

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 |
|----------|----------|
|----------|----------|



FortiCarrier Systems

Hardware Accelerated Performance

FortiASIC processors provide assurance that the security device will not become a bottleneck in the network

Additional Capacity on Demand

Fortinet expansion slots provide greater flexibility by supporting additional hardware-accelerated ports and localized storage of event data

Unified Security Architecture

FortiCarrier multi-threat security provides better protection and lowered costs over multiple point security products

Centralized Management

FortiManager and FortiAnalyzer centralized management and reporting appliances simplify the deployment, monitoring, and maintenance of your security infrastructure

| Technical Specifications | FortiCarrier-3810A |
|--|---|
| General | |
| SFP Ports | 2 |
| 10/100/1000 Base-T Ports | 8 |
| SFP Transceivers Included | 2 (SX) |
| Maximum SFP Ports | 26 ¹ |
| AMC Expansion Slots | 2 Double-Width 2 Single-Width |
| Performance | |
| Concurrent Sessions (TCP) | 2 M |
| New Sessions / Sec (TCP) | 40,000 |
| SIP Signalling Throughput | 10,000 messages per second |
| SIP Call Setup Throughput | 2,000 call attempts per second (CAPS) |
| SIP Signalling Sessions (Max) | 500,000 |
| Firewall Throughput | 7 / 37 Gbps ¹ |
| VPN (IPSec) Throughput | 1 Gbps / 19 Gbps ¹ |
| Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM) | 10,000 / 5,000 |
| Client-to-Gateway IPSec VPN Tunnels | 64,000 |
| Recommended SSL-VPN Users (Max) | 5,000 |
| IPS Throughput | 4 Gbps |
| Antivirus Throughput | 500 Mbps |
| MMS Antivirus Throughput | 400 messages per second |
| Unlimited User Licenses | Yes |
| Maximum Policies | 100,000 |
| Virtual Domains (Standard/Optional Upgrade) | 10 / 250 |
| Environment | |
| Power Consumption (AVG) | 270 W |
| Heat Dissipation | 921 BTU |
| Operating Temperature | 32 – 104 deg F (0 – 40 deg C) |
| Storage Temperature | -13 – 158 deg F (-35 – 70 deg C) |
| Humidity | 5 to 90% non-condensing |
| Dimensions | |
| Height | 3.5 in (88.9 mm) |
| Width | 16.9 in (429.3 mm) |
| Length | 18.5 in (469.9 mm) |
| Weight | 36 lb (16.4 kg) |
| Power | |
| Dual Power Supplies | Yes (Hot Swappable) |
| AC Power (FCR-3810A) | 100-240 VAC, 50-60 Hz, 8 Amp (Max) |
| DC Power (FCR-3810A-DC) | -48v (Normal) |
| Compliance | |
| | FCC Class A Part 15, UL/CUL, C Tick, VCCI |

FortiCarrier-3810A Multi-Threat Security Appliances

FortiCarrier-3810A appliances offer high levels of performance, scalability, and security in a compact appliance form factor. Combine the FortiCarrier-3810A with optional modules to match your performance and functional requirements.



FortiCarrier-3810A Multi-Threat Security Appliance
(Shown with no optional AMC Modules)

FortiCarrier-5000 Series Multi-Threat 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-5001A-DW Multi-Threat Security Blade
(shown with optional ADM-XB2 Module)

| Technical Specifications | FortiCarrier-5001A-DW |
|--|---|
| General | |
| SFP Ports | Requires AMC Module |
| 10/100/1000 Base-T Ports | 2 |
| SFP Transceivers Included | -- |
| Maximum Ports | 10 |
| AMC-Based Expansion Slot | 1 Double-Width |
| Performance | |
| Concurrent Sessions | 2 M |
| New Sessions / Sec | 50,000 |
| SIP Signalling Throughput | 10,000 messages per second |
| SIP Call Setup Throughput | 2,000 call attempts per second (CAPS) |
| SIP Signalling Sessions (Max) | 500,000 |
| Firewall Throughput | 2 / 13 Gbps ¹ |
| VPN (IPSec) Throughput | 800 Mbps / 7 Gbps ¹ |
| Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM) | 10,000 / 5,000 |
| Client-to-Gateway IPSec VPN Tunnels | 64,000 |
| Recommended SSL-VPN Users (Max) | 5,000 |
| IPS Throughput | 2 / 4 Gbps ¹ |
| Antivirus Throughput | 500 Mbps |
| MMS Antivirus Throughput | 400 messages per second |
| Unlimited User Licenses | Yes |
| Maximum Policies | 100,000 |
| Virtual Domains (Standard/Optional Upgrade) | 10 / 250 |
| Environment | |
| Power Consumption (AVG) | 148 W |
| Heat Dissipation | 505 BTU |
| Operating Temperature | 32 – 104 deg F (0 – 40 deg C) |
| Storage Temperature | -13 – 158 deg F (-35 – 70 deg C) |
| Humidity | 5 to 90% non-condensing |
| Compliance | |
| | FCC Class A Part 15, UL/CUL, C Tick, VCCI |

All performance values are "up to" and vary depending on system configuration.

Firewall and IPS performance is benchmarked using UDP traffic

Antivirus performance is benchmarked using HTTP traffic (32 Kbyte Objects)

SIP performance is benchmarked using signalling traffic only

MMS performance varies and depends on message size

¹ Higher performance number combines performance provided by AMC modules.

| Technical Specifications | FortiGate-5020 | FortiGate-5050 | FortiGate-5140 |
|------------------------------------|---|---|---|
| ATCA Chassis | | | |
| Available Slots | 2 | 5 | 14 |
| High Availability Backplane Fabric | Built-in | Built-in | Built-in |
| Dual Switch Module Support | No | Yes | Yes |
| Max Firewall Throughput | Up to 26 Gbps | Up to 65 Gbps | Up to 182 Gbps |
| Max VPN (IPSec) Performance | Up to 14 Gbps | Up to 35 Gbps | Up to 98 Gbps |
| Concurrent Sessions | Up to 4 Million | Up to 10 Million | Up to 28 Million |
| Dimensions | | | |
| Height | 5.25" | 8.75" | 21" |
| Width | 17" | 17" | 19" |
| Length | 15.5" | 15.5" | 19" |
| Weight | 35.5 lb (16.1 Kg) | 26.75 lb (12.1 Kg) | 64.5 lb (29.3 Kg) |
| Environment | | | |
| Power Required | AC | DC/AC ¹ | DC/AC ¹ |
| Power Consumption (AVG) | | | 531.2 W |
| Heat Dissipation | | | 1812.5 BTU |
| Operating Temperature | 32 – 104 deg F (0 – 40 deg C) | 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) | -13 – 158 deg F (-35 – 70 deg C) |
| Humidity | 5 to 90% non-condensing | 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 | FCC Class A Part 15, UL/CUL, C Tick, VCCI |

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 Multi-Threat Security System



FortiGate-5050 Multi-Threat Security System



FortiGate-5140 Multi-Threat 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 |

FortiGate-5000 Series Networking Blades

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



FortiSwitch-5003 Network Blade



FortiSwitch-5003A Network Blade



FortiController-5208 Network Blade

| Technical Specifications | FortiSwitch-5003 | FortiSwitch-5003A | FortiController-5208 |
|---------------------------------|---|---|---|
| Networking Blades | | | |
| Fabric Channel Interfaces | 3 10/100/1000 | 8 10-GbE SFP+ | 2 10-GbE XFP 8 GbE SFP |
| Base Channel Interfaces | 1 10/100/1000 | 1 10-GbE SFP+ 2 10/100/1000 | 1 10/100/1000 |
| Transceivers Included | -- | 2 10-GbE SFP+ SR | 2 10-GbE XFP SR 2 GbE SFP SX |
| Total Switching Throughput | -- | 225 Gbps | -- |
| 10-GbE Backplane Fabric Support | -- | Yes (Requires RTM-XB2/RTM-XD2) | -- |
| GbE Backplane Fabric Support | Yes | Yes | Yes |
| 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) | 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) | -13 – 158 deg F (-35 – 70 deg C) |
| Humidity | 5 to 90% non-condensing | 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 | FCC Class A Part 15, UL/CUL, C Tick, VCCI |

Security Processing Modules

Accelerate Intrusion Prevention and Multicast applications.



ADM-FE8 Module



ADM-XE2 Module



ASM-CE4 Module

See the respective module datasheet for complete technical specifications for AMC Modules.

Bypass Modules

Provide power-failure bypass operation to FortiGate system.



ASM-CX4 Module



ASM-FX2 Module

Storage Modules

Enable FortiOS security and administration functions that require local storage.



ASM-S08 Module

Accelerated Interface Modules

Accelerate Firewall and VPN applications.



ADM-XD4 Module



ADM-XB2 Module



ADM-FB8 Module



ASM-FB4 Module

Ordering Information

| Chassis | SKU | Description |
|---------------------------------------|----------------|---|
| FortiGate 5020 Chassis | FG-5020AC | 2-slot chassis with fan and dual AC power supplies |
| FortiGate 5020 Fan Tray | FG-5020FA | Spare, Fan tray for FG-5020 chassis |
| FortiGate 5020/5050 Power Supply | FG-5020PS | FortiGate-5020/5050 power supply |
| FortiGate 5050 Chassis | FG-5050-DC | 5-slot chassis with fan, 1 shelf manager card, DC powered |
| FortiGate 5050 Fan Tray | FG-5050FA | Fan tray for FG-5050 chassis |
| FortiGate-5050 Shelf Manager | FG-5050SM | Shelf manager for FG-5050 chassis |
| FortiGate-5050 SAP | FG-5050SAP | Shelf alarm panel for FG-5050 chassis |
| FortiGate 5140 Chassis | FG-5140-DC | 14-slot chassis with fan, 1 shelf manager card, no power supply included (DC powered) |
| FortiGate 5140 Power Supply | FG-5140PS | FortiGate-5140 power supply |
| FortiGate-5140 Shelf Manager | FG-5140SM-12 | Shelf manager for FG-5140 chassis |
| FortiGate-5140 SAP | FG-5140SAP | Self alarm panel for FG-5140 chassis |
| FortiGate 5140 Fan Tray | FG-5140FA | Spare, Fan Tray for FG-5140 Chassis |
| FortiGate-5053 Power Converter Tray | FG-5053 | Power converter shelf for FG-5000 series, no power supplies included |
| Security Blades | SKU | Description |
| FortiCarrier-3810A (AC Powered) | FCR-3810A | 8 10/100/1000 Ports, 2 SFP accelerated ports, and 4 AMC slots, Carrier Edition, AC Powered |
| FortiCarrier-3810A (DC Powered) | FCR-3810A-DC | 8 10/100/1000 Ports, 2 SFP accelerated ports, and 4 AMC slots, Carrier Edition, DC Powered |
| FortiCarrier-5001A-DW | FCR-5001A-DW | Security blade with 2 10/100/1000 ports and 1 double-width AMC slot, Carrier Edition |
| Networking Blades | SKU | Description |
| FortiSwitch-5003 Networking Blade | FS-5003 | Networking blade for FortiGate-5000 series with 4 10/100/1000 ports |
| FortiSwitch-5003A Networking Blade | FS-5003A | Networking blade for FortiGate-5000 series with 8 SFP+ fabric ports, 1 SFP+ base port, 2 10/100/1000 base ports |
| FortiController-5208 Networking Blade | FCTRL-5208 | Load-balancing blade with 8 SFP interfaces (2 SX-type transceivers included) and 2 XFP ports (2 XFP Transceivers included) |
| Modules | SKU | Description |
| ASM-FB4 Module | ASM-FB4 | AMC Accelerated Interface Module, single-width, 4-port SFP, includes 4 SX SFP transceivers (Accelerated FW/VPN) |
| ASM-S08 Module | ASM-S08 | AMC Storage Module, single-width, 80 GB hard disk drive (Local Disk-Based Storage) |
| ASM-CX4 Module | ASM-CX4 | AMC Bypass Module, single-width, 4-port 10/100/1000 (Power Failure Bypass) |
| ASM-FX2 Module | ASM-FX2 | AMC Bypass Module, single-width, 2-port fiber bypass module, LC-type Connectors (Power Failure Bypass) |
| ASM-CE4 Module | ASM-CE4 | AMC Security Processing Module, single-width, 4-port 10/100/1000, (Accelerated IPS / Multicast) |
| ADM-FB8 Module | ADM-FB8 | AMC Accelerated Interface Module, double-width, 8-port SFP, includes 4 SX SFP transceivers (Accelerated FW/VPN) |
| ADM-XB2 Module | ADM-XB2 | AMC Accelerated Interface Module, double-width, two port 10-GbE XFP, includes 2 SR XFP transceivers (Accelerated FW/VPN) |
| ADM-XD4 Module | ADM-XD4 | AMC Accelerated Interface Module, double-width, 4 port 10-GbE SFP+, includes 2 SR SFP+ transceivers (Accelerated FW/VPN) |
| ADM-XE2 Module | ADM-XE2 | AMC Security Processing Module, double-width, 2 port 10-Gig XFP, accelerated IPS, includes 2 SR XFP transceivers (Accelerated FW/VPN) |
| ADM-FE8 Module | ADM-FE8 | AMC Security Processing Module, double-width, 8-port SFP, includes 2 SR SFP transceivers (Accelerated IPS / Multicast) |
| 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-Gig transceiver, short range SFP+ module for all FortiGate models with SFP+ interfaces |
| XFP Transceiver Module | FG-TRAN-XFPSR | 10-Gig transceiver, short range XFP module for all FortiGate models with XFP interfaces |
| SFP+ Long Range Transceiver Module | FG-TRAN-SFP+LR | 10-Gig transceiver, SFP+, Long Range |
| XFP Long Range Transceiver Module | FG-TRAN-XFPLR | 10-Gig transceiver, XFP, Long Range |

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

MULTI-THREAT SECURITY

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

MULTI-THREAT 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 Multi-Threat 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

FortiOS Carrier 4.0—Software Features by Industry (Continued)

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 (Inspect Only) & NAT (Rewrite SIP Header) Operating Modes
 Supports SIP Servers in Proxy or Redirect Operating Mode
 Configurable RTP 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 to Prevent SIP Server Flooding / Overload
 IP Topology Hiding of SIP & RTP Server (via NAT and NAPT)
 Configurable SIP Command Control Blocks
 Unauthorized 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
 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

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 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

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

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 (up to 1000) & APN (up to 2000) 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



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
 61 Robinson Road, #09-04 Robinson Centre
 Singapore 068893
 Tel +65-6513-3730
 Fax +65-6223-6784

