FortiOS-Carrier Upgrade License

Highlights

Mobile Security

- GPRS Tunneling Protocol (GTP)
- Packet Forwarding Control Protocol (PFCP)

Traffic Inspection

- High-performance and high-density

One-Time Upgrade for FG-7000, 4000, 3000, 2000 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 5G/4G/IoT infrastructures. The service provides GTP and PFCP inspection at massive scale to complement rich security functionalities of the standard FortiOS.

FOS

Available in

Appliance

Virtual

Features

Flexible Product Offerings

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

5G Core (5GC) and Evolved Packet Core (EPC) Security

FortiOS-Carrier provides an EPC with a complete perimeter protection against cyber and access network attacks. FortiOS-Carrier covers architectures using Control and User Plane Separation (CUPS) as well as the roaming and RAN-Core interfaces.

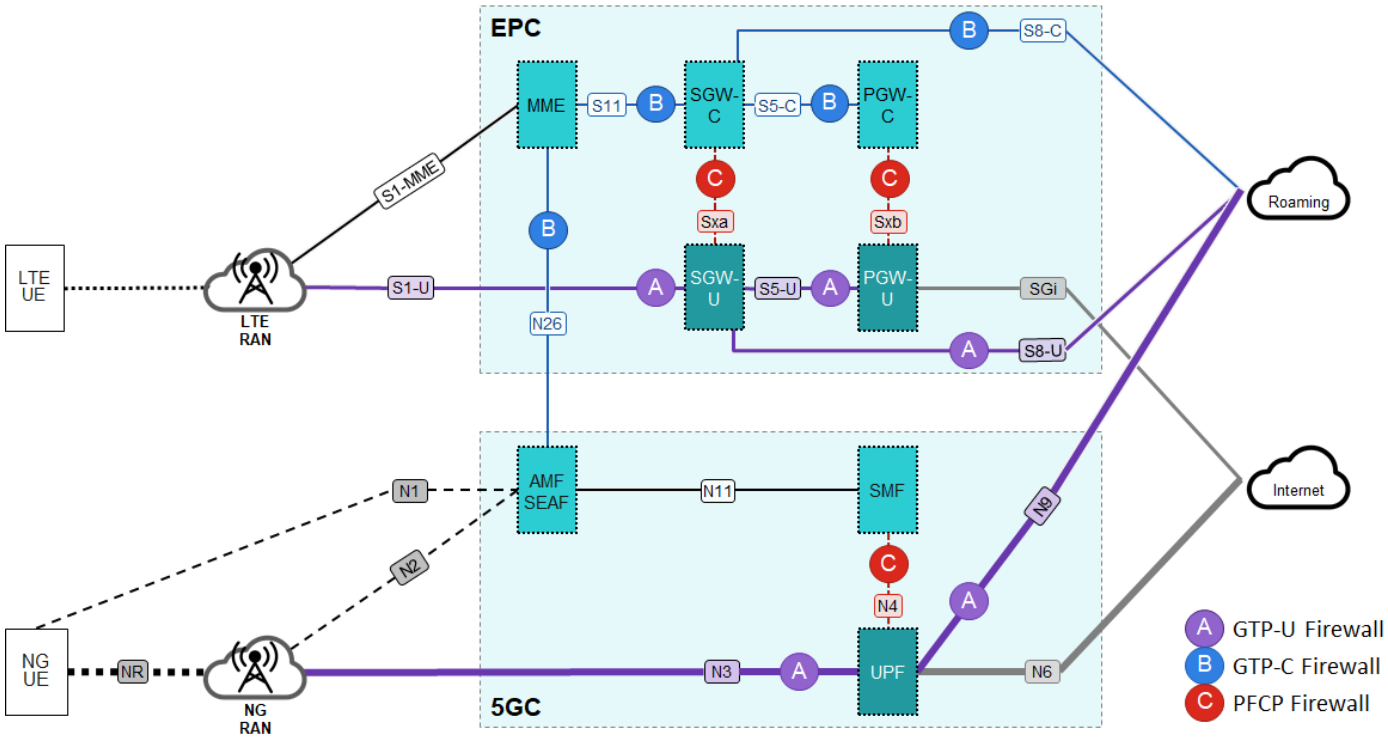
Rich Security Features

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.

