Blended Security Threats

Network security threats are devastating to enterprise networks. Intellectual property, revenue, customer and company records, and other mission-critical resources are at risk. Unfortunately enterprise networks often lack adequate security solutions much less the human resources to recognize the business risks – that is until the damage is already done. Point-products providing security solutions for specific purposes may provide adequate protection against specific single-threaded threats, however a new breed of blended-threats and attacks utilize a multitude of attack vectors. Furthermore assembling an array of point products is costly and requires significant expertise to engineer, maintain and manage. Most small to medium size businesses cannot afford such overhead, yet should tragedy strike the potential business costs are enormous. Fortunately cost-effective, evergreen multi-threat protection is now available to businesses of any size. The FortiGate®-200 through -800 series of advanced security systems integrate all-in-one multi-threat protection into cost-effective plug-n-play security platforms that effectively block today’s blended attacks including intrusion attempts, viruses, worms, phishing, spyware, spam and many other types of malware. The Fortinet FortiGuard® global 24x7 threat detection and update service provides the networking industry’s fastest response time to ensure latest security threats are detected and automatic security updates are available before your business is impacted.

Security Platforms That Meet the Challenge

FortiGate security platforms are based on Fortinet’s revolutionary FortiASIC™ Content Processor technology, which enables a comprehensive suite of real-time security solutions while delivering the highest levels of network performance. The FortiGate-200-800 series platforms provide a complete security solution including content inspection firewall, IPSEC and SSL VPN, intrusion prevention, Web filtering, antispy, anti-virus, anti-spyware, and IM and P2P controls that prevent blended attacks, as well as providing integrated traffic shaping functions, making them the most cost effective, convenient and powerful network protection solutions available. In addition, Fortinet’s per-device security subscriptions and turnkey appliance design makes them an affordable and easy-to-manage security solution for small-to-medium enterprises.

FortiNet’s Multi-Layered Security Solution

Fortinet’s multi-layered security solutions efficiently and economically provide an integrated set of security services in a single, easy-to-manage high-performance appliance that is capable of supporting a wide range of deployment scenarios. In addition, FortiGuard Subscription Services include everything from technical support, antivirus updates, antispyware, antispy, and Web content filtering to ensure that your security environment remains current and your corporate resources are protected against the latest blended threats. FortiGate systems come with a one-year limited hardware warranty and 90-day limited software warranty.
Fortinet’s family of mid-range security appliances are designed for mid-size enterprise networks.

Secure Web Access
Firewall + Antivirus + Web Filtering

The primary source of threats to the Enterprise network is undoubtedly from uncontrolled employee access to the Internet and Web-based services. Yet today every business not only relies on the Internet for productivity enhancements and competitive advantage, but literally depends on the Internet for business success. With all the benefits of the Internet, also come potential risks such as viruses and worms that disrupt services or destroy valuable data, and a myriad of security challenges including information theft/leakage, inappropriate usage and the need to comply with regulatory mandates. The FortiGate-200-800 series of mid-range security appliances provide a turn-key suite of ICSA Labs certified multi-layered security applications to stop blended attacks from affecting your business.

Secure Perimeter Access
Firewall + VPN+ Intrusion Prevention + Antivirus

Enterprises often have complex network topologies and, therefore, complex network security requirements. Typical deployments mean linking several sites together—ranging from home offices to larger remote offices—and ensuring that the security implementation is seamless. Security devices for these environments need to provide a wide variety of performance metrics and connectivity options. Fortinet’s line of mid-range security appliances offer integrated 4-port switches, 10/100/1000 Ethernet ports, up to 1 Gbps firewall throughput, and up to 200 Mbps 3DES VPN throughput. These options include the full security suite of ICSA Labs certified multi-layered security applications to stop blended attacks from affecting your enterprise’s productivity.

Secure Messaging Access
Antispam + Antivirus + IM / P2P Controls

The FortiGate line of security appliances has a flexible architecture that allows each one to quickly adapt to emerging technologies and threats such as IM, P2P, and VOIP applications and identity theft methods such as spyware, phishing, and pharming attacks. Flexible deployment options such as NAT, Route, and Transparent modes allow FortiGate devices to be easily deployed into most network designs. Core networking features, such as High Availability (HA) and support for dynamic routing protocols like RIP, OSPF, and BGP, allow them to be deployed into complex full mesh network environments that require maximum network availability.
**Technical Specifications**

**HARDWARE SPECIFICATIONS**

<table>
<thead>
<tr>
<th></th>
<th>FortiGate-200A</th>
<th>FortiGate-224B</th>
<th>FortiGate-300A</th>
<th>FortiGate-400A</th>
<th>FortiGate-500A</th>
<th>FortiGate-800/800F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total 10/100 Interfaces</td>
<td>8</td>
<td>26</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>Configurable Ports</td>
<td>n/a</td>
<td>n/a</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Switch Interfaces</td>
<td>4</td>
<td>24</td>
<td>n/a</td>
<td>n/a</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Fixed WAN / DMZ Ports</td>
<td>2/2</td>
<td>2</td>
<td>n/a</td>
<td>n/a</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Total 10/100/1000 Interfaces (Copper)</td>
<td>n/a</td>
<td>2 (switched)</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4 (FG-800 only)</td>
</tr>
<tr>
<td>1Gb SFP Interfaces (Fiber)*</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

* SX transceivers are standard; LX transceivers are available as an additional option.

**SYSTEM PERFORMANCE**

<table>
<thead>
<tr>
<th></th>
<th>FortiGate-200A</th>
<th>FortiGate-224B</th>
<th>FortiGate-300A</th>
<th>FortiGate-400A</th>
<th>FortiGate-500A</th>
<th>FortiGate-800/800F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Throughput</td>
<td>150 Mbps</td>
<td>150 Mbps</td>
<td>400 Mbps</td>
<td>500 Mbps</td>
<td>600 Mbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>VPN 3DES Throughput</td>
<td>70 Mbps</td>
<td>70 Mbps</td>
<td>120 Mbps</td>
<td>140 Mbps</td>
<td>150 Mbps</td>
<td>150 Mbps</td>
</tr>
<tr>
<td>Antivirus Throughput</td>
<td>30 Mbps</td>
<td>30 Mbps</td>
<td>70 Mbps</td>
<td>100 Mbps</td>
<td>120 Mbps</td>
<td>150 Mbps</td>
</tr>
<tr>
<td>IPS Throughput</td>
<td>100 Mbps</td>
<td>100 Mbps</td>
<td>200 Mbps</td>
<td>300 Mbps</td>
<td>400 Mbps</td>
<td>600 Mbps</td>
</tr>
<tr>
<td>Dedicated IPSec VPN Tunnels</td>
<td>200</td>
<td>200</td>
<td>1,500</td>
<td>2,000</td>
<td>3,000</td>
<td>3,000</td>
</tr>
<tr>
<td>Unlimited User Licenses</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Concurrent Sessions</td>
<td>400,000</td>
<td>400,000</td>
<td>400,000</td>
<td>400,000</td>
<td>400,000</td>
<td>400,000</td>
</tr>
<tr>
<td>New Sessions/Second</td>
<td>4K</td>
<td>4K</td>
<td>10K</td>
<td>10K</td>
<td>10K</td>
<td>10K</td>
</tr>
<tr>
<td>Policies</td>
<td>2,000</td>
<td>2,000</td>
<td>5,000</td>
<td>5,000</td>
<td>8,000</td>
<td>20,000</td>
</tr>
</tbody>
</table>

* Antivirus performance is measured based on HTTP traffic with 32Kbyte file attachments and IPS performance is measured base on UDP traffic with 512 byte packet size.

**DIMENSIONS**

<table>
<thead>
<tr>
<th></th>
<th>FortiGate-200A</th>
<th>FortiGate-224B</th>
<th>FortiGate-300A</th>
<th>FortiGate-400A</th>
<th>FortiGate-500A</th>
<th>FortiGate-800/800F</th>
</tr>
</thead>
<tbody>
<tr>
<td>(H, W, L, weight)</td>
<td>1.75 inches</td>
<td>1.75 inches</td>
<td>1.75 inches</td>
<td>1.75 inches</td>
<td>1.75 inches</td>
<td>1.75 inches</td>
</tr>
<tr>
<td></td>
<td>1.6 inches</td>
<td>1.6 inches</td>
<td>1.6 inches</td>
<td>1.6 inches</td>
<td>1.6 inches</td>
<td>1.6 inches</td>
</tr>
<tr>
<td></td>
<td>10 inches</td>
<td>10 inches</td>
<td>10 inches</td>
<td>10 inches</td>
<td>10 inches</td>
<td>10 inches</td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rack Mountable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**AC POWER REQUIRED**

<table>
<thead>
<tr>
<th></th>
<th>100-240 VAC, 50-60 Hz, 8.0 Amp (Max)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100W</td>
<td>110W</td>
</tr>
<tr>
<td>120W</td>
<td>130W</td>
</tr>
<tr>
<td>140W</td>
<td>100W</td>
</tr>
</tbody>
</table>

**ENVIRONMENTAL**

- Operating temperature: 32 to 104 deg F (0 to 40 deg C)
- Storage temperature: -13 to 158 deg F (-25 to 70 deg C)
- Humidity: 5 to 95% non-condensing

**COMPLIANCE**

- FCC Class A Part 15, UL/CUL, C Tick, CE, VCCI

**CERTIFICATIONS**

- ICSA Labs: Firewall, IPsec, SSL, Antivirus, IPS

*(Please contact your Fortinet Sales Representative for a complete list of product certifications)*

---

**Fortinet Unified Security Solutions**

- **All-inclusive, cost-effective security solution**: Fortinet offers a lower total cost of ownership with the most complete set of functions including: antivirus, intrusion prevention, antispyware, web content filtering, and antispam

- **Automated updates of antivirus/antispyware and IPS security content**: Around-the-clock protection against the latest threats. Virus and intrusion encyclopedia covers more than 60,000 different threats

- **High performance custom hardware**: The Fortinet FortiASIC delivers superior performance and reliability, ensuring that the security appliance does not become a network bottleneck

- **Integrated multi-port switch**: Eliminates the need for external switches and provides enhanced connectivity options

- **Secure Web UI for easy deployment and management**: Quick and easy configuration wizard walks administrators through initial setup and graphical user interface offers at-a-glance security event and performance monitoring

- **Security hardened custom Operating System (OS)**: Underlying FortiOS™ is ICSA Labs-certified and offers a comprehensive command-line interface

**Fortinet’s ASIC-Based Advantage**

FortiASIC is the foundation of Fortinet’s unique hardware technology. FortiASIC is a family of purpose built, high-performance network and content processors that uses an intelligent proprietary content scanning engine and multi-algorithms to accelerate compute-intensive security services. FortiASIC provides the performance required to deliver enterprise and carriers-class UTM services. Coupled with the FortiOS security hardened Operating System, FortiASIC delivers extreme performance and security.

**FortiOS: Developed for Security**

FortiOS is the software foundation of FortiGate multi-threat security platforms. Developed solely for security, performance and reliability, it is a purpose-built operating system that leverages power of the the FortiASIC content and network processors. FortiOS enables a comprehensive suite of security services – content inspection firewall, IPS, antivirus, web filtering, antispam, IM/P2P, virtual network security and bandwidth shaping. FortiOS is a complete suite of UTM security services and is certified for Common Criteria EAL 4+.
FortiGate-200-800 Series

FortiGate-200-800-series platforms provide the following security features:

**FIREWALL**
- ICSA Labs Certified (Enterprise Firewall)
- NAT, PAT, Transparent (Bridge)
- Routing Mode (RIP v1 & v2, OSPF, BGP, & Multicast)
- Policy-Based NAT
- Virtual Domains (NAT/Transparent mode)
- VLAN Tagging (802.1Q)
- User Group-Based Authentication
- SIP/H.323 NAT Traversal
- WINS Support
- Customized Protection Profiles

**VIRTUAL PRIVATE NETWORK (VPN)**
- ICSA Labs Certified (IPSec & SSL)
- PPTP, IPSec, and SSL
- Dedicated Tunnels
- DES, 3DES, and AES Encryption Support
- SHA-1/MD5S Authentication
- PPTP, L2TP, VPN Client Pass Through
- IKE Certificate Authentication
- IPSec NAT Traversal
- Dead Peer Detection
- RSA SecurID Support

**INTRUSION PREVENTION SYSTEM (IPS)**
- ICSA Labs Certified (NIPS)
- Protection From Over 3000 Threats
- Protocol Anomaly Support
- Custom Signature Support
- Automatic Attack Database Update

**ANTIVIRUS**
- ICSA Labs Certified (Gateway Antivirus)
- Includes AntiSpyware and Worm Prevention
- HTTP/SMTP/POP3/IMAP/FTP/IM and Encrypted VPN Tunnels
- Automatic “Push” Virus Database Update
- File Quaranline Support
- Block by File Size or Type

**WEB FILTERING**
- URL/Keyword/Phrase Block
- URL Exempt List
- Content Profiles
- Blocks Java Applet, Cookies, Active X
- FortiWeb Guard Filtering Support

**ANTISPAM**
- Real-Time Blacklist/Open Relay Database Server
- MIME Header Check
- Keyword/Phrase Filtering
- IP Address Blacklist/Exempt List
- Automatic Real-Time Updates From FortiGuard Network

**TRAFFIC SHAPING**
- Policy-based Traffic Shaping
- Differentiated Services (DiffServ) Support
- Guarantee/Max/Priority Bandwidth

**NETWORKING/ROUTING**
- Multiple WAN Link Support
- PPPoE Support
- DHCP Client/Server
- Policy-Based Routing
- Dynamic Routing (RIP v1 & v2, OSPF, BGP, & Multicast)
- Multi-Zone Support with Routing Between Zones
- Route Between Virtual LANs (VDOMs)

**MANAGEMENT/ADMINISTRATION OPTIONS**
- Console Interface (RS-232)
- WebUI (HTTP/HTTPS) and Command Line Interface
- Telnet / Secure Command Shell (SSH)
- Role-Based Administration
- Multi-language Support
- Support for Customized Attacks and User Levels
- Upgrades and Changes Via FTP and WebUI System Software Rollback
- Central Management via FortiManager (optional)

**LOGGING/MONITORING**
- Internal Logging
- Log to Remote Syslog/WELF server
- Graphical Real-Time and Historical Monitoring
- SNMP
- Email Notification of Viruses And Attacks
- VPN Tunnel Monitor
- Optional FortiAnalyzer Logging

**USER AUTHENTICATION OPTIONS**
- Local Database
- Windows Active Directory (AD) Integration
- External RADIUS/LDAP Integration
- IP/MAC Address Binding
- Xauth over RADIUS for IPSec VPN
- RSA SecurID Support

**VIRTUAL DOMAINS (VDOMs)**
- Separate Firewall/Routing domains
- Separate Administrative domains
- Separate VLAN interfaces
- 10 VDOMs (standard)

**HIGH AVAILABILITY (HA)**
- Active-Active, Active-Passive
- Stateful Failover (FW and VPN)
- Device Failure Detection and Notification
- Link Status Monitor
- Link failover

**INSTANT MESSENGER / PEER-TO-PEER ACCESS CONTROL**
- AOL IM, Yahoo, MSN
- ICQ
- Gnutella
- BitTorrent
- WinNY
- Skype
- eDonkey
- KaZaa

FortiGuard Security Subscription Services

With FortiGuard Security Subscription services enabled, customers can rest assured that their Fortinet security platforms are performing optimally and protecting their corporate assets with the latest security intelligence. FortiGuard services deliver the latest security content directly to Fortinet products. Fortinet offers four standard subscription services: Antivirus, Intrusion Prevention, Web Filtering and Antispam services to protect against multiple types of new and emerging threats. FortiGuard services are updated by the Fortinet Global Threat Research Team, a team of experts working around the clock and around the world to keep Fortinet customers secure. The Fortinet Global Threat Research Team enables Fortinet to deliver comprehensive multi-threat protection, including zero-day protection from new and emerging threats. The FortiGuard Network is a network of global data centers that automatically deliver updates quickly and reliably to Fortinet products.

For customers requiring guaranteed response time to suspicious malware threats, Fortinet offers a premier version of the FortiGuard Antivirus Security Subscription service. Along with Service Level Agreements (SLAs), the premier service provides the customer with a direct conduit to the Fortinet Global Threat Research Team.

Fortinet also offers a premier version of the FortiGuard Web Filtering Security Subscription service. This higher-tier service offering includes guaranteed SLAs and a larger quota for rating URLs submitted to the Fortinet Global Threat Research Team.

FortiCare Support Services

- 24/7/365 FortiCare Web-based support
- Technical account management service available
- 8x5 telephone-based technical support (24x7 - optional)
- Professional services available
- 1-Year limited hardware warranty
- 90-day limited software warranty

©2006-2008 Fortinet, Inc. All rights reserved. Fortinet, Fortigate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are trademarks or registered trademarks of the Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600. Although Fortinet has attempted to provide accurate information in these materials, Fortinet assumes no legal responsibility for the accuracy or completeness of the information. Please note that no Fortinet statements herein constitute or contain any guarantee, warranty or legally binding representation. All materials contained in this publication are subject to change without notice, and Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice.