DATASHEET

FortiGate®-3040B

10-GbE Multi-Threat Security Appliances

FortiGate-3040B multi-threat security appliances offer exceptional levels of performance, deployment flexibility, and security for large enterprise networks. Built from the ground up by Fortinet, FortiGate-3040B appliances combine three essential elements to achieve these benefits: custom hardware including FortiASIC™ processors, high port density, and multi-threat security from the FortiOS™ operating system. Moreover, whether protecting virtualized infrastructure, cloud-providing infrastructure, or traditional IT infrastructure, the inclusion of 10-GbE ports and up to 40 Gbps of firewall performance make this appliance a very pragmatic security solution for high-bandwidth networks.

High-Performance Hardware

The FortiGate-3040B appliance provides up to 40 Gbps of wire-speed firewall performance and up to 16 Gbps of VPN performance through the use of innovative FortiASIC processors. In addition, the FortiGate-3040B appliance boasts impressive multi-threat security performance in a variety of configurations. With the FortiGate-3040B, you can ensure that your security can keep up with the rest of your network.

High 10-GbE Port Density

The FortiGate-3040B appliance includes eight 10-Gigabit Ethernet (10-GbE) ports standard. This makes the appliance ideal for your data center or other high-bandwidth application. And with a total of 20 ports on the system, comprised of SFP+, SFP, and RJ-45 ports, there is deployment flexibility in abundance.

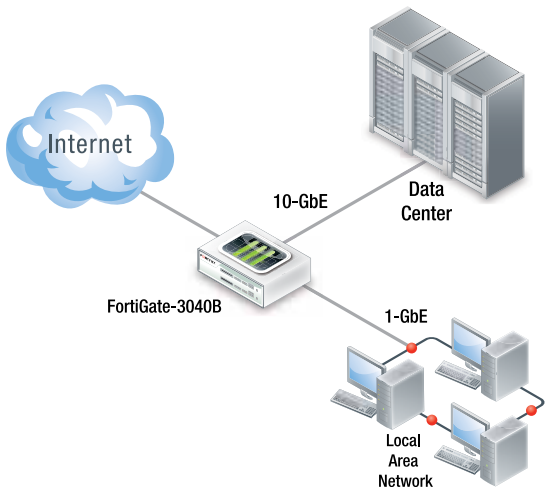
Multi-Threat Security

Using the advanced FortiOS operating system, the FortiGate-3040B appliance effectively neutralizes a wide range of security threats facing networks today. Whether used as a high-performance firewall or as a comprehensive multi-threat security solution, the FortiGate-3040B protects assets with some of the most effective security available.

FortiGate-3040B Benefits

The FortiGate-3000 series offers high-performance and comprehensive protection against network, content, and application-level threats. In addition, FortiGate-3040B appliances offer these benefits:

- Outstanding value as a 10-GbE network security appliance with best-in-class firewall price-performance
- Highest 10-GbE port density in its class
- Improved network performance with WAN optimization and web caching features
- Exceptional content-inspection performance in several key configurations



FortiGate Certifications

ICSA labs CERTIFIED ANTI-VIRUS
ICSA labs CERTIFIED FIREWALL - CORPORATE
ICSA labs CERTIFIED IPSEC - BASIC
ICSA labs CERTIFIED ANTI-SPAM
ICSA labs CERTIFIED NETWORK IPS
FIPS 140-2 VALIDATED
COMMON CRITERIA EAL 4+ CERTIFIED

The FortiASIC Advantage

The FortiGate-3040B includes our latest FortiASIC network processors (NP) and content processors (CP). These purpose-built and high-performance processors use proprietary digital engines to accelerate resource-intensive security services.

The FortiASIC-NP4 network processors work inline with the flow of traffic and accelerate firewall and VPN functions.

FortiASIC network processors provide these functions:

- Wire-speed firewall performance at any packet size
- VPN acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing

The FortiASIC-CP7content processor work outside the direct flow of traffic and are designed to provide high-speed cryptography and content inspection services.

FortiASIC content processors provides these functions:

- Encryption and decryption offloading
- Signature-based content inspection acceleration

FortiGate-3040B Appliance (Front)

FortiGate-3040B Appliance (Rear)

FortiGuard and FortiCare Services

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, application control, vulnerability and compliance management, and database security services.

For more information about FortiGuard Services, please visit www.fortiguard.com.

