

# 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

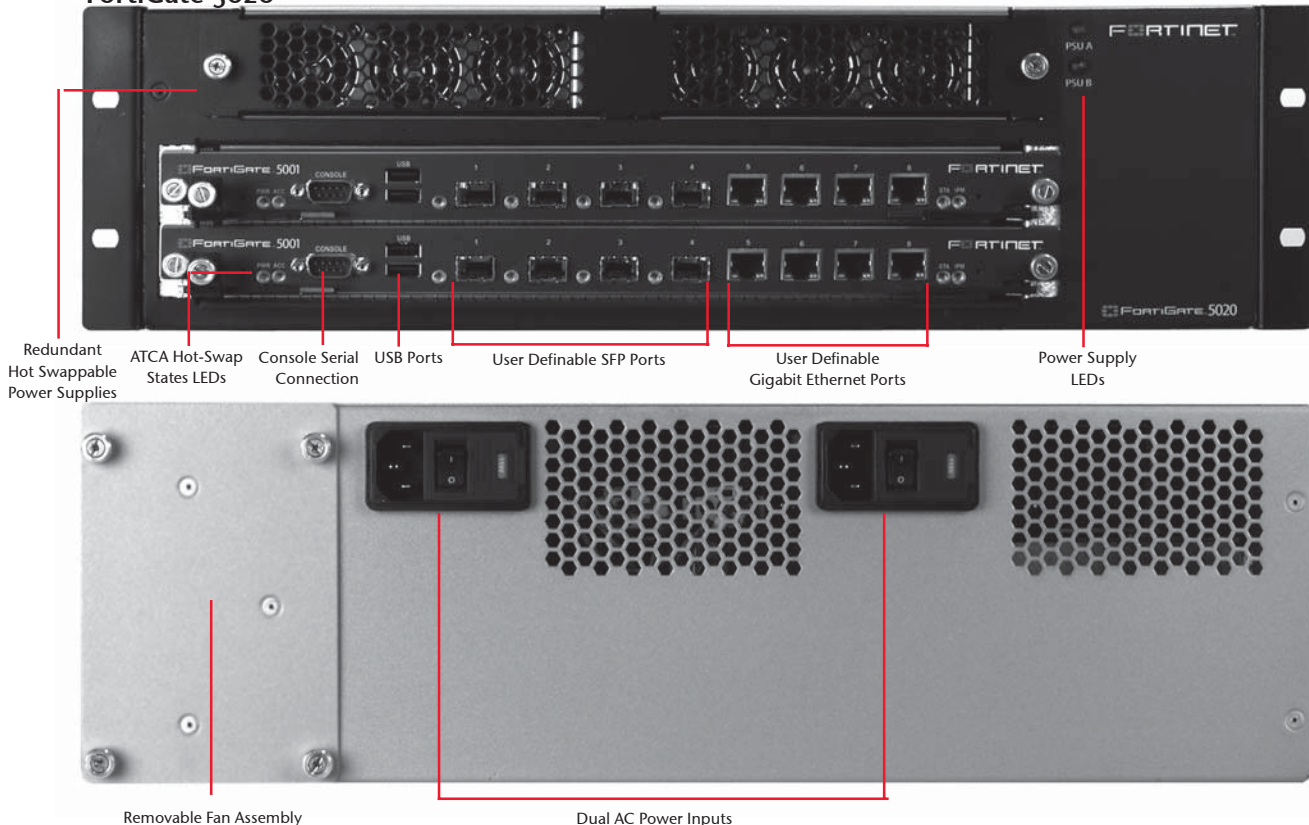
# FORTIGATE™ 5020

## 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



Redundant Hot Swappable Power Supplies | ATCA Hot-Swap States LEDs | Console Serial Connection | USB Ports | User Definable SFP Ports | User Definable Gigabit Ethernet Ports | Power Supply LEDs

Removable Fan Assembly | Dual AC Power Inputs



**Specifications**

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

**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