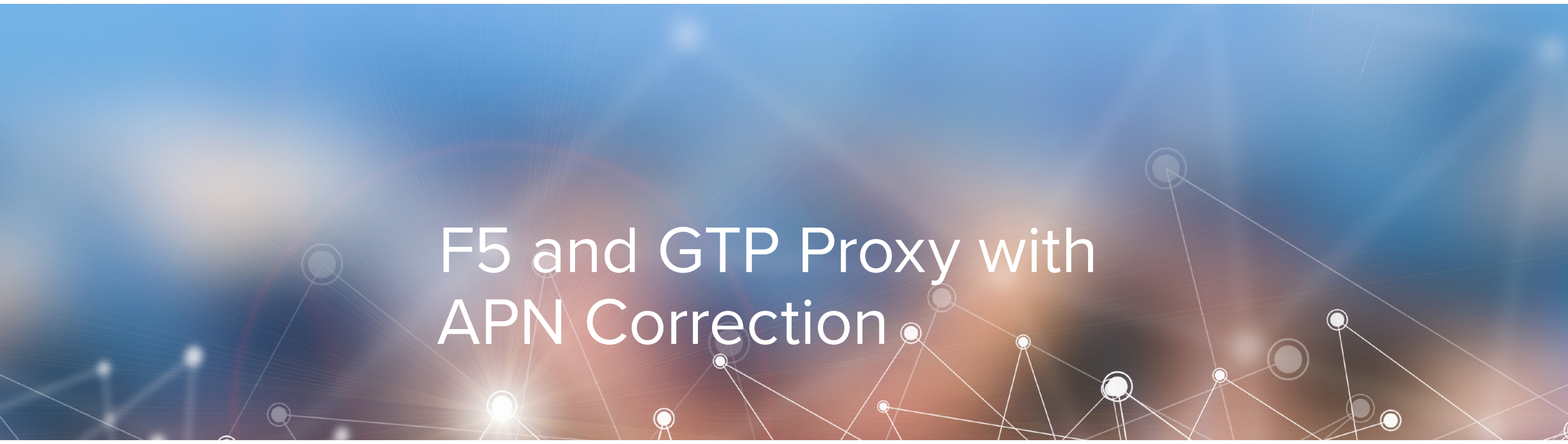
USE CASE



F5 and GTP Proxy with APN Correction

For years, F5 BIG-IP solutions have managed GPRS Tunneling Protocol (GTP) traffic. Initially, BIG-IP was used primarily for its load balancing functionality, but more and more customers and partners are also now benefitting from the GTP Proxy with Access Point Name (APN) correction functionality. This feature allows the mobile virtual network operator (MVNO) full control over the roaming services it wants to offer and how to charge for them. Let's examine some use cases that address how operators deal with scaling and securing GTP traffic, and how smart proxy functionalities can make better use of GTP signaling.

What is GTP?

GPRS Tunneling Protocol (GTP) is a group of IP-based communications protocols used to carry General Packet Radio Service (GPRS) within GSM, UMTS, and LTE networks. GTP is also expected to be used widely in 5G networks.

GTP is a set of three separate protocols: GTP-Control (GTP-C), GTP-User (GTP-U), and GTP Prime (GTP'). For this document we will focus on GTP-C which is used within the Mobile Core Network for signaling between various relevant nodes. (See Figure 1.)

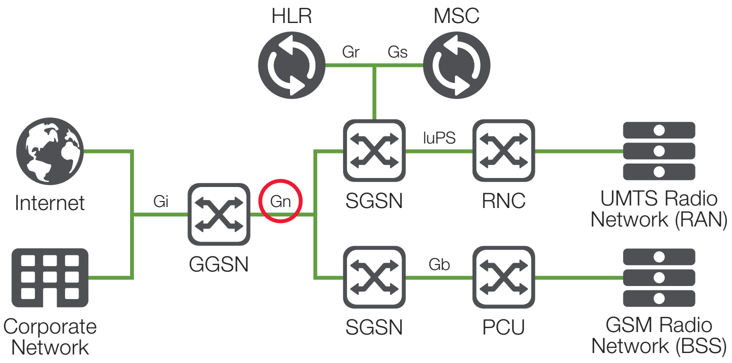


Figure 1: An example of a 3G network; Gn (circled in red) is a GTP-based interface.

GTP beyond GPRS

GTP was originally used in GPRS (2.5G networks), later developing a similar role in 3G and 4G networks. For 4G, the key nodes have different names and, to a certain extent, are comparable to nodes used in 3G networks.

Use cases: GTP

As data over mobile networks continues to grow, more network nodes are needed to handle this increased traffic. In these instances, GTP load balancing typically comes into play to help operators scale their network and its traffic handling. There are various use cases in this area. The same applies to security; while traffic is growing and more vulnerabilities are discovered, additional GTP security measures are required. One of the key use cases supported by BIG-IP is GTP firewalling.

A key challenge is how to effectively route and distinguish between GTP traffic. Subscriber traffic on a home network is different from MVNO traffic and from IoT (sliced) traffic. A smart GTP routing function selects the right Packet Gateway (PGW) or network slice best suited to a specific service.

In addition to these use cases, various GTP Proxy use cases exist, such as routing MVNO and a service provider's own traffic to different destinations using the same APN. While doing this, GTP information can be modified to better suit its specific purpose (for example, overriding the default APN a specific type of handset selects if it will cause problems for an MVNO who wants to manage its traffic based on the APN that a customer selected).

Use case: APN correction

What problem do we need to solve?

MVNOs would like to offer their own specific services and use the hosts national network to carry the MVNO traffic—but with different or additional services offered by the MVNO. If an MVNO customer is in a different country, the MVNO either needs to have roaming agreements with hundreds of roaming partners OR the hosting service provider can offer a Dual-IMSI service. This means that two IMSIs (international mobile subscriber identities) can be used. While in the country and on the host network, the IMSI used is from the MVNO-specific IMSI range assigned by the host network. While roaming, the IMSI of the host network is used in order to benefit from the existing roaming relationships the host has already established (and which continue to work well). Based on this IMSI, a foreign network will know how to route the traffic back to the home hosting network, typically via an IP Exchange (IPX) carrier, just as it does for any other IMSI from the host network's range.

Sometimes, an MVNO might like to receive specific APNs, and—based on those APNs—the MVNO might assign special services or charging conditions. Once a routing decision is made, the APN must be changed to a pre-configured value specifically for that MVNO. Only then can the MVNO send the GTP traffic to the PGW(s) for its own IMSIs with its own defined APNs. In this way, the MVNO can have full control over the services it wants to offer and how to charge for them.

The solution

F5 BIG-IP can be inserted not only to load balance GTP traffic to the best suited and healthiest PGW, it can also verify whether certain IMSIs or APNs need to be routed to one or more specific PGWs.

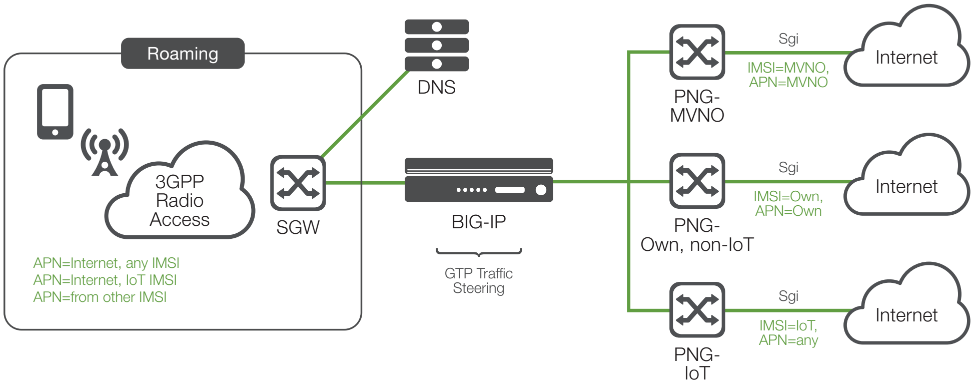


Figure 2: GTP Proxy—Correct APN and route on IMSI range.

When directed to do so, BIG-IP can also check the submitted APN and whether it came from an MVNO customer or—even if from a customer—from specific IMSI ranges (such as an IoT deployment). If the criteria match, a special rewrite for the APN value could be necessary. (Rewrite means a functionality that takes any GTP Information Element content, like the APN, and, if needed, replaces it with other pre-defined content and forwards the message onwards.)

For the potential APN change, BIG-IP will check which IMSI ranges it was pre-provisioned to change. If the IMSI matches one of those IMSI ranges, there will be an explicit new APN created. This APN will be inserted into the original GTP-C message (or replace the original APN) and is then routed onwards to the MVNO PGWs or PGW(s) handling the IoT traffic.

Now the receiving PGW receives information that is explicitly destined only for this PGW (or MVNO network in the case of Dual-IMSI) and it has a set of services and specific charging it can apply. The MVNO is now in full control of its own customers.

Conclusion

GTP is a vital protocol for signaling and transporting mobile data, whether in the initial GRPS networks via 3G and 4G, or the developing 5G network. Strong mobile user data growth requires better scaling of the networks while operators respond to the GSMA-driven initiative to be more aware of the GTP's security risks and better able to respond to vulnerabilities. This GTP proxy with APN correction use case is an example of how smart proxy functionalities can make better use of GTP signaling.

To learn more about Service Provider signaling solutions, visit f5.com.