GTP Firewall and PFCP Firewall Deployments in 4G and 5G Networks



Deployment

GTP Firewall Platform

The GPRS Tunneling Protocol (GTP) is a protocol that is used 1) to encapsulate user traffic for mobility and roaming use cases (called GTP-U), and 2) to carry control information about the subscriber sessions (called GTP-C).

The FortiGate GTP Firewall provides GTP protection of today's 5G, 4G, and 3G 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 security, and NGFW and UTM support for IPv4/ IPv6 networks, dynamic filtering of subscribers, and device-type policies. In addition, FortiOS supports GTP-U scanning which, extends the content filtering, antimalware, and data leaking prevention (DLP) capabilities of FortiOS into GTP-U carried services.

The GTP Firewall can be used in the 3GPP interfaces N3, N9, N26, S1-U, S11, S10, S5, S8, S4, S3, S4, S2a, S2b, Gn, Gp.

In the N3 and S1-U interfaces, the GTP Firewall functionality can be combined with a Security Gateway (SecGW) functionality when combined with a relevant control-plane input such as N4, S11.

PFCP Firewall Platform

The Packet Forwarding Control Protocol (PFCP) is a protocol that is used to carry control information about the subscriber sessions between the control plane network functions and the user plane network functions in network architectures using CUPS (Control and User Plane Separation).

The FortiGate PFCP Firewall provides PFCP protection of today's 5G and 4G networks. PFCP Firewall solutions can scale to support the security requirements of many thousands of concurrent users.

The PFCP Firewall can be used in the 3GPP interfaces N4, Sxa, Sxb.

Highlights

Service providers including voice operators, mobile and GRX/IPX (roaming) operators will benefit from the many 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. On top of the security features available in FortiOS, The FortiOS Carrier license upgrade provides additional features benefitting service providers, some of which are described here.

Mobile Provider Security

FortiGate appliances running FortiOS Carrier can protect mobile network infrastructure and services 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 anomaly detection blocks an array of GTP attacks.

Additionally, FortiOS provides GTP-U payload scanning that inspects traffic on GTP-based user plane interfaces (like N9, S8, or Gp), and includes antivirus, flood detection, email antispam, data leakage prevention, and mobile content filtering to block attacks.

Control and User Plane Separation

Starting with 3GPP R14 a new architecture has been implemented for both EPC and 5GC, where the control and user plane network functions have been separated to allow independent scaling for each traffic plane and the possibility of remotely controlling the forwarding nodes. This functionality has been enabled by the use of the Packet Forwarding Control Protocol (PFCP). Subscriber session information is now communicated between the control plane and the user plane using PFCP.

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. FortiGate nodes running both FortiOS Carrier and FortiOS devices can be managed together within a common management environment. Furthermore, the support of the FortiOS REST API enables additional orchestration and integration options.

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

PFCP Carrier Networking

- Protect and inspect PFCP traffic:
  - PFCP message tracking
  - PFCP message filtering
  - PFCP protocol anomaly detection
  - PFCP message logging
- HA/FGCP support

GTP Firewall

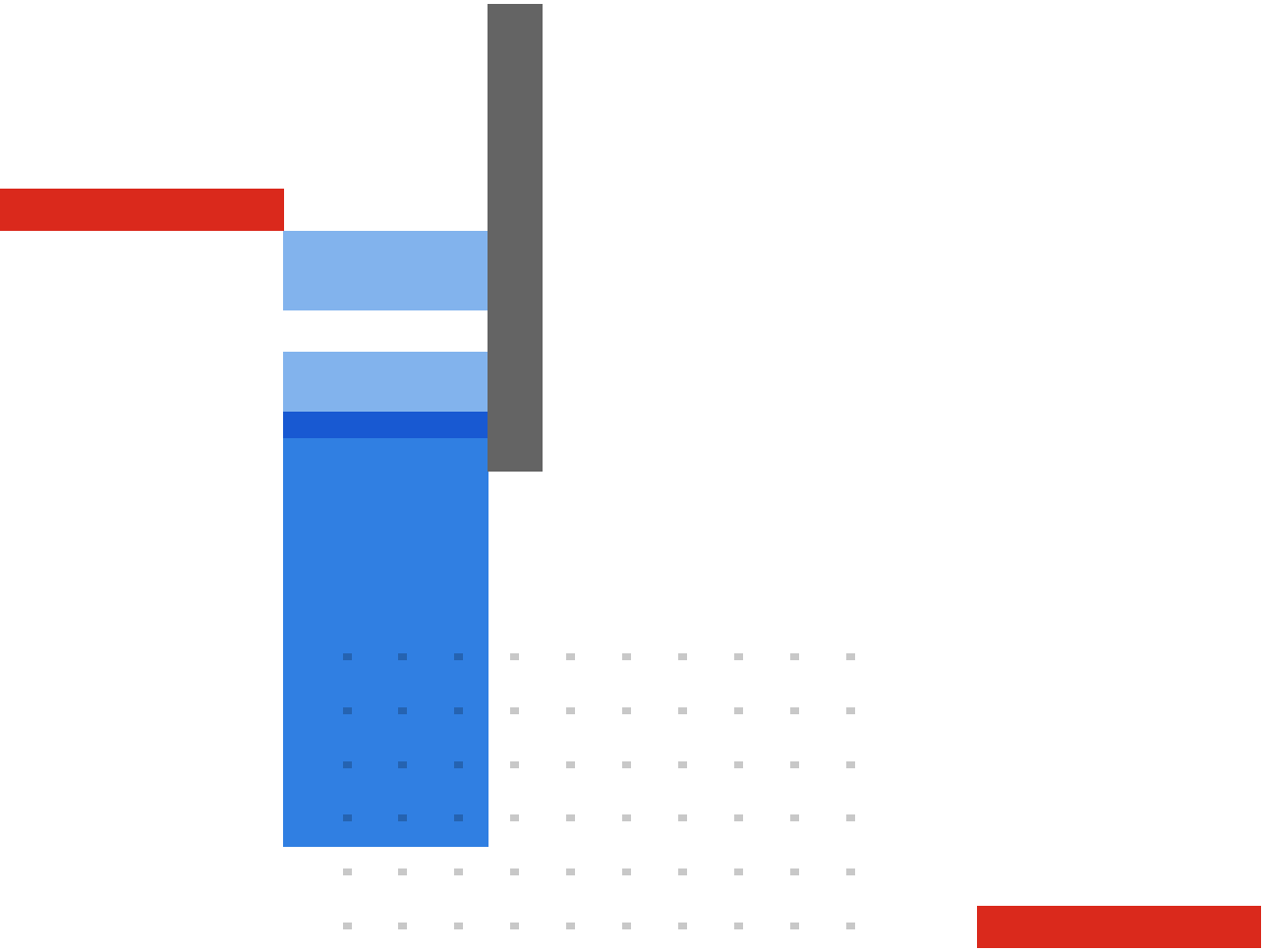
- Integrated Intrusion Prevention Inspection for GTP Payloads
- For N26 (5GC/EPC interworking) S10, S11 and S5/S8 Interfaces (LTE/EPC), and S3, Gn/Gp Interfaces (older 3GPP):
  - GTP Tunnel Fail-Over for High Availability
  - GTP IMSI Prefix (up to 1000) and APN (up to 2000) Filtering
  - GTP Protocol Anomaly Detection and Exploit Prevention
  - GSN Tunnel Limiting and Rate Limiting
  - GGSN and SGSN Redirection
  - Anti-Overbilling Together with Gi Firewall
  - Encapsulated Traffic Filtering with Anti-spoofing Capabilities
  - Usage for other less common interfaces like S2a and S2b
  - 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
- For 5G N3 and N9 interfaces (5GC), S5/S8 Interfaces (LTE/EPC), and S4, Gn/Gp Interfaces (older 3GPP)
- GTP Packet Sanity Check, Length Filtering, and Type Screening
- GTP Stateful Inspection

Ordering Information

Product	SKU	Description
FortiOS-Carrier License Upgrade	FCR-EUPG	FortiCarrier Upgrade License Certificate for supported FortiGate models (260xF, 3000 series and above, VM08/VM08-v, VM16/VM16-v, VM32/VM32-v, VMUL/VMUL-v. Note: VM S-Series is not supported).

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

December 21, 2023

FCR-OS-DAT-R8-20231221