September 2020

PROXY EDGE FUNCTION FOR CLOUD BASED 5G CORE

Anal Srivastava

Sri Gundavelli

Vimal Srivastava

Oliver Bull

PROXY EDGE FUNCTION FOR CLOUD BASED 5G CORE

AUTHORS:
Anal Srivastava
Sri Gundavelli
Vimal Srivastava
Oliver Bull

ABSTRACT

For deployments where the 5G control (5GC) plane function is in the cloud and the user plane function (UPF) is on-prem, there are number issues that may be result of unstable wide area network (WAN) link connection. This solution addresses these issues by introducing an proxy edge function on-premises and a corresponding proxy peer in the cloud.

DETAILED DESCRIPTION

Presented herein is a solution to address an issue that potentially can happen when the 5G Core Control Plane functions (Access and Mobility Management Function (AMF) and Session Management Function (SMF)) are deployed in the cloud and a user plane function (UPF) is on-premises (on-prem).

In such a deployment if the transport link between on-prem and cloud becomes disconnected, this will lead to disruption of services including user equipment's (UE's) ability to do any data transfer. This can be very critical for an industrial Internet of Things (IOT) type of deployment where an entire manufacturing operation can come to stand still.

The cause of this disruption is because the gNB (radio access network (RAN)) will detect a transport failure (connection between gNB and AMF breaks) and it will eventually lead to releasing the UE context and thereby impacting the UEs that were doing any data transfer.

A solution is presented such that that while a control plane function is inaccessible, the data should not be impacted. The solution also results in network optimization.

In the cloud-based deployment, a proxy-edge function is deployed on-prem along with gNBs and UPFs. The gNBs view the proxy-edge function as an AMF. The gNBs no longer communicate directly with the AMF in the cloud.

The gNB establishes the Stream Control Transmission Protocol (SCTP) connection with the proxy-edge function. The proxy-edge function connects to the cloud based 5GC using an HTTP/2 connection over Transport Layer Security (TLS) protocol. This HTTP/2 connection can be through regular HTTP exchanges or over an upgraded WebSocket connection. Moreover, the use of future HTTP over QUIC or HTTP/3 is also possible.

There is a corresponding cloud proxy-edge as an endpoint for the HTTP/2 / TLS connection that will make SCTP connections to the AMF - so that AMF procedures remain unchanged. There is a proxy-edge to cloud proxy-edge establishment procedure when the SCTP connection from the gNB is established in order for the gateway-to-AMF SCTP connection to be made.

The proxy-edge receives signaling messages from the gNB over the SCTP connection and it transparently relays these messages to the cloud-based 5GC over the HTTP/2 connection. Similarly, signaling messages received from the cloud will be relayed to the gNB over the SCTP connection.

With this approach, if the link to the cloud goes down, the gNB remains unaffected, i.e. gNB doesn't see any loss of connectivity to the control plane. This will result in the current data sessions not being affected and continuing to work. The non-access stratum (NAS) or Next Generation Application Protocol (NGAP) level signaling exchange with the AMF will not be possible as the link between the proxy-edge and AMF will not be up. This solution does not propose to solve this, and it is expected that protocols running on the UE, gNB or AMF will take care of resolving any issues arising out of loss of signaling. Again, when the link comes up, various network entities reconcile the state through the applicable protocol procedures.

An added benefit of this solution relates to network optimization. The proxy-edge function acts as an aggregator for gNB transport connections. The AMF in the cloud has just one connection coming from proxy-edge function. Thus, the number of connections going to the cloud reduces to a great extent if there are a large amount of on-prem deployments each having a handful of gNBs. If gNBs and the proxy-edge function are in a secured environment, the interface level security (e.g., Internet Protocol Security (IPsec) protocol) is not needed. Without the proxy-edge function, the gNB would connect to the AMF in the cloud and necessarily needs to secure the signaling connection between the gNB and the AMF through a suitable secure protocol, such as IPSec. There is no need to deploy an IPsec security gateway (SecGW) function in the cloud. Further, any SCTP load balancer functionality is not needed in the cloud. Finally, there is a possibility to re-use existing methods for HTTP/2 and TLS load balancing in the cloud.

Set forth below are Figures 1 and 2, which illustrate a network architecture without the proxy-edge function and with the proxy-edge function.

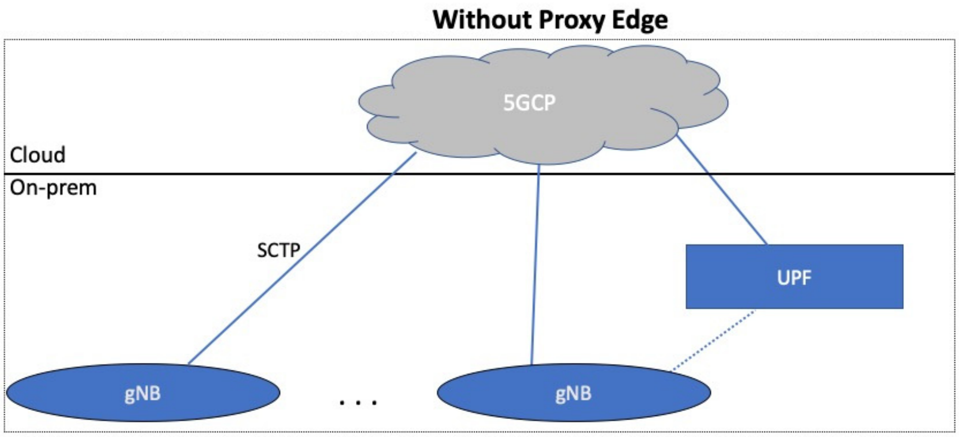

Figure 1 – Architecture without Proxy Edge Function

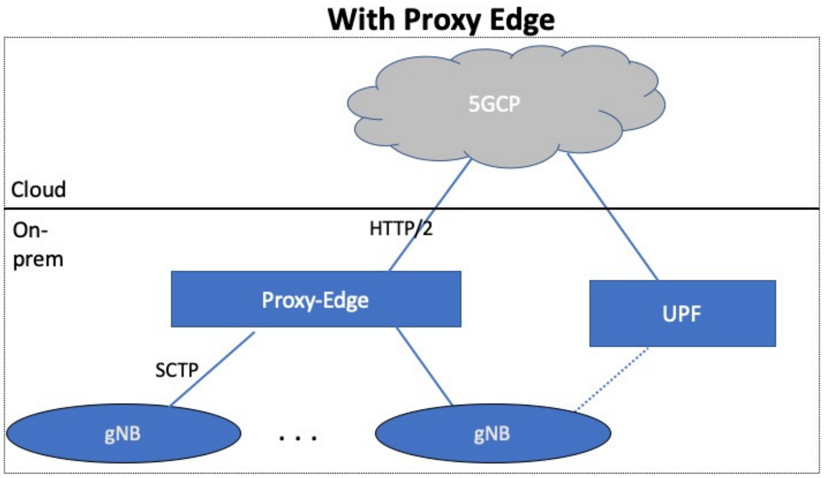

Figure 2 – Architecture with Proxy Edge Function

In summary, for deployments where the 5G control plane function is in the cloud and the UPF is on-prem, there are number issues that may be result of unstable WAN link connection. This solution addresses these issues by introducing a proxy edge function on-prem and a corresponding proxy peer in the cloud.