KEY DIAMETER USE CASES INCLUDING TRAFFIC SHAPING, IoT, AND SECURITY

F5 AND DIAMETER

The volume of mobile data continues to increase at an exponential rate, and as a result the need to provide security mechanisms for the Diameter protocol has increased as well. There is high demand for smart, flexible, and secure Diameter traffic management—in both hardware and virtualized environments. F5 BIG-IP has been used to manage Diameter traffic since 2011. In this document we will explain what the Diameter protocol is and offer market-proven use cases which show how BIG-IP provides a significant, value-added Diameter solution.

Diameter is a signaling protocol that has been defined by the Internet Engineering Task Force (IETF) as a base protocol "intended to provide an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility in both local and roaming situations."[1] Although Diameter is used in fixed and other networks, we will focus on the use of Diameter for signaling in mobile networks.

It should be noted that Diameter can be used for services that do not fall into the AAA framework, such as 3rd Generation Partnership Project Internet Multimedia System (3GPP IMS) interfaces. In those cases, other specifications should be referenced (for mobility management, authentication, charging, policy, or machine-to-machine communication, for example).

As network architectures have evolved, so have signaling protocols. Signaling System 7 (SS7) was used as the key signaling protocol in 3G networks (in addition to Diameter for charging and policy signaling). With the global rise in 4G networks, Diameter became the primary signaling protocol. And with the advent of 5G Core networks which rely on HTTP/2 protocol, Diameter-to-HTTP/2 protocol inter-functionality will be essential. As mentioned above, Diameter can also be used in IMS interfaces (which also play a role in 5G networking), as well as for the Internet of Things (IoT).

This paper identifies five Diameter use cases:

- **Use Case 1: Load balance to alternative Diameter peers**
- **Use Case 2: DDoS protection and overload control**
- **Use Case 3: Diameter normalization**
- **Use Case 4: Diameter Director, Online Charging System (OCS)**—ensuring that charging messages with specific content or profile get to the right OCS
- **Use Case 5: Diameter Firewall**

KEY USE CASES FOR DIAMETER

USE CASE 1: LOAD BALANCE TO ALTERNATIVE DIAMETER PEERS

F5 BIG-IP helps the network to select the best available resource from the various pools of Diameter servers. There are any number of servers that can handle the Diameter signaling, but the right resource needs to be selected based on best availability while also minimizing the impact to nodes when capacity is increased. And, it's important that the Diameter load balancer gets the full benefit of this new capacity seamlessly and without changing any source configuration.

Problem Statement

- An operator wants to use its Diameter servers in the most efficient way, including changing capacity without reconfiguring the client side.
- When a pool or server is unavailable, an alternative resource must be found automatically and without making any changes to the source.

Solution

- Use F5 BIG-IP load balancing capabilities, easily addressable via one IP address.
- Various load balancing algorithms can be selected, such as round robin, least connections, fastest, etc.
- Load balancing can be done on various parameters—such as source and destination—but also on specific message content.

Initially, the BIG-IP Diameter load balancer is provisioned with the destination pool, its members, and the preferred load balancing algorithm. When Diameter traffic arrives, the load balancing functionality assesses the targeted destination and uses the pre-configured algorithm to shift traffic over the various pools that meet the load balancing criteria (such as source, destination, Diameter message content, etc.) If a server (or multiple servers) is extended, that additional capacity is included in the BIG-IP configuration, the load balancer will scale automatically, and that extended destination will receive more traffic. (See Figure 1.)

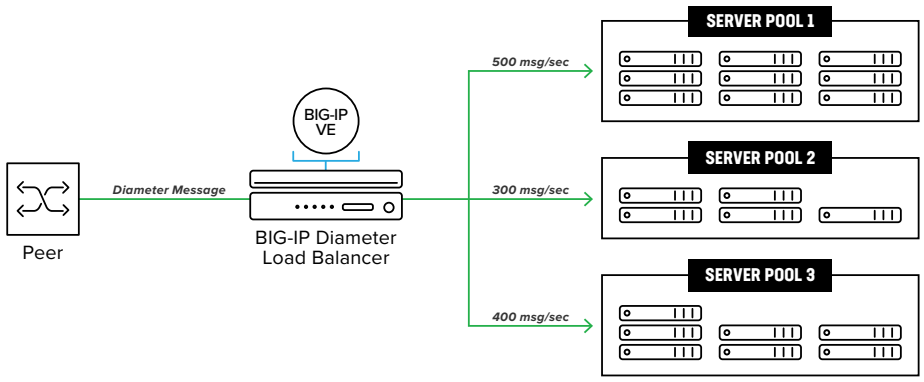

Figure 1: Diameter traffic management—load balancing.