FortiGuard Subscription Services						
Product	**Antivirus**	**Intrusion Prevention**	**Web Filtering**	**Antispam**	**Application Control**	**Vulnerability & Compliance**
FortiGate-3040B	Supported	Supported	Supported	Supported	Supported	Supported

FortiCare™ Support Services offerings provide global support for all Fortinet products and services. Customer satisfaction and responsiveness is Fortinet's number one priority. With FortiCare support, customers can be assured that their Fortinet security products are performing optimally and protecting their corporate assets with the best security technology at the best possible price.

Fortinet offers end-users multiple options for FortiCare contracts so that they can obtain the right level of support for their organization's needs. Attractively priced options include 24x7 support with advanced hardware replacement, 8x5 support with enhanced Web features, Premium Support with technical account management, and Premium RMA support with enhanced service levels.

Additionally, Fortinet Professional Services can be engaged for projects with critical deadlines projects that are large in scope, or initial deployments.

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. FortiOS software enables a comprehensive suite of security services: Firewall, VPN, intrusion prevention, antivirus/antispyware, antispam, web filtering, application control, data loss prevention, SSL inspection, and end point network access control.

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 multiple algorithms to accelerate compute-intensive security services. FortiASIC provides the performance required to deliver enterprise and carrier-class UTM services. Coupled with the FortiOS security hardened Operating System, FortiASIC delivers extreme performance and security.

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
- Granular Per-Policy Protection Profiles
- Explicit Proxy Support

VIRTUAL PRIVATE NETWORK (VPN)
- ICSA Labs Certvified (IPSec)
- PPTP, IPSec, and SSL
- Dedicated Tunnels
- 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
- PPPoE 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, Administrative Access, Management)

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

ANTIVIRUS
- ICSA Labs Certified (Gateway Antivirus)
- Includes Antispyware and Worm Prevention

HTTP/HTTPS	SMTP/SMTPS
POP3/POP3S	IMAP/IMAPS
FTP	IM Protocols

- Automatic "Push" Content Updates from FortiGuard
- File Quarantine Support
- IPv6 Support

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

APPLICATION CONTROL
- Identifiy and Control Over 1000 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 Standard, Upgradable to More

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

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
- Local Event 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 / Reporting
- Optional FortiGuard Analysis and Management Service

Firewall

Fortinet firewall technology delivers industry-leading performance for network and application firewalling, including Web 2.0 application policies based on the application identity. Our technology identifies traffic patterns and links them to the use of specific applications, such as instant messaging and peer-to-peer applications, permitting application access control. By coupling application intelligence with firewall technology, the FortiGate platform is able to deliver real-time security with integrated application content level inspection, thereby simplifying security deployments.

Firewall	
Features	NAT, PAT and Transparement (Bridge)
	Policy-Based NAT
	SIP/H.323/SCCP NAT Traversal
	VLAN Tagging (802.1Q)
	IPv6 Support
Performance	
Firewall (1518 Byte)	40 Gbps
Firewall (512 Byte)	40 Gbps

Intrusion Prevention

IPS technology provides protection against current and emerging network level threats. In addition to signature-based detection, we perform anomaly-based detection whereby our system alerts users to traffic that fits a profile-matching attack behavior. This behavior is then analyzed by our threat research team to identify threats as they emerge and generate new signatures that will be incorporated into our FortiGuard services.

Intrusion Prevention System	
Features	Automatic Database Updates
	Protocol Anomaly Support
	IPS and DoS Prevention Sensor
	Custom Signature Support
	IPv6 Support
Performance	
IPS Throughput (UDP)	5 Gbps
IPS Throughput (HTTP)	1.6 Gbps

Antivirus / Antispyware

Antivirus content inspection technology provides protection against virus, spyware, worms, phishing, and other forms of malware being transmitted over the network infrastructure. By intercepting application content in transit, and reassembling the data into user expected content, the FortiGate Antivirus service ensures that malicious threats hidden within legitimate application content is identified and removed from the data stream destined for internal (or external) recipients. FortiGuard subscription services ensure that each FortiGate has access to updated malware signatures, resulting in high levels of accuracy and detection capabilities, including emerging and newly discovered viruses.

Antivirus	
Features	Automatic Database Updates
	Proxy Antivirus
	Flow-based Antivirus
	File Quarantine
	IPv6 Support
Performance	
Antivirus	1.2 Gbps

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. Benefits of the FortiGate VPN service include the ability to enforce complete content inspection and multi-threat security as part of the VPN service, including antivirus, intrusion prevention, and Web filtering. The FortiGate-3040B appliance also supports traffic optimization, providing prioritization for critical communications traversing VPN tunnels.

