WHITE PAPER

Providing Enhanced GTP Security in Mobile Networks

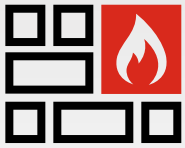
Fortinet GTP Firewall and NetNumber Signaling Firewall Integration

Executive Summary

The constantly evolving attack techniques used by different threat actors demand extensive and advanced detection and protection. Comprehensive signaling firewall solutions are needed to secure the vulnerable roaming connections of the 2G/3G and 4G/LTE mobile networks, as well as in 5G non-standalone (NSA) roaming scenarios.

The Fortinet FortiGate GTP Firewall and NetNumber Signaling Firewall are integrated to provide mobile operators an advanced, flexible, and all-encompassing solution to secure their mobile roaming against current and future threats.

The solution and its integration between different security tools to create a cooperative security system for roaming GTP-based attacks is fully aligned with Gartner's Cybersecurity Mesh Architecture (CSMA)[1] as an effective implementation strategy to the rapid evolution and sophistication of cyberattacks. The solution's further integration with more security tools, such as Fortinet Security Information and Event Management (SIEM), is part of the Fortinet Security Fabric, built from the foundation as a security mesh platform.



The Fortinet FortiGate GTP Firewall and NetNumber Signaling Firewall are integrated to provide mobile operators an advanced, flexible, and all-encompassing solution to secure their mobile roaming against current and future threats.

Secure Mobile Roaming Traffic with Integrated Signaling Firewalls

Mobile services continuity while traveling is the de facto expectation of mobile devices and users, also applicable to Internet-of-Things (IoT) roaming device use cases (e.g., automotive tracking and tracing). Roaming involves comprehensive interactions between the visited network and the home network, initially achieved with SS7 and GTP signaling protocols for 2G/3G networks, and later with Diameter and GTP for 4G/LTE and 5G NSA roaming.

These interactions provide the home operator, who is responsible for the mobile service, with constant updates as to the subscriber's location (location updates). They also support the transfer of credentials to authenticate the connecting device and the transfer of service settings to the visited network. Finally, these interactions open data connections, apply specific policies for data usage, and feed the wholesale and retail billing processes.

Because these older signaling protocols lack built-in security features and their protection initially relied on the physical protection of separated network transport resources, these interactions involve the open transfer of critical and privacy sensitive data. The data security provided by the physical protection of network resources degraded with the evolution to the use of IP as the transport layer. In addition, risk associated with an ever-increasing attack surface became even more prevalent with the opening of the signaling networks for services like track and trace and remote network management via internet connections.

As cyber threats evolve, including bank fraud and location tracking, mobile operators are being demanded by regulatory authorities and guided by standardization organizations like 3GPP and GSMA to protect their networks and subscribers with signaling firewalls. Continued technical improvements and features are needed to keep up with the evolving threat landscape. One such improvement is the intelligent use of federated data from all SS7, Diameter, and GTP firewalls to detect and defeat the latest wave of advanced exploits.

Signaling Firewall and GTP Firewall

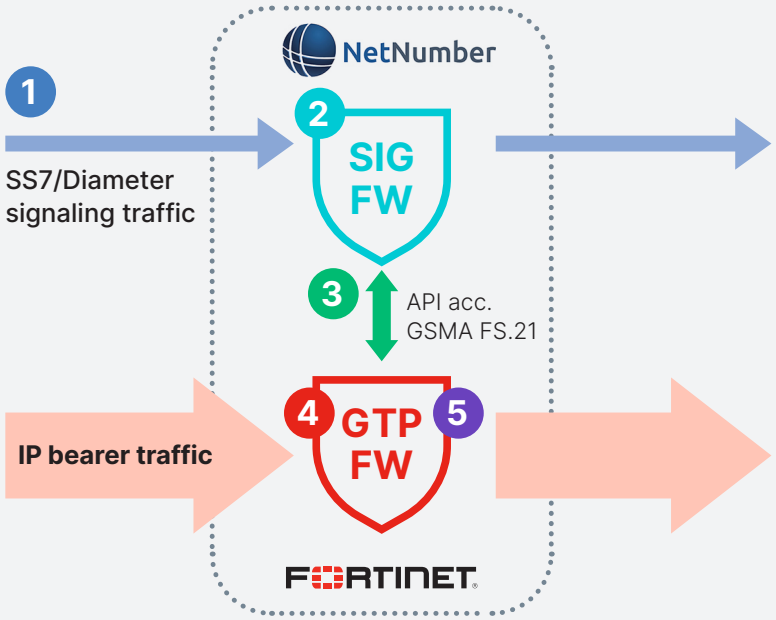
Mobile roaming involves SS7 and Diameter for mobility management and GTP for data-session management. Both control capabilities are very distinct. SS7 and Diameter are low-volume signaling protocols used for a wide variety of network control actions, including SMS as a simple user content transfer capability. In a complimentary way, GTP facilitates the high-volume user data transfer using elementary control actions for data session management.