USE CASE 2: DDOS PROTECTION AND OVERLOAD CONTROL

BIG-IP Diameter Overload Control helps operators to protect Diameter servers from distributed denial-of-service (DDoS) attacks or overload. For example, after a network element goes down—either for planned maintenance, because of a failure, or caused by a misconfiguration—there will be a flood of signaling messages toward critical nodes when that network element comes back online. As devices and applications automatically start to send Diameter signaling to reconnect with the network, nodes—such as Home Subscriber Server (HSS), the online charging system (OCS), and the Policy and Charging Rules Function (PCRF)—are inundated with signaling messages for authentication, authorization, and mobility management, as well as for charging and policy control.

In the case of IoT, many devices are connected to a single network and—if they all start to act at the same time—could cause massive spikes in traffic. Vital network elements need to be protected against these potential overload situations. (See Figure 2.)

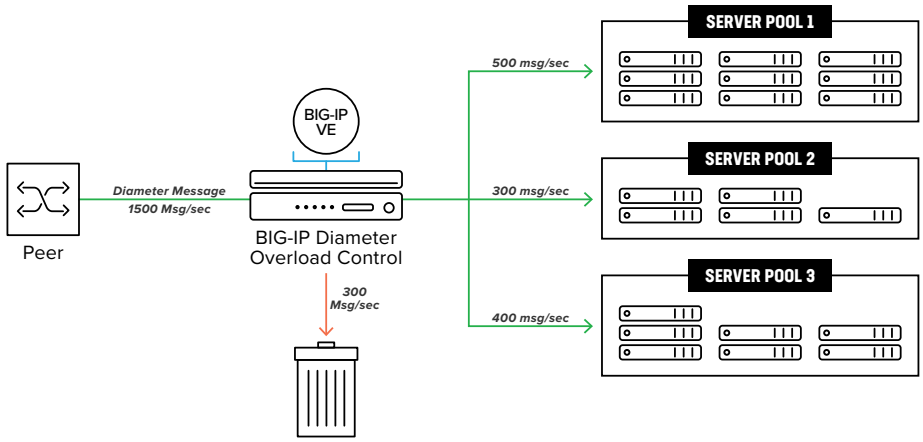

Figure 2: Diameter Traffic Management–DDoS protection and overload control

Problem Statement

- A customer wants to protect Diameter servers against DDoS or overload situations.
- A customer wants to protect the network against unwanted IoT traffic patterns, especially in case of failures.
- Without proper DDoS and overload control, network elements could easily go down and result in a very negative customer experience.

Solution

- Use F5 BIG-IP load balancing capabilities, easily addressable via one IP address.
- Use BIG-IP Diameter Overload Control to limit the traffic to a specific pool (or specific pool server).
- Use BIG-IP capabilities to define what should happen when more traffic is offered than the destination can handle, such as “throw away” or “inform the source.”

Initially, BIG-IP Diameter Overload Control is provisioned with the maximum throughput that the various servers should be able to manage. Optionally, there is an 80% threshold provision and an explicit maximum. When the Diameter traffic increases, the regular load balancer continues to shift the Diameter traffic to the various destinations, but while doing so it also checks that the traffic does not exceed the thresholds set for each destination (either individual and/or a group of servers). Once the 80% threshold is met, an alarm can be generated or active measures can be taken, such as only allowing Diameter messages related to an existing session to pass through and directing messages related to new sessions to another destination.

As traffic continues to increase, it could reach the next threshold: absolute maximum. When that threshold is reached and a destination is in an overload condition, BIG-IP will automatically redistribute traffic to alternate destinations (if they exist) until levels return to a manageable state.

If there is too much traffic and if existing alternate destinations cannot handle the overload, then BIG-IP can provide options for how to deal with this surplus of traffic.

- The easiest option is to simply ignore the traffic beyond the maximum level and not actively inform the source. Alarms will be generated by BIG-IP, but no active communication would be initiated.
- Alternatively, BIG-IP can be configured to inform the source that messages are being discarded—typically via Diameter Error Signaling. If the source has the intelligence and capabilities to adjust, it will decrease the Diameter signaling to that destination.
- As a next step there could be a demand to support the IETF-defined overload control mechanism (see IETF RFC 7683, *Diameter Overload Indication Conveyance*), where the destination and source communicate via Diameter signaling to reduce the traffic for a defined time to a requested maximum level.

USE CASE 3: DIAMETER NORMALIZATION

In many networks, there are multiple suppliers for the nodes that support Diameter signaling. However, not every vendor uses the same interpretation of the relevant IETF and 3GPP Diameter specifications and, as a result, each may implement a Diameter interface in slightly different ways. In some cases—such as roaming for LTE—the Global System for Mobile Communications Association (GSMA) has specified requirements for how Diameter signaling is to be used between various operators. In situations where multiple vendors are involved, one operator cannot control how fast the solution can be adjusted—if at all—on “the other side” (that is, by the roaming partner). In these instances, it may be best to simply accept the Diameter signaling and follow up at a later date with vendors regarding changes to improve interoperability between parties. (See Figure 3.)

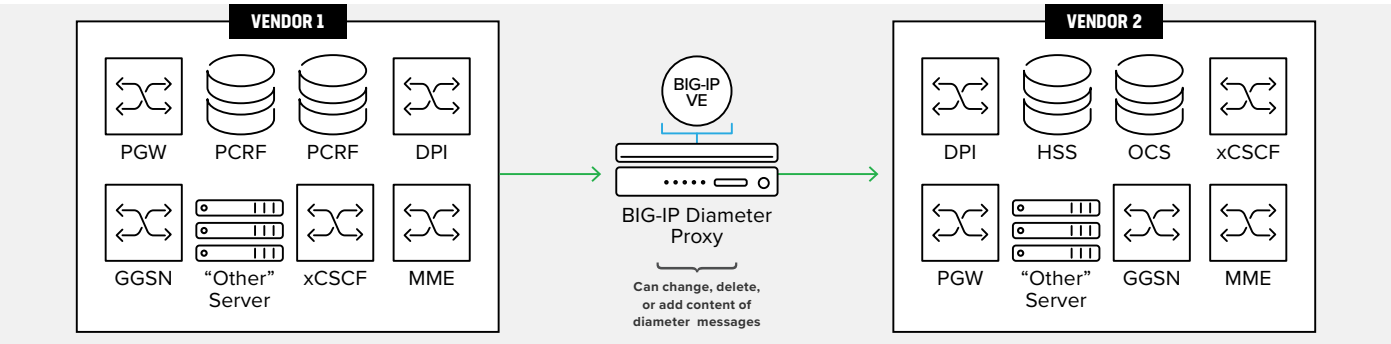

Figure 3: Diameter normalization

Problem Statement

- Because there are many different types of the same Diameter interfaces—especially for IT nodes such as OCS and new nodes such as those for IMS—there are many initial issues which prevent disparate vendors from connecting.
- In the case of roaming for LTE, there will always be at least two vendors involved, with potentially different implementations.

Solution

- Utilize BIG-IP and F5's extensive experience in Diameter mediation.
- Offload servers from Diameter normalization and save on total network costs.
- Speed time-to-market, reduce risks, and lower costs.
- In addition to implementing a flexible engine to modify Diameter messages, we can show you how to get the most out of the full proxy architecture of BIG-IP.

BIG-IP has a full proxy architecture by nature. For situations where no Diameter is used, the whole BIG-IP platform has evolved into an extremely flexible tool to adjust for protocol settings. So, if necessary, BIG-IP can also solve interoperability issues at the Transmission Control Protocol (TCP) or Stream Transmission Control Protocol (SCTP) level, for example. If addressing potential interoperability issues at the transport layer are not solving higher layer Diameter application issues, BIG-IP is able to parse Diameter Attribute Value Pairs (AVPs), with no limitation on how deep parameters are nested. BIG-IP understands the use of different Diameter interfaces, as well as the value of the various AVPs, and can place this insight into situational context. In addition to the information available to BIG-IP—either as pre-configured via the Diameter messages itself or via other protocols supported by BIG-IP—there is also the ability to check with external databases or sources to obtain additional information that can be used to make the correct changes to a specific Diameter message. Note that this external information can be used for routing and load balancing purposes, as well as information to change a Diameter message. Changing could include delete, amend, or correct a specific value—or to add completely new AVP content, if required.

