POINT OF VIEW

Value-Add, Slice-Based Cybersecurity Services

Executive Summary

To effectively enable an increasingly scalable and dynamic environment of mobile-connected devices, consumers, and enterprises, all with different characteristics and requirements, the division of public and private 5G networks into logical slices stands out as a cost-effective way to provide customized cellular communications services to different vertical industries and large enterprise customers.

Providing cybersecurity services as part of unique slice resources, configuration, services, and service level agreements (SLAs) will facilitate enterprises adopting network slicing services. It will serve as an additional source of revenue and differentiation for the mobile provider.

This paper discusses Fortinet's approaches and solutions to providing slicing-based cybersecurity services, assuming that the management and implementation of the slicing architecture and mechanism within the mobile domain are secure and adhere to industry standards, recommendations, and regulations.

Driving Slice Value, Monetization, and Adoption with Cybersecurity

5G network slicing provides independent logical networks over a common public or private mobile network. A mobile provider may use network slicing to logically allocate physical or virtual resources across one or more slices, where each slice may have a different characteristics, configurations, and policies, to meet a variety of use cases and SLAs.

Network slicing should be a premium, high-value, revenue generating service targeting enterprises looking to implement use cases requiring specific mobile connectivity privacy and SLAs. By 2028, ABI Research anticipates roughly $12.6 billion in 5G slicing revenue and growth at a striking 109% Compound Annual Growth Rate (CAGR) between 2022 and the end of the forecast period."[1] As use cases and the slices serving them will differ in cybersecurity requirements, such as confidentiality, availability, attack surface, compliancy, and reporting, delivering an appropriate set of value-add, revenue-generating, slice-based cybersecurity services and SLAs is important in driving enterprise adoption and operator revenue.

Static vs. Dynamic Slicing: Different Security Considerations

Static network slices are manually configured and managed by the operator. These are created to meet common use case families that can then be used internally and as an enterprise service offering. This mode of operation creates a significant overhead and limits the operator's ability to deliver slices in a scalable and granular way.

Dynamic network slices provide the possibility for application functions (AF), developers, and enterprises, to establish and destroy their own slices. To do so, the appropriate OSS, BSS, slicing automation, orchestration, and life-cycle management must be in place and provide exposure to external AF and third parties for on-demand slicing management. Such an API exposure must be protected with a layer of cybersecurity that goes beyond authentication and encryption, as provided by the Fortinet FortiWeb web application and API protection (WAAP).

One Platform Delivering Granular Slice-Based Cybersecurity

The type and granularity of slice-based cybersecurity services will depend on the “slice buyer” and the overall set of use cases it is used for:

Example of slice buyers with obvious different security requirements and regulations are:

- Governments
- Enterprises
- Law enforcement
- Cloud hyperscalers

Examples of different use cases with different cybersecurity requirements are:

- Fixed wireless access (FWA)
- Remote process control
- Premium cloud gaming
- Sensitive-sites automated surveillance and response

Using a siloed solution for each combination of cybersecurity services and tenant is prohibited due to cost, integration, scalability limitations, and management complexity. The Fortinet Security Platform, a consolidated cybersecurity platform, provides a rich set of granular cybersecurity services applicable to all vertical slice buyers’ (OT security, anti-botnet, antivirus, application security, next-generation firewall, zero-trust access, and more) use cases while providing a single point for life-cycle management and orchestration.

Discovery and Enforcement of Slice-Based Cybersecurity

Slice discovery

To deliver the appropriate slice-based cybersecurity resources and services, one must identify:

- The UEs within a given slice (slice UE members)
- Security services
  - per slice
  - per session within a slice

The Fortinet Security Platform delivering the cybersecurity services identifies slices and their UE members in real time in the following possible manners:

1. SMF Radius messages notifying the Fortinet Security Fabric function of slices and slice UE members
2. Integration with a third-party tool capable of providing the required information such as Fortinet FortiGate integration with One Layer
3. Integration with a slicing orchestration platform through open APIs

The physical or virtual security network function (PNF/VNF) is deployed, and life-cycle managed by the slicing orchestration platform along the rest of the per-slice components. The Fortinet security PNF/VNF provides native multitenancy support to reduce complexity and cost. A single PNF/VNF supports multiple isolated virtual domains (VDOMs/ADOMs) where each provides full security services and capabilities and is independently managed and orchestrated. Each domain can be dynamically instantiated (and destroyed) and associated to a slice or a group of slices.

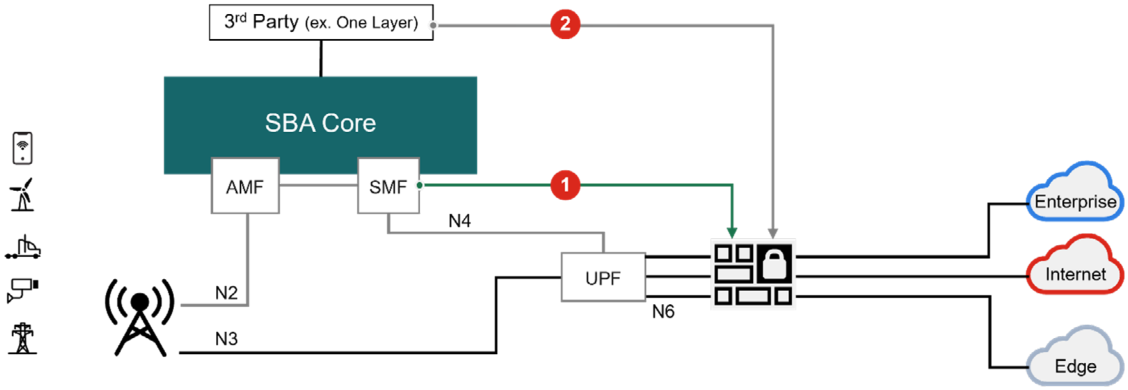
Enforcement

Once the slice information required is obtained by one of the above means, the appropriate cybersecurity services are enforced based on predefined slice and UE-specific profiles.

There are two possible interfaces where the cybersecurity services and SLA are enforced along the user plane, the N3 interface between the RAN and the UPF and the N6 interface between the UPF and any network, such as the internet, edge compute, enterprise network, or the provider's network. Fortinet considers the N6 interface to be the most suitable enforcement point:

1. Unlike the N3 interface, sessions on the N6 interfaces have gone through the UPF, enforcing slice-related SLA.
2. N3 traffic is encapsulated in GTP-U, which creates an overhead de-encapsulation of the tunnels to provide granular cybersecurity services.
3. The N6 interface is the most exposed interface to cyberthreats and risks.

The below diagram depicts the most straightforward architecture to provide slice-based granular cybersecurity services using SMF radius message or third-party integration. In both cases, the N6 interface will be the enforcement point.



1 Native SMF integration for slice-related information. Slice-based cybersecurity enforced on N6.

2 3rd party integration for slice-related information. Slice-based cybersecurity enforced on N6.

Summary

Network slicing provides enormous business potential for mobile providers, especially in the enterprise segment. As 5G capabilities drive new revenue streams and use cases requiring a different array of QoS and cybersecurity capabilities and SLAs, the ability to provide slice-based cybersecurity services will empower slice adoption and revenue.

Fortinet provides a powerful, rich, and easy to deploy cybersecurity platform, enabling operators to offer and deploy granular slice-based cybersecurity services to facilitate enterprise network slicing adoption and generate additional revenue and differentiation in the market. Learn more about Fortinet cybersecurity solution for mobile providers.

[1] "5G Network Slicing Challenges and Opportunities," Allied Business Intelligence, Inc., accessed October 4, 2023.

FORTINET

www.fortinet.com

October 5, 2023 11:01 PM

2376270-0-0-EN