration provided by custom FortiASIC™ processors, delivering the most comprehensive suite of security and networking services available within a single device.

Most Secured Network Protection Solution
Today’s organizations are facing numerous challenges as the network environment, usage patterns and threats evolve. The FortiOS Next Generation Firewall modules resolve these challenges with their rich feature offerings, proven security and ease of use. Administrators are able to also gain vital insights to real-time network and threat status, empowering them to take swift and effective actions.

Future-Proof Security Gateway
The FortiOS extensible architecture allows organizations to activate security modules easily without the need for complex licensing and hardware modules. Administrators also enjoy the benefits of the flexible platforms with single-plane-of-glass management and correlated logs and reports. With these, FortiOS enables customers to significantly reduce TCO and complexity while achieving high-value protection.

Key Features & Benefits

| Next Generation Firewall Capabilities | Protects against today’s threats and controls network access with a robust firewall, IPS, application control and identity awareness and control. |
| Visibility with powerful context information | Reduces complexity and decreases costs as all functions can be managed through one console. Manages users and devices with consistency. |

Rich feature set for protecting your critical digital assets.

- Outstanding manageability with consolidated security and access control setup.
- Robust feature set to meet sophisticated enterprise requirements.
- Strong user and device management with multiple authentication options.

FortiCare
Worldwide 24x7 Support
support.fortinet.com

FortiGuard
Threat Research & Response
www.fortiguard.com
HIGHLIGHTS

Proven Security with Industry Validation
FortiGate running FortiOS holds more industry certifications than any competitive product, assuring feature quality and providing you best-of-breed protection.

Ease of Use
Configuration errors by administrators are often cited as the weakest link in protecting organizations. FortiOS lowers operational costs and reduces IT staff workloads and mistakes with its easy yet innovative webUI. Intuitive single-pane-of-glass management ensures consistent policy creation and enforcement while minimizing deployment and configuration challenges.

Detailed Contextual Visibility
FortiOS allows greater traffic visibility and more consistent, granular control over users, devices, applications and sensitive data. Dashboard Widgets and drill-in viewers allows administrators to quickly view and understand real-time network activities and threat situations. This information is presented with comprehensive contextual associations such as the device types and bandwidth usage.

Extensive Network Support
FortiOS supports numerous network design requirements and interoperates with other networking devices. This includes support for a wealth of routing, multicasting and network resiliency protocols. Administrators can also configure interfaces for VLANs, VLAN trucks, port aggregation and one-armed sniffer mode.

It also offers robust high-availability and clustering options, including advanced sub-second failover, virtual clusters and much more.

Intelligent Traffic Handling
FortiOS allows organizations to setup beyond basic access control. By analyzing the allowed traffic, The FortiGate is able to apply sophisticated decisions such as policy routing and traffic shaping. Web caching is available on most models that improves user experience and reduces bandwidth usage.

Unified Access Security
FortiOS empowers organizations to apply consistent policies across various types of networks, simplifying policy enforcement in today’s complex environments. Its Wireless Controller features extends the same protection to wireless networks while Endpoint Control capabilities provision and enforce security for mobile users even when they are away from office.
**Identity-Centric Enforcement**
FortiOS supports both local and remote authentication services such as LDAP, Radius and TACACS+ to identify users and apply access policies and security profiles accordingly.

FortiOS simplifies identity-based implementations and also provides a seamless user authorization experience with various single sign-on capabilities. FortiOS can capture terminal service user or wireless login credentials, among others, and intelligently apply policies and profiles without additional user input.

**Sophisticated Application Control**
Identifying applications and providing relevant enforcement is essential in the current Web 2.0 and cloud environment. FortiOS offers gradual controls and can identify over 3,000 applications, even those on encrypted channels. It also offers mitigation against sophisticated botnet activities that easily evade traditional firewalls.

**Advanced Intrusion Protection**
Next Generation IPS technology from Fortinet protects networks from evasive and advanced attacks at the application layer. Analysis using contextual information and behavior prevents unknown zero-day attacks from damaging critical digital assets and services. The FortiGuard Intrusion Prevention Service, with a database of more than 4000 known threats, updates customers with up-to-date defenses against stealthy network-level threats.

**Powerful & Scalable Management**
FortiManager makes it easy to provision and manage thousands of FortiGates in a distributed organization in-built also provides customers with the ability to set up sophisticated policy implementation and provisioning workflows for compliance or operational requirements. Detailed configuration audit trails are supported and can reside externally on secured storage with FortiAnalyzer.

FortiOS also integrates well with third-party solutions such as Network Management Systems and SIEMs through our technology alliances.

**World-Class Technical Support and Documentation**
Fortinet FortiCare support offerings provide comprehensive global support for all Fortinet products and services. You can rest assured your Fortinet security products are performing optimally and protecting your users, applications, and data around the clock.

---

**FortiGate® - High performance Network Security Platform**

- **ASIC-Powered Performance**
  FortiGate purpose-built hardware delivers unmatched price/performance for the most demanding networking environments. FortiASIC processors ensure that your network security solution does not become a network bottleneck.

- **High speed and Flexible Connectivity**
  The FortiGate product family offer a variety of interfaces for today’s network, ranging from integrated WAN interfaces, 3G/4G USB wireless broadband support to high speed 40G interfaces for data centers.

- **Broad Product Offerings**
  The FortiGate product family scales from desktop units for remote branch offices, mid-range for small and medium enterprises to high-end platforms for service providers and data centers.
FEATURE SUMMARY

Network Services and Support

Built-in DHCP, NTP, DNS Server and DNS proxy (available on most models)

- FortiGuard HTIP, DUNS and FortiDNS management; allow address
  resolution, IP 黄页, DNS records (A, MX, NS, AAAA, CNAME)

- Hybrid WAN support: load balancing and redundancy with link health check on monitoring
  using TWAMP

- Support USB 3.0/3G Wireless WAN modems

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

- Multicast traffic: sparse and dense mode, PM support

- Content routing: WCCP and ICA

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

- IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunneling, firewalls and UTM for IPv6 traffic

User & Device Identity Control

- Local user database

- Remote user authentication service support: LDAP, Radius and TACACS+


- Agent, Radius (accounting message), POP3/IMAP, user access (902:1, captive portal) authentication

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

- 2-factor authentication: 3rd party support, integrated token server with physical, SMS and Soft Tokens

- Device identification, device and OS fingerprinting, automated classification, inventory management

- User and device-based policies

Firewall

- Operating modes: NAT/route and transparent (bridge)

- Schedules: one-time, recurring

- Session helpers & ALGs: tcp, dns-tcp, tcp-udp, ftp, H.245.1, H.245.0, H.323, MOCP, MMSP, FTP, PPTP, RAS, H.323, SP, TFTP, TNS (Oracle)

- VoIP traffic support: SIP/H.323/SCCP NAT traversal, H.245 pin mapping

- Protocol type support: STCP, TCP, UDP, ICMP, IP

- Filters and detection objects: expected, unexpected

- Session or global policy management view

- Policy objects: predefined, custom, object grouping, tagging and coloring

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

- NAT configuration: per policy based and central NAT Table

- NAT support: NAT64, NAT46, static NAT, NAT64, NAT46, NAT64, IPv6 IPCS VPN

- 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/or port). Application and/or protocol

- IDS sniffer mode

Application Control

- Detects over 5,000 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)

- Virus Protection: file reputation, file names, file activities and information

- Antivirus database type selection (on selected models)

- Flow-based Antivirus: protocols supported - HTTP/HTTPS, SMTP/SMTPS, POP3/IMAP, IMAP/IMAP, FTP/SFTP, SMB, ICQ, XM, NNTP
Proxy-based Antivirus:
- External cloud-based file analysis (OS sandbox) support
- File submission blacklisting and whitelisting
- File quarantine (local storage required)
- Heuristic scanning option

Web filtering inspection mode support: proxy-based, flow-based and DNS
- Manually defined web filtering based on URL, web content & MIME header
- Dynamic web filtering with cloud-based realtime categorization database: over 250 Million URLs rated into 79 categories, in 70 languages
- Safe Search enforcement: transparently inserts Safe Search parameter to queries.
- Supports Google, Yahoo!, Bing & Yandex, definable YouTube Education Filter

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

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

DLP File Filter:
- Protocol Supported: HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAP, 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 archiving: records full content in email, FTP, IM, NNTP, and web traffic

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

Redundant heartbeat interfaces

Failover:
- Port, local & remote link monitoring
- stateful failover
- sub-second failover
- Failure detection notification

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

Standalone session synchronization

Administration, Monitoring & Diagnostics
Management Access: HTTPS via web browser, SSH, telnet, console

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

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

Systems Integration: SNMP, sFlow, syslog, alliance partnerships

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

Dynamic, real-time dashboard status & drill-in monitoring widgets

Log & Reporting
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: Forwarded, violated sessions, local traffic, invalid packets

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

Brief traffic log format option

IP and service port name resolution option

Certification
ICSA Firewall, SSL-VPN, PSec-VPN, AV and IPS certification

USGv6 IPv6 Certified (when operated in IPS mode)

Common Criteria EAL-4 (on selected models)

NOTE: Feature set based on FortiOS V5.2.1+, some features or certification may not apply to all models.

ADDITIONAL REFERENCES

<table>
<thead>
<tr>
<th>Resource</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>The FortiOS Handbook</td>
<td><a href="http://docs.fortinet.com/ftg.html">http://docs.fortinet.com/ftg.html</a></td>
</tr>
<tr>
<td>The Complete Guide</td>
<td></td>
</tr>
<tr>
<td>Fortinet Knowledge Base</td>
<td><a href="http://kbase.fortinet.com/">http://kbase.fortinet.com/</a></td>
</tr>
</tbody>
</table>