Technical Disclosure Commons

Defensive Publications Series

October 17, 2018

SECURED ENTERPRISE ANCHORED 5G CORE USER PLANE FUNCTION

Eric Stewart

Jiming Shen

SECURED ENTERPRISE ANCHORED 5G CORE USER PLANE FUNCTION

AUTHORS:
Eric Stewart
Jiming Shen

ABSTRACT

Techniques provided herein extend User Plane mobile core Functions (UPFs) outside the conventional service provider boundary to the enterprise customers' premises. Between the enterprise-hosted UPF and packet core, secured ES1u/EN3 and ESx/EN4 interfaces and call flows are defined in addition to those in the 3rd Generation Partnership Project (3GPP) standards. These new secured interfaces are further protected by white-list server authorization before secure tunnels are established.

DETAILED DESCRIPTION

One of the key security requirements for many Enterprise applications is that their traffic should never leave the Enterprise network. In cases where Enterprise users are Bring Your Own Device (BYOD) clients, Enterprise applications that they access when connected to the Enterprise Wi-Fi® are not accessible when they roam outside the Enterprise to the Service Provider (SP)'s macro network without some form of Virtual Private Network (VPN) arrangement. The VPN arrangement may be between the SP and Enterprise, or use a client-based VPN client. When Enterprise users are connected to the macro network, they are anchored to that SP's User Plane mobile core Function (UPF). When that same Enterprise user moves indoors, still connected via the macro, in-building Distributed Antenna System (DAS), or small cells, the Enterprise user is still connected to that SP's UPF with no direct access to the Enterprise without a VPN solution.

3GPP Technical Specification 23.214 established architecture enhancements for control and user plane separation of Evolved Packet Core (EPC) nodes, and provides for the separation of the UPF from the mobile packet core. The separation, and placement of the UPF, within the Enterprise network provides for secure access to Enterprise applications. BYOD users are connected to the SP's macro, DAS, or small cell Radio Access Networks (RANs). Seamless hand-in/out is provided as Enterprise users move between the Enterprise Wi-Fi and SP's RAN.

The Secure Enterprise Anchored 5G UPF is the UPF of a 5G core securely deployed in the Enterprise on-premise network by an SP as part of a Managed Service offering, or deployed by the Enterprise as part of an SP's subscription service. The placement of the UPF in the Enterprise network permits Enterprise BYOD users to securely access Enterprise applications while on-premise or on the move by connecting to a mobile provider's RAN network.

Figure 1 below illustrates a secure enterprise anchored UPF with enhanced interfaces EN3 and EN4.

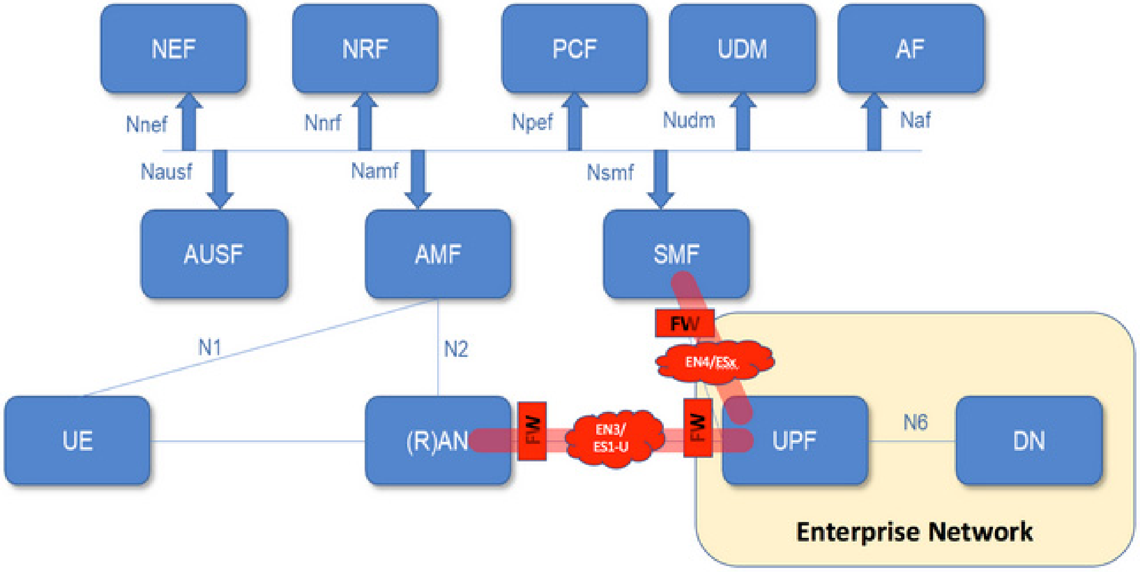

Figure 1

Provided are secure and enhanced EN3 (Internet Protocol Security (IPSec) Encapsulated N3 and LTE S1-U) and EN4 (IPSec Encapsulated N4/SX) interface definitions for communication between the UPF in the Enterprise domain behind a firewall and the Session Management Function (SMF) in the SP network, also behind a firewall. The N3 and N4 traffic may ride securely over the public Internet. Secured EN3 and EN4 is protected by whitelist authorization, Internet Key Exchange version 2 (IKEv2) with Certificate Authority (CA), and IPSec encryption.

Figure 2 below illustrates EN4 secure SX-C/U session establishment procedures.

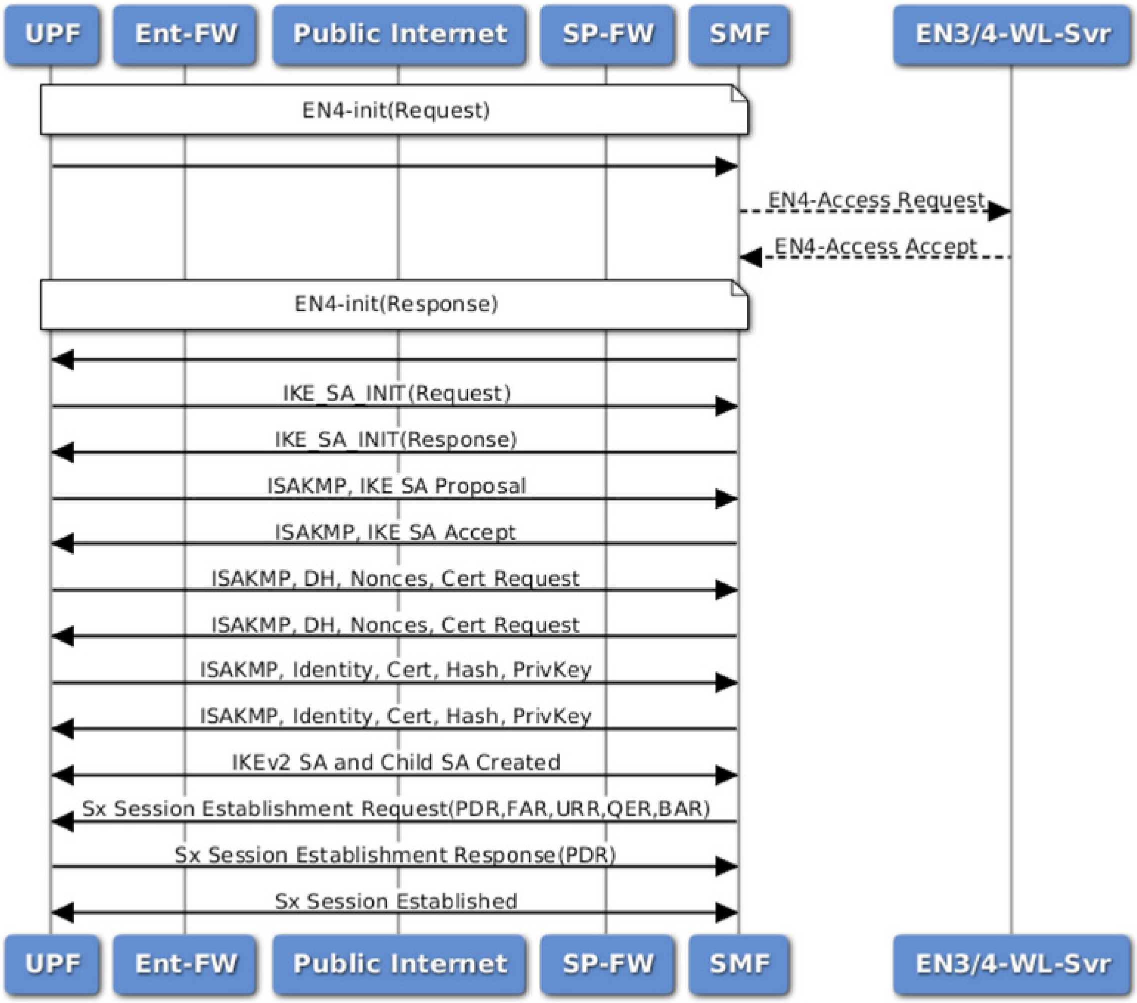

Figure 2

Figure 3 below illustrates EN3 secure user plane establishment procedures.

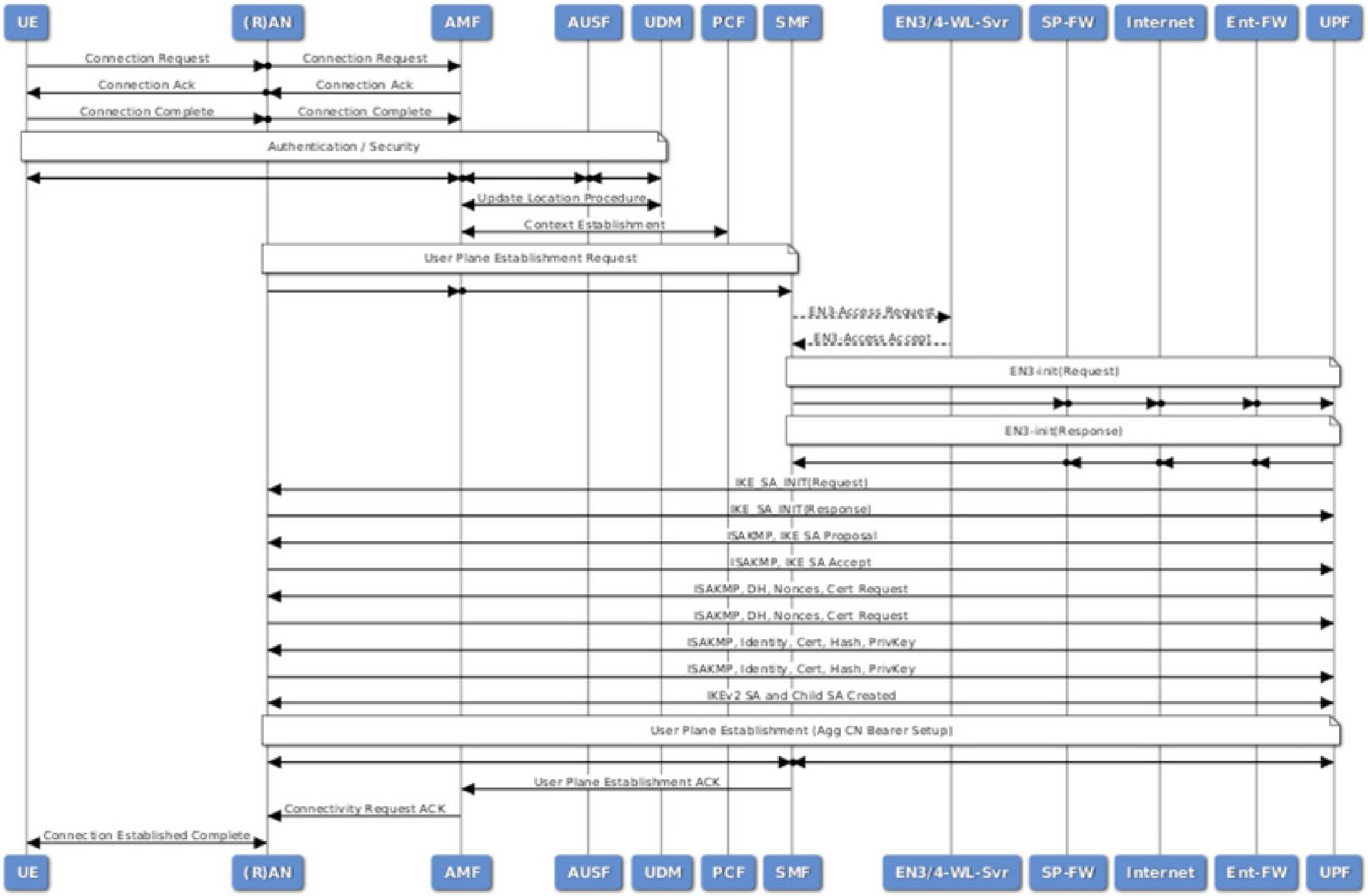

Figure 3

Described herein is an indoor/outdoor mobile traffic steering procedures based on single Access Point Name (APN), Domain Name System (DNS), and Uniform Resource Locator (URL) destination matching.

In summary, techniques provided herein extend UPFs outside the conventional service provider boundary to the enterprise customers' premises. Between the enterprise-hosted UPF and packet core, secured ES1u/EN3 and ESx/EN4 interfaces and call flows are defined in addition to those in the 3rd Generation Partnership Project (3GPP) standards. These new secured interfaces are further protected by white-list server authorization before secure tunnels are established.