

# FORTIGATE™ 5020

## High Density Solution for High Performance Content Security

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-5020 platform is the entry level system in the FortiGate 5000 series. FortiGate-5020 systems are configured using a FortiGate-5020 chassis outfitted with 1 or 2 blades to meet varying throughput, redundancy, and interface requirements. The FortiGate-5020 chassis is compliant with the AdvancedTCA (ATCA) specifications for next generation carrier-class equipment. Hot-swappable power and fan modules on the FortiGate-5020 chassis ensure high-availability power and cooling. The FortiGate-5020 chassis accommodates FortiGate-5001 blades, each of which is equipped with the FortiASIC™ Content Processor chip for high speed network and content security services. Each FortiGate-5001 blade module has 4 Gigabit speed Small Form-factor Pluggable (SFP) ports and 4 tri-speed gigabit ethernet ports. The FortiGate-5020 backplane interconnect provides a hardwired high availability connectivity for active-active and active-passive failover configurations. The FortiGate-5020 unit is 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

- Optimal solution for Large Enterprise and Managed Security Service Providers (MSSPs)
- Scans and eliminates viruses and worms from HTTP, SMTP, POP3, IMAP, and FTP traffic without degrading network performance
- Provides complete network protection functionality: network-based antivirus, web content filtering, firewall, VPN, network-based intrusion detection and prevention, traffic shaping, and antispyam protection
- “Transparent mode” operation supports deployments for antivirus and content filtering in conjunction with existing firewall, VPN, intrusion detection and prevention, or other existing systems
- Reduces exposure to threats by detecting and preventing over 1300 different intrusions, including DoS and DDoS attacks
- VLAN and security zone support provides granular network segmentation into zones with independent security and access control policies
- Real-time system status monitoring lowers the total cost of ownership by providing an easy graphical view of CPU and memory utilization, network and session status, virus and intrusion detection
- Delivers superior performance and reliability from hardware accelerated, ASIC-based architecture and redundant, hot-swappable power supplies
- Automatically downloads the latest virus and attack database and can accept instant “push” updates from the FortiProtect Network
- Underlying FortiOS™ is ICSA-certified for Antivirus, Firewall, IPSec VPN and Intrusion Detection