VPN	
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
Performance	
IPSec VPN	16 Gbps
Recommended Max # of SSL Users	20,000

WAN Optimization

With WAN Optimization, you can accelerate applications over your wide area links while ensuring multi-threat security. FortiOS 4.0 software not only eliminates unnecessary and malicious traffic as one of its core capabilities, it also optimizes legitimate traffic and reduces the amount of bandwidth required to transmit data between applications and servers across the WAN. This results in improved performance of applications and network services, as well as helping to avoid additional higher-bandwidth provisioning requirements.

WAN Optimization	
Features	Gateway-to-Gateway Optimization
	Bi-directional Gateway-to-client Optimization
	Web Caching
	Secure Tunnel
	Transparent Mode

SSL Inspection

SSL-Encrypted Traffic Inspection protects clients as well as web and application servers from malicious SSL-encrypted traffic, to which many security devices are blind. SSL Inspection intercepts encrypted traffic and inspects it for threats, prior to routing it to its final destination. SSL Inspection applies to both client-oriented SSL traffic (such as users connecting to an SSL-encrypted hosted CRM site) and inbound traffic to an organization's own web and application servers. You now have the ability to enforce appropriate use policies on inappropriate encrypted web content, and protect servers from threats within encrypted traffic flows.

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

Endpoint NAC

Endpoint NAC enforces the use of the FortiClient Endpoint Security application (either Standard or Premium editions) on your network. The feature verifies the installation of the version of the FortiClient application, ensures that antivirus signatures are up-to-date, and ensures that the FortiClient firewall is enabled before allowing the traffic from that endpoint to pass through the FortiGate platform. You also have the option to quarantine endpoints running applications that violate policies and require remediation.

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

Data Loss Prevention

It is imperative for you to control the vast amount of confidential, regulated, and proprietary data traversing your network. Working across multiple applications (including those encrypting their communications), DLP uses a sophisticated pattern-matching engine to identify and then prevent the communication of sensitive information outside the network perimeter. In addition to protecting your organization's critical information, DLP also provides audit trails for data and files to aid in demonstrating policy compliance. You can use the wide range of configurable actions to log, block, and archive data, as well as ban or quarantine users.

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

Web Filtering

Web filtering technology is a pro-active defense feature that identifies known locations of malware and blocks access to these malicious sources. In addition, the technology enables administrators to enforce policies based on website content categories ensuring users are not accessing content that is inappropriate for their work environment. The technology restricts access to denied categories based on the policy by comparing each Web address request to a Fortinet hosted database.

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

Logging, Reporting & Monitoring

FortiGate units provide extensive logging capabilities for traffic, system, and network protection functions. They also allow you to compile reports from the detailed log information gathered. Reports provide historical and current analysis of network activity to help identify security issues that will reduce and prevent network misuse and abuse.

Logging and Monitoring	
Features	Internal Log storage and Report Generation
	Graphical Real-Time and Historical Monitoring
	Graphical Report Scheduling Support
	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 almost every FortiGate model.

High Availability (HA)	
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 on your endpoints, regardless of the port or the protocol used for communication. Application classification and control is essential to manage the explosion of new web-based applications bombarding networks today, as most application traffic looks like normal web traffic to traditional firewalls. Fortinet's application control technology identifies application traffic and then applies security policies defined by the administrator. The end result is more flexible and granular policy control, with deeper visibility into your network traffic.

Application Control	
Features	Identify and Control Over 1,200 Applications
	Traffic Shaping (Per Application)
	Control Popular IM/P2P Apps Regardless of Port / 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.

Virtual Domains	
Features	Separate Firewall / Routing Domains
	Separate Administrative Domains
	Separate VLAN Interfaces
VDOMs (Max / Default)	250 / 10

Setup / Configuration Options

Fortinet provides administrators with a variety of methods for configuring FortiGate appliances for initial deployment. From simple-to-use interfaces such as the Web user interface (UI), to the advanced capabilities of the Command-line interface, FortiGate systems work the way you are most comfortable.

Setup / Configuration Options	
Features	Web-based User Interface
	Command Line Interface (CLI) over serial connection
	Pre-configured settings from USB drive

Wireless Controller

The Wireless controller integrated into every FortiGate platform centralizes the management and monitoring of all FortiAP secure access points. All wireless traffic is directed to the FortiGate multi-threat security platform and undergoes identity-aware firewall policies and UTM engine inspection, with only authorized wireless traffic being forwarded. From a single console you can control network access, update policies quickly and easily, and monitor compliance.

