August 2023

COMMUNICATION ACROSS ACCESS TECHNOLOGIES WITH APPLICATION-SPECIFIC POP SELECTION IN SOFTWARE-DEFINED ENTERPRISE FABRIC

Prakash C Jain

Vinay Saini

Sanjay K Hooda

Snezana Mitrovic

COMMUNICATION ACROSS ACCESS TECHNOLOGIES WITH APPLICATION-SPECIFIC POP SELECTION IN SOFTWARE-DEFINED ENTERPRISE FABRIC

AUTHORS:
Prakash C Jain
Vinay Saini
Sanjay K Hooda
Snezana Mitrovic

ABSTRACT

Techniques are presented herein that add to the existing 3rd Generation Partnership Project (3GPP) fifth generation (5G), private 5G, and secure access service edge (SASE) connectivity options for remote hosts when such hosts are located in an enterprise software-defined access (SDA) network. The techniques aid in connecting remote terrain, Industry 4.0, Internet of things (IoT), and private 5G devices through enterprise SDA/SDN networks (or any other intermediary overlay networks) and provide inter-access technology communication between 5G and existing access technology endpoints in an enterprise SDA fabric. The techniques also bring point of presence (PoP) service-level agreement (SLA) information (such as latency measures, performance details, etc.) to an edge or access element of a network to facilitate 5G application-specific PoP selection and a redirection of traffic to the correct PoP. That information may be used to select an application-specific PoP exit which meet applicable SLA requirements and/or select a service using a particular border, and then select a specific PoP, thus meeting the SLA requirements. The techniques also augment a security solution when a physical firewall is not directly connected to the service border but, rather, is available as a 5G application, such as under a firewall as a service paradigm in a SASE environment.

DETAILED DESCRIPTION

Currently, an enterprise or campus network may encompass one or more sites (with each site containing some number of connected buildings, usually within a range of one to two miles) that are interconnected through a multisite enterprise networking technology such as a software-defined wide area network (SD-WAN), the Internet Protocol (IP) over a virtual private network (VPN), a software-defined access (SDA)-based transit, etc. For

each such enterprise, usually within a site, wired access or Wi-Fi access is sufficient to connect all of the different hosts and allow communication with and roaming among those hosts. However, there are many enterprises (such as oil production and refining operations and mining industries) where a site may span many miles, extending beyond the few buildings of a typical enterprise network.

To provide connectivity within such extended sites (from, for example, a remote mine or refinery field to a business or commercial office), wired or Wi-Fi access is insufficient. What is needed is long-range radio access through, for example, a private 3rd Generation Partnership Project (3GPP) fifth generation (5G) environment.

Additionally, within such an environment remote private 5G endpoints need to communicate with their commercial office endpoints, which are on wired or Wi-Fi access, without transiting a service provider network. With a modern enterprise, the number of such endpoints (including mobile phones, tablets, Internet of things (IoT) devices, portable devices, etc.) is continuously increasing. To provide seamless connectivity and mobility among such endpoints at scale, overlay SDA and software-defined networking (SDN) fabric networks have evolved and have become necessary for all future enterprises.

To connect modern enterprises to their remote locations (including, as described above, mines, refineries, etc.) it is necessary for a current SDA/SDN/fabric network to leverage long-distance access networks like private 5G technology to expand beyond the current few miles of a single site to sites that span hundreds of miles. Such private 5G network support is required within SDA/SDN/fabric networks as a new type of access to allow for the intercommunication of private 5G endpoints with other local enterprise access endpoints (without needing to transit service provider 5G networks) as well as with external network endpoints (e.g., over the Internet and within a cloud). Within the above-described context, it is envisioned that most of the 5G, private 5G, and Wi-Fi 6 applications and services may be deployed through a hybrid cloud. Figure 1, below, presents elements of an illustrative arrangement as described above.

