SOLUTION BRIEF

GTP FIREWALL IN 4G AND 5G MOBILE NETWORKS

STRONG PROTECTION FOR ALL GTP INTERFACES

OVERVIEW

5G promises higher speeds, lower latency, and a multitude of new IoT applications. Operators are aware that secure, seamless interconnection with low latency and high speed is essential for a quality subscriber experience and to capture the new industrial and commercial 5G opportunities.

But with this new opportunity also comes higher security risks as cyberattacks grow in sophistication and volume and use lightly protected mobile and IoT devices in their botnets or targeted attacks.

GPRS Tunneling Protocol (GTP) has been at the heart of providing seamless interconnection and is responsible for carrying traffic between roaming or home subscribers and key network interfaces in 4G, 5G non-standalone (NSA), 5G standalone (SA), and mobile edge compute architectures. As traffic, devices and interconnection partners surge, so does the use of GTP. The transition to 5G will take time and most operators will opt to deploy 5G in stages, using a common 4G core as they build out the 5G RAN. As a result, threats to 4G core elements from GTP-based attacks will still be present during this hybrid period.

Operators must now include a GTP firewall as part of their current network security posture and as they evolve the network to 5G.

SECURE GTP NEEDED THROUGHOUT 5G MIGRATION

GPRS Tunneling Protocol (GTP) has been used to carry traffic and signaling through mobile networks since early 3G (2.5G) and has continued to be used in 4G/LTE and recent 5G non-standalone architectures. In 4G and 5G NSA, GTP control and user plane are used for the roaming (S8) interface and between eNodeB and SGW on the S1U, and between SGW and PGW on the S5. (See Figure 1)

The 5G non-standalone (NSA) models defined by 3GPP, combined with multi-access edge compute provide a path for mobile network operators to upgrade existing RANs to 5G while still leveraging a common 4G core. In pure 5G, or 5G standalone (SA), the GTP control plane will be replaced by HTTP/2, but the GTP user plane will remain, located on the N3 and N9 interfaces between the user plane function and the Security Edge Protection Proxy (SEPP-U).

CHALLENGE

To capture new opportunities, operators must offer secure, low latency, fast and seamless service wherever needed and with any device type. In this ultra-fast digital world, operators must protect their networks and subscribers from growing threats at interfaces using GTP.

SOLUTION

Boost security for 4G and 5G NSA networks with GTP firewall, part of the 5G security portfolio. GTP firewall aims to protect against GTP protocol vulnerabilities, fraudulent use, confidentiality breaches, DDoS attacks by malicious peers and other threats.

BENEFITS

Meet growing network requirements for new applications while protecting the network and subscribers from malicious attacks via GTP interfaces. Highest performance and lowest latency is maintained as packets are inspected for suspicious abnormalities.

MOBILE OPERATOR CHALLENGES

The GTP protocol used in the roaming and other evolved packet core (EPC) interfaces has known vulnerabilities that can be readily exploited by malicious actors. As vulnerable devices and partners expand, so does the attack surface available for malicious purposes. Operators must meet the growing security challenges while also providing a seamless subscriber experience – wherever they travel, whatever devices they use, whatever network is accessed.

SCALABLE SECURITY REQUIRED

The mobile network must now support higher throughput, higher session counts at smaller packet sizes and lower latency. In addition, operators are rapidly moving to distributed mobile edge architectures requiring virtualized core elements and container-based applications.

For GTP firewalls, (which touch a significant amount of control and data traffic between the RAN / roaming interfaces and the core) high scalability, high performance and built-in security are essential and in all form-factors used - physical, virtual and container.

INTERNATIONAL ROAMING TRAFFIC SURGES AND SO DO THE VULNERABILITIES

For a successful transition to 5G, mobile operators need to provide secure, seamless interconnect through roaming and IPX partners.

In 4G networks, International roaming traffic (using GTP protocol through the S8) has already significantly increased with the launch of the EU Roam Like at Home legislation in 2017 which prohibited excessive roaming fees. Global international roaming traffic – voice and data – has surged. and it is expected to grow 32X by 2022 and to reach over 1.5 Mb per subscriber annually.[1] Roaming traffic now has the same characteristics and usage patterns of all other mobile traffic, including roaming IoT devices, and the same security vulnerabilities. Partly because roaming traffic had previously been relatively small, many operators had deployed minimal or no security devices at the roaming interface (S8) in their LTE networks.

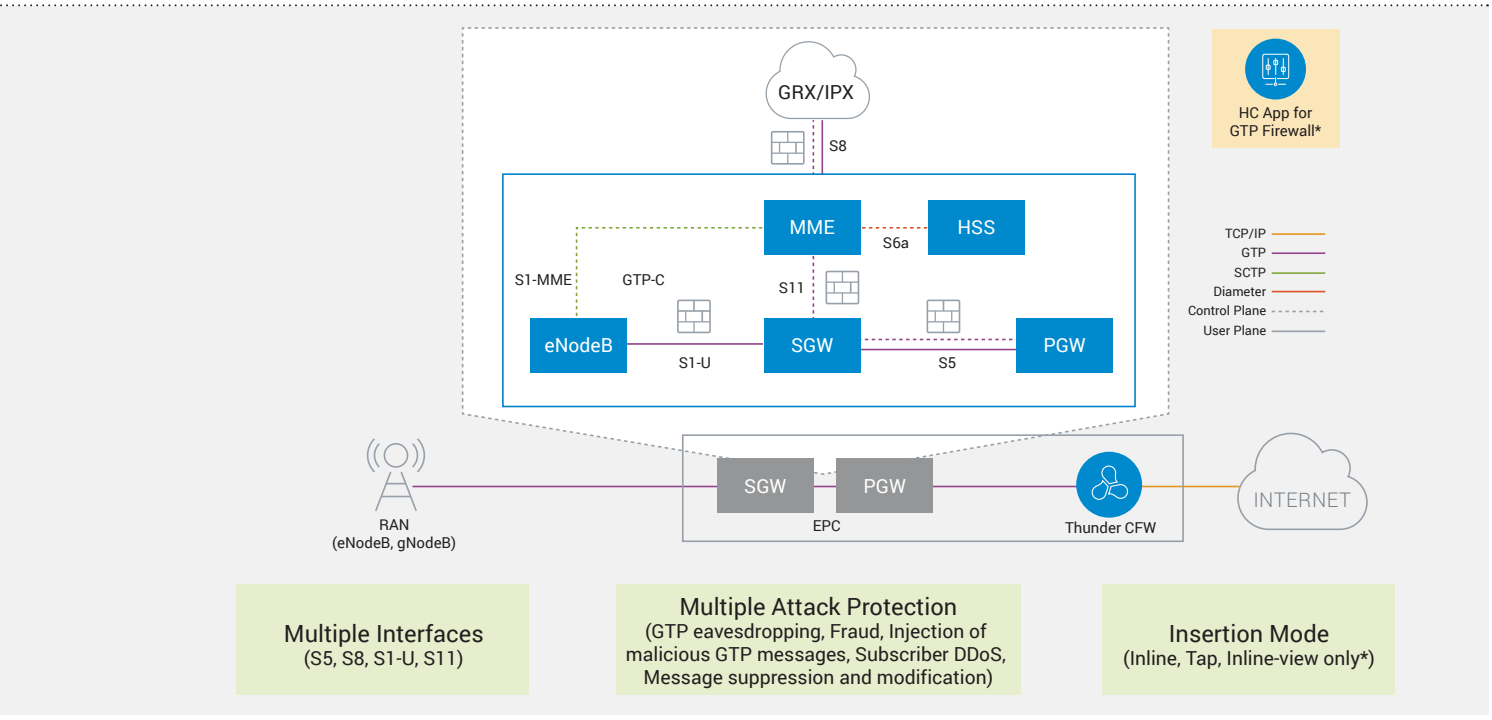

Figure 1. A10 Networks GTP firewall network insertion points

[1]Juniper Research, "Roam Like at Home - Impact Explained".

GTP THREATS AND VULNERABILITIES

GTP was never designed with security in mind and therefore has no inherent security mechanisms. GTP vulnerabilities have been well known by the industry and are documented in GSMA FS.20 – GPRS Tunneling Protocol Security and IR.88 LTE and EPC Roaming Guidelines, and others, which recommend deployment of a GTP firewall between the EPC and IPX roaming network. Attackers try to exploit GTP vulnerabilities by abusing GTP interfaces exposed to the network. Attackers can include cybercriminals or malicious peers that have been able to control the GRX/IPX roaming links. These attacks target both mobile subscribers and mobile network infrastructure. Common GTP security issues include confidential data disclosures, denial of service, network overloads, and a range of fraud activities.

GTP FIREWALL FOR 4G, MEC AND 5G DEPLOYMENTS[2]

The A10 Networks GTP firewall protects network infrastructure and subscribers against GTP-based attacks, including the following common attack types:

- **Eavesdropping** – intercepting and snooping into GTP traffic gaining valuable and confidential subscriber information
- **Fraud**: Attackers can use services at the expense of the operator or another subscriber using invalid or hijacked IMSI
- **Injection of malicious GTP messages**: Disrupting sessions and creating DDoS
- **Subscriber denial of service**: Generate excessive volumes of malicious messages causing service disruption
- **Message Suppression and Modification**: Prevent message delivery or allow malicious content delivery, disrupting service
- **Network Overload / DDoS**: Malicious, malformed or invalid signaling packets are sent that overwhelm network elements or cause vulnerable elements to fail.

The above checks can be performed by the GTP firewall when it has access to control information in 4G, 5G-NSA, 5G SA (via SEPP or other network element). The GTP firewall is part of the A10 Networks 5G solution portfolio and uses the A10 Thunder® Convergent Firewall (CFW) product.

Thunder CFW is a high-performance, converged security product for mobile service providers that consolidates firewall functions for mobile network interfaces with CGNAT, IPsec VPN, ADC, DPI for visibility, subscriber-aware intelligent traffic steering and rate limiting into a single solution. A single Thunder CFW, available in physical, virtual, container or bare metal form factors delivers unmatched performance and comprehensive security services to support the 5G-ready mobile infrastructure and evolving multi-access edge computing (MEC) architectures. This solution is a cost-effective approach for strengthening security postures, protecting network infrastructure without the need for disparate point products that add latency and complexity.

The GTP firewall can be inserted into multiple interfaces carrying the GTP traffic. The primary use case is being inserted on S5-Gn and S8-Gp (roaming firewall) interfaces. The GTP firewall can operate as a standalone instance (after proper configuration) or can be integrated with several components residing in the operator ecosystem.

FEATURES AND BENEFITS

GTP firewall provides security and scalability, while protecting the mobile core against GTP-based threats such as information leaks, malicious packet attacks, and DDoS attacks through GTP interfaces in the access networks and GRX/IPX interconnect to support uninterrupted operations. GTP firewall features are included in A10 Networks Advanced Core Operating System (ACOS) and as part of the of the A10 Thunder Convergent Firewall (CFW), along with other key components such as stateful layer 4 firewall, L7 visibility, granular SCTP filtering, integrated DDoS protection and CGNAT.

GENERAL FIREWALL FEATURES

- **Multi-purpose, multi-interface**: The same GTP functions can be deployed on multiple mobile network interfaces using the multi-function CFW. This simplifies operations and helps reduce both OPEX and CAPEX.
- **Flexible form factors**: The software can be deployed on all Thunder CFW physical appliances[3], vThunder (virtual), bare metal or container options. This provides operators maximum deployment flexibility for hybrid and MEC networks.

[2]Available on ACOS 5.0 shipments.
[3]Thunder 14045 CFW excluded.

- **Highest performance and scale**: Thunder CFW is a powerful and comprehensive security solution that delivers the ultra-high performance needed to meet current and future mobile network deployments for 4G, 5G-NSA, 5G-SA, and MEC architectures, with industry-leading throughput, low latency and concurrent session processing in compact physical and virtual network form factors.

GTP SECURITY FEATURES

- Compliant with GSMA Guidelines in FS.20
- Supports GTPv0-C, GTPv1-C, GTPv2-C, GTP-U
- Stateful inspection and protocol validation
- Message validation
  - On interface, network, transport and protocol levels
  - Integrity validation and plausibility checks
  - Message anomaly identification and filtering, including unsupported types, out of order and invalid fields
- Filtering based on IMSI, APN, MSISDN, RAT type
- Correlation between data on the same layer and information from different layers
- GTP in GTP Identification
- Granular real-time monitoring and visibility
- Anti-spoofing (end-user IP address) – drops and logs GTP-U messages
- GTP-C/U correlation and logging
- GTP rate limiting per peer, APN prefix, tunnel

ANALYTICS, REPORTING, MANAGEMENT

- Integration with GTP Analytics systems on Harmony Controller
- Event-driven logging messages
- Full-featured RESTful APIs offer rapid integration with third-party management consoles

SOLUTION COMPONENTS

- GTP firewall
- Thunder Convergent Firewall (CFW)
- Harmony Controller
- RESTful APIs for integration with third-party management systems

PROVIDE SECURE MOBILE SERVICES

The GTP firewall feature set is included in the A10 Thunder CFW, along with several other key components such as integrated DDoS protection and CGNAT. This comprehensive and consolidated approach provides best-in-class performance, efficiency and scale to protect the mobile infrastructure while reducing OPEX and CAPEX costs.

NEXT STEPS

For more information on A10 Networks' 5G solution portfolio and GTP firewall, please visit www.a10networks.com/5g or contact your A10 Networks representative

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19202-EN-01 JUL 2019