DATA SHEET

FortiOS-Carrier Upgrade Licence

One-Time Upgrade for FG-7000, 5000, 3000 Series, and VMs

The FortiOS-Carrier upgrade license extends capabilities to FortiGate appliances and modular chassis running FortiOS. The extended capabilities are specifically designed for the mobile carriers, mobile virtual network operators (MVNOs), and 4G/5G/IoT infrastructures. The service provides GTP and SCTP inspection at massive scale to complement rich security functionalities of the standard FortiOS.

FortiOS-Carrier

Flexible Product Offerings

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

Evolved Packet Core (EPC) Security

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

Rich Security Features

FortiOS-Carrier upgrade license provides enhanced security to protect the mobile core network infrastructure from malformed GTP packets, denial of service attacks, and out-of-state GTP messages.

Lower Operating Costs

Increased operational efficiency and lower costs with dynamic context security policy.

Highlights

Mobile Security

- VoIP Security
- SCTP Firewall
- GPRS Tunneling Protocol (GTP)

Traffic Inspection

- High-performance, high-density VPN Concentrator (IPSec and SSL)
- Antivirus/Antispyware and Antispam
- Intrusion Prevention System (IPS)
- SSL-encrypted Traffic Inspection
- Data Loss Prevention (DLP)
- Application Control
- Web Filtering

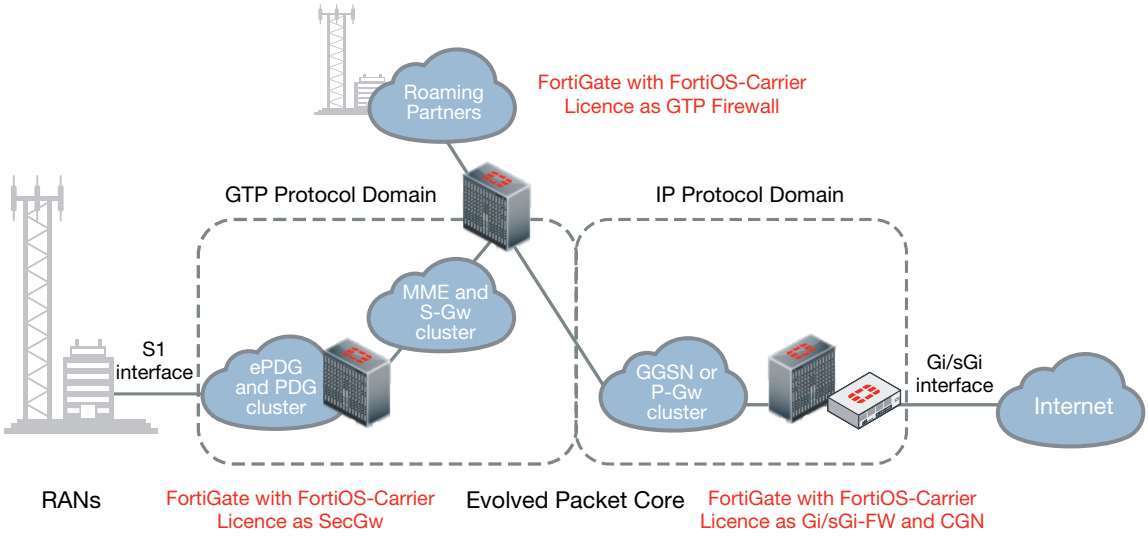
Deployment

Security Gateway (SecGW) Platforms

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) and 5G 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 SecGW functions into 3GPP software interfaces and device roles.

GTP Firewall Platform

The FortiGate GTP Firewall provides GTP protection of today's HSPA+, LTE, and LTE-Advanced, IoT and 5G networks. GTP Firewall solutions need to be capable of scaling to support the security requirements of many thousands of concurrent users. FortiOS Carrier provides GTP-C and GTP-U security, and NGFW and UTM support for IPv4/ IPv6 networks, dynamic contexting of subscribers, and device-type policies. Included in FortiOS Carrier is support for GTP-U scanning which, extends the content filtering, antimalware, and data leaking prevention (DLP) capabilities of FortiOS into GTP-U carried services.



SecGW, GTP-FW, and Gi-FW Deployment in Service Provider Networks

Highlights

Service providers including voice operators, mobile and GRX/IPX (roaming) 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 onwards plus additional features benefitting service providers, some of which are described here.

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 GTPv0, GTPv1, and GTPv2. This integrated functionality ensures compatibility with a broad range of deployment scenarios. Fully integrated intrusion prevention blocks an array of GTP attacks. GTP-U scanning inspects traffic on GTP based interfaces (like Gp and S8), and includes antivirus, flood detection, email antispam, data leakage prevention, and mobile content filtering to block phishing attacks.

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.

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 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.

Features

Managed Security

- 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
- Set the option to only accept sessions from dynamic profile users
- Record event log messages for dynamic profile events
- Activate HTTP header option to extract source IP addresses and carrier end points in communication sessions
- Set Cookie Override, also known as browser-based override, to 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

Voice Security

- Stateful and SIP Protocol-Aware Firewall
- SIP Transparent (Inspect Only) and NAT (Rewrite SIP Header) Operating Modes
- Supports SIP Servers in Proxy or Redirect Operating Mode Configurable RTP Pinholing Support
- Supports Complex Source and Destination SIP NAT Environments (SIP and RTP Protocols)
- 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 and 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)
- NAT IP Preservation Retains Originating IP Address for Administrative Purposes (e.g. Billing)
- Intrusion Prevention System with VoIP Protocol Anomaly and 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
- Hardware Accelerated RTP Processing for Reduced Packet Loss, Packet Latency, and Jitter

Carrier Networking

- SCTP over IPsec VPN with multihoming support
- Protect and inspect SCTP traffic according to RFC4960
- IPS DoS protection against known threats to SCTP traffic, including INIT/ACK flood attacks, and SCTP fuzzing

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, and Type Screening
  - GTP Stateful Inspection
  - Hanging GTP Tunnel Cleanup
  - GTP Tunnel Fail-Over for High Availability
  - GTP IMSI Prefix (up to 1000) and APN (up to 2000) Filtering
  - GTP Sequence Number Validation
  - Detecting GTP-in-GTP Packets
  - GTP Traffic Counting and Logging
  - GTP Protocol Anomaly Detection and Exploit Prevention
  - IP Fragmentation of GTP Messages
  - GSN Tunnel Limiting and Rate Limiting
  - GGSN and SGSN Redirection
  - Anti-Overbilling Together with Gi Firewall
  - Encapsulated Traffic Filtering with Antispoofing Capabilities
  - Rate Limiting
  - Session Timer Settings
  - Usage for other less common interfaces like S2a and S2b
  - Support for 5G N9 interface
  - Handover Group Control to prevent Session Hijacking
  - Message filtering (unknown/path/tunnel/mobility/trace management messages, restauration and recovery, CS Fallback and SRVCC related messages
  - Handover groups
  - MNC/MCC filtering
  - Message type filtering
  - RAT type filtering
  - Location filtering
  - IMEI filtering
  - MSISDN filtering
  - IE removal policy

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.

Product	SKU	Description
FortiOS-Carrier License Upgrade	FCR-EUPG	FortiCarrier Upgrade License Certificate for supported FortiGate models (3240C, 3600C, 3xxxD, 3900E series, 3950B, 5001B, 5001C, 5001D, 5001E, 5101C, 7000E series, 6000F Series, VM08, VM16, VM32, VMUL. Note: VMxxV and VM subscription series are not supported).

FST-PROD-DS-FCR2

FCR-OS-DAT-R6-202010