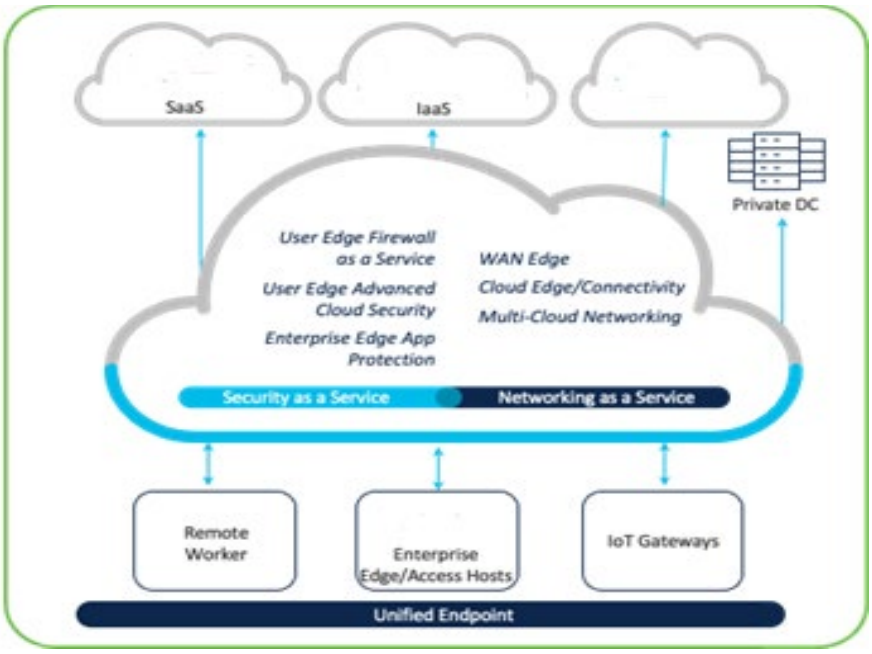

Figure 1: Illustrative Arrangement

Cloud application providers may deploy applications using regional points of presence (PoPs) to reduce application latency and improve performance, thus providing a real 5G experience, especially for remote enterprise sites where there are no local servers for the utilized applications. Hence, in addition to the inter-access technology communication an application-specific PoP selection capability and a redirection of traffic to an appropriate 5G PoP would also be required.

Techniques are presented herein that support 5G, private 5G, and Wi-Fi 6 access in an SDA/SDN/fabric network, allowing for inter-access technology communication and roaming across the different access technology's endpoints. Additionally, the presented techniques support 5G, private 5G, and Wi-Fi 6 endpoint connectivity to 5G cloud applications with the selection of an application-specific PoP.

As will be described and illustrated below, the presented techniques support inter-access communication between 5G, private 5G, and Wi-Fi 6 endpoints, and other access technology endpoints, by inserting an enterprise fabric between the 5G gNodeB connectivity and a 5G packet core by mapping mobile backhaul tunnels to SDA tunnels. To briefly illustrate such an approach, consider elements of an illustrative flow for an existing arrangement (i.e., which lacks SDA tunnels) – 5G radio → gNodeB → mobile

backhaul tunnels →5G PoP). In contrast, consider elements of an illustrative flow for an arrangement that employs the presented techniques (i.e., which incorporates SDA tunnels) – P5G radio → gNodeB → mobile backhaul tunnels → SDA access tunnels → P5G PoP.

Since SDA-based access already includes other access technologies, the presented techniques provide 5G, private 5G, and Wi-Fi 6 endpoints with an interworking capability with other access technologies without any actual traffic going out to a 5G core. Aspects of the presented techniques may support a 5G application-specific PoP selection mechanism. Further aspects of the presented techniques may employ the Locator/ID Separation Protocol (LISP), or a similar pull-based overlay protocol, to provide enterprise interconnection for secured 5G applications.

Figure 2, below, presents elements of an exemplary solution (that supports the selection of the best SDA exit to reach a PoP or Mobile Edge Computing (MEC) element that is specific to an application, thus preserving an enhanced 5G experience) that is possible according to the presented techniques and which is reflective of the above discussion.

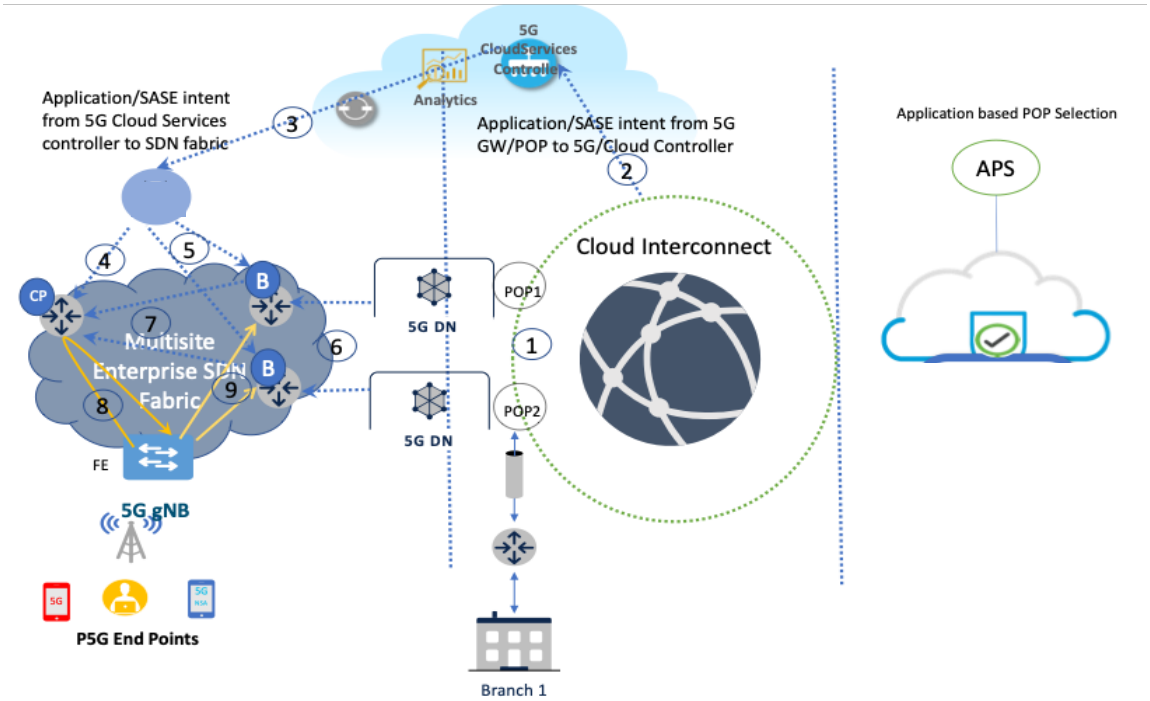

Figure 2: Exemplary Solution

Figure 2, above, depicts various of the steps that the presented techniques may follow to achieve the required conveyance of an application's or PoP's knowledge (not

necessarily the complete PoP or application gateway (GW) information) to an edge or access element of the SDA network and a redirection of the traffic at the SDA edge.

During a first step (1), a 5G MEC PoP may monitor its connectivity to applications and software as a service (SaaS) provider for any service-level agreement (SLA) requirements through a cloud interconnect. A PoP, as a secure access service edge (SASE) engine, may also provide secure access policies for an application.

Under a second step (2), for 5G applications a PoP may also encompass network functions (NFs) such as a UPF and a SMF. In such a case, a cloud or application controller may receive all of the information (including an application's performance monitoring data, policies, etc.) from a PoP and then provision or update an application's regional gateways accordingly. Importantly, an application gateway may dynamically update a PoP based on traffic, policies, and SLA requirements.

At a third step (3), the cloud or application controller may communicate to an enterprise controller to update a 5G PoP with application information and then, at a fourth step (4), the enterprise controller may provision or update an SDA service control plane (CP) for 5G applications and services.

During a fifth step (5), the enterprise controller may provision any enterprise borders (B) as service or application borders to provide, and dynamically update, 5G application and service connectivity as well as all of the parameters for a secured application or service (including security or SASE policies). Then, under a sixth step (6), an enterprise border may monitor the 5G PoP connectivity and register to the service CP (or LISP map server (MS) and map resolver (MR)) for secured applications or services with all of the service parameters.

During a seventh step (7), when the application gateway changes (e.g., based on SLA monitoring) at a PoP, a service border may detect such a change and then update a service CP (or LISP MS and MR) with the change in the preferred 5G application service border and its parameters.

At an eighth step (8), when traffic from the host arrives at an enterprise edge or access element, the same may map-request the service CP (or LISP MS and MR) to provide destination routing locators (RLOCs) and policy information and the service CP (or LISP MS and MR) may map-reply with a service RLOC and related policy details.

Finally, under a ninth step (9) the enterprise edge or access element (e.g., a fabric edge (FE) or LISP xTR) may apply the policy and create a redirection path towards the appropriate service border to send the traffic, encapsulated through virtual extensible local area network (VXLAN) technology, towards the service border. The service border may then forward the traffic to the best (i.e., optimized) PoP for the 5G service/application.

Under the presented techniques, the above-described steps create a complete loop (comprising enterprise edge FE → service border B → 5G PoP or application gateway → application or cloud controller → enterprise controller → service border B → service CP → enterprise edge FE) that allows for a dynamic PoP selection for 5G applications based on service or application availability, performance monitoring, and SLA requirements in a LISP-based enterprise fabric. In the above-described flow, the enterprise controller may manage the SDA functionality (e.g., an SDA FE and the SDA fabric) with no influence on the 5G core. It may also receive SLA monitoring information from an application-side controller or PoP and communicate the same to the SDA side in support of the selection of the correct fabric border (FB) for 5G traffic (by determining which PoP best meets the SLA requirements).

The presented techniques may augment an enterprise security solution when a physical firewall is not directly connected to the service border but, rather, is available as a 5G application, such as under a firewall as a service paradigm in a SASE environment. Further, the presented techniques may also add to an existing 5G, private 5G application, or SASE solution for remote hosts (that are directly connected through the Internet) when such hosts are located in an enterprise network. Further still, the techniques are also applicable to the Industry 4.0 initiative and Internet of things (IoT) devices that are connected through enterprise SDA networks or any other intermediary overlay networks (instead of being directly connected to the Internet).

Thus, the presented techniques bring PoP information (such as latency measures, performance details, etc.) to an edge or access element of an SDA network to facilitate 5G application-specific PoP selection and a redirection of the traffic to the correct PoP. That information may be used to select an application-specific PoP exit which meets the SLA requirements and/or select a service using a particular border, and then select a specific PoP, thus meeting the SLA requirements. Additionally, the techniques support and allow

inter-access technology communication among 5G, private 5G, and Wi-Fi 6 endpoints and other wired or wireless access technologies.

Importantly, the presented techniques support different ways of interfacing an SDA and an enterprise fabric with a 5G environment. A first approach for interfacing encompasses integrating the fabric on an N6 interface so that no changes are necessary to the relevant 5G standards. Figure 3, below, depicts elements of such an approach.

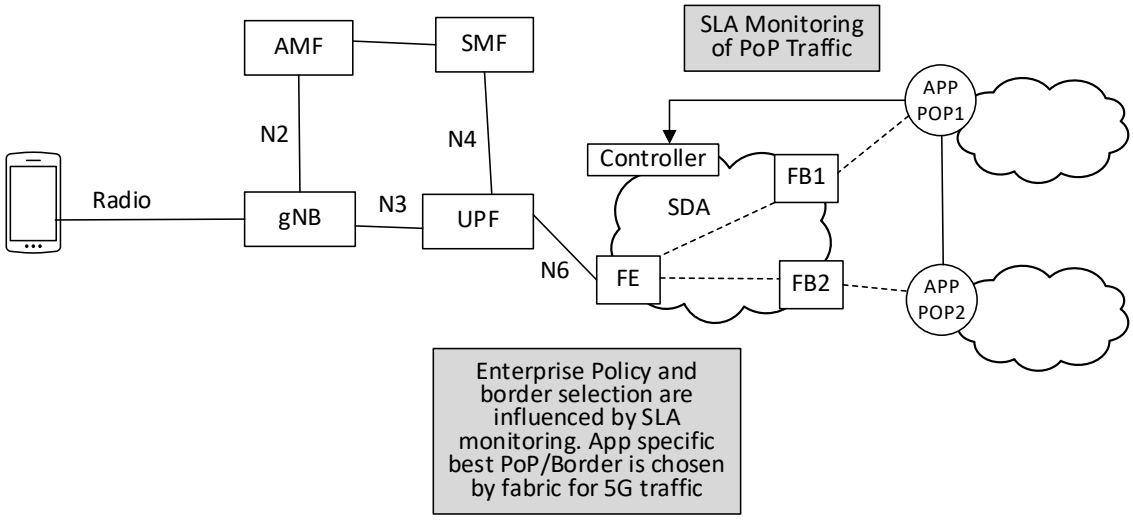

Figure 3: SDA Fabric on N6 Interface

By placing the fabric on an N6 interface, the presented techniques do not interfere or influence the 3GPP 5G standards-based path selection process. Here, an enterprise policy and SDA border selection is influenced by SLA monitoring and an application-specific best PoP or border exit is chosen by the SDA fabric for 5G traffic using policy-based tunnels. Under such an arrangement, an exemplary network path may consist of user equipment (UE) (e.g., an application) → private 5G, Wi-Fi, or radio → gnodeB → general packet radio service (GPRS) tunnelling protocol (GTP) → UPF – N6 → SDA edge (FE) → policy-based tunnels → SDA fabric borders (FBs) → data network (DN) PoP (e.g., an application). Within such a flow, a UE sends all of its traffic to a UPF (which is at the east side of the SDA and fabric), the SDA and fabric tunnels carry the N6 traffic from the FE to the fabric border(s), the appropriate fabric border(s) are chosen by the fabric which then forwards the traffic to the best (i.e., optimized) PoP for the application, and the SDA FE

and SDA fabric borders may be managed by an enterprise controller while a DN PoP may be managed by an application-side controller.

A second approach for interfacing encompasses the integration of a UPF inside of a FE. Figure 4, below, depicts elements of such an approach.

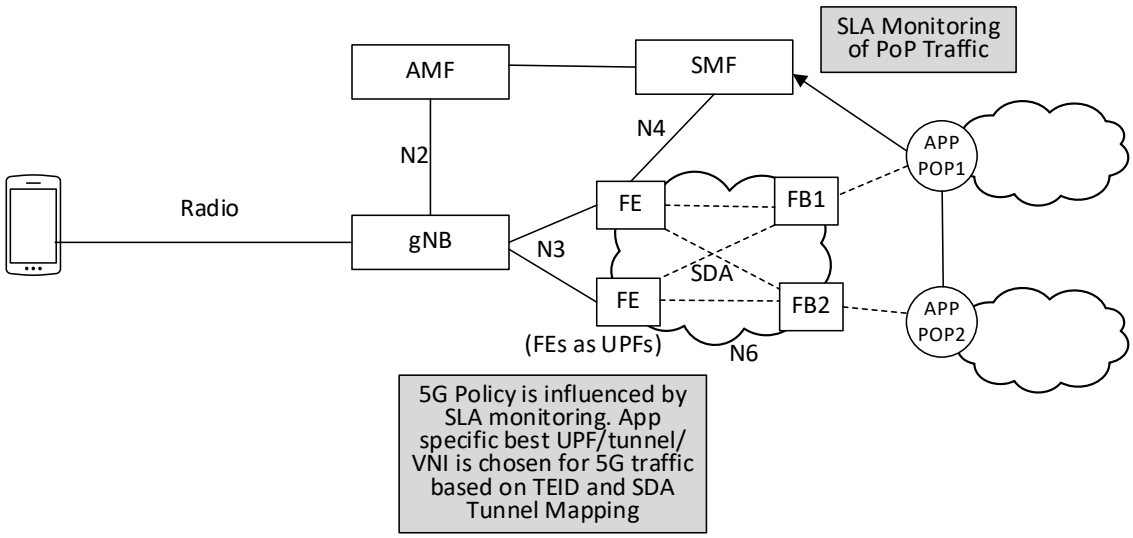

Figure 4: UPF Integrated within FE

The above-described approach does influence the 3GPP 5G standards-based path selection process, but in ways that are allowed by the standards. Here, a 5G policy itself is influenced by SLA monitoring. An application-specific best UPF and then a fabric tunnel and VXLAN network identifier (VNI) on that UPF-FE combination are chosen for the 5G traffic using a tunnel endpoint identifier (TEID)-to-SDA tunnel and VNI mapping. Under such an arrangement a fabric tunnel may also be policy-based. Figure 5, below, presents elements of an exemplary sequence diagram for such an approach with the above-described modifications highlighted in red.

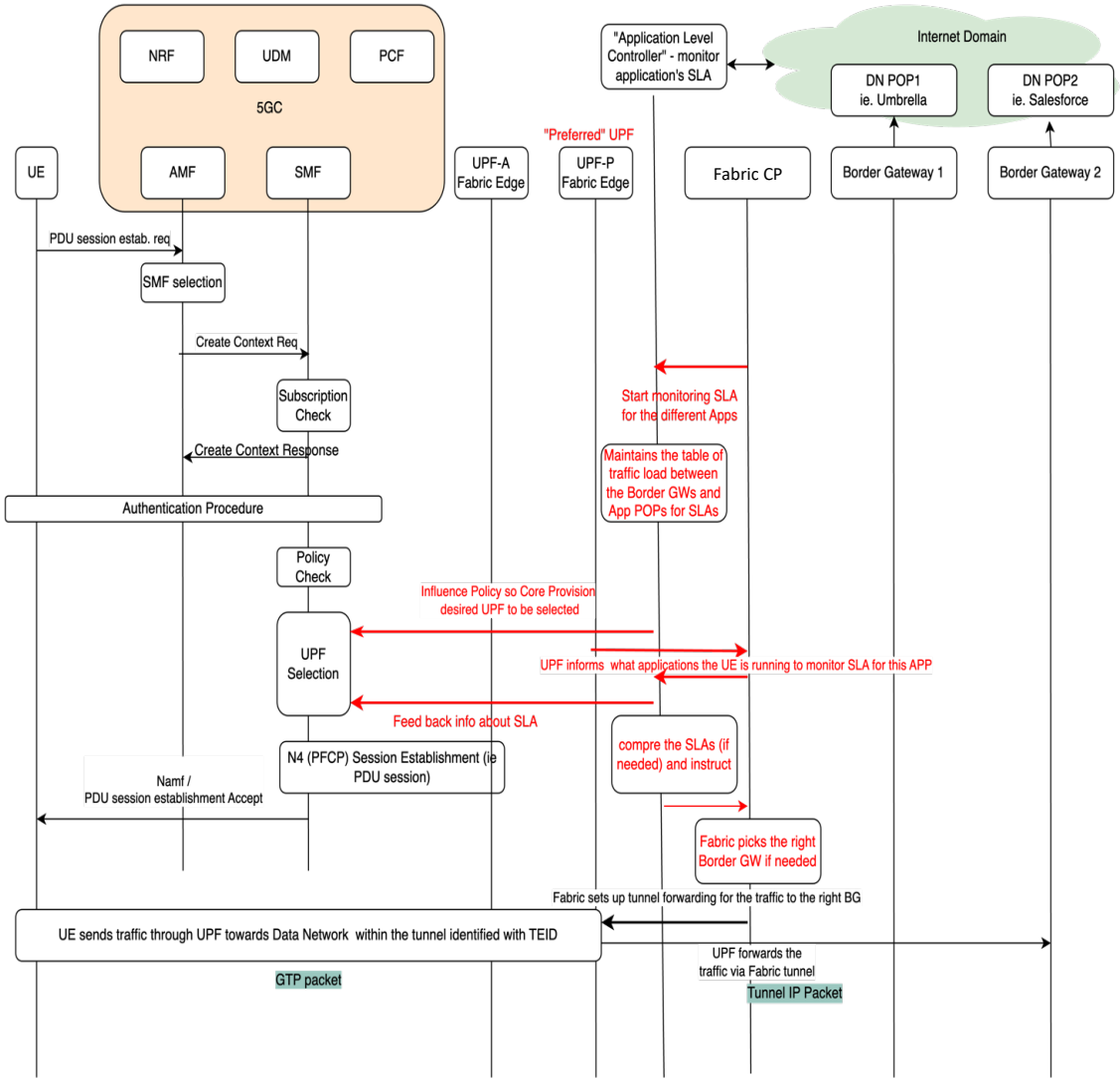

Figure 5: Exemplary Sequence Diagram

In summary, techniques have been presented herein that add to the existing 5G, private 5G, and SASE connectivity options for remote hosts when such hosts are located in an enterprise SDA network. The techniques aid in connecting remote terrain, Industry 4.0, IoT, and private 5G devices through enterprise SDA/SDN networks (or any other intermediary overlay networks) and provide inter-access technology communication between 5G and existing access technology endpoints in an enterprise SDA/SDN fabric. The techniques also bring PoP SLA information (such as latency measures, performance details, etc.) to an edge or access element of a network to facilitate 5G application-specific

PoP selection and a redirection of traffic to the correct PoP. That information may be used to select an application-specific PoP exit which meet SLA requirements and/or select a service using a particular border, and then select a specific PoP, thus meeting the SLA requirements. The techniques also augment a security solution when a physical firewall is not directly connected to the service border but, rather, is available as a 5G application, such as under a firewall as a service paradigm in a SASE environment.