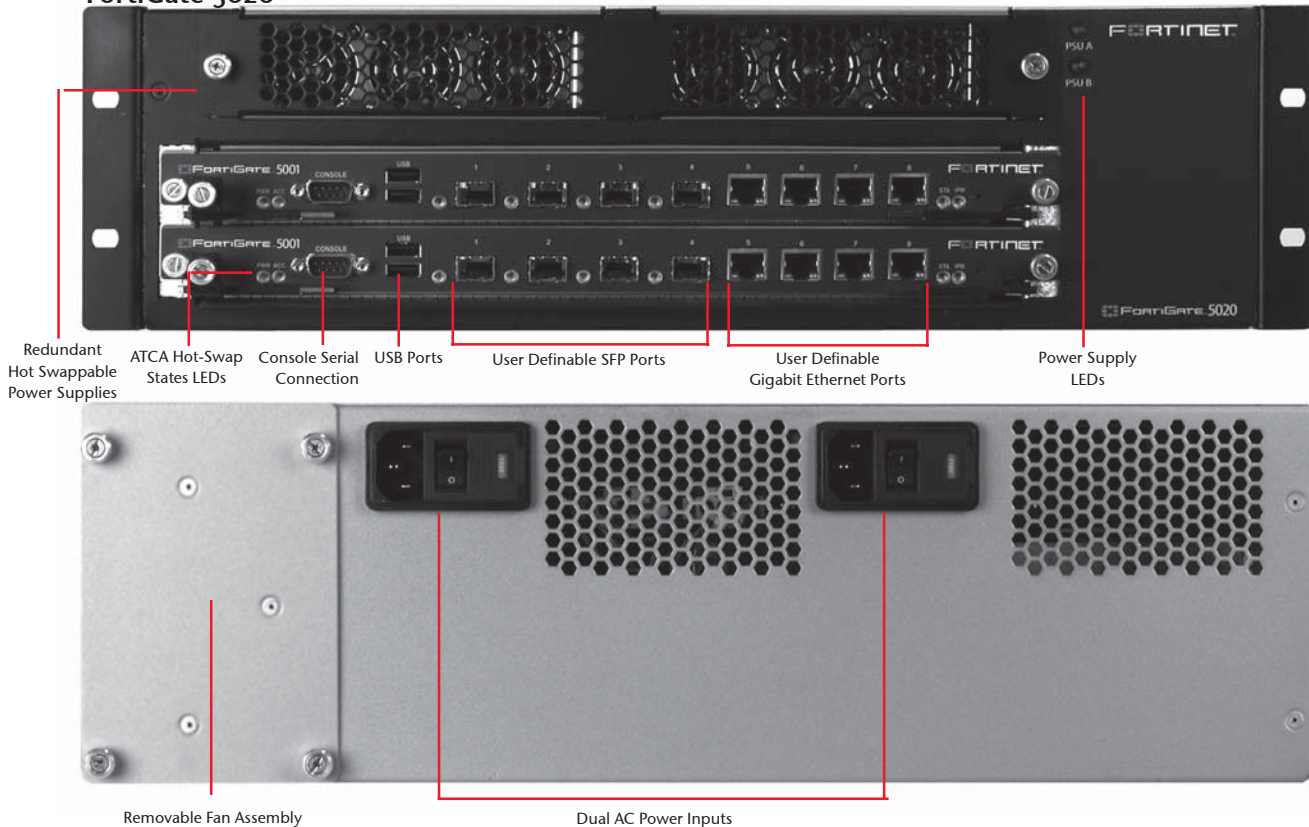
# FORTIGATE™ 5020

## Key Features & Benefits

Feature	Description	Benefit
<b>Network-based Antivirus</b> (ICSA Certified)	Detects and eliminates viruses and worms in real-time. Scans incoming and outgoing email attachments (SMTP, POP3, IMAP), HTTP and FTP traffic including web-based email, and encrypted VPN tunnels	Closes the vulnerability window by stopping viruses and worms before they enter the network
<b>Intrusion Detection and Prevention System (IPS)</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. Also supports FortiGuard policy-based URL filtering	Assures improved productivity for enterprise and regulatory compliance for CIPA-compliant educational institutions
<b>Firewall</b> (ICSA Certified)	Industry standard stateful inspection firewall	Certified protection, maximum performance and scalability
<b>VPN</b> (ICSA Certified)	Industry standard PPTP, L2TP, and IPSec VPN 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 FortiClient Host Security Software	Low cost, anytime, anywhere access for mobile and remote workers and telecommuters

