DATASHEET

FortiGate®-1240B

Consolidated Security Appliance

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 4.0 Software Redefines Networks Security

FortiOS 4.0 is a purpose-built operating system that leverages the power of specialized FortiASIC processors to offer increased levels of security and performance. Fortinet developed FortiOS 4.0 software solely for the FortiGate consolidated security platform. FortiOS software enables a comprehensive suite of security services – firewall, VPN, intrusion prevention, anti-malware, antispam, Web filtering, application control, data loss prevention, vulnerability management, and endpoint network access control.

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.

Features	Benefits
Consolidated Security Architecture	FortiGate consolidated security offers better protection and lower cost of ownership than multiple point security products
Hardware Accelerated Performance	FortiASIC processors provide assurance that the security device will not become a bottleneck in the network
High Port Density	Forty total ports (standard) facilitate numerous internal segmentation points throughout the network
Modular Expansion	AMC and FSM slots provide greater flexibility by supporting additional hardware-accelerated ports and localized storage of event data
Centralized Management	FortiManager and FortiAnalyzer centralized management and reporting appliances simplify deployment, monitoring, and maintenance of your security infrastructure

FortiOS 4.0 Software—Raising The Bar

FortiOS 4.0: Redefining Network Security

FortiOS 4.0 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 the power of FortiASIC processors.

Fortinet's ASIC-Based Advantage

FortiASICs are a family of purpose-built, high performance processors that use an intelligent proprietary content scanning engine and multiple algorithms to accelerate security and network services.

FortiOS Security Services

FIREWALL
- ICSA Labs Certified (Enterprise Firewall)
- NAT, PAT, Transparent (Bridge)
- Routing Mode (RIP, OSPF, BGP, Multicast)
- Policy-Based NAT
- Virtual Domains (NAT/Transparent mode)
- VLAN Tagging (802.1Q)
- Group-Based Authentication & Scheduling
- SIP/H.323 /SCCP NAT Traversal
- WINS Support
- Explicit Proxy Support (Citrix/TS etc.)
- VoIP Security (SIP Firewall/RTP Pinholing)
- Granular Per-Policy Protection Profiles
- Identity/Application-Based Policy
- Vulnerability Management
- IPv6 Support (NAT/Transparent mode)

VIRTUAL PRIVATE NETWORK (VPN)
- ICSA Labs Certified (IPSec)
- PPTP, IPSec, and SSL Dedicated Tunnels
- SSL-VPN Concentrator (incl. iPhone client support)
- DES, 3DES, and AES Encryption Support
- SHA-1/MD5 Authentication
- PPTP, L2TP, VPN Client Pass Through
- Hub and Spoke VPN Support
- IKE Certificate Authentication (v1 & v2)
- IPSec NAT Traversal
- Automatic IPSec Configuration
- Dead Peer Detection
- RSA SecurID Support
- SSL Single Sign-On Bookmarks
- SSL Two-Factor Authentication
- LDAP Group Authentication (SSL)

NETWORKING/ROUTING
- Multiple WAN Link Support
- DHCP Client/Server
- Policy-Based Routing
- Dynamic Routing for IPv4 and IPv6 (RIP, OSPF, BGP, & Multicast for IPv4)
- Multi-Zone Support
- Route Between Zones
- Route Between Virtual LANs (VDOMS)
- Multi-Link Aggregation (802.3ad)
- IPv6 Support (Firewall, DNS, Transparent Mode, SIP, Dynamic Routing, Admin Access, Management)
- VRRP and Link Failure Control
- sFlow Client

USER AUTHENTICATION OPTIONS
- Local Database
- Windows Active Directory (AD) Integration
- External RADIUS/LDAP Integration
- Xauth over RADIUS for IPSEC VPN
- RSA SecurID Support
- LDAP Group Support

DATA CENTER OPTIMIZATION
- Web Server Caching
- TCP Multiplexing
- HTTPS Offloading
- WCCP Support

