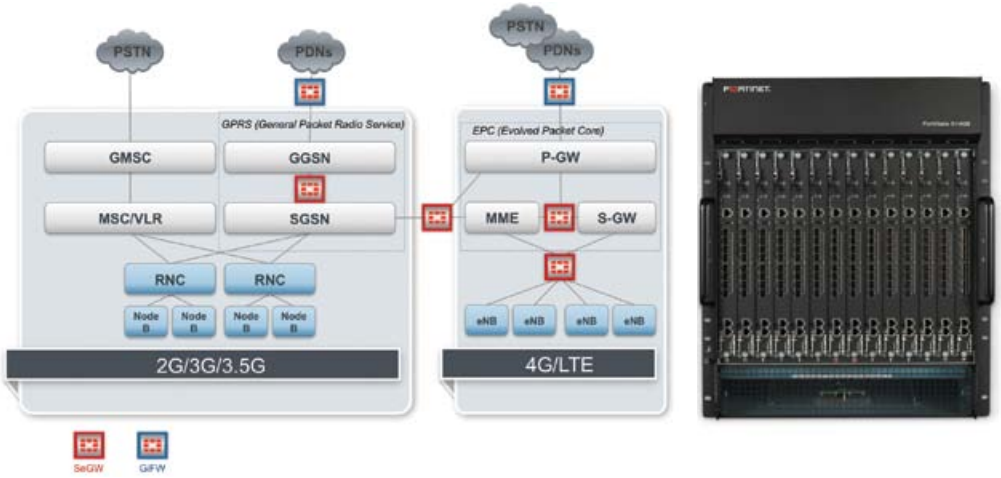
FORTINET

# FortiCarrier™ 5.0 Software

## Specialized security for service providers

### FortiCarrier 5.0 — Consolidated Security for Carriers and Service Providers

Faced with explosive growth in the number of devices and applications being added to today's mobile networks, carriers and service providers are turning to FortiGate appliances running FortiCarrier OS to provide high-performace/high-capacitance security solutions, offering long-term scalability and reliability.




### Security Gateway (SeGW) Platform

FortiCarrier OS provides the GTP and SCTP firewall functionality to secure software interfaces in both older 2G/3G GPRS core mobility networks, as well as current LTE evolved packet core (EPC) environments. Growth in supporting the large numbers of deployed evolved NodeB (eNB) platforms in the form of microcells is supported by FortiCarrier OS's high-performance/high-density VPN support. The use of virtual domains (VDOMs) in FortiCarrier OS deployments simplifies the segregation of SeGW functions into 3GPP software interfaces and device roles.

### *FortiCarrier 5.0 Security Features*

- IPv6-ready Stateful Firewall
- Dynamic Security Profiles and Groups
- Managed Security
- Voice Security
- MMS Security
- GPRS Tunneling Protocol (GTP)
- SCTP Firewall
- High-Performance and High Density VPN Concentrator – IPSec and SSL
- SSL-encrypted Traffic Inspection
- Antivirus/Antispyware and Antispam
- Intrusion Prevention System (IPS)
- Data Loss Prevention (DLP)
- Application Control
- Web Filtering
- Botnet Protection
- Client Reputation Tracking
- Endpoint Network Access Control (NAC)
- Vulnerability Management
- WAN Optimization
- Wireless Controller
- Monitoring, Logging and Reporting
- Virtual Domains
- High Availability
- Layer 2/3 Routing Services
- FortiGuard Security Updates

## Gi Firewall (GiFW) Platform

BYOD devices accessing the Internet and other data center and cloud-based packet data networks (PDNs), combined with the performance demands of today's HPSA+, LTE, and Advanced-LTE networks, GiFW solutions need to be capable of scaling to support the security requirments of many thousands of concurrent users. FortiCarrier OS provides NGFW and UTM support for IPv4/IPv6 networks, dynamic contexting of subscribers and device-type policies. Included in FortiOS Carrier is support for MMS Scanning, which extends the content filtering, antimalware, and data leaking prevention (DLP) capabilities of FortiOS into MMS-based services.

## Simplified Management

In addition to supporting a rich set of built-in GUI/CLI-based management, including internal logging and reporting, FortiCarrier OS is fully supported by FortiManager device management and FortiAnalyzer logging and analysis platform. FortiGates running both FortiCarrier OS and FortiOS devices can be managed together within a common management environment.

## FortiCarrier 5.0 — Complete Content and Network Protection for Service Providers

Service providers including MSSPs, voice operators and mobile operators will benefit from the hundreds of security-related features included with FortiCarrier 5.0. As networks migrate to IPv6 and service providers expand their portfolios to unlock new business opportunities, FortiGate consolidated security appliances running FortiCarrier OS are ready to deploy and scale as needed. FortiCarrier 5.0 includes all of the security features available in FortiOS 5.0 (see FortiOS 5.0 brochure) plus additional features benefitting service providers, some of which are highlighted below:

### Mobile Provider Security

FortiGate appliances running FortiCarrier can protect mobile network infrastructures with integrated GPRS Tunneling Protocol (GTP) Firewall functionality, which includes support for GTPv2, ensuring compatibility with a broad range of deployment scenarios. Fully integrated intrusion prevention blocks an array of GTP attacks. MMS Scanning inspects traffic on MM1/3/4/7 interfaces, and includes antivirus, flood detection, email antispam, data leakage prevention, and mobile content filtering to block phishing attacks.

### Dynamic Contexts

As their customer bases grow, carriers and services providers find themselves managing hundreds of security policies and thousands of end-users. With Dynamic Contexts, administrators can apply security policies to end-users automatically, greatly reducing the need for manual provisioning and lowering operating expenses.

### Voice Security

The Session Initiation Protocol (SIP) Signaling Firewall included with FortiGate appliances running FortiCarrier OS protects voice infrastructure interfacing with untrusted access, peering and trunking networks. Compatible with IP Multimedia Subsystem (IMS) and pre-IMS deployments, the FortiCarrier platform helps to ensure Quality of Service (QoS) by preventing flooding and network availability attacks. The SIP firewall integrates seamlessly with the FortiCarrier 5.0 intrusion prevention system, protecting voice infrastructure from Denial of Service (DoS) attacks and other network-based threats.

## How FortiCarrier OS is Licensed

Prior to FortiOS 5.0, running FortiCarrier OS required the use of dedicated FortiCarrier hardware models, which included the following:

- FortiCarrier 3810A
- FortiCarrier 3950B
- FortiCarrier 5001A-DW

Customers with dedicated FortiCarrier hardware may continue to purchase these models, as well as upgrade to FortiCarrier 5.0.

However, with the release of FortiOS 5.0, certain FortiGate models running FortiOS 5.0 can be upgraded to run FortiCarrier 5.0 with the application of a FortiCarrier Upgrade License. This is a one-time upgrade, with no additional support or recurring costs other than the initial upgrade. Currently, the FortiGate models supported by the FortiCarrier Upgrade License include:

- FortiGate 3240C
- FortiGate 3600C
- FortiGate 3700D
- FortiGate 3950B
- FortiGate 5001B
- FortiGate 5001C
- FortiGate 5101C

# FEATURES

## Managed Security

### Dynamic Contexts

- 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
- 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

### 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

### SIP Signalling 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)

### SIP Signalling Firewall (continued)

- 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)
- 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 (VDOM) Support for Additional Isolation of Infrastructure within the Same Physical Environment

## Mobile Security

### 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

- Integrated Intrusion Prevention Inspection for GTP Payloads
- For Gn/Gp Interfaces (older 3GPP) and S11 & S5/S8 Interfaces (LTE)
  - 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 Antispoofing Capabilities
  - GTP Protocol Anomaly Detection and Exploit Prevention
  - Handover Control to prevent Session Hijacking
- For Gi Interface
  - Anti-Overbilling together with Gn/Gp Firewall

# SERVICES

## FortiOS Networking

### Networking/Routing

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

### 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

### Virtual Domains (VDOMs)

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

### Data Center Optimization

- Web Server Caching
- TCP Multiplexing
- HTTPS Offloading
- WCCP Support

### 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
- Requires a FortiGate device with Hard Drive

## FortiOS Management

### Management/Administration Options

- Web UI (HTTP/HTTPS)
- Telnet / Secure Command Shell (SSH), and Command Line Interface (CLI)
- Role-Based Administration
- Multi-language Support: English, Japanese, Korean, Spanish, Chinese (Simplified & Traditional), French
- Multiple Administrators and User Levels
- System Software Rollback
- Configurable Password Policy
- Customizable Dashboard Widgets (Web UI)
- Central Management via FortiManager (optional)

### Logging/Monitoring/Vulnerability Management

- Network Vulnerability Scanning
- Graphical Report Scheduling Support
- Graphical Real-Time and Historical Monitoring
- Local and Remote Syslog/WELF server logging
- SNMP Support
- Email Notification of Events
- VPN Tunnel Monitor
- Optional FortiAnalyzer Logging (including per-VDOM)
- Optional FortiGuard Analysis and Management Service

### Firewall User Authentication Options

- Local Database
- Windows Active Directory (AD) Integration (w/ FSAE)
- External RADIUS/LDAP/TACACS+ Integration
- Xauth over RADIUS for IPSEC VPN
- RSA SecurID Support
- LDAP Group Support
- FortiToken Support

### 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

# ORDER INFORMATION

| Product | SKU | Description |
|---|---|---|
| FortiCarrier Upgrade | FCR-UPG | FortiCarrier Upgrade License Certificate for supported FortiGate models (3240C, 3600C, 3700D, 3950B, 5001B, 5001C, 5101C). |


**GLOBAL HEADQUARTERS**
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

**EMEA SALES OFFICE**
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

**APAC SALES OFFICE**
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

**LATIN AMERICA SALES OFFICE**
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480