Real Time Network Protection for Large Enterprise and Service Providers

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-3000 Antivirus Firewall addresses the requirements for gigabit performance and exceptional reliability in large enterprise and service provider applications. Providing 3 gigabit-per-second interfaces, the FortiGate-3000 establishes new levels of price performance, and offers a complete array of antivirus, firewall, content filtering, VPN, network-based intrusion detection/prevention (IDP), and traffic shaping capabilities. The FortiGate-3000 deploys easily in existing networks and can be used for antivirus and content filtering only or can be deployed as a complete network protection solution. Highly available operation and redundant hot-swappable power supplies add to the robust reliability of the FortiGate-3000 to ensure non-stop operation. The FortiGate-3000 provides granular security with independent security zones and policies mapped to VLAN tags. The FortiGate-3000 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

- Ideal solution for Managed Security Service Providers (MSSPs) looking to add new security services
- Eliminates viruses and worms from email, file transfer, and real-time (Web) traffic without degrading network performance
- Provides complete network protection functionality: network-based antivirus, web content filtering, firewall, VPN, dynamic intrusion detection and prevention, traffic shaping, and anti-spam
- Front-panel LCD and keypad ease deployment by setting basic system parameters without an external console
- High availability operation supports transparent failover for mission-critical applications
- Reduces exposure to threats by detecting and preventing over 1300 different intrusions, including DoS and DDoS attacks
- Multi-zone support allows granular network segmentation into zones with independent security and access control policies
- 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™ operating system is ICSA-certified for Antivirus, Firewall, IPSec VPN and Intrusion Detection
- Virus quarantine enables easy submission of attack samples to the Fortinet Threat Response Team
- Easy to use and deploy – quick and easy configuration wizard walks administrators through initial setup with graphical user interface
Key Features & Benefits

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

System Specifications

FortiGate-3000

- Keypad and LCD Display
- User Definable 10/100 Ports Ports 1-3
- Gigabit Port (Copper)
- Gigabit Ports (Fiber)
- Power & Status Light
- Console Serial Connection
- Redundant Power Connections

REAL TIME NETWORK PROTECTION
### Specifications

**FortiGate-3000**

#### Interfaces
- 10/100 Ethernet Ports: 3
- 1000Base-SX Ports (Fiber): 2*
- 1000Base-T Ports (Copper): 1

#### System Performance
- Concurrent sessions: 975,000
- New sessions/second: 20,000
- Firewall throughput (Gbps): 2.25Gbps
- 168-bit Triple-DES throughput (Mbps): 530
- Unrestricted concurrent users: •
- Policies: 50,000
- Schedules: 256

#### Antivirus, Worm Detection & Removal
- Automatic virus database update from FortiProtect Network: •
- Scans HTTP, FTP, SMTP, POP3, IMAP, and encrypted VPN Tunnels: •
- Quarantine infected messages: •
- Block by file size: •

#### Firewall Modes
- NAT, PAT, Transparent (bridge): •
- Routing mode (RIP v1, v2): •
- VLAN tagging (802.1q): •
- Virtual domains: Up to 250
- User/user group based authentication: •
- H.323 NAT Traversal: •
- WINS support: •

#### VPN
- PPTP, L2TP, and IPSec: •
- Dedicated tunnels: 5000
- Encryption (DES, 3DES, AES): •
- SHA-1 / MDS authentication: •
- PPTP, L2TP, VPN client pass though: •
- Hub and Spoke VPN architecture: •
- IKE certificate authentication: •
- IPSec NAT Traversal: •
- Dead peer detection: •

#### Content Filtering
- URL/keyword/phrase block: •
- URL Exempt List: •
- Protection profiles: 32
- Blocks Java Applet, Cookies, Active X: •
- FortiGuard™ web filtering support: •

#### Anti-Spam
- Real-time Blacklist/Open Relay Database Server: •
- MIME header check: •
- Keyword/phrase filtering: •
- IP address blacklist/exempt list: •

#### Dynamic Intrusion Detection and Prevention
- Intrusion prevention for over 1300 attacks: •
- Detection and prevention on multiple Interfaces: •
- Customizable detection signature list: •
- Automatic real-time updates from the FortiProtect Network: •

#### Logging/Monitoring
- Internal logging: 20G
- Log to remote Syslog/WELF server: •
- Graphical real-time and historical monitoring: •

### Network Performance
- SNMP: •
- Email notification of viruses and attacks: •
- VPN tunnel monitor: •

#### High Availability (HA)
- Active-active/active-passive HA: •
- Stateful failover (FW and VPN): •
- Device failure detection & notification: •
- Redundant power supplies (hot-swappable): •
- Link status monitor: •

#### Networking
- Multiple WAN link support: •
- Route between zones: •
- Policy-based routing: •

#### System Management
- Console interface (RS-232): •
- WebUI (HTTPS): •
- Multi-language support: •
- Command line interface: •
- Secure Command Shell (SSH): •
- FortiManager System: •

#### Administration
- Role-based administration: •
- Multiple administrators and user levels: •
- Upgrades & changes via TFTP & WebUI: •
- System software rollback: •

#### User Authentication
- Internal database: •
- External LDAP/RADIUS database support: •
- RSA SecurID: •
- Xauth over RADIUS support for IPSec VPN: •
- IP/MAC address binding: •

#### Traffic Management
- DiffServ setting: •
- Guaranteed/maximum/priority bandwidth: •

#### Dimensions
- Height/Width/Length: 3.5 inches/16.75 inches/13.5 inches
- Weight: 17.5 lb (8 kg)
- Rack Mountable: •

#### Power
- AC input voltage: 100 to 240VAC
- AC input current: 6A
- Frequency: 50 to 60Hz
- Power Dissipation: 460W max

#### Environmental
- Operating Temperature: 32 to 104 °F (0 to 40 °C)
- Storage Temperature: -13 to 158 °F (-25 to 70 °C)
- Humidity: 5 to 95% non-condensing

#### Regulatory
- FCC Class A Part 15: •
- CSA/CUS: •
- CE: •
- UL: •
- ICSA Antivirus, Firewall, IPSec, and IDS: •

*Optional 1000Base-LX ports are available, please refer to model number FG-3000LX2/LX4 in the price list.