ANTIVIRUS / ANTISPYWARE
- ICSA Labs Certified (Gateway Antivirus)
- Includes Antispyware and Worm Prevention:
  - HTTP/HTTPS
  - SMTP/SMTPS
  - POP3/POP3S
  - IMAP/IMAPS
  - FTP
  - IM Protocols
- Flow-Based Antivirus Scanning Mode
- Automatic "Push" Content Updates
- File Quarantine Support
- Databases: Standard, Extended, Extreme, Flow
- IPv6 Support

WEB FILTERING
- 76 Unique Categories
- FortiGuard Web Filtering Service Categorizes over 2 Billion Web pages
- HTTP/HTTPS Filtering
- Web Filtering Time-Based Quota
- URL/Keyword/Phrase Block
- URL Exempt List
- Content Profiles
- Blocks Java Applet, Cookies, Active X
- MIME Content Header Filtering
- IPv6 Support

APPLICATION CONTROL
- Identify and Control Over 1400 Applications
- Control Popular IM/P2P Apps Regardless of Port/Protocol:

AOL-IM	Yahoo	MSN	KaZaa
ICQ	Gnutella	BitTorrent	MySpace
WinNY	Skype	eDonkey	Facebook

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

WAN OPTIMIZATION
- Bi-directional / Gateway to Client/Gateway
- Integrated Caching and Protocol Optimization
- Accelerates CIFS/FTP/MAPI/HTTP/HTTPS/Generic TCP

VIRTUAL DOMAINS (VDOMs)
- Separate Firewall/Routing Domains
- Separate Administrative Domains
- Separate VLAN Interfaces
- 10 VDOM License Std. (more can be added)

WIRELESS CONTROLLER
- Unified WiFi and Access Point Management
- Automatic Provisioning of APs
- On-wire Detection and Blocking of Rogue APs
- Virtual APs with Different SSIDs
- Multiple Authentication Methods

TRAFFIC SHAPING
- Policy-based Traffic Shaping
- Application-based and Per-IP Traffic Shaping
- Differentiated Services (DiffServ) Support
- Guarantee/Max/Priority Bandwidth
- Shaping via Accounting, Traffic Quotas

INTRUSION PREVENTION SYSTEM (IPS)
- ICSA Labs Certified (NIPS)
- Protection From Over 3000 Threats
- Protocol Anomaly Support
- Custom Signature Support
- Automatic Attack Database Update
- IPv6 Support

DATA LOSS PREVENTION (DLP)
- Identification and Control Over Sensitive Data in Motion
- Built-in Pattern Database
- RegEx-based Matching Engine for Customized Patterns
- Configurable Actions (block/log)
- Supports IM, HTTP/HTTPS, and More
- Many Popular File Types Supported
- International Character Sets Supported

ANTISPAM
- Support for SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS
- 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

ENDPOINT COMPLIANCE AND CONTROL
- Monitor & Control Hosts Running FortiClient Endpoint Security

MANAGEMENT/ADMINISTRATION
- Console Interface (RS-232)
- WebUI (HTTP/HTTPS)
- Telnet / Secure Command Shell (SSH)
- Command Line Interface
- Role-Based Administration
- Multi-language Support: English, Japanese, Korean, Spanish, Chinese (Simplified & Traditional), French
- Multiple Administrators and User Levels
- Upgrades and Changes via TFTP and WebUI
- System Software Rollback
- Configurable Password Policy
- Optional FortiManager Central Management

LOGGING/MONITORING/VULNERABILITY
- Local Event Logging
- Log to Remote Syslog/WELF Server
- Graphical Real-Time and Historical Monitoring
- SNMP Support
- Email Notification of Viruses And Attacks
- VPN Tunnel Monitor
- Optional FortiAnalyzer Logging / Reporting
- Optional FortiGuard Analysis and Management Service

Note: The list above is comprehensive and may contain FortiOS features which are not available on all FortiGate appliances.
Consult FortiGate system documentation to determine feature availability.

