

FortiCarrier™ Systems

Specialized Security for Service Providers





As the communications industry continues its convergence toward an all-IP model, service providers of all types are challenged with transforming their infrastructure into a modern service delivery network. A service provider's next generation network must be adaptable and able to support new services faster, while also lowering operational costs. As service providers abandon the "stove-pipe" approach to service delivery in favor of next generation architectures, it is critical that they address the security of their new solutions to ensure service uptime and prevent fraud.

From a financial perspective, securing the service delivery platform is key to driving revenue, profitability, and long-term success. A well-designed security infrastructure can be used to both secure the provider's networks and deliver a range of security services to end-users, which increase revenue for the service provider and increase value for the end-user. Fortinet provides such a solution with its FortiCarrier product line, addressing the security needs of both the operator and the end-user in a single, yet extensible, security offering.

FortiCarrier platforms represent a range of security solutions that extend the integrated security concept to protect critical applications across a service provider's IP network. The platforms are designed to secure the business of mobile operators, voice operators, Managed Security Service Providers (MSSPs), and large enterprises, enabling the migration to next generation network architectures. FortiCarrier platforms facilitate rapid service deployment while simultaneously delivering the lowest total cost of ownership for security infrastructure.

FortiCarrier Specialized Security Solutions

FortiCarrier specialized security solutions enable security as a service offerings with an integrated set of security technologies that support a wide range of service provider requirements. FortiCarrier systems provide the essential security services from the FortiGate product line, with fully integrated firewall, Virtual Private Network (VPN), intrusion prevention, antivirus/antispyware, Web filtering, antispam, data leakage prevention, and application control services. In addition, FortiCarrier systems extend the integrated security model for service providers to offer signaling firewalling, GTP firewalling, MMS malware scanning, and MMS antispam filtering. FortiCarrier platforms can also dynamically assign security profiles to a subscriber's traffic, automating the provisioning and ongoing management of security services provided to a customer.

Features	Benefits
 <p>FortiCarrier-3950B</p>	<p>Hardware Accelerated Performance</p> <p>FortiASIC processors provide assurance that the security device will not become a bottleneck in the network</p>
	<p>Additional Capacity on Demand</p> <p>Fortinet expansion slots provide greater flexibility by supporting additional hardware-accelerated ports and localized storage of event data</p>
	<p>Unified Security Architecture</p> <p>FortiCarrier multi-threat security provides better protection and lowered costs over multiple point security products</p>
 <p>FortiCarrier-5001B</p>	<p>Centralized Management</p> <p>FortiManager and FortiAnalyzer centralized management and reporting appliances simplify the deployment, monitoring, and maintenance of your security infrastructure</p>

FortiCarrier-3950B Consolidated Security Appliances

FortiCarrier-3950B appliances offer high levels of performance, scalability, and security in a compact appliance form factor. Combine the FortiCarrier-3950B with optional modules to match your performance and functional requirements.

Technical Specifications - Appliances	FortiCarrier-3950B
Total Network Interfaces (Base / Max)	8 / 108 ¹
Hardware Accelerated 10-GbE SFP+ Interfaces	2 / 12 ¹
Hardware Accelerated GbE SFP Interfaces	4 / 104 ¹
Accelerated 10/100/1000 Interfaces	100 ¹
Management 10/100/1000 Interfaces	2
Transceivers Included	2x SR SFP+
Fortinet Mezzanine Card (FMC) Expansion Slots	5
Internal Storage	256 GB
System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	20 / 20 / 20 - 120 / 120 / 120 Gbps ^{1,2}
Firewall Latency (64 byte UDP packets)	4 μs
Firewall Throughput (Packets Per Second)	30 - 180 Mpps ^{1,2}
Concurrent Sessions (TCP)	20 Million
New Sessions/Sec (TCP)	250,000
Firewall Policies (System / VDOM)	100,000 / 50,000
IPSec VPN Throughput (512 byte packets)	8 - 50.5 Gbps ^{1,2}
Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM)	10,000 / 5,000
Client-to-Gateway IPSec VPN Tunnels	64,000
SSL-VPN Throughput	1.2 Gbps
Concurrent SSL-VPN Users (Recommended Max)	25,000
IPS Throughput	5 - 20 Gbps ³
Antivirus Throughput (Proxy Based / Flow Based)	4 / 5 - 15 Gbps ³
Virtual Domains (Default / Max)	10 / 500
Max Number of FortiAPs	1,024
Max Number of FortiTokens	5,000
High Availability Configurations	Active/Active, Active/Passive, Clustering
Unlimited User Licenses	Yes
Dimensions and Power	
Height x Width x Length	5.25 x 17.5 x 27.65 in (133 x 444 x 702 mm)
Weight	60.0 lb (27 Kg)
Rack Mountable	Yes
AC Power	100-240 VAC, 50-60 Hz, 7.0 - 12.0 Amp (Max)
Power Consumption (Avg/Max)	382 W / 470 W
Heat Dissipation	1,603 BTU/h
Redundant Power Supplies (hot-swappable)	Yes
Operating Environment and Certifications	
Operating Temperature	32 – 104 deg F (0 – 40 deg C)
Storage Temperature	-13 – 158 deg F (-25 – 70 deg C)
Humidity	20 to 90% non-condensing
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN



FortiCarrier-3950B (Front)



FortiCarrier-3950B (Rear)

FortiCarrier-3950B consolidated security appliances also include:

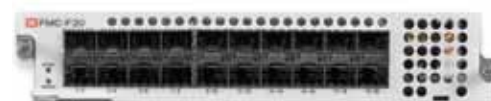
- Multiple Deployment Modes (Transparent/Routing)
- Backplane Switch Fabric
- Advanced Layer-2/3 Routing Capabilities
- High Availability (Active/Active, Active/Passive, Clustering)
- Virtual Domains (VDOMs)
- Data Center Traffic Optimization
- Traffic Shaping and Prioritization
- WAN Optimization
-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



FMC-C20 Module



FMC-F20 Module



FMC-XD2 Accelerated Interface Module (Firewall Acceleration)



FMC-XG2 Security Processing Module (IPS Acceleration)



FMC-XH0 Security Processing Module (IPS Acceleration)

Technical Specifications - FMC Modules	FMC-XD2	FMC-XG2	FMC-XH0	FMC-C20	FMC-F20
Total Network Interfaces	2	2	0	20	20
Hardware Accelerated 10-GbE SFP+ Interfaces	2	2	-	-	-
Hardware Accelerated 1-GbE SFP Interfaces	-	-	-	-	20
Hardware Accelerated 10/100/1000 Interfaces	-	-	-	20	-
Transceivers Included	2x SR SFP+	2x SR SFP+	-	-	4x SX SFP
Firewall Throughput (1518 byte UDP packets)	20 Gbps	18 Gbps	19 Gbps	20 Gbps	20 Gbps
Firewall Throughput (512 byte UDP packets)	20 Gbps	17 Gbps	19 Gbps	20 Gbps	20 Gbps
Firewall Throughput (64 byte UDP packets)	20 Gbps	4.5 Gbps	10.5 Gbps	20 Gbps	20 Gbps
IPSec VPN Throughput (512 byte packets)	8 Gbps	6 Gbps	16.5 Gbps	8.5 Gbps	8.5 Gbps
IPS Throughput	-	2.5 Gbps	4 Gbps	-	-
Antivirus Throughput (Flow-based)	-	2 Gbps	4 Gbps	-	-
Environment					
Power Consumption (Avg)	45 W	68 W	48 W	74.3 W	59.6 W
Power Consumption (Max)	54 W	81.6 W	73 W	89 W	71.5 W
Heat Dissipation	154 BTU/h	278 BTU/h	249 BTU/h	304 BTU/h	244 BTU/h

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.

¹ Higher figure uses FMC modules to achieve the stated performance.

² Maximum Firewall and VPN system performance is based on fully populated system with FMC-XD2 modules.

³ Maximum IPS and flow-based antivirus performance is based on fully populated system with FMC-XG2 modules.

FortiCarrier-5000 Series Consolidated Security Blades

FortiCarrier security blades provide core security services for FortiCarrier systems. Combine FortiCarrier security blades with a FortiGate-5000 series chassis, FortiGate-5000 series networking blades, and optional modules to create a system that uniquely matches your performance and functional requirements.



FortiCarrier-5001B Multi-Threat Security Blade

Technical Specifications	FortiCarrier-5001B
Interfaces and Storage	
10-GbE SFP+ Ports	8
10/100/1000 Base-T Ports	2
Total Ports	10
FortiASIC Network Processor Accelerated Ports	8
Local Storage	64 GB SSD
Performance	
Firewall Throughput (1518 byte UDP packets)	40 Gbps
Firewall Throughput (512 byte UDP packets)	40 Gbps
Firewall Throughput (64 byte UDP packets)	40 Gbps
Firewall Latency (64 byte UDP packets)	4 μ s
Firewall Throughput (Packets Per Second)	60 Mpps
Concurrent Sessions (TCP)	20 Million
New Sessions/Sec (TCP)	170,000
Firewall Policies (System / VDOM)	100,000 / 50,000
IPSec VPN Throughput (512 byte packets)	17 Gbps
Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM)	10,000 / 5,000
Client-to-Gateway IPSec VPN Tunnels	64,000
SSL-VPN Throughput	530 Mbps
Concurrent SSL-VPN Users (Recommended Max)	20,000
IPS Throughput	7.8 Gbps
Antivirus Throughput (Proxy Based / Flow Based)	2 / 2.5 Gbps
Virtual Domains (Default / Max)	10 / 500
Max Number of FortiAPs	1,024
Max Number of FortiTokens	5,000
Unlimited User Licenses	Yes
Environment	
Power Consumption (AVG)	187 / 225 W
Heat Dissipation	768 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	
Certifications	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

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.

FortiGate-5000 Series Networking Blades

Provide advanced switching and load-balancing functions to FortiGate systems.



FortiSwitch-5003B Networking Blade



FortiSwitch-5203B Networking/Security Blade

Technical Specifications	FortiSwitch-5003B	FortiSwitch-5203B ³
Networking Blades		
Interfaces		
Fabric Channel Interfaces	8x 10-GbE SFP+	8x 10-GbE SFP+
Base Channel Interfaces	2x 10-GbE SFP+ 1x 10/100/1000	2x 10-GbE SFP+ 1x 10/100/1000
Transceivers Included	2x 10-GbE SFP+ SR	2x 10-GbE SFP+ SR
Total Switching Throughput	225 Gbps	300 Gbps
10-GbE Backplane Fabric Support	Yes	Yes
GbE Backplane Fabric Support	Yes	Yes
Environment		
Power Consumption (Avg/Max)	150 / 180 W	210 / 250 W
Heat Dissipation	614 BTU/h	853 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		
Certifications	ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN	
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	

³ Operating in distributed mode.

Technical Specifications	FortiGate-5020	FortiGate-5060	FortiGate-5140B
ATCA Chassis			
Available Slots	2	6	14
High Availability Backplane Fabric	Built-in	Built-in	Built-in
Dual Switch Module Support	No	Yes	Yes
Max Firewall Throughput	44 Gbps	240 Gbps	560 Gbps
Max Concurrent Sessions (TCP)	4 Million	120 Million	280 Million
Max New Sessions/Sec (TCP)	100,000	1.41 Million	3.29 Million
Max IPSec VPN Throughput	17 Gbps	132 Gbps	308 Gbps
Max IPS Throughput	7 Gbps	56.4 Gbps	131.6 Gbps
Dimensions			
Height x Width x Length	5.25 x 17 x 15.5 in (13.3 x 43.2 x 39.4 cm)	8.86 x 17.64 x 18.82 in (22 x 44.8 x 47.8 cm)	22.63 x 19 x 22.6 in (57.5 x 48.3 x 57.4 cm)
Weight	35.5 lb (16.1 Kg)	38 (17.3 Kg)	84 lb (38 Kg)
Environment			
Power Required	AC	DC/AC ¹	DC/AC ¹
Chassis Power Consumption (Avg)	-	350 W	530 W
Heat Dissipation	-	1194 BTU/h	1808 BTU/h
Operating Temperature	32 – 104 F (0 – 40 C)	41 – 104 F (5 – 40 C)	32 – 104 F (0 – 40 C)
Storage Temperature	-13 – 158 F (-35 – 70 C)	23 – 131 F (-5 – 55 C)	-13 – 158 F (-35 – 70 C)
Humidity	5 to 90% non-condensing	5 to 85% non-condensing	5 to 90% non-condensing
Compliance			
Certifications	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, UL/cUL		
Note: All performance values are "up to" and vary depending on system configuration.			
¹ Optional FortiGate-5053B Power Supply Shelf used to provide AC power to the FortiGate-5060 and FortiGate-5140B chassis.			

The FortiCarrier/FortiGate-5000 series security systems also include

- Multiple Deployment Modes (Transparent/Routing)
- Backplane Switch Fabric
- 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)



FortiGate-5020 Security System



FortiGate-5060 Security System



FortiGate-5140B Security System



RTM-XB2 Rear Transition Module



RTM-XD2 Rear Transition Module

Rear Transition Modules

Provide enhanced 10-Gigabit Ethernet (10-GbE) backplane fabric connectivity to FortiGate systems. They include FortiASIC Network Processors for secure and low-latency communications.

All performance values are "up to" and vary depending on system configuration. Antivirus performance is benchmarked using HTTP traffic (32 Kbyte objects).

¹ Optional FortiGate-5053 Power Supply Shelf used to provide AC power to the FortiGate-5050 or FortiGate-5140 chassis.

Technical Specifications	RTM-XD2	RTM-XB2
Rear Transition Modules		
Application	Wire-Speed 10-GbE backplane fabric	10-GbE backplane fabric
FortiASIC Hardware Acceleration	FortiASIC NP4	FortiASIC NP2
Compatible Chassis Models	FortiGate-5140 FortiGate-5050	FortiGate-5140 FortiGate-5050
Compatible Networking Blade	FortiSwitch-5003A	FortiSwitch-5003A
Compatible Security Blades	FortiGate-5001A-SW FortiGate-5001A-DW	FortiGate-5001A-SW FortiGate-5001A-DW
Configuration Notes	1 RTM-XD2 module per FortiGate security blade	1 RTM-XB2 module per FortiGate security blade
Performance		
Firewall Performance (64B UDP)	20 Gbps	11 Gbps
Firewall Performance (512 / 1518 B UDP)	20 Gbps	11 Gbps
IPSec VPN	8 Gbps	8 Gbps
Environment		
Power Consumption (AVG)	148 W	148 W
Operating Temperature	32 – 104 deg F (0 – 40 deg C)	32 – 104 deg F (0 – 40 deg C)
Storage Temperature	-13 – 158 deg F (-35 – 70 deg C)	-13 – 158 deg F (-35 – 70 deg C)
Humidity	5 to 90% non-condensing	5 to 90% non-condensing
Compliance		
	FCC Class A Part 15, UL/CUL, C Tick, VCCI	FCC Class A Part 15, UL/CUL, C Tick, VCCI

FortiOS Carrier 4.0—Software Features by Industry

MANAGED SECURITY FEATURES

DYNAMIC SECURITY PROFILES

Assignment of Service Policy by User (Up to 600,000 Users)
Service Policy Can Define the Settings for Any of the Advanced Security Services Provided by FortiOS Carrier
Enables Parental Control and Opt-Out Services

VIRTUAL DOMAIN (VDOM)

Support for Hundreds of Enterprise Customers per Physical Blade/Appliance, Scaling to Thousands of Enterprise Customers per Chassis

CONSOLIDATED SECURITY

Firewall (ICSA Labs Certified)
IPSec VPN (ICSA Labs Certified)
SSL-VPN (ICSA Labs Certified)

CONSOLIDATED SECURITY (CONTINUED)

Intrusion Prevention System (ICSA Labs Certified)
Gateway Antivirus (ICSA Labs Certified)
Web Filtering (Over 2 Billion URLs Categorized)
Antispam Filtering
Application Control (Thousands of Applications Categorized)
Data Loss Prevention (DLP)
L2 / L3 Routing with Rate Limiting
SSL-Based Traffic Inspection

Refer to FortiOS 4.0 Software Brochure for Complete Details on the Wide-Range of Consolidated Security Features Offered

CENTRALIZED LOGGING AND ALERTING

Provided by FortiAnalyzer Appliances
All Log and Alert Functions Configurable per Customer
Consolidates Security and System Event Logs
Event Correlation, Graphical Reports, Network Data Statistics

CENTRALIZED MANAGEMENT

Provided by FortiManager Appliances
Deployment Configuration / Provisioning
Real-Time Monitoring
Device & Security Policy Maintenance
Localized Security Content Update Server & Rating Database for Managed Devices

VOICE SECURITY FEATURES

SIP SIGNALING FIREWALL

Stateful and SIP Protocol-Aware Firewall
Hardware Accelerated RTP Processing for Reduced Packet Loss, Packet Latency, and Jitter.
SIP Transparent Mode (Inspect Only) & SIP NAT Mode (Rewrite SIP Header) for Topology Hiding
Supports SIP Servers in Proxy or Redirect Operating Mode
Configurable RTP/RTCP Pinholing Support
Supports Complex Source & Destination SIP NAT Environments (SIP & RTP Protocols)
NAT IP Preservation Retains Originating IP Address for Administrative Purposes (e.g. Billing)
SIP Tracking over Session Lifespan
SIP Session Failover for Active-Passive High Availability
SIP Session Load Balancing (via Virtual IP Load Balancing)

SIP SIGNALING FIREWALL (CONTINUED)

Geographical Redundancy Support
SIP Rate Limiting (per SIP Method) to Prevent SIP Server Flooding / Overload
IP Topology Hiding of SIP & RTP Server (via NAT and NAPT)/already in the SIP NAT Mode
Configurable SIP Command Control Blocks
Unauthorized and Unwanted SIP Methods
Configurable SIP Blocking for Messages that Exceed Defined Maximum Header Length
SIP Registrar Exclusively Option to Avoid Spoofing of Clients
SIP Communication Logging to FortiAnalyzer Appliances
SIP Statistics (Active Sessions, Total Calls, Calls Failed/Dropped, Call Succeeded)

ADDITIONAL VOICE SECURITY TECHNOLOGIES

Intrusion Prevention System with VoIP Protocol Anomaly & VoIP Protocol Aware Signature-Based Inspection Capabilities
VoIP Specific Signature creation for extreme short term Reaction
Denial of Service (DoS) Sensor Protects Trusted Zones from Flooding Attacks
Integrated IPSec for Secured Tunnels Between Trusted Zones
Virtual Domain (VDM) Support for Additional Isolation of Infrastructure within the Same Physical Environment

MOBILE SECURITY FEATURES

GTP FIREWALL

Based on 3GPP 29.060 version 6.9.0
Integrated Intrusion Prevention Inspection for GTP Payloads
For Gn/Gp Interfaces
GTP Packet Sanity Check, Length Filtering & Type Screening
GSN Tunnel Limiting & Rate Limiting
GTP Stateful Inspection
Hanging GTP Tunnel Cleanup
GTP Tunnel Fail-Over for High Availability
GTP IMSI Prefix (more than 5000) & APN (more than 10000) Filtering
GTP Sequence Number Validation
IP Fragmentation of GTP Messages
GGSN & SGSN Redirection
Detecting GTP-in-GTP Packets
GTP Traffic Counting & Logging
Anti-Overbilling Together with Gi Firewall
Encapsulated Traffic Filtering with Anti-Spoofing Capabilities
GTP Protocol Anomaly Detection and Exploit Prevention
Handover Control to Prevent Session Hijacking
For Gi Interface
Anti-Overbilling Together with Gn/Gp Firewall

GTPv2 FIREWALL

Based on 3GPP TS 29.274 v9.4.0 (2010-09)
GTPv2 Based Protocol Support
GTPv2 Packets Forwarding and Routing
Packet Sanity Checking
Stateful Inspection
APN, IMSI, MSISDN filtering
High Availability Clustering
Logging

MMS ANTIVIRUS

Monitor Only & Active Blocking Modes (Per Interface Type)
Simultaneous Malware Scanning of MM1/MM3/MM4/MM7 Message Types
Remove Malicious Content Only Option (Allows Message Transaction to Complete)
File Type Analysis with Configurable Block or Intercept Actions (File Extension Independent)
Configurable Retrieve Message Scanning (MM1) to Avoid Redundant Inspection
Per Sender Scanning with Configurable Block/Archive/Intercept Actions
MM1/MM7 Client & Server Comforting

DYNAMIC SECURITY PROFILES

Assignment of Service Policy by MSISDN (Mobile Station)
Service Policy Can Define the Settings for Any of the Advanced Security Services Provided by FortiOS Carrier
Enables Parental Control and Opt-Out Services

MMS GENERAL

Support for Multiple MMS Policy Profiles for Consolidated or MVNO Deployments
Customizable Notification Messages (Per MVNO)
MSISDN Header Parsing (Including Cookie Extraction & Hex-Based Conversions for MM1/MM7 Message Types)
MMS File Intercept to FortiAnalyzer Appliances for Forensic Analysis
MMS Content Archive (Full MMS Message Archiving to FortiAnalyzer Appliances with HTTP/SMTP Transport Headers)
Per MSISDN & Per Mobile Station Type Reporting of Malicious Activity via FortiAnalyzer Appliances

MMS ANTISPAM / ANTIFRAUD

MM1/MM4 Flood Detection with Three Configurable Thresholds with Discrete Actions
MM1/MM4 Duplicate Message Detection with Configurable Thresholds and Actions
Configurable Alert Notification to Administrator of Spam or Fraud Activity
MM1/MM7 Banned Word Scoring with Configurable Block/Pass Actions

Ordering Info		
Chassis	SKU	Description
FortiGate-5020 Chassis	FG-5020AC	2-slot chassis with fan and dual AC power supplies
FortiGate-5020/5050 Power Supply	FG-5020PS	FortiGate-5020/5050 power supply
FortiGate-5020 Fan Tray	FG-5020FA	Fan tray for FG-5020 chassis
FortiGate-5060 Chassis	FG-5060-DC	6-slot chassis with fan trays, power entry modules, shelf alarm panel and 1 shelf manager
FortiGate-5060 Fan Tray	FG-5060FA	Fan tray for FG-5060 chassis
FortiGate-5060 Shelf Manager	FG-5060SM	Shelf manager for FG-5060 chassis
FortiGate-5060 Shelf Alarm Panel	FG-5060SAP	Shelf alarm panel for FG-5060 chassis
FortiGate-5140B Chassis	FG-5140B-DC	14-slot chassis with fan, 1 shelf manager card, no AC power supply included (DC powered)
FortiGate 5053B Power Converter Tray	FG-5053B	AC power converter shelf for high capacity 5000 chassis, supports up to 4 PSU-5000B power supply units, unpopulated
FortiGate-5000 Series Power Supply Unit	PSU-5000B	Power Supply Unit for FG5000 series, AC power supply unit, 1,200 Watts max, requires FortiGate-5053B shelf
FortiGate-5140B Fan Tray	FG-5140B-FAN	FG-5140B Fan Unit
FortiGate-5140B Shelf Manager	FG-5140B-SM	FG-5140B Shelf Manager with Mezzanine Card
FortiGate-5140B Shelf Alarm Manager	FG-5140B-SAM	Shelf Alarm Manager for FG-5140B
Security Appliances Blades	SKU	Description
FortiCarrier-3950B	FCR-3950B	2 SFP+ 10-Gig ports (2 SFP+ SR-type transceivers included), 4 SFP 10/100/1000 FortiASIC accelerated ports, 2 10/100/1000 ports, 5 FMC slots, and dual AC power supplies, Carrier Edition
FortiCarrier-3950B-DC	FCR-3950B-DC	2 SFP+ 10-Gig ports (2 SFP+ SR-type transceivers included), 4 SFP FortiASIC accelerated ports, 2 10/100/1000 ports, 5 FMC slots, and dual DC power supplies, Carrier Edition
FortiCarrier-5001B	FCR-5001B	FCR-5001B blade with 8 10-Gig SFP+, includes 2 SR SFP+ transceivers, onboard 64G SSD, Carrier Edition
Networking Blades	SKU	Description
FortiSwitch-5003B Network Blade	FS-5003B	Networking blade for FortiGate-5000 series with 8 SFP+ fabric ports, 2 SFP+ base ports, 1 10/100/1000 management port, includes 2 SR SFP+ transceivers
FortiSwitch-5203B Network Blade	FS-5203B	Networking blade for FortiGate-5000 series with 8 SFP+ Fabric ports, 2 SFP+ base ports, 1 10/100/1000 management port, includes 2 SR SFP+ transceivers
Modules	SKU	Description
FMC-XD2 Firewall Module	FMC-XD2	2 10-Gig SFP+ ports, includes 2 SR SFP+ transceivers
FMC-XG2 IPS Module	FMC-XG2	2 10-Gig SFP+ ports, includes 2 SR SFP+ transceivers
FMC-XH0 IPS Module	FMC-XH0	Security Processing Module (SP3), no external interfaces
FMC-C20 FW Module	FMC-C20	FW module, 20 10/100/1000 ports
FMC-F20 FW module	FMC-F20	FW module, 20 SFP 1-Gig ports, includes 4 SX SFP transceivers
RTM-XB2 Module	RTM-XB2	Rear Transition Module for FG-5000 series, 2 10-GbE internal ports for backplane fabric
RTM-XD2 Module	RTM-XD2	Rear transition module for FG-5000 series, 2 10-GbE internal ports for backplane fabric
Other Accessories	SKU	Description
LX Transceiver Module	FG-TRAN-LX	Transceiver LX module for all FortiGate models with SFP interfaces
TX Transceiver Module	FG-TRAN-GC	Transceiver Base-T (Copper) module for all FortiGate models with SFP interfaces, supports 10/100/1000 operation
SX Transceiver Module	FG-TRAN-SX	Transceiver SX module for all FortiGate models with SFP interfaces
SFP+ Transceiver Module	FG-TRAN-SFP+SR	10-GbE transceiver, short range SFP+ module for all FortiGate models with SFP+ interfaces
XFP Transceiver Module	FG-TRAN-XFPSR	10-GbE transceiver, short range XFP module for all FortiGate models with XFP interfaces
SFP+ Long Range Transceiver Module	FG-TRAN-SFP+LR	10-GbE transceiver, SFP+, Long Range
XFP Long Range Transceiver Module	FG-TRAN-XFPLR	10-GbE transceiver, XFP, Long Range



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



NEBS
LEVEL 3



Copyright© 2012 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.