October 16, 2018

CREATING A COMMON SECURED TUNNEL FOR NETWORK FUNCTIONS

Ravi Shekhar

Ameo Ghosh

CREATING A COMMON SECURED TUNNEL FOR NETWORK FUNCTIONS

AUTHORS:
Ravi Shekhar
Ameo Ghosh

ABSTRACT

Techniques are described herein for efficient tunnel management for secured communication between Network Functions (NFs) across different Public Land Mobile Networks (PLMNs) through Security Edge Protection Proxies (SEPPs). A common secured tunnel is created for all the NFs to interact between visited SEPPs (vSEPP) and home SEPPs (hSEPPs). There is a choice to select different authentication methods between different vSEPP-hSEPP pairs.

DETAILED DESCRIPTION

In 5G architecture, a Security Edge Protection Proxy (SEPP) is defined to provide topology hiding and message filtering/policing between inter - Public Land Mobile Network (PLMN) control plane interfaces. Network Functions (NFs) between different PLMNs exchange control plane messages through SEPP. Visited SEPPs (vSEPP) and home SEPPs (hSEPPs) use secured tunnels between them. Different types of authentication methods are available for securing tunnels between vSEPPs and hSEPPs, and each NF interaction can lead to the creation of a new tunnel between SEPPs. This may lead to the existence of too many tunnels between SEPPs. Also, supporting different authentication methods between different SEPP pairs is challenging in current designs.

As described herein, Hypertext Transfer Protocol 2 (HTTP/2) header metadata is used to exchange bitstrings to understand types of security methods supported and mutually agreed based on received responses and lists of preferred headers. Otherwise, a fallback option may be employed for static configuration based Transport Layer Security (TLS) over HTTP/2.

Each roaming partner (PLMN) may have a different type of support preference for security. There may be a common secured tunnel between a vSEPP-hSEPP pair. Moreover, there may be multiple vSEPP-hSEPP pairs, each using different authentication methods.

Published by Technical Disclosure Commons, 2018

As illustrated in Figure 1 below, the SEPP may advertise the supported authentication method(s) to all the peers as part of a bootstrapping procedure.

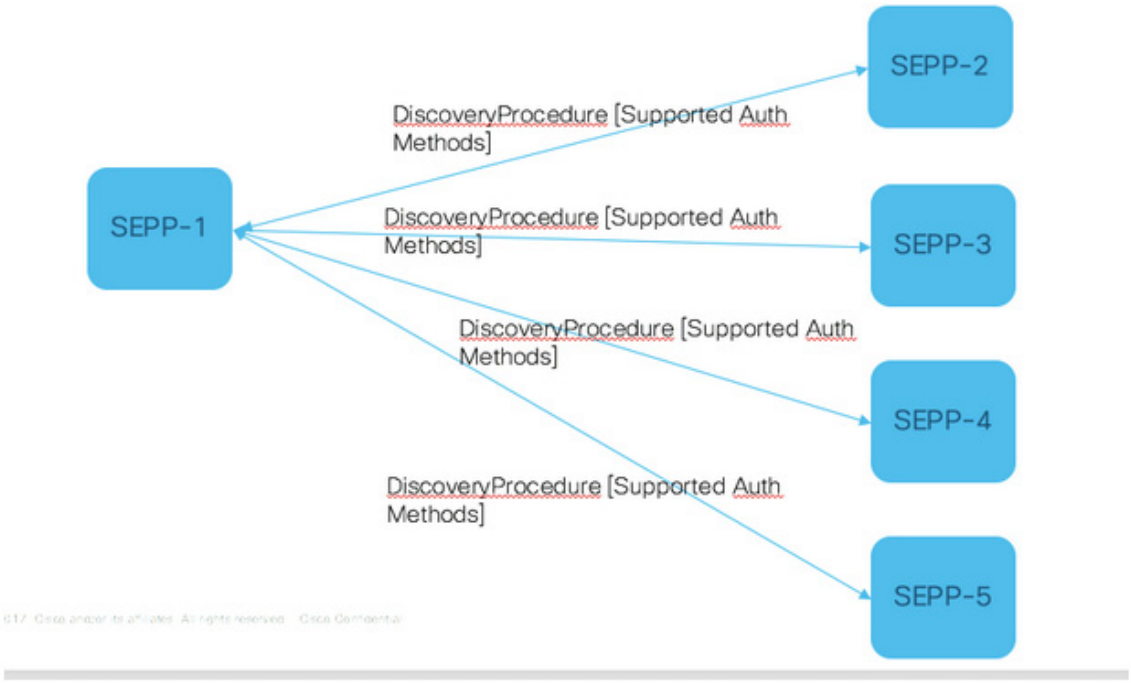

Figure 1: Discovery/Handshake of Authentication methods supported with peers during bootstrap

Each peer SEPP may respond back with the supported authentication method during an initial handshake (during bootstrapping). As illustrated in Figure 2 below, once a secured tunnel is established between a vSEPP-hSEPP pair, that tunnel can also be used for all the NFs control plane interactions between those two PLMNs.

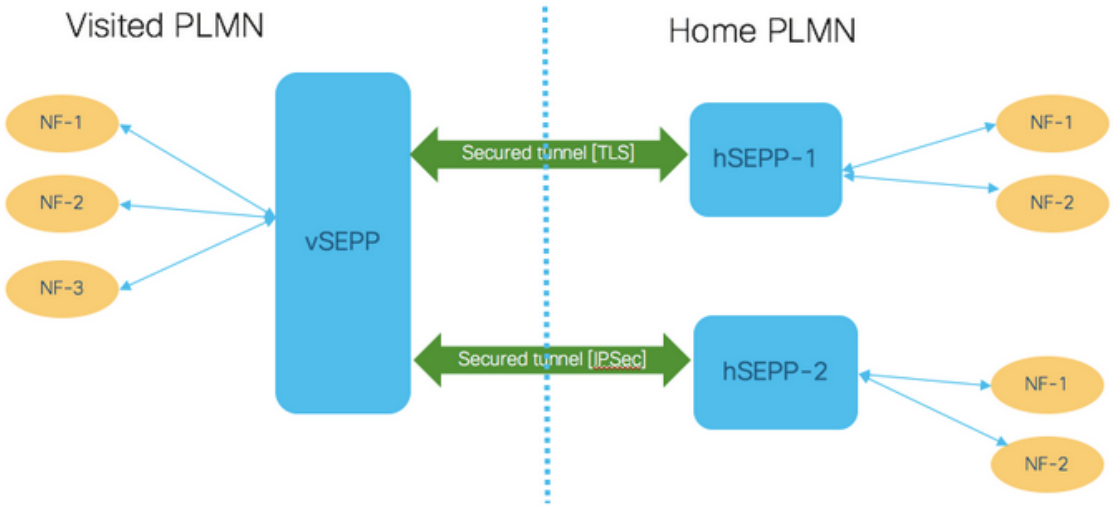

Figure 2: Common Secured tunnel between vSEPP-hSEPP pair.

When requested to connect to the User Equipment (UE)'s home NF, the visited NF may send Service Based Interface (SBI) - defined messages to a Uniform Resource Identifier (URI) exposed by the vSEPP. On the other side, one or more of the same type of secured connections based on discovery involving HTTP/2 header metadata may be used to exchange a list of supported authentication schemes in response to the initial registration header list of current authentication schemes at the visited side.

For each subscriber, the same PLMN visiting area tunnel may be used as streaming. The same link may be reused for multiple requests.

In case of idle connections, a keep-alive scheme may ensure that costly endpoints are brought down. Alternatively, multiple connections may be trimmed down to just one connection depending on the particular configuration.

In summary, techniques are described herein for efficient tunnel management for secured communication between NFs across different PLMNs through SEPPs. A common secured tunnel is created for all the NFs to interact between vSEPP and hSEPPs. There is a choice to select different authentication methods between different vSEPP-hSEPP pairs.