## System Specifications

FortiGate-5020





**Specifications**

	FortiGate-5001 Blade	FortiGate-5020 System (2 blades)		FortiGate-5001 Blade	FortiGate-5020 System (2 blades)
<b>Interfaces</b>			Email notification of viruses and attacks	•	•
SFP Ports	4	8	VPN tunnel monitor	•	•
10/100/1000Base-T Ports	4	8			
<b>System Performance</b>			<b>High Availability (HA)</b>		
Concurrent sessions	1,000,000	2,000,000	Active-active/Active-passive HA	•	•
New sessions/second	25,000	50,000	Stateful failover	•	•
Firewall throughput (Gbps)	4Gbps	8Gbps	Device failure detection & notification	•	•
168-bit Triple-DES throughput (Mbps)	600	1.2Gbps	Link status monitor	•	•
Unlimited concurrent users	•	•	Link failover	•	•
Policies	50,000	100,000	<b>Networking</b>		
Schedules	256	512	Multiple WAN link support	•	•
<b>Antivirus, Worm Detection &amp; Removal</b>			Multi-zone support	•	•
Scans HTTP, FTP, SMTP, POP3, IMAP, and encrypted VPN Tunnels	•	•	Route between zones	•	•
Block by file size	•	•	Policy-based routing	•	•
<b>Firewall Modes</b>			<b>System Management</b>		
NAT, PAT, Transparent (bridge)	•	•	Console interface	•	•
Routing mode (RIP v1, v2)	•	•	WebUI (HTTPS)	•	•
Policy-based NAT	•	•	Multi-language support	•	•
VLAN tagging (802.1q)	•	•	Command line interface	•	•
Virtual Domains	Up to 250	Up to 250	Secure Command Shell (SSH)	•	•
User/Group based authentication	•	•	FortiManager System	•	•
H.323 NAT Traversal	•	•	<b>Administration</b>		
WINS Support	•	•	Role-based administration	•	•
<b>VPN</b>			Multiple administrators and user levels	•	•
PPTP, L2TP, and IPSec	•	•	Upgrades & changes via TFTP & WebUI	•	•
Dedicated tunnels	5000	10,000	System software rollback	•	•
Encryption (DES, 3DES, AES)	•	•	<b>User Authentication</b>		
SHA-1 / MD5 authentication	•	•	Internal database	•	•
PPTP, L2TP, VPN client pass though	•	•	External LDAP/RADIUS database support	•	•
Hub and Spoke VPN architecture	•	•	RSA SecurID	•	•
IKE certificate authentication (X.509)	•	•	Xauth over RADIUS support for IPSec VPN	•	•
IPSec NAT Traversal	•	•	IP/MAC address binding	•	•
Aggressive mode	•	•	<b>Traffic Management</b>		
Replay protection	•	•	DiffServ setting	•	•
Dead peer detection	•	•	Policy-based traffic shaping	•	•
Interoperability with major VPN vendors	•	•	Guaranteed/Maximum/Priority bandwidth	•	•
<b>Content Filtering</b>			<b>Dimensions</b>		
URL/keyword/phrase block	•	•	Height / Width / Length	5.25 inches, 17 inches, 15.5 inches	
URL Exempt List	•	•	Weight		35.5 lb (16.1 kg)
Content profiles	32	64	Rack Mountable		•
Blocks Java Applet, Cookies, Active X	•	•	<b>Power</b>		
FortiGuard™ web filtering support	•	•	AC input voltage		100 to 240VAC
<b>Dynamic Intrusion Detection and Prevention</b>			AC input current		10A
Intrusion prevention for over 1300 attacks	•	•	Frequency		47 to 63Hz
Automatic real-time updates from FortiProtect Network	•	•	Power Dissipation		800W max
Customizable detection signature list	•	•	<b>Environmental</b>		
<b>Anti-Spam</b>			Operating Temperature		32 to 104 °F (0 to 40 °C)
Real-time Blacklist/Open Relay Database Server	•	•	Storage Temperature		-13 to 158 °F (-25 to 70 °C)
MIME header check	•	•	Humidity		5 to 95% non-condensing
Keyword/phrase filtering	•	•	<b>Regulatory</b>		
IP address blacklist/exempt list	•	•	FCC Class A Part 15		•
<b>Logging/Monitoring</b>			CE		•
Log to remote Syslog/WELF server	•	•	UL		•
Graphical real-time and historical monitoring	•	•	ICSA Antivirus, Firewall, IPSec, and NIDS		•
SNMP	•	•			



### Australia

Level 17, 201 Miller Street  
North Sydney 2060  
Australia

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

### China

Cyber Tower, Suite B-903  
2 Zhongguancun Nan Ave.  
Hai Dian, 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

Kokusai Tameike Building 6F  
2-12-10 Akasaka, Minato-ku  
Tokyo 107-0052  
Japan

Tel: +81-3-5549-1640  
Fax: +81-3-5549-1641

### 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