FORTINET

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

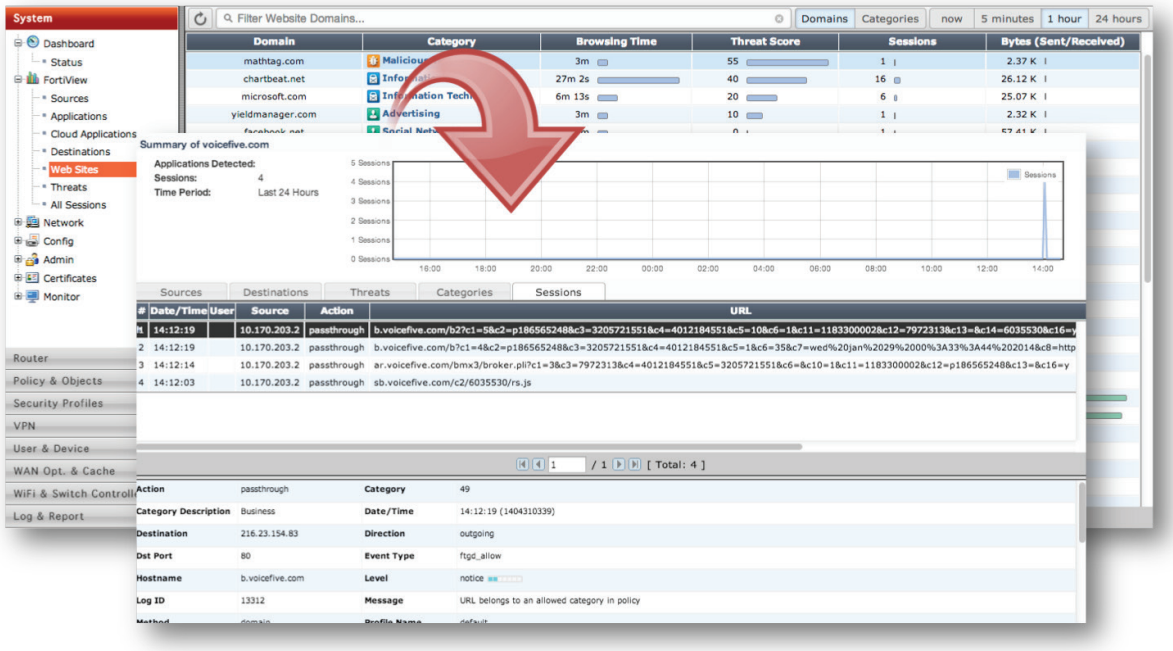
Unified Threat Management	Comprehensive network security protection with advanced threat protection, email filtering, data-loss prevention and vulnerability scanning.
Intuitive and Customizable	Easy to configure and manage with the flexibility to choose the security and UTM options you need.
Advanced Network Segmentation	Support for multiple zones and VDOMs to meet your data protection and compliance requirements.

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.

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 — FortiView on-demand query tool

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.

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.

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.

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

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), virtual hardware, software and VLAN switches (available on most models)

Static and policy routing

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

Support USB 3G/4G Wireless WAN modems

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

Traffic shaping and QoS per policy or applications: 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

IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunnelling, 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 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

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

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 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 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)

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

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 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 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

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: 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 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

Deep Application visibility: login names, files/video actvities and information

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

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

SSH Inspection

Anti-Malware / Advanced Threat Protection

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

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
- 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)

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, 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

Vulnerability Scanning

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

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 (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

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, Netflow, syslog, alliance partnerships

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

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: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

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

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
UTM Solution Page	http://www.fortinet.com/solutions/unified_threat_management.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