

# FORTIGATE™ 200/300

## Real-time Network Protection for Small and Medium Businesses



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-200 and FortiGate-300 Antivirus Firewalls serve environments that include small and medium sized businesses as well as branch and remote offices. Featuring 3 auto-sensing 10/100 Base-T Ethernet ports, the FortiGate-200 and FortiGate-300 provide high-performance, network-based antivirus, content filtering, firewall, VPN, network-based intrusion detection/prevention, and traffic shaping. ASIC-based acceleration delivers high performance for small to mid-sized organizations that require real-time network security services. Logging capabilities are built into the FortiGate-200 and FortiGate-300 through an internal, high capacity hard drive. The FortiGate-300 offers a customizable DMZ/High Availability port for organizations that require redundant configurations. The FortiGate-200 and FortiGate-300 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 through a combination of network-based antivirus, web and email content filtering, firewall, VPN, dynamic intrusion detection and prevention, and traffic shaping
- Eliminate viruses and worms from email, file transfer, and real-time (Web) traffic without degrading network performance
- Front-panel LCD and keypad on FortiGate-300 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
- Delivers superior performance and reliability from hardware accelerated, ASIC-based architecture
- User definable DMZ/HA port allows for flexible deployment
- Automatically downloads the latest virus and attack database and can accept instant “push” updates from the FortiProtect Network
- Underlying FortiOS™ operating system is ICSA-certified for Antivirus, Firewall, IPSec VPN, and Intrusion Detection
- Easy to use and deploy – quick and easy configuration wizard walks administrators through initial setup with graphical user interface
- Web-based graphical user interface (GUI) and content filtering support multiple languages
- Virus quarantine enables easy submission of attack samples to the Fortinet Threat Response Team

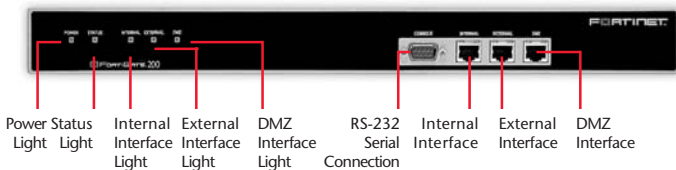
# FORTIGATE™ 200/300

## Key Features & Benefits

Feature	Description	Benefit
<b>Network-based Antivirus</b> (ICSA Certified)	Detects, quarantines, and eliminates viruses and worms in real-time. Scans incoming and outgoing email attachments (SMTP, POP3, IMAP), Web (HTTP) and FTP traffic, and encrypted VPN tunnels – without degrading Web performance	Closes the vulnerability window by stopping viruses and worms before they enter the network
<b>Dynamic Intrusion Detection and Prevention</b> (ICSA Certified)	Detection and prevention of over 1300 intrusions and attacks, based on user-configurable thresholds. Automatic update of IPS signatures from FortiProtect Network	Stops attacks that evade conventional antivirus products, with real-time response to fast-spreading threats
<b>Web Content Filtering</b>	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
<b>Firewall</b> (ICSA Certified)	Powerful stateful inspection firewall	Certified protection, maximum performance and scalability
<b>VPN</b> (ICSA Certified)	Industry standard PPTP, L2TP, and ICSA-certified IPSec VPN support. Supports WLAN deployment with user authentication, encrypted tunnels, and LDAP support	Lower costs by using the public Internet for private site-to-site and remote access communications
<b>Transparent Mode</b>	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
<b>Remote Access</b>	Supports secure remote access from any PC equipped with Fortinet Remote VPN Client	Low cost, anytime, anywhere access for mobile and remote workers and telecommuters

## System Specifications

FortiGate-200



FortiGate-300



# FORTIGATE™ 200/300

## Specifications

	FortiGate-200	FortiGate-300		FortiGate-200	FortiGate-300
<b>Interfaces</b>			<b>High Availability (HA)</b>		
10/100 Ethernet Ports	3	3	Active-active HA		•
<b>System Performance</b>			Active-passive HA		•
Concurrent sessions	400,000	400,000	Stateful failover (FW and VPN)		•
New sessions/second	4,000	10,000	Device failure detection & notification		•
Firewall throughput (Mbps)	120	200	Link status monitor		•
168-bit Triple-DES throughput (Mbps)	50	65	<b>Networking</b>		
Unlimited concurrent users	•	•	Multiple WAN link support	•	•
Policies	2000	5000	PPPoE client	•	•
Schedules	256	256	DHCP client/server	•	•
<b>Antivirus, Worm Detection &amp; Removal</b>			Policy-based routing	•	•
Scans HTTP, FTP, SMTP, POP3, IMAP, and encrypted VPN Tunnels	•	•	<b>System Management</b>		
Quarantine infected messages	•	•	Console interface (RS-232)	•	•
Block by file size	•	•	WebUI (HTTPS)	•	•
Automatic update of antivirus database from FortiProtect Network	•	•	Command line interface	•	•
<b>Firewall Modes and Features</b>			Secure Command Shell (SSH)	•	•
NAT, PAT, Transparent (bridge)	•	•	FortiManager System	•	•
Routing mode (RIP v1, v2)	•	•	<b>Administration</b>		
User Group-based authentication	•	•	Multiple administrators and user levels	•	•
H.323 NAT Traversal	•	•	Upgrades & changes via TFTP & WebUI	•	•
WINS Support	•	•	System software rollback	•	•
<b>VPN</b>			Trusted host enforcement (IP/mac binding)	•	•
PPTP, L2TP, and IPSec	•	•	<b>User Authentication</b>		
Dedicated tunnels	100	1500	Internal database	•	•
Encryption (DES, 3DES, AES)	•	•	LDAP support	•	•
SHA-1 / MD5 authentication	•	•	RADIUS (external) database	•	•
PPTP, L2TP, VPN client pass though	•	•	RSA SecurID	•	•
Hub and Spoke VPN support	•	•	Xauth over RADIUS support for IPSec VPN	•	•
IKE certificate authentication	•	•	IP/MAC address binding	•	•
IPSec NAT Traversal	•	•	<b>Traffic Management</b>		
Dead peer detection	•	•	DiffServ setting	•	•
<b>Content Filtering</b>			Polcy-based traffic shaping	•	•
URL/keyword/phrase block	•	•	Guaranteed/Maximum/Priority bandwidth	•	•
URL Exempt List	•	•	<b>Dimensions</b>		
Protection profiles	32	32	Height	1.75 inches	1.75 inches
Blocks Java Applet, Cookies, Active X	•	•	Width	16.8 inches	16.75 inches
FortiGuard™ web filtering support	•	•	Length	10 inches	11 inches
<b>Dynamic Intrusion Detection and Prevention</b>			Weight	7.3 lb (3.3 kg)	7.3 lb (3.3 kg)
Intrusion prevention for over 1300 attacks	•	•	<b>Power</b>		
Automatic real-time updates from FortiProtect Network	•	•	AC input voltage	100 to 240VAC	100 to 250VAC
Customizable detection signature list	•	•	AC input current	1.6A	1.5A
<b>Anti-Spam</b>			Frequency	50 to 60Hz	47 to 63Hz
Real-time Blacklist/Open Relay Database Server	•	•	Power Dissipation	50W max	100W max
MIME header check	•	•	<b>Environmental</b>		
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)
<b>Logging/Monitoring</b>			Humidity	5 to 95% non-condensing	5 to 95% non-condensing
Internal logging/removable HD	20G	20G	<b>Regulatory</b>		
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	•	•	ICSA Antivirus, Firewall, IPSec, NIDS	•	•
VPN tunnel monitor	•	•			


**FORTIGATE™ 200/300**
**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