FortiOS-Carrier Upgrade License

Faced with the explosive growth of smart personal devices, IoT sensors and applications, mobile carriers and mobile virtual network operators (MVNOs) are challenged by the ever-rising security attacks that threaten the subscribers, critical infrastructure components and their corporate brand images.

Fortinet FortiOS-Carrier license provides extended capabilities to the FortiGate appliances and modular chassis running FortiOS. The **extended capabilities are specifically designed for the mobile networks**, providing GTP, SCTP and MMS traffic inspection at massive scale to complement rich security functionalities of the standard FortiOS.

Flexible Choice of Platforms

From the cost-effective high-performance appliances to the modular carrier-grade chassis and high-end virtualized machines.

Security for Evolved Packet Core (EPC)

FortiOS-Carrier provides an EPC with a complete perimeter protection against cyber and access network attacks.

Rich Feature Set

Security functionalities such as Gi/sGi firewall for both IPv4/v6 traffic, GTP/SCTP/MMS content inspection and high-scale Security Gateway (SeGw).

Highlights

- IPv6-ready Stateful Firewall
- Dynamic Security Profiles and Groups
- VoIP 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
- Gi/sGi Firewall

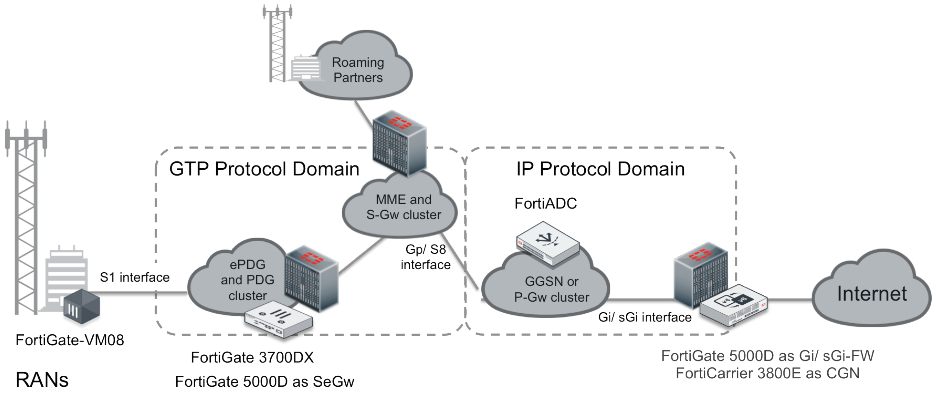
DEPLOYMENT

Security Gateway (SeGW) Platform

FortiOS Carrier 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 FortiOS Carrier's high-performance/high-density VPN support. The use of virtual domains (VDOMs) in FortiOS Carrier deployments simplifies the segregation of SeGW functions into 3GPP software interfaces and device roles.

Gi/sGi Firewall 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 LTE-Advanced, IoT and future 5G networks, GiFW solutions need to be capable of scaling to support the security requirments of many thousands of concurrent users. FortiOS Carrier 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.



HIGHLIGHTS

Service providers including voice operators and mobile operators will benefit from the hundreds of security-related features included with FortiOS Carrier upgrade license. As networks migrate to IPv6 and service providers expand their portfolios to unlock new business opportunities, FortiGate consolidated security appliances running upgrade license are ready to deploy and scale as needed. The license upgrade includes all of the security features available in FortiOS 5.6 plus additional features benefitting service providers, some of which are highlighted below:

Mobile Provider Security

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

Simplified Management

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

SPECIFICATIONS

FORTIOS CARRIER ADD-ON FEATURES	
Managed Security	
Dynamic Profiles and Groups	Assign policy profiles using RADIUS Start record with subscribers' identifying information and profile group names
	Maintain a current dynamic user context list — a list of current carrier end points, IP addresses, and profile group names received in RADIUS Start records
	Option to only accept sessions from dynamic profile users only
	Record event log messages for dynamic profile events.
	HTTP header option to extract source IP addresses and carrier end points in communication sessions
	Cookie Override, also known as browser-based override, can identify different users with differing levels of URL access, for example an adult and a child, if both users have the same IP address. One reason for this situation to occur is when multiple users are behind the same NAT device.
Carrier Networking	
SCTP Support	Protect and inspect SCTP traffic, according to RFC4960
	SCTP over IPsec VPN
	IPS DoS protection against known threats to SCTP traffic, including INIT/ACK flood attacks, and SCTP fuzzing
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)
	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
	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

Mobile Security	
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 and 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) Filterin ▪ 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/sGi Interfaces ▪ Anti-Overbilling together with Gn/Gp Firewall

ORDER INFORMATION

With the release of FortiOS 5.0, supported FortiGate models running FortiOS 5.0 and above can be upgraded with the application of a FortiOS Carrier 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, 3600C, 3950B, 3xxxD, 5001B, 5001C, 5101C, 5001D and FortiGate-VM08/16/32/UL

Product	SKU	Description
FortiOS-Carrier Upgrade	FCR-UPG	FortiOS-Carrier Upgrade License Certificate for supported FortiGate models (3240C, 3600C, 3xxxD, 3950B, 5001B, 5001C, 5001D, 5101C, VM08, VM16, VM32, VMUL).

GLOBAL HEADQUARTERS
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990