

FORTIGATE™ 400/500

Real-time Network Protection for Enterprises

FortiGate™ Antivirus Firewalls are dedicated, hardware-based units that deliver complete, real-time network protection services at the network edge. Based on Fortinet's revolutionary FortiASIC™ Content Processor chip, the FortiGate platforms are the only systems that can detect and eliminate viruses, worms, and other content-based threats without reducing network performance — even for real-time applications like Web browsing. FortiGate systems also include integrated firewall, content filtering, VPN, intrusion detection and prevention, and traffic shaping functions, making them the most cost effective, convenient, and powerful network protection solutions available.

The FortiGate-400 and FortiGate-500 Antivirus Firewalls meet enterprise-class requirements for security, performance, flexibility, and reliability. Flexible deployment options allow FortiGate users to customize ports and assign Route and NAT mode options to individual interfaces. The FortiGate-400 and FortiGate-500 Antivirus Firewalls provide granular security through multi-zone capabilities, which allows administrators to segment their network into zones and create policies between zones. Featuring 4 and 12 auto-sensing 10/100 Base-T Ethernet ports, the FortiGate-400 and FortiGate-500, respectively, offer award-winning network-based antivirus, firewall, content filtering, VPN, network-based intrusion detection and prevention, and traffic shaping services. Additionally, the FortiGate-400 and 500 support high availability operation with stateful failover to a redundant stand-by unit. The FortiGate-400 and FortiGate-500 are kept up to date automatically by Fortinet's FortiProtect™ Network, which provides continuous updates that ensure protection against the latest viruses, worms, Trojans, and other threats — around the clock, and around the world.



Product Highlights

- Provides complete network protection functionality through a combination of network-based antivirus, web content filtering, firewall, VPN, dynamic intrusion detection and prevention, traffic shaping, and anti-spam
- Eliminate viruses and worms from email, file transfer, and real-time (Web) traffic without degrading network performance
- Front-panel LCD and keypad ease deployment by setting basic system parameters without an external console
- Reduces exposure to threats by detecting and preventing over 1300 different intrusions, including DoS and DDoS attacks
- Easy to use and deploy – quick and easy configuration wizard walks administrators through initial setup with graphical user interface
- High availability option supports transparent failover for mission-critical applications
- Multi-zone support allows granular network segmentation into zones with individual security and access control policies
- Delivers superior performance and reliability from hardware accelerated, ASIC-based architecture
- Automatically downloads the latest virus and attack database and can accept instant “push” updates from the FortiProtect Network
- Virus quarantine enables easy submission of attack samples to the Fortinet Threat Response Team
- Underlying FortiOS™ operating system is ICSA-certified for Antivirus, Firewall, IPSec VPN, and Intrusion Detection

FORTIGATE™ 400/500

Key Features & Benefits

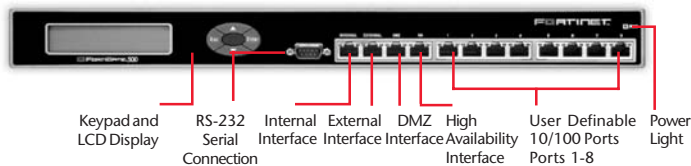
Feature	Description	Benefit
Network-based Antivirus (ICSA Certified)	Detects and eliminates viruses and worms in real-time. Scans incoming and outgoing email attachments (SMTP, POP3, IMAP), FTP and HTTP traffic including web-based email – without degrading Web performance	Closes the vulnerability window by stopping viruses and worms before they enter the network
Dynamic Intrusion Detection and Prevention (ICSA Certified)	Detection and prevention of over 1300 intrusions and attacks, including DoS and DDoS attacks, based on user-configurable thresholds. Automatic updates of IPS signatures from FortiProtect Network	Stops attacks that evade conventional antivirus products, with real-time response to fast-spreading threats
Firewall (ICSA Certified)	Powerful stateful inspection firewall	Certified protection, maximum performance and scalability
Web Content Filtering	Processes all Web content to block inappropriate material and malicious scripts via URL blocking and keyword.phrase blocking	Assures improved productivity for enterprise and regulatory compliance for CIPA-compliant educational institutions
VPN (ICSA Certified)	Industry standard IPSec, PPTP, and L2TP VPN support	Provide secure communication tunnels between networks and clients
Transparent Mode	FortiGate units can be deployed in conjunction with existing firewall and other devices to provide antivirus, content filtering, and other content-intensive applications	Easy integration/investment protection of legacy systems
Remote Access	Supports secure remote access from any PC equipped with FortiClient Host Security software	Low cost, anytime, anywhere access for mobile and remote workers and telecommuters

System Specifications

FortiGate-400



FortiGate-500



FORTIGATE™ 400/500

Specifications

	FortiGate-400	FortiGate-500		FortiGate-400	FortiGate-500
Interfaces			High Availability (HA)		
10/100 Ethernet Ports	4	12	Active-active HA	•	•
System Performance			Active-passive HA	•	•
Concurrent sessions	400,000	400,000	Stateful failover (FW and VPN)	•	•
New sessions/second	10,000	10,000	Device failure detection & notification	•	•
Firewall throughput (Mbps)	280	280	Link status monitor	•	•
168-bit Triple-DES throughput (Mbps)	80	90	Networking		
Unlimited concurrent users	•	•	Multiple WAN link support	•	•
Policies	5,000	8,000	Multi-zone support	•	•
Schedules	256	256	Route between zones	•	•
Antivirus, Worm Detection & Removal			Policy-based routing	•	•
Automatic virus database update from FortiProtect Network	•	•	System Management		
Scans HTTP, FTP, SMTP, POP3, IMAP, and encrypted VPN Tunnels	•	•	Console interface (RS-232)	•	•
Quarantine infected messages	•	•	WebUI (HTTPS)	•	•
Firewall Modes and Features			Multi-language support	•	•
NAT, PAT, Transparent (bridge)	•	•	Command line interface	•	•
Routing mode (RIP v1, v2)	•	•	Secure Command Shell (SSH)	•	•
VLAN tagging (802.1q)	•	•	FortiManager System	•	•
Access control list (Source IP, Destination IP, TCP port, and UDP port)	•	•	Administration		
User Group-based authentication	•	•	Multiple administrators and user levels	•	•
H.323 NAT Traversal	•	•	Upgrades & changes via TFTP & WebUI	•	•
WINS support	•	•	System software rollback	•	•
VPN			User Authentication		
PPTP, L2TP, and IPSec	•	•	Internal database	•	•
Dedicated tunnels	2000	2000	LDAP support	•	•
Encryption (DES, 3DES, AES)	•	•	RADIUS (external) database	•	•
SHA-1 / MD5 authentication	•	•	RSA SecurID	•	•
PPTP, L2TP, VPN client pass though	•	•	Xauth over RADIUS support for IPSec VPN	•	•
Hub and Spoke VPN support	•	•	IP/MAC address binding	•	•
IKE certificate authentication (X.509)	•	•	Traffic Management		
IPSec NAT Traversal	•	•	DiffServ setting	•	•
Dead peer detection	•	•	Policy-based traffic shaping	•	•
Content Filtering			Guaranteed/Maximum/Priority bandwidth	•	•
URL/keyword/phrase block	•	•	Dimensions		
URL Exempt List	•	•	Height	1.75 inches	1.75 inches
Protection profiles	32	32	Width	16.75 inches	16.75 inches
Blocks Java Applet, Cookies, Active X	•	•	Length	12 inches	12 inches
FortiGuard™ web filtering support	•	•	Weight	11 lb (5 kg)	11 lb (5 kg)
Dynamic Intrusion Detection and Prevention			Rack Mountable	•	•
Intrusion prevention for over 1300 attacks	•	•	Power		
Automatic real-time updates from FortiProtect Network	•	•	AC input voltage	100 to 240VAC	100 to 240VAC
Customizable detection signature list	•	•	AC input current	4A	4A
Anti-Spam			Frequency	47 to 63Hz	47 to 63Hz
Real-time Blacklist/Open Relay Database Server	•	•	Power Dissipation	180W max	180W max
MIME header check	•	•	Environmental		
Keyword/phrase filtering	•	•	Operating Temperature	32 to 104 °F (0 to 40 °C)	32 to 104 °F (0 to 40 °C)
IP address blacklist/exempt list	•	•	Storage Temperature	-13 to 158 °F (-25 to 70 °C)	-13 to 158 °F (-25 to 70 °C)
Logging/Monitoring			Humidity	5 to 95% non-condensing	5 to 95% non-condensing
Internal logging/removable HD	20G	20G	Regulatory		
Log to remote Syslog/WELF server	•	•	FCC Class A Part 15	•	•
Graphical real-time and historical monitoring	•	•	CSA/CUS	•	•
SNMP	•	•	CE	•	•
Email notification of viruses and attacks	•	•	UL	•	•
VPN tunnel monitor	•	•	ICSA Antivirus, Firewall, IPSec, NIDS	•	•


FORTIGATE™ 400/500
Australia

Level 17, 201 Miller Street
North Sydney 2060
Australia

Tel: +61-2-8923-2555
Fax: +61-2-8923-2525

China

Suite B-903
Zhongdian Information Building
2 Zhongguancun Nan Ave.
Beijing 100086, China

Tel: +8610-8251-2622
Fax: +8610-8251-2630

France

69 rue d'Aguesseau
92100 Boulogne Billancourt
France

Tel: +33-1-4610-5000
Tech Support: +33-4-9300-8810
Fax: +33-1-4610-5025

Germany

Feringapark
Feringastrasse 6
85774 München-Unterföhring
Germany

Tel: +49-(0)-89-99216-300
Fax: +49-(0)-89-99216-200

Hong Kong

Room 3206, 32/F
Convention Plaza - Office Tower
1 Harbour Road, WanChai
Hong Kong

Tel: +852-3171-3000
Fax: +852-3171-3008

Japan

32nd floor
Shinjuku-Nomura Building
1-26-2 Nishi-Shinjuku
Shinjuku-Ku
Tokyo, Japan 163-0532
Japan

Tel: +81-3-5322-2813
Fax: +81-3-5322-2929

Korea

27th Floor
Korea World Trade Center
159 Samsung-Dong
Kangnam-Ku
Seoul 135-729
Korea

Tel: +82-2-6007-2007
Fax: +82-2-6007-2703

Taiwan

18F-1, 460 SEC.4
Xin-Yi Road
Taipei, Taiwan, R.O.C.

Tel: +886-2-8786-0966
Fax: +886-2-8786-0968

United Kingdom

1 Farnham Road
Guildford, Surrey GU2 4RG
United Kingdom

Tel: +44-(0)-1483-549061
Fax: +44-(0)-1483-549165

United States

920 Stewart Drive
Sunnyvale, CA 94085
USA

Tel: +1-408-235-7700
Fax: +1-408-235-7737
Email: sales@fortinet.com