Wireless Controller	
Highlights	Managed and Monitor FortiAP product
	Rogue AP Detection, Control and Reporting
	Virtual AP with different SSID

	FortiGate-3040B
Technical Specifications - Appliances	
Total Network Interfaces	20
Hardware Accelerated 10-GbE SFP+ Interfaces	8
Hardware Accelerated 1-GbE SFP Interfaces	10
Non-Accelerated 10/100/1000 Interfaces	2
Transceivers Included	2 SR SFP+
Fortinet Storage Module (FSM) Expansion Slot	4
Included Local Disk-Based Storage	1
USB Server	2
RJ45 Serial Console	1
System Performance	
Firewall Throughput (64 / 512 / 1518 byte UDP packets)	40Gbps
IPSec VPN Throughput (AES256+SHA1)	16 Gbps
IPS Throughput (UDP)	5 Gbps
IPS Throughput (HTTP)	1.6 Gbps
Antivirus Throughput	1.2 Gbps
Static IPSec VPN Tunnels (System / VDOM)	10,000 / 5,000
Concurrent IPSec VPN Tunnels	64,000
Concurrent Sessions	4.0 Million
New Sessions/Sec	100,000
Concurrent SSL-VPN Users (Recommended Max)	20,000
SSL-VPN Throughput	500 Mbps
Firewall Policies (VDOM/System)	50,000 / 100,000
Virtual Domains (Max / Default)	Up to 250 / 10
Unlimited User Licenses	Yes
Redundant Power Supplies (Hot Swappable)	Yes
Dimensions	
Height	3.46" (8.80 cm)
Width	17.40" (44.2 cm)
Length	21.85" (55.5 cm)
Weight	35 lb (15.88 Kg)
Rack Mountable	Yes
Environment	
AC Power	100 - 240 VAC, 50-60 Hz, 3.2 - 6.3 Amp (Max)
Power Consumption (AVG)	366 W
Heat Dissipation	1249 BTU
Operating Temperature	32 – 104 deg F (0 – 40 deg C)
Storage Temperature	-31 – 158 deg F (-35 – 70 deg C)
Humidity	20 to 90% non-condensing
Compliance	
	FCC Class A Part 15, UL/CUL, C Tick, VCCI

FortiGate-3040B multi-threat security appliances also include

Multiple Deployment Modes (Transparent/Routing)
Integrated Switch Fabric (ISF)
Advanced Layer-2/3 Routing Capabilities
High Availability (Active/Active, Active/Passive, Clustering)
Virtual Domains (VDOMs)
Data Center Traffic Optimization
Traffic Shaping and Prioritization
WAN Optimization
Multiple Device Authentication Options

MANAGEMENT OPTIONS

Local Web-Based Management Interface
Command Line Management Interface (CLI)
Local Event Logging (Memory / Disk if available)
Centralized Management (FortiManager Appliance Required)
Centralized Event Logging (FortiAnalyzer Appliance Required)

Actual performance values may vary depending on the network traffic and system configuration. Firewall performance is based on 512 Byte UDP packets processed with the FortiGate-3040B operating in NAT mode. VPN performance is based on on 512 Byte UDP packets processed with the FortiGate-3040B using AES256+SHA1 encryption algorithms. IPS performance (UDP) is based on 1518 Byte UDP packets processed with the FortiGate-3040B operating in NAT mode with IPS anomaly enabled. IPS performance (HTTP) is based on HTTP traffic with 32KB files. Antivirus performance is measured using HTTP traffic with 32 KB file attachments and the FortiGate-3040B configured to use the regular antivirus database.

Ordering Info	
Product Description	**SKU**
FortiGate-3040B, 8 SFP+ 10-Gig ports (2 SFR+ SR-type transeivers included), 10 SFP 10/100/1000 FortiASIC accelerated ports, 2 SFP 10/100/1000 ports, 4 FSM Slots, 1 FSM-064 with 64 GB SSD storage, and dual AC power supplies	FG-3040B
Optional Accessories	**SKU**
Fortinet Storage Module (FSM), 64 GB Solid State Drive for FortiGate with FSM slot	FSM-064
10-Gig transceiver, Short Range SFP+ module for all FortiGate models with SFP+ interfaces	FG-TRAN-SFP+SR
10-Gig transceiver, Long Range SFP+ module for all FortiGate models with SFP+ interfaces	FG-TRAN-SFP+LR

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 +65-6513-3730
Fax +65-6223-6784