FORTINET

FortiOS® 5 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 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-pane-of-glass management and correlated logs and reports. With these, FortiOS enables customers to significantly reduce TCO and complexity while achieving high-value protection.

Rich feature set for protecting your critical digital assets.

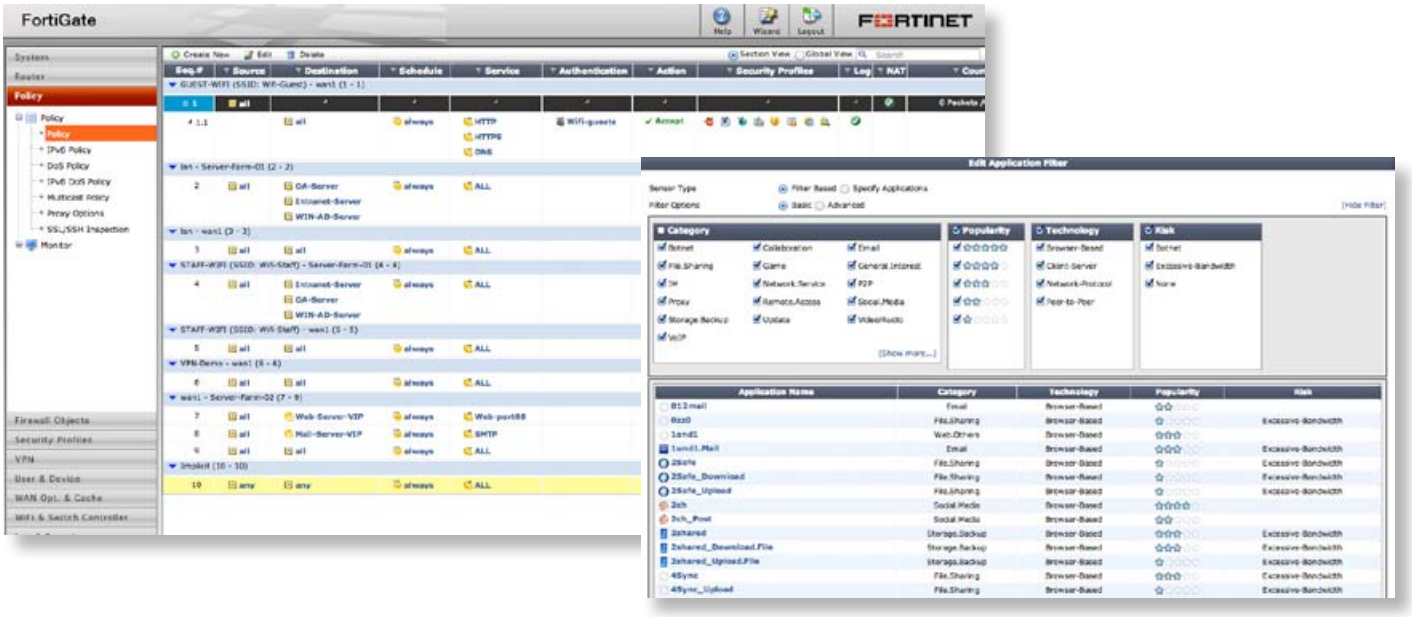
- Outstanding manageability with consolidated security and access control setup.
- Robust feature set to meet sophisticated enterprise requirements.
- Strong user and device management with multiple authentication options

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.

ICSA labs CERTIFIED ANTI-VIRUS · ICSA labs CERTIFIED NETWORK IPS · ICSA labs CERTIFIED SSL VPN · ICSA labs CERTIFIED FIREWALL - CORPORATE · ICSA labs CERTIFIED IPSEC - BASIC

HIGHLIGHTS



FortiOS web-based GUI — firewall policy table and application control settings.

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 allow 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 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.

HIGHLIGHTS

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 and Scalable Management

FortiManager makes it easy to provision and manage thousands of FortiGates in a distributed organization in-build. It 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 offers 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 NTP, DDNS and DNS service

Interface modes: sniffer, port aggregated, loopback, VLANs (802.1Q and Trunking), hardware and software switches (available on most models)

Static and policy routing

WAN load balancing with ECMP (Equal Cost Multi-Path) and redundancy

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

Multicast traffic: sparse and dense mode, PIM support

Content routing: WCCP and ICAP

Explicit proxy support

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

User and Device Identity Control

Local user database

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

Single-sign-on: Windows AD, Novell eDirectory, FortiClient, Citrix and Terminal Server Agent, Radius (accounting message), 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

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

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

User and device-based policies

Firewall

Operating modes: NAT/route and transparent (bridge)

Schedules: one-time, recurring

Session helpers & ALGs: dcerpc, 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

Section or global policy management view

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

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

NAT configuration: per policy based and central NAT Table

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

Traffic shaping and QOS: shared policy shaping, per-IP shaping, maximium & guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS) and Differentiated Services (DiffServ) support

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
- Replay detection
- Autokey keep-alive for Phase 2 SA

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

SSL portal concurrent users limiting

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

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

IPS

IPS engine: 7,000+ up-to-date signatures, protocol anomaly 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 over 3,000 applications in 19 Categories:
Botnet, Collaboration, Email, File Sharing, Game, General Interest, IM, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)

Custom application signature support

Advanced Instant Messenger (IM) & Facebook control

Filter based selection: by category, popularity, technology, risk, vendor and/or protocol

Actions: block, reset session, monitor only, application control traffic shaping

SSH Inspection

Threat Protection

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

Botnet server IP blocking with global IP reputation database

Antivirus database type selection (on selected models)

Flow-based Antivirus: protocols supported - HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP

Proxy-based Antivirus:
- Protocol Support: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
- External cloud-based file analysis (OS sandbox) support
- File submission blacklisting and whitelisting
- File quarantine (local storage required)
- Heuristic scanning option

FEATURE SUMMARY

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
- 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

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)

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:
- Protocol 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

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
- allows client activities logging implementation

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

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 & 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

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: USB auto-install, local and remote script execution

Dynamic, real-time dashboard status & 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: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

Certification

ICSA Firewall, SSL VPN, IPSEc VPN, AV and IPS certification

FIPS 140-2 Validated (when operated in FIPS mode)

USGv6 IPv6 Certified

Common Criteria EAL-4 (on selected models)

NOTE: Feature set based on FortiOS V5.0.6+, some features or certification may not apply to all models.

ADDITIONAL REFERENCES

Resource	URL
The FortiOS Handbook — The Complete Guide	http://docs.fortinet.com/fgt.html
Fortinet Knowledge Base	http://kb.fortinet.com/
Product Datasheets & Matrix	http://www.fortinet.com/resource_center/datasheets.html
NGFW Solution Page	http://www.fortinet.com/solutions/next_generation_firewall.html

GLOBAL HEADQUARTERS

Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE

120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE

300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE

Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

FST-PROD-DS-NGFW

FOS-NGFW-DAT-R2-201403