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	Base Unit	With AMC
1518 Byte Packets	40 Gbps	44 Gbps
512 Byte Packets	40 Gbps	44 Gbps
64 Byte Packets	38 Gbps	42 Gbps

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	
IPS	5 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	
Antivirus Throughput	900 Mbps

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	Base Unit	With AMC
IPSec VPN Throughput	16 Gbps	18.5 Gbps
SSL VPN Throughput	370 Mbps	
Concurrent SSL VPN Users Recommended (Max)	1,500	
Client-to-Gateway IPSec VPN Tunnels (System/VDOM)	10,000 / 5,000	

WAN Optimization

Wide Area Network (WAN) optimization accelerates applications over geographically dispersed networks, while ensuring multi-threat inspection of all network traffic. WAN optimization eliminates unnecessary and malicious traffic, optimizes legitimate traffic, and reduces the amount of bandwidth required to transmit data between applications and servers. Improved application performance and delivery of network services reduces bandwidth and infrastructure requirements, along with associated expenditures.

Features
Gateway-to-Gateway Optimization
Bidirectional Gateway-to-client Optimization
Web Caching
Secure Tunnel
Transparent Mode

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

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

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

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

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 1,400 Applications
- Traffic Shaping (Per Application)
- Control Popular IM/P2P Apps Regardless of Port or Protocol
- Popular Applications include:

AOL-IM	Yahoo	MSN	KaZaa
ICQ	Gnutella	BitTorrent	MySpace
WinNY	Skype	eDonkey	Facebook

and more...

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: 25
- Default VDOMs: 10

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 byte UDP packets)	40 / 44 Gbps *
Firewall Throughput (512 byte UDP packets)	40 / 44 Gbps *
Firewall Throughput (64 byte UDP packets)	38 / 42 Gbps *
IPSec VPN Throughput (AES-256 + SHA-1)	16 / 18.5 Gbps *
IPS Throughput	5.0 Gbps
Antivirus Throughput (Proxy-based)	900 Mbps
Antivirus Throughput (Flow-based)	1.5 Gbps
Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM)	10,000 / 5,000
Client-to-Gateway IPSec VPN Tunnels	20,000
Concurrent Sessions	2 Million
New Sessions/Sec	100,000
Concurrent SSL-VPN Users (Recommended Max)	1,500
SSL-VPN Throughput	370 Mbps
Firewall Policies (Max)	100,000
Virtual Domains (Max / Default)	25 / 10
Unlimited User Licenses	Yes
Mean Time Between Failures	More than 5 years
Redundant Power Supplies (Hot-swappable)	Yes
Dimensions	
Height	3.5 in (8.87 cm)
Width	17.3 in (44 cm)
Length	21 in (53 cm)
Weight	36 lb (16.4 Kg)
Rack Mountable	Yes
Environment	
AC Power (FG-1240B)	100 – 240 VAC, 50 – 60 Hz 6.3 Amp (Max)
DC Power (FG-1240B-DC Required)	-48V DC (Normal)
Power Consumption (AVG)	263.2 W
Heat Dissipation	1,167 BTU/h
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	
Safety Certifications	FCC Class A Part 15, UL/CUL, C Tick, VCCI

FortiGate consolidated security appliances also include the following important features

- Multiple Deployment Modes (Transparent/Routing)
- Advanced Layer-2/3 Routing Capabilities
- Traffic Shaping and Prioritization
- Virtual Domains (VDOMs)
- Data Center Traffic Optimization
- High Availability (Active/Active, Active/Passive, Clustering)
- WAN Optimization
- Local Web-Based Management Interface
- Command Line Management Interface
- Centralized Management Interface (FortiManager Appliance Required)
- Local Event Logging
- Centralized Event Logging (FortiAnalyzer Appliance Required)
- FortiGuard Analysis and Management Service Support
- Multiple Device Authentication Options

* Higher performance figures achieved with AMC module installed.
Note: All performance values are "up to" and vary depending on system configuration. Antivirus performance is benchmarked using HTTP traffic (32 Kbyte objects). IPS performance measured using 44 Kbyte HTTP files (similar to NSS Labs test methodology).

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, antispam, 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
06560, 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

FG-1240B-DAT-R9.2-201110