SOLUTION OVERVIEW

F5 DIAMETER FIREWALL FOR MOBILE OPERATORS

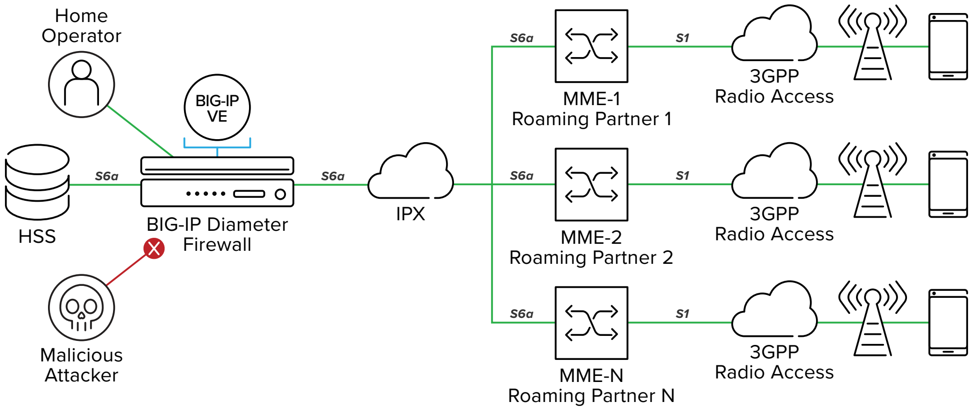
To reduce risks to diameter protocol, mobile operators need to be aware of the GSMA-driven measures they can take to scale and secure their networks against common diameter security risks such as confidential data disclosures, location tracking, denial-of-service attacks, network overloads and a range of fraud activities.

F5 DIAMETER SECURITY SOLUTION FOR MOBILE OPERATORS

F5 delivers a high-performance, stateful, full-proxy network security solution designed to guard the diameter protocol against threats that enter the network. The F5® Diameter Firewall security solution gives mobile operators the scalability, flexibility, performance, and control needed to mitigate the most aggressive, volumetric DDoS attacks. The F5 Diameter Firewall is compliant with GSMA-FS-19 Diameter Security requirements. It checks Diameter signaling against security rules and checks for all signaling instances or for a specific roaming partner.

As part of the Diameter protocol conformance, the F5 Diameter Firewall determines whether Diameter messages are constructed in accordance with the rules as defined in the 3GPP specifications (such as 29.272 Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) Diameter protocol interfaces). This means that Diameter attribute-value pairs (AVPs) are checked to see if they are mandatory or optional to determine whether the length is according to specification and that the right type of variable is used as shown below.

Figure 1: F5 Diameter Firewall Confirms Messages Conform to 3GPP Rules



For example, F5 Diameter Firewall checks if the value and volumes of Diameter messages (and included AVPs) meet Diameter security rules in order to detect and take action on vulnerabilities (as described in the GSMA FS.19 Diameter Security document).

To eliminate third-party visibility into the connected diameter hosts, the F5 Diameter Firewall obscures topology by proxying and rewriting the Diameter Origin Host, Origin Real, Destination Host, and Destination Realm information. It can hide the identity of a network node, and mask and replace any other reference deep inside any Diameter AVP with a dummy name or reference. With unique node names you can hide the exact topology of your network and reduce the chance of a targeted attack.

5G AND HTTP/2 FIREWALL

HTTP/2, the new signaling protocol for 5G Core networks and its service-based-architecture (SBA) as defined by 3GPP, is replacing Diameter signaling. The current F5 Diameter Firewall is based on the same generic design as the HTTP/2 Signaling Firewall for 5G networks (in development).

GSMA may define an equivalent HTTP/2 Security document as it did for Diameter (e.g. FS.19 Diameter Security) by adding an HTTP/2 signaling message library so that the same Firewall can be used for HTTP/2 protocol conformance checks and specific security rules. Other security functions and specifications also can be added as defined by 3GPP in the Security Edge Protection Proxy (SEPP).

F5 DIAMETER FIREWALL, PART OF THE BIG-IP ADVANCED FIREWALL MANAGER

BIG-IP AFM AND F5 DIAMETER FIREWALL CHECK DIAMETER PROTOCOL CONFORMANCE TO GSMA REQUIREMENTS AND REDUCE RISK WITH OVER 100 HARDWARE-BASED ATTACK SIGNATURES—MORE THAN ANY OTHER FIREWALL.

The F5 Diameter Firewall functionality is built into the F5® BIG-IP® Advanced Firewall Manager (AFM) to give mobile operators the scalability, flexibility, performance, and control needed to mitigate the most aggressive, volumetric distributed denial-of-service (DDoS) attacks.

The unique application-centric design of BIG-IP AFM and F5 Diameter Firewall enable greater effectiveness in guarding against targeted, network-level attacks. The solution tracks the state of network sessions, maintains deep application awareness, and uniquely mitigates attacks based on more granular details than traditional firewalls. With BIG-IP AFM and F5 Diameter Firewall, organizations receive protection from over 100 attack signatures—more hardware-based signatures than any other leading firewall vendor—and unsurpassed programmability, interoperability and visibility into threat conditions.

F5 iRules can also be used to customize BIG-IP Diameter Firewall ingress, egress and retransmission functionality and usage. There are over 15 iRules that can be implemented for greater control of Diameter events. Additionally, mobile network administrators can get help from the F5 DevCentral Community where 200,000 iRules users provide code and assistance.

Virtual editions of BIG-IP software, including BIG-IP AFM and Diameter Firewall, run on commodity servers and support the range of hypervisors and performance requirements. These virtual editions provide agility, mobility, and fast deployment of app services in software-defined data centers and cloud environments.

As part of the BIG-IP AFM solution, the F5 Diameter Firewall protects your users and network, in accordance with GMSA recommendations, without the need for additional licenses.

For more information go to f5.com/solutions/service-providers/signaling.