FortiOS® 5.2 Network Security Operating System
For Unified Threat Management

FortiOS is a security-hardened, purpose-built Operating System that is the foundation of all FortiGate® network security platforms from our entry-level devices to our most powerful carrier-grade models. FortiOS 5.2 includes over 150 standard features, and many new enhancements that help fight advanced threats, simplify FortiGate installations and expand threat reporting and management.

Robust Complete Network Security

No matter how large or small your organization is, you face numerous challenges as your network environment, usage patterns and security threats evolve. FortiOS gives you the latest in all-in-one network security protection that's easy to deploy and manage. Besides the industry's best firewall, intrusion protection and VPN you get Advanced Threat Protection that fights against advanced persistent threats (ATPs) and additional features like email filtering, data-loss prevention and vulnerability scanning - a complete Unified Threat Management (UTM) solution for your business.

Flexible Architecture that Adapts with Your Needs

Whether you need a simple firewall or a complete UTM installation, FortiOS gives you the flexibility to easily configure the options you need for your environment. From a “single pane of glass” you can set up, manage, and get detailed reporting on your network and security threats, all within minutes.

Key Features & Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intuitive and Customizable</td>
<td>Easy to configure and manage with the flexibility to choose the security and UTM options you need.</td>
</tr>
<tr>
<td>Advanced Network Segmentation</td>
<td>Support for multiple zones and VDOMs to meet your data protection and compliance requirements.</td>
</tr>
</tbody>
</table>

Rich feature set for protecting your applications, data and users.

- Enterprise grade security for any sized organization.
- Easy to deploy and manage.
- Outstanding manageability with consolidated security and access control setup.
- Strong and flexible user and device management with multiple authentication options.
HIGHLIGHTS

Complete Security
Fortinet designed and built FortiOS 5.2 to deliver the advanced protection and performance that standalone products simply can’t match. The services work together as a system to provide better visibility and mitigation of the latest network and application threats, stopping attacks before damage can occur.

Unique Visibility and Control
Advanced security features such as flow-based inspection and integrated wireless controller capability allow you to monitor and protect your wired and wireless networks from endpoints to the core, and from remote offices to headquarters. FortiOS allows greater traffic visibility and more consistent, granular control over users, applications and sensitive data.

Securing Mobile Devices
FortiOS 5.2 helps secure mobile device and BYOD environments (including iOS®, Android® and Windows® clients) by identifying devices and applying specific access policies as well as security profiles, according to the device type or device group, location, and usage.

Easier to Manage
FortiOS 5.2 lowers costs and reduces IT staff workloads. Physical or virtual FortiGate appliances give you the flexibility to match your security to your environment while enforcing a uniform security policy. Single pane of glass management and centralized analysis ensure consistent policy creation and enforcement while minimizing deployment and configuration challenges.

Client Reputation
Signature-based security alone is not enough anymore; it is now critical to understand how devices on your network are behaving. FortiView with threat score provides a cumulative security ranking of each client device on your network based on a range of behaviors. It provides specific, actionable information that helps identify compromised systems and potential zero-day attacks in real time.

Smart Policies
FortiOS 5.2 enables intelligent, automatic adjustment of role-based policies for users and guests based on location, data, and application profile. Enhanced reporting and analysis provides deeper insights into the behavior of your network, users, devices, applications and threats.
HIGHLIGHTS

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 trunks, 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.

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 extend the same protection to wireless networks while endpoint control capabilities provision and enforce security for mobile users even when they are away from the office.

Device ID and User ID Access Control
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. It 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.

As device types continue to evolve, you’ll be ready with device access control. You can apply security policies based on the type of device such as computers, tablets or phones and apply different policies depending if the devices are company or privately owned.

Sophisticated Application Control
Identifying applications and providing relevant enforcement is essential in the current Web 2.0 and cloud environments. 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.

Physical and Virtual Segmentation
From simple small wired networks to the complex multi-tenant managed datacenter environments, FortiOS supports everything you need to set up and manage your network traffic. You can configure physical network segmentation using the LAN ports built-in to every FortiGate, or you can provide virtual segmentation using virtual LANs (VLANs).

Powerful & Scalable Management
FortiManager makes it easy to provision and manage thousands of FortiGate devices in a distributed organization. Using standardized setup profiles, you get the ability to configure a standard set of policy and provisioning workflows to meet your business needs or compliance standards. 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 Fortinet’s technology alliances.

---

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.
FEATURING SUMMARY

Network Services and Support
Built-in DHCP, NTP, DNS Server and DNS proxy (available on most models)
Dynamic and policy routing
Hybrid WAN support: load balancing and redundancy with link health check on monitoring
USB 30/4G Wireless WAN modems
Dynamic routing protocols:
RIP1, v2, OSPF, V2 and v3, ISIS, BGP4
Multicast traffic: sparse and dense mode, PIM support
Content routing: WCCP and ICAP
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 (DSCP) and Differentiated Services (Diffserv) support
IPv6 Support: any-enumeration over any transport protocols, IPv6 tunneling, firewall and UTM for IPv6 traffic
NAT46, NAT64, IPv6 IPSec VPN

WAN Optimization, Web Cache and Explicit Proxy
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 protocols: MACE, MCTOP
Secure tunneling option: use AES-128bit-GCM SSL to encrypt the traffic in the WAN optimization tunnel
Tunnel sharding option: multiple WAN optimization sessions share the same tunnel
Web caching: object caching 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 rewrite, Max conc object size, negative response duration, fresh factor, Max/Min TTL, proxy FDQN, Max HTTP request/message length, ignore options, cache expired objects, revalidated prama-no-cache
Explicit web & FTP proxy: FTP, HTTP, and HTTPS proxying on one or more interfaces
Proxy auto-configuration: multiple WAN optimization sessions share the same tunnel
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 and proxy chaining
Explicit web proxy authentication: IP-Based authentication and per session authentication
WAN optimization and web cache monitor

User & Device Identity Control
Local user database & remote user authentication service support: LDAP, Radius and TACACS+, 2-factor authentication
Single-sign-on: Windows AD, Novell director, FortiClient, Citrix and Terminal Server
Agent, Radius (accounting messages), POP3/POP3S, user access (902.1x, captive portal) authentication
PKI and certificates: X.500 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support
Device Identification: device and OS fingerprinting, automatic classification, inventory management
User and device-based policies

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

Firewall
Operating modes: NAT/route and transparent (bridge)
Supports multi-protocol, multi-user, and multi-tenancy
IPSec, PPTP, GRE
Other VPN support: L2TP client (on selected models) and server mode, L2TP over IPSec, PPTP, GRE over IPEC

VPN
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
- Repeat replay detection
- Autokey keep-alive for Phase 2 SA

IPSEC Configuration Wizard for termination with popular 3rd 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
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 bookmark management: allow administrators to view and maintain remote client bookmarks
SSL VPN web mode: for thin client 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
Single-sign-on: Windows AD, Novell director, FortiClient, Citrix and Terminal Server
Agent, Radius (accounting messages), POP3/POP3S, user access (902.1x, captive portal) authentication
PKI and certificates: X.500 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support
Device Identification: device and OS fingerprinting, automatic classification, inventory management
User and device-based policies

Integrated Token Server
Integrated token server that provisions and manages physical, SMS and Soft One Time Password (OTP) Tokens
# Feature Summary

## SSL Inspection
Inspect SSL Encrypted traffic option for IPS, application control, antivirus, web filtering and DLP

## IPS
**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: log, monitor, lockdowns P and Victim IP (incoming interface) with expiry time
- Filter Based Selection: severity, target, OS, application and/or protocol
- Packet logging option
- IPSs exemption from specified IPS signatures

## 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 SPODY protocol
- Deep Application visibility: login names, files/video activities and information
- Filter based selection: by category, popularity, technology, risk, vendor and/or protocol
- Actions: block, reset session, monitor only, application control traffic shaping

## Anti-Malware / Advanced Threat Protection
Botnet server IP blocking with global IP reputation database

- Flow-based Antivirus: protocols supported - HTTP/HTTPS, SMTP/IMAP, POP3/POP3S, IMAP/IMAPS, MAP, FTP/SFTP, SMB, ICMP, YNTP
- 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
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 78 categories, in 70 languages
- Safe Search enforcement: transparently inserts Safe Search parameter to queries.
- Supports Google, Yahoo!, Bing & 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
  - Restrict access to Google Corporate Accounts only

## Data Leak Prevention (DLP)
Web filtering inspection mode support: proxy-based, flow-based and DNS

- DLP message filter:
  - Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAP, NNTP
  - Actions: log only, block, quarantine user/IP/Interface
- 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 fingerprinting: allows filter files that pass through the FortiGate unit and contains 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.

## Endpoint Control
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
- Client software support: Windows, OS X, iOS, Android

## Vulnerability Scanning
Network Vulnerability Scan: protect network assets (servers and workstations) by scanning them for security weaknesses.
- On-demand or scheduled scanning
- Scan Modes: Quick, standard or Full
- - authenticated scanning

- Vulnerability Result: detailed scan results are logged with direct reference on threat encyclopedia

## Wireless and Switch Controller
Manages and provisions settings for local and remote Thin Access points or switches

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

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

## High Availability
High availability modes: active-passive, active-active, virtual clusters, VRRP, FG-6000 series clustering

- HA reserved management interface
- - Geographically dispersed HA
- - Full mesh HA
- - HA with link aggregation

## DLP Archiving
Records full content in email, FTP, IM, NNTP, and web traffic

## Management Access
- HTTPS via web browser, SSH, telnet, console
- Central management
- Basic Security: User ID, Password, SSH, Telnet, console
- Advanced Security: RADIUS, TACACS+, TACACS+, LDAP, Radius, SSH, Telnet, console

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

- Central management
- Basic Security: User ID, Password, SSH, Telnet, console
- Advanced Security: RADIUS, TACACS+, TACACS+, LDAP, Radius, SSH, Telnet, console
- Dynamic, real-time dashboard status & drill-in monitoring widgets
FEATURE SUMMARY

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

ADDITIONAL REFERENCES

<table>
<thead>
<tr>
<th>Resource</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet Knowledge Base</td>
<td><a href="http://kb.fortinet.com/">http://kb.fortinet.com/</a></td>
</tr>
</tbody>
</table>

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


d详目

Comprehensive event logs: systems & administrators activity audits, routing & networking,

VPN, user authentications, Wi-Fi related events

Brief traffic log format option

IP and service port name resolution option

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.