example, a public WLAN or femtocell access network). Trusted access networks include access networks that the network operator considers have a level of trust from a security stand point and may interface directly with the EPC network.

[0006] In the new set of 5G standards, a Non-3GPP Access Network (N3AN) is treated as a 5G Access Network and part of the 5G System (5GS). For untrusted non-3GPP access, a Non-3GPP Interworking Function (N3IWF) provides termination of signaling interfaces for control-plane and user-plane respectively, same as an NG-RAN node. Thus, 5G capable UEs can access the 5G core network (5GCN) by connecting to Non-3GPP Access Network as a 5G Access Network via the N3IWF. The N3IWF relays uplink and downlink control-plane signaling between the UE and the 5GCN. In addition, the N3IWF provides user plane connection between the UE and the 5GCN for sessions over non-3GPP access networks.

[0007] Currently, the signaling procedures between the UE and N3IWF are specified when certain security authentication establishment is accepted by the network. However, there is no method available to handle the case when the security association establishment is not accepted by the network. Similarly, for user plane connections, a method needs to be specified to handle the case when the user plane security association establishment is not accepted by the network.

[0008] Therefore, a need exists to provide a system and method that supports handling failure during security association establishment for access to 5GCN via non-3GPP access networks. Other needs and benefits are also provided with embodiments described herein.

SUMMARY

[0009] The following presents a summary of the disclosed subject matter in order to provide a basic understanding of some aspects of the disclosed subject matter. This summary is not an exhaustive overview of the disclosed subject matter. It is not intended to identify key or critical elements of the disclosed subject matter or to delineate the scope of the disclosed subject matter. Its sole purpose is to present some concepts in a simplified form as a prelude to the more detailed description that is discussed later.

[0009a] In an aspect, the present disclosure refers to an interworking function node (N3IWF) for managing a network connection over an untrusted access network to a core network, the N3IWF comprising: a first network interface configured to communicate with user equipment (UE) over the untrusted access network; a second network interface configured to communicate with one or more nodes in the core network; and a processing device configured to cause the N3IWF to perform at least: processing a request to establish a secure

connection to the core network, received from the UE over the untrusted access network; providing, to the one or more nodes in the core network via the second network interface, an authentication and secure connection establishment request; determining, based upon a response from the one or more nodes in the core network in response to the authentication and secure connection establishment request, that establishment of secure connections over untrusted access networks is not allowed by the core network; providing, to the UE, a response message comprising an indication that the request to establish the secure connection is not approved because connection establishment over the untrusted access network is not allowed by the core network; and receiving, from the UE, in response to the response message, a stop message terminating the request to establish the secure connection to the core network.

[0009b] In another aspect, the present disclosure refers to an Access and Mobility management Function (AMF) device for handling a network connection request to a core network received from an interworking function node (N3IWF), the AMF device comprising: a network interface configured to communicate with the N3IWF and an authentication function in the core network; and a processing device configured to cause the AMF device to perform at least: receiving, from the interworking function node, over the network interface, an authentication and secure connection establishment request, the authentication and secure connection establishment request being associated with a request for connection establishment with the core network received by the N3IWF, from a user equipment (UE), over an untrusted access network; in response to receiving the authentication and secure connection establishment request, providing a request for authentication and subscription check towards an Authentication Server Function (AUSF) of the core network; in response to determining that the authentication and subscription check by the AUSF has failed, generating a response message to the authentication and secure connection establishment request received from the N3IWF by encapsulating in the response message a cause value indicating that secure access to the core network is not allowed to be requested or established over untrusted access networks; and providing the response message to the N3IWF.

[0009c] In another aspect, the present disclosure refers to a user equipment (UE), comprising: a network interface configured to communicate with an interworking function node (N3IWF) of a core network over an untrusted access network; and a processing device configured to

cause the UE to perform at least: generating a registration request for secure session establishment to the core network; sending, over the untrusted access network, to the N3IWF of the core network, the registration request; receiving, in response to the registration request, from the N3IWF of the core network, a response message, the response message comprising an indication of whether access to the core network over untrusted access networks is allowed by the core network; determining, from the response message, that secure session establishment with the core network over untrusted access networks is not allowed by the core network; and in an instance in which secure session establishment with the core network over untrusted access networks is not allowed by the core network, providing, to the N3IWF, a stop message to terminate the request for the secure session establishment with the core network.

[0010] In one example, an interworking function node for managing a network connection over an untrusted access network to a core network includes a first network interface configured to communicate with user equipment (UE) over the untrusted access network and a second network interface configured to communicate with one or more nodes in the core network. The interworking function node includes a processing device configured to process a request for a connection establishment to the core network from the UE in the untrusted

CLAIMS

1. An interworking function node (N3IWF) for managing a network connection over an untrusted access network to a core network, the N3IWF comprising:

a first network interface configured to communicate with user equipment (UE) over the untrusted access network;

a second network interface configured to communicate with one or more nodes in the core network; and

a processing device configured to cause the N3IWF to perform at least:

processing a request to establish a secure connection to the core network, received from the UE over the untrusted access network;

providing, to the one or more nodes in the core network via the second network interface, an authentication and secure connection establishment request;

determining, based upon a response from the one or more nodes in the core network in response to the authentication and secure connection establishment request, that establishment of secure connections over untrusted access networks is not allowed by the core network;

providing, to the UE, a response message comprising an indication that the request to establish the secure connection is not approved because connection establishment over the untrusted access network is not allowed by the core network; and

receiving, from the UE, in response to the response message, a stop message terminating the request to establish the secure connection to the core network.

2. The N3IWF of claim 1, wherein the processing device is further configured to cause the N3IWF to perform:

receiving, from the UE, over the first network interface, the request to establish the secure connection over the untrusted access network;

transmitting, over the second network interface, towards the one or more nodes of the core network, the authentication and secure connection establishment request;

receiving, from the one or more nodes of the core network, over the second network interface, an authentication and secure connection establishment response ; and

generating an Internet Key Exchange (IKE) response message to the UE with a Non-Access Stratum (NAS) payload including the indication that the establishment of the secure connection over the untrusted access network is not allowed by the core network.

3. The N3IWF of claim 2, wherein the processing device is further configured to cause the N3IWF to perform:

receiving a response from an Access and Mