Complex Security Threats are Driving Consolidation

The evolution of network security threats is driving the consolidation of multiple threat recognition systems into a single appliance. FortiGate consolidated security appliances from Fortinet integrate essential security and networking functions into a single device to identify and stop multiple threats effectively and efficiently. Never before has so much security functionality been consolidated into a single high-performance appliance at such a low total cost of ownership.

Hardware-Accelerated Performance with High Port Density

The FortiGate-1240B appliance raises the bar for network security devices by integrating purpose-built FortiASIC™ processors. The FortiASIC Network Processor accelerates thirty-eight of forty total ports on the system to switching speeds, allowing networks to enforce firewall policies between network segmentation points for layered security with switch-like performance. In addition, the FortiASIC Content Processor provides acceleration for content intensive security technologies such as intrusion prevention (IPS) and antivirus scanning.

Advanced Mezzanine Card (AMC) and Fortinet Storage Module (FSM) expansion slots provide the option to add even more ASIC-accelerated ports for additional throughput, or disk-based storage for local logging and content archiving. Numerous accelerated security interfaces allow organizations to create multiple security zones for various departments, users, access methods, and even devices to enforce network security at switching speeds.

FortiOS The World’s Most Advanced Security Operating System

FortiOS provides high performance, ultra low latency multi-threat security by leveraging the hardware acceleration provided by purpose-built FortiASIC processors. This combination of custom hardware and software gives you the best security and performance possible from a single device. FortiOS allows greater traffic visibility and more consistent, granular control over users, applications and sensitive data.

The FortiASIC Advantage

FortiASIC processors power FortiGate platforms. With exclusive hardware, the purpose built, high-performance Network, Security, and Content processors use intelligent and proprietary digital engines to accelerate resource-intensive security services.

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consolidated Security Architecture</td>
<td>FortiGate consolidated security offers better protection and lower cost of ownership than multiple point security products</td>
</tr>
<tr>
<td>Hardware Accelerated Performance</td>
<td>FortiASIC processors provide assurance that the security device will not become a bottleneck in the network</td>
</tr>
<tr>
<td>High Port Density</td>
<td>Forty total ports (standard) facilitate numerous internal segmentation points throughout the network</td>
</tr>
<tr>
<td>Modular Expansion</td>
<td>AMC and FSM slots provide greater flexibility by supporting additional hardware-accelerated ports and localized storage of event data</td>
</tr>
<tr>
<td>Centralized Management</td>
<td>FortiManager and FortiAnalyzer centralized management and reporting appliances simplify deployment, monitoring, and maintenance of your security infrastructure</td>
</tr>
</tbody>
</table>
Intrusion Prevention
IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection which alerts users to any traffic that matches attack behavior profiles. The Fortinet threat research team analyzes suspicious behavior, identifies and classifies emerging threats, and generate new signatures to include with FortiGuard Service updates.

Features
- Automatic Database Updates
- Protocol Anomaly Support
- IPS and DoS Prevention Sensor
- Custom Signature Support
- IPv6 Support

IPS Throughput
- Base Unit: 5 Gbps
- With AMC: 8 Gbps

Antivirus / Antispyware
Antivirus content inspection technology protects against viruses, spyware, worms, and other forms of malware which can infect network infrastructure and endpoint devices. By intercepting and inspecting application-based traffic and content, antivirus protection ensures that malicious threats hidden within legitimate application content are identified and removed from data streams before they can cause damage. FortiGuard subscription services ensure that FortiGate devices are updated with the latest malware signatures for high levels of detection and mitigation.

Features
- Automatic Database Updates
- Proxy-based Antivirus
- Flow-based Antivirus
- File Quarantine
- IPv6 Support

Antivirus Performance
- Proxy-based: 1.2 Gbps
- Flow-based: 1.6 Gbps

Firewall
Fortinet firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features. Application control, antivirus, IPS, Web filtering and VPN, along with advanced features such as an extreme threat database, vulnerability management and flow-based inspection work in concert to identify and mitigate the latest complex security threats. The security-hardened FortiOS operating system works together with purpose-built FortiASIC processors to accelerate inspection throughput and identification of malware.

Features
- NAT, PAT and Transparent (Bridge)
- Policy-Based NAT
- SIP/H.323/SCCP NAT Traversal
- VLAN Tagging (802.1Q)
- Vulnerability Management
- IPv6 Support

Firewall Throughput
<table>
<thead>
<tr>
<th></th>
<th>Base Unit</th>
<th>With AMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1518 Byte Packets</td>
<td>40 Gbps</td>
<td>44 Gbps</td>
</tr>
<tr>
<td>512 Byte Packets</td>
<td>40 Gbps</td>
<td>44 Gbps</td>
</tr>
<tr>
<td>64 Byte Packets</td>
<td>38 Gbps</td>
<td>42 Gbps</td>
</tr>
</tbody>
</table>

VPN
Fortinet VPN technology provides secure communications between multiple networks and hosts, using SSL and IPsec VPN technologies. Both services leverage our custom FortiASIC processors to provide acceleration in the encryption and decryption steps. The FortiGate VPN service enforces complete content inspection and multi-threat protections including antivirus, intrusion prevention and Web filtering. Traffic optimization provides prioritization for critical communications traversing VPN tunnels.

Features
- IPSec and SSL VPN
- DES, 3DES, AES and SHA-1/MD5 Authentication
- PPTP, L2TP, VPN Client Pass Through
- SSL Single Sign-On Bookmarks
- Two-Factor Authentication

VPN Performance
<table>
<thead>
<tr>
<th></th>
<th>Base Unit</th>
<th>With AMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec VPN Throughput</td>
<td>16 Gbps</td>
<td>18.5 Gbps</td>
</tr>
<tr>
<td>Concurrent SSL VPN Users</td>
<td>37 Gbps</td>
<td>370 Mbps</td>
</tr>
<tr>
<td>Recommended (Max)</td>
<td>1,500</td>
<td></td>
</tr>
<tr>
<td>Client-to-Gateway IP/Sec VPN Tunnels</td>
<td>50,000</td>
<td></td>
</tr>
</tbody>
</table>

Antivirus / Antispyware

Features
- Automatic Database Updates
- Proxy-based Antivirus
- Flow-based Antivirus
- File Quarantine
- IPv6 Support

Antivirus Performance
- Proxy-based: 1.2 Gbps
- Flow-based: 1.6 Gbps
SSL-Encrypted Traffic Inspection
SSL-encrypted traffic inspection protects endpoint clients and Web and application servers from hidden threats. SSL Inspection intercepts encrypted traffic and inspects it for threats prior to routing it to its final destination. It can be applied to client-oriented SSL traffic, such as users connecting to cloud-based CRM site, and to inbound Web and application server traffic. SSL inspection enables you to enforce appropriate use policies on encrypted Web content and to protect servers from threats which may be hidden inside encrypted traffic flows.

Features
- Protocol support: HTTPS, SMTPS, POP3S, IMAPS
- Inspection support: Antivirus, Web Filtering, Antispam, Data Loss Prevention, SSL Offload

Endpoint NAC
Endpoint NAC can enforce the use of FortiClient Endpoint Security for users connecting to corporate networks. Endpoint NAC verifies FortiClient Endpoint Security installation, firewall operation and up-to-date antivirus signatures before allowing network access. Non-compliant endpoints, such as endpoints running applications that violate security policies can be quarantined or sent to remediation.

Features
- Monitor & Control Hosts Running FortiClient
- Vulnerability Scanning of Network Nodes
- Quarantine Portal
- Application Detection and Control
- Built-in Application Database

Web Filtering
Web filtering protects endpoints, networks and sensitive information against Web-based threats by preventing users from accessing known phishing sites and sources of malware. In addition, administrators can enforce policies based on Website categories to easily prevent users from accessing inappropriate content and clogging networks with unwanted traffic.

Features
- HTTP/HTTPS Filtering
- URL / Keyword / Phrase Block
- Blocks Java Applet, Cookies or Active X
- MIME Content Header Filtering
- Flow-based Web Filtering
- IPv6 Support

Data Loss Prevention
DLP uses a sophisticated pattern-matching engine to identify and prevent the transfer of sensitive information outside of your network perimeter, even when applications encrypt their communications. In addition to protecting your organization’s critical data, Fortinet DLP provides audit trails to aid in policy compliance. You can select from a wide range of configurable actions to log, block, and archive data, and quarantine or ban users.

Features
- Identification and Control Over Data in Motion
- Built-in Pattern Database
- RegEx Based Matching Engine
- Common File Format Inspection
- International Character Sets Supported
- Flow-based DLP

Logging, Reporting and Monitoring
FortiGate consolidated security appliances provide extensive logging capabilities for traffic, system, and network protection functions. They also allow you to assemble drill-down and graphical reports from detailed log information. Reports can provide historical and current analysis of network activity to aid with identification of security issues and to prevent network misuse and abuse.

Features
- Internal Log storage and Report Generation
- Graphical Real-Time and Historical Monitoring
- Graphical Report Scheduling Support
- Graphical Drill-down Charts
- Optional FortiAnalyzer Logging (including per VDOM)
- Optional FortiGuard Analysis and Management Service
High Availability

High Availability (HA) configurations enhance reliability and increase performance by clustering multiple FortiGate appliances into a single entity. FortiGate High Availability supports Active-Active and Active-Passive options to provide maximum flexibility for utilizing each member within the HA cluster. The HA feature is included as part of the FortiOS operation system and is available with most FortiGate appliances.

Features

- Active-Active and Active-Passive
- Stateful Failover (FW and VPN)
- Link State Monitor and Failover
- Device Failure Detection and Notification
- Server Load Balancing

Virtual Domains

Virtual Domains (VDOMs) enable a single FortiGate system to function as multiple independent virtual FortiGate systems. Each VDOM contains its own virtual interfaces, security profiles, routing table, administration, and many other features. FortiGate VDOMs reduce the complexity of securing disparate networks by virtualizing security resources on the FortiGate platform, greatly reducing the power and footprint required as compared to multiple point products. Ideal for large enterprise and managed service providers.

Features

- Separate Firewall / Routing Domains
- Separate Administrative Domains
- Separate VLAN Interfaces
- Maximum VDOMs: 250
- Default VDOMs: 10

Application Control

Application control enables you to define and enforce policies for thousands of applications running across networks regardless of port or the protocol used for communication. The explosion of new Internet-based and Web 2.0 applications bombarding networks today make application control essential, as most application traffic looks like normal Web traffic to traditional firewalls. Fortinet application control provides granular control of applications along with traffic shaping capabilities and flow-based inspection options.

Features

- Identify and Control Over 1,800 Applications
- Traffic Shaping (Per Application)
- Control Popular Apps Regardless of Port or Protocol
- Popular Applications include:
  - AOL-IM
  - Yahoo
  - MSN
  - KaZaa
  - ICQ
  - Gnutella
  - BitTorrent
  - MySpace
  - WinNY
  - Skype
  - eDonkey
  - Facebook
  - and more...

Setup / Configuration Options

Fortinet provides administrators with a variety of methods and wizards for configuring FortiGate appliances during deployment. From the easy-to-use Web-based interface to the advanced capabilities of the command-line interface, FortiGate systems offer the flexibility and simplicity you need.

Features

- Web-based User Interface
- Command Line Interface (CLI) Over Serial Connection
- Pre-configured Settings from USB Drive

Wireless Controller

All FortiGate and FortiWiFi™ consolidated security platforms have an integrated wireless controller, enabling centralized management of FortiAP™ secure access points and wireless LANs. Unauthorized wireless traffic is blocked, while allowed traffic is subject to identity-aware firewall policies and multi-threat security inspection. From a single console you can control network access, update security policies, and enable automatic identification and suppression of rogue access points.

Features

- Unified WiFi and Access Point Management
- Automatic Provisioning of APs
- On-wire Detection and Blocking of Rogue APs
- Supports Virtual APs with Different SSIDs
- Supports Multiple Authentication Methods
### Technical Specifications | FortiGate-1240B
---|---
**HARDWARE**
Total Network Interfaces | 40
Hardware Accelerated GbE SFP Interfaces | 24
Hardware Accelerated 10/100/1000 Interfaces | 14
Non-Accelerated 10/100/1000 Interfaces | 2
Advanced Mezzanine Card (AMC) Expansion Slots | 1 Single Width
Fortinet Storage Module (FSM) Expansion Slots | 6
Local Storage Included | 1 FSM-064 (64 GB SSD)

**SYSTEM PERFORMANCE**
Firewall Throughput (1518 / 512 / 64 byte UDP packets) | 40 / 40 / 38 Gbps - 44 / 44 / 42 Gbps *
Firewall Latency (64 byte UDP packets) | 7 μs
Firewall Throughput (packets Per Second) | 57 - 63 Mpps *
Concurrent Sessions (TCP) | 5 Million
New Sessions/Sec (TCP) | 120,000
Firewall Policies | 100,000
IPSec VPN Throughput (512 byte packets) | 16 - 18.5 Gbps *
Gateway-to-Gateway IPSec VPN Tunnels | 10,000
Client-to-Gateway IPSec VPN Tunnels | 50,000
SSL-VPN Throughput | 370 Mbps
Concurrent SSL-VPN Users (Recommended Max) | 1,500
IPS Throughput | 5 - 8 Gbps *
Antivirus Throughput (Proxy Based / Flow Based) | 1.2 / 1.6 Gbps
Virtual Domains (Default / Max) | 10 / 250
Max Number of FortiAPs | 512
Max Number of FortiTokens | 5,000
Max Number of Registered FortiClients | 8,000
High Availability Configurations | Active/Active, Active/Passive, Clustering
Unlimited User Licenses | Yes

### Technical Specifications | FortiGate-1240B
---|---
**DIMENSIONS AND POWER**
Height x Width x Length | 3.5 x 17.3 x 21 in (88.7 x 439 x 530 mm)
Weight | 36 lb (16.4 Kg)
Rack Mountable | Yes
AC Power (FG-1240B) | 100 – 240 VAC, 50 – 60 Hz 6.3 Amp (Max)
Power Consumption (AVG / Max) | 263.2 / 342 W
Heat Dissipation | 1,167 BTU/h
DC Power (FG-1240B-DC Required) | -48V DC (Normal)
Redundant Power Supplies (Hot-swappable) | Yes

**ENVIRONMENT AND CERTIFICATIONS**
Operating Temperature | 32 – 104 deg F (0 – 40 deg C)
Storage Temperature | -13 – 158 deg F (-35 – 70 deg C)
Humidity | 20 to 90% non-condensing
Compliance | FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certification | ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN

Note: All performance values are “up to” and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files. * Higher performance figures achieved with AMC module installed.

**FortiGuard® Security Subscription Services** deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispyware, vulnerability and compliance management, application control, and database security services.

**FortiCare™ Support Services** provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with return and replace hardware support or 24x7 Comprehensive Support with advanced hardware replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and a 90-day limited software warranty.

---

**GLOBAL HEADQUARTERS**
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

**EMEA SALES OFFICE – FRANCE**
Fortinet Incorporated
120 rue Albert Caquot
06660, Sophia Antipolis, France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

**APAC SALES OFFICE – SINGAPORE**
Fortinet Incorporated
300 Beach Road #20-01
The Concourse, Singapore 199555
Tel: +65-6513-3734
Fax: +65-6295-0015

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard® are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.