To improve protection against GTP vulnerabilities and attacks, detailed information that is seen in SS7 and Diameter can provide additional context to assist a GTP firewall with pin holing and quality-of-service actions in user plane security policies. In the following diagram, the combined operation of the NetNumber Signaling Firewall and the Fortinet FortiGate GTP Firewall via API integration, based on GSMA FS.21 guidelines ("Interconnect Signaling Security Recommendations"), is illustrated.

1. NetNumber SIG FW secures the roaming management traffic via SS7 and Diameter
2. Fully configure Message Dissectors to extract SS7 and Diameter parameters
3. Real-time cross-checks between SIG FW and GTP FW to authorize GTP sessions
4. High volume screening of GTP-U/GTP-C user traffic and control signaling flow
5. GTP session requests are verified, and non-authorized sessions are blocked

Solution

Combined NetNumber SIG FW and Fortinet GTP FW using a shared API for data exchange



The combination of Fortinet GTP Firewall and NetNumber SIG Firewall offers a unique combination in the industry, as both vendor products are designed and deployed as carrier-grade platforms for mission-critical services. This enables an inline deployment on the interfaces for both the time-critical high-volume GTP user plane traffic and the low-volume core network SS7 and Diameter control plane traffic. The resulting 100% traffic screening and filtering has no impact on availability or performance.

In addition, monitoring all roaming traffic makes the operation of the combined solution fully independent. Thus, there is rarely a need to query other network elements such as HLR or HSS, avoiding possible DDOS effects on these critical network elements.

This enhanced GTP security solution can be added as an incremental innovation in networks that have the Fortinet FortiGate GTP Firewall and NetNumber Signaling Firewall already deployed or added to networks that already have one of the two components.

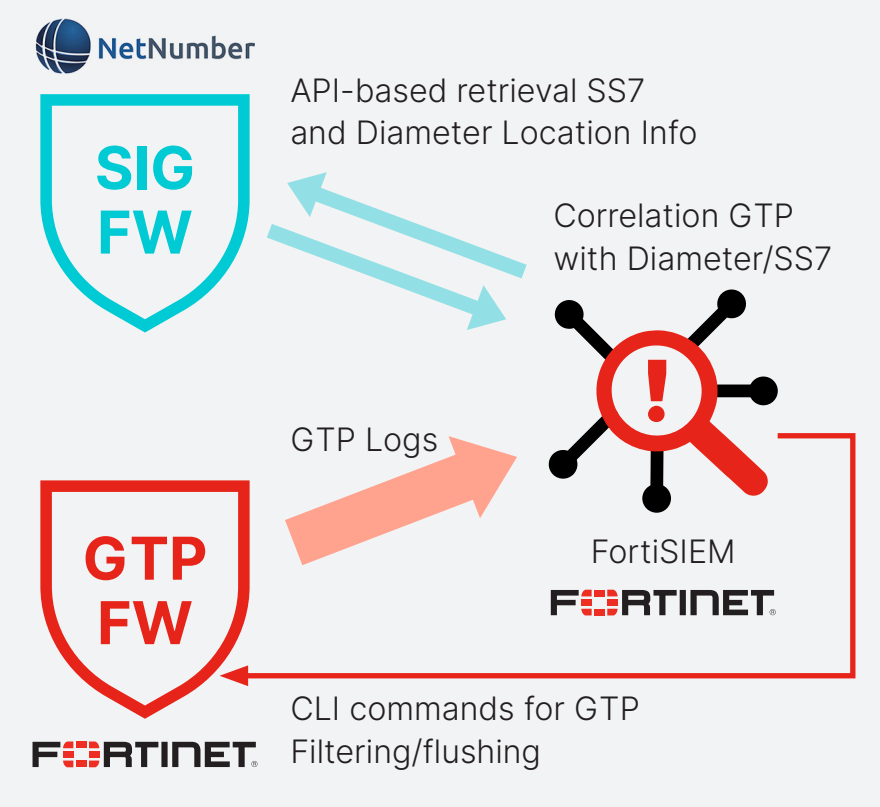
Protecting Against GTP-based Attack Scenarios

Billing fraud and subscriber impersonation

Various attacks that depend on manipulations of the GTP signaling messages can be prevented by real-time correlation and cross-checking of the GTP source with the subscriber location known via Diameter/SS7 location updates. Examples of well-known attack scenarios with manipulated GTP messages are:

- **Billing fraud:** Exploitation of spoofed or stolen IMSIs in GTP messages can be avoided by verification of the subscriber locations with the current location available from the NetNumber Signaling Firewall, or when not already available, via Diameter or SS7 MAP signaling queries to the HSS/HLR.
- **Subscriber impersonation:** Use of spoofed MSISDN for abusive web authentication can be protected against by cross-validation of the MSISDN with the MSISDN known by the NetNumber Signaling Firewall, or when not already known, via Diameter or SS7 MAP signaling queries to the HSS/HLR.

The following figure depicts how Fortinet FortiSIEM GTP correlation retrieves the current device location from the NetNumber SIG Firewall, learned by inspecting Diameter and SS7 MAP location updates and optionally by querying the HSS or HLR.



The FortiSIEM correlates the GTP source with the last known device location and can instruct the FortiGate GTP Firewall to reject the GTP session in case a violation is detected between the GTP source and the last known end-user location.

Redirecting GTP traffic

This refers to attack instances where the traffic on the GTP downlink is redirected to a false serving gateway (SGW). This can be prevented by blocking manipulated Update PDP Context or Modify Bearer Request messages, thereby avoiding the possibility that an existing data session be rerouted and listened to. Such detection relies on GTP Cat.3 plausibility checks by the Fortinet GTP Firewall and FortiSIEM correlation with subscriber location information available from the NetNumber SIG FW via Diameter and SS7 MAP message inspection, or when not already available at the SIG Firewall via queries to the HSS/HLR.

Malware attacks on mobile core networks

Various mobile networks have been subject to highly sophisticated intrusion techniques by intruder groups like LightBasin,[2] with extensive knowledge of telecommunications protocols and the ability to execute remote attacks exploiting compromised devices via encapsulated command and control (C2C) instructions delivered as part of GTP roaming sessions.

Thus far these manipulation techniques were assumed to be used for intelligence gathering purposes. They used non-intrusive means to retrieve specific information about the location and call data information of traced mobile subscribers. However, the same techniques could also be abused for more destructive purposes.

Real-time correlation with the location information exchanged via Diameter and SS7 MAP can detect and block these abusive GTP sessions, in addition to scanning for inconsistencies between IP addresses.

Evolving GTP Attack Scenarios

This non-exhaustive list of GTP-based attack scenarios demonstrate the attacks' evolution, which calls for a more extensive and advanced inter-signaling detection and protection.

In addition, GTP in isolation has become a more attractive target as mobile operators around the world tighten the protection of their SS7 and Diameter roaming interfaces with more precise network configuration data and the deployment of SS7 and Diameter integrated signaling firewalls.

Future extension to 5G SA roaming scenarios

The GTP-U protocol is used in 5G user plane for carrying user data. Thus, in the 5G standalone (SA) roaming scenarios, i.e., between 5G Core networks with HTTP/2 as roaming interfaces, the same integration between SIG Firewall and GTP Firewall will be needed.

In addition, this migration to 5G SA roaming scenarios will take a long time in a global perspective, implying that an investment in the Fortinet and NetNumber integrated solution for GTP security across 2G/3G and 4G/LTE (including 5G NSA) is reusable and expandable to the 5G SA roaming scenarios.

Conclusion and Future Perspective

In 2G/3G and 4G/LTE, the correlation between GTP Firewall policies and Diameter and/or SS7 MAP mobility management information is becoming increasingly critical to better protect both end-users and mobile core networks from sophisticated attacks involving billing fraud, impersonation, data interception, and malware delivery.

Correlating GTP Firewall actions with Diameter and/or SS7 MAP mobility management information is future-proof and extendable to 5G.

This white paper is intended to provide an overview of the capabilities afforded by the combined deployment of Fortinet's FortiGate GTP Firewall and NetNumber's Signaling Firewall and is subject to change from time-to-time. Application to any specific network is dependent on network characteristics. For more information, please contact your Fortinet and/or NetNumber representative.

About NetNumber

NetNumber, Inc. brings more than two decades of experience delivering core network signaling control platforms that power global telecom and enterprise networks. Our industry leading TITAN™ Centralized Signaling and Routing Control (CSRC) platform has been deployed by operators across the globe to simplify core networks in order to deliver new services and reduce operating costs.

TITAN.IUM™, the latest evolution for NetNumber, is an innovative, intergenerational framework for 5G that bridges legacy 2G, 3G, and 4G technology to the new cloud-native era. TITAN.IUM enables our customers to migrate multiple generations of services, to a common, secure, simplified modern ecosystem. This means that the legacy applications can benefit from the technology of next generation of networks that are containerized, scalable and ultra-low latency. For more information visit www.netnumber.com.

[1] "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Gartner, October 18, 2021.

[2] Jamie Harris and Dan Mayer, "LightBasin: A Roaming Threat to Telecommunications Companies," October 19, 2021.

FORTINET

www.fortinet.com

April 11, 2022 11:37 PM

1550965-0-0-EN