USE CASE 4: DIAMETER DIRECTOR—ENSURING THAT CHARGING MESSAGES WITH SPECIFIC CONTENT OR PROFILE GET TO THE RIGHT OCS

Operators typically want to make changes to their Online Charging System (OCS) in a phased and well-controlled way. If operators want specific OCS servers to manage charging for specific applications or devices, how can we ensure that this information becomes part of the routing and load balancing? And how do we do it in an easy and scalable way (given that millions of specific routing rules could very well be possible)? In some limited cases, a special node is defined—SLF (Subscriber Location Function)—and specific Diameter interfaces have been defined to communicate with such a node (Diameter Cx or Dx, for example). In cases where an SLF *and* an alternative database (that potentially is not supporting a Diameter interface) exist, F5 BIG-IP Diameter Director supports various alternatives to access such an external resource or database.

Problem Statement

- A customer wants to distribute Diameter Gy charging messages over multiple destinations.
- A customer wants to make sure that charging messages with specific content or profile get to the right OCS.
- A customer wants to route information from a third-party database.

Solution

- Selection for OCS pool can be done on various static load balancing parameters.
- F5 BIG-IP Diameter Director has preconfigured/onboard rules regarding how to select the right OCS.
- F5 BIG-IP Diameter Director queries an external database about the subscriber, then routes to correct OCS based on parameters received from the database.

With BIG-IP, an operator can use a graphical user interface (GUI) to very easily define the logical steps for what to do with a charging message, and/or to query an external database to provide additional information. The types of supported functions include determining whether a certain parameter is within or contains a certain value, and—whether or not a match exists—deciding to delete the message. But it can also be used to create more complex rules if certain information is present. For example, if an AVP has the relevant mobile station international subscriber directory number (MSISDN), BIG-IP can query an external database via protocols like SQL, LDAP, or Diameter. Then, based on the information included in the response from that external source, a decision can be made to change or delete a message or to add additional information via a changed or new AVP. (See Figure 4.)

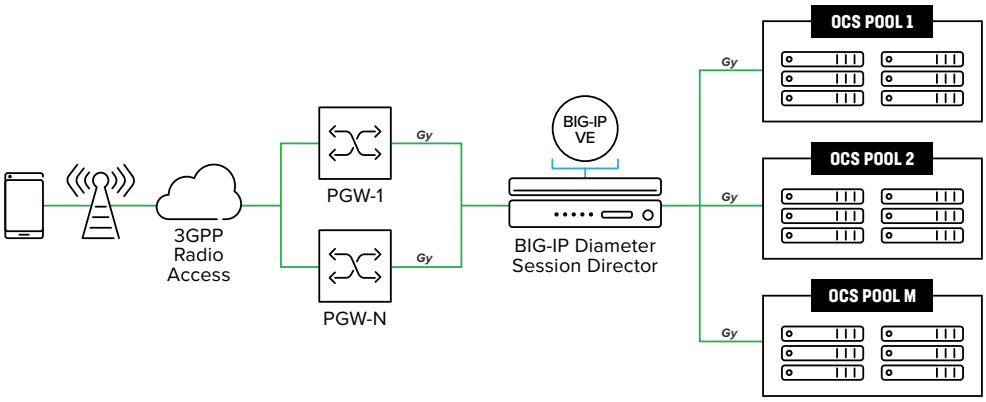

Figure 4: Diameter Director–Ensuring that charging messages with specific content or profile get to the right OCS

USE CASE 5: DIAMETER FIREWALL

For this use case, we look at security—or more specifically at Diameter signaling security. Recently, the GSMA raised awareness regarding security vulnerabilities stemming from the fact that the native Diameter protocol lacks strong, built-in security mechanisms. Various protocols have been investigated by the GSMA Fraud Security group and the resulting FS.19 document (entitled *Diameter Security*) currently acts as guideline for GSMA members, who are encouraged to implement security measures for the addressed vulnerabilities.

Common Diameter security issues include confidential data disclosures, location tracking, denial of service, network overloads, and a range of fraud activities. Prevention depends on circumstance but, as a minimum, solutions that provide full traffic visibility and an all-encompassing DDoS protection should be in place.

Problem Statement

- If a customer roams, the Mobility Management Entity (MME) is in the visited network and the Diameter signaling towards the Home Subscriber Service (HSS) is transported via the S6a interface.
- The home operator has no control on the Diameter traffic entering its network.

Solution

- Diameter signaling is checked on protocol conformance.
- Diameter signaling is checked against security rules.
- Diameter signaling can be checked in general or for a specific roaming partner.

For this use case-which is a combination of security use cases—we look at BIG-IP as a Diameter Firewall that checks on Diameter protocol conformance and against specific security rules.

With Diameter Protocol conformance, the firewall determines whether the Diameter messages are constructed following the rules as defined in the 3GPP specifications (such as 29.272 Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on the Diameter protocol). This means that Diameter AVPs are checked on being mandatory or optional, to determine whether the length is according to specification, to confirm that the right type of variable is used, etc. (See Figure 5.)

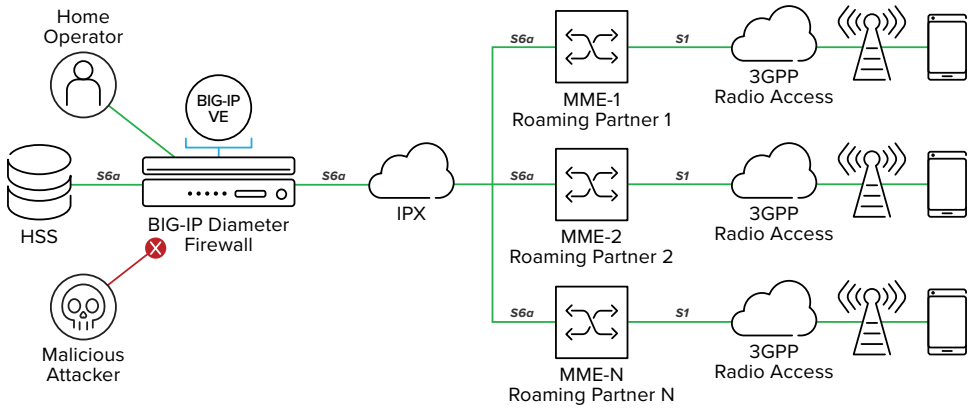

Figure 5: Diameter Firewall

Topology Hiding is supported, even though it is more a function of a Diameter Edge Agent (DEA) as specified by GSMA, and not a pure Diameter Firewall function. The topology of network elements like MME and HSS (as well as PCRF or other nodes, if desired) can be hidden by replacing the name of such a node with a dummy name. This can be done in a static way, which would mean a one-to-one replacement of the identity of a node by a dummy identity, or in a dynamic way where BIG-IP remembers what source and session identification should be linked to what general dummy (session identification “123” from node with identity MME-1 to Node_from_Operator, for example). In this way, the operator can be protected against targeted DDoS attacks and the number of network nodes and their topology can also be hidden. This can all be done on Diameter header level (Origin-Host-Identification, for example) or at any other level.

With Diameter security rules, various checks are implemented to detect and potentially take action on vulnerabilities described in the GSMA FS.19 Diameter Security document. For other cases or new security issues that are not yet covered in FS.19 a path that is currently being explored involves the use of machine learning to detect abnormal patterns and—based on that insight—to automatically generate new firewall rules. In this way, information detected on one firewall could be used to update other firewalls before the same problem occurs.

Future developments will also allow the Diameter traffic to be correlated with signaling information from other protocols; for example, GTP signaling could indicate that the Location-Update procedure was done from location x (where the GTP traffic is generated from another location).

OTHER DIAMETER USE CASES

These use cases are the most common, but it certainly is not a comprehensive list. Other use cases include: Intelligent Roaming (includes Steering of Roaming), Session Binding for Policy signaling (for linking LTE to IMS signaling to the same PCRF, for example), proxy for IMS/VoLTE signaling, OCS optimization, OCS Proxy, Message enrichment (for VoWifi, adding Location Information, adding Charging Identification for IMS, etc.), Machine Type of Communication (MTC) proxy (for Diameter interfaces defined for MTC, also called M2M or Machine-to-Machine), SCEF proxy (NB-IOTs Service Capability Exposure Function proxy and gateway for Diameter Configuration REST API), etc.

CONCLUSION

In this document, we have presented some use cases that address how various operators deal with scaling and securing Diameter traffic, as well as how smart proxy functionalities can make better use of Diameter signaling. Diameter is a vital signaling protocol for mobile data (and, less significantly, for voice). Diameter is used in the initial UMTS networks (via 3G and 4G) to the still-being-defined 5G networks where it will, at the very least, be used in the IMS components. With the exponential increase in mobile user data comes the need to better scale and secure the networks. This includes making operators aware of Diameter security risks and the GSMA-driven measures they can take to protect against those threats.

Please contact F5 if you are interested in more details regarding specific use cases or go to f5.com/solutions/service-providers for more information.

[1] Internet Engineering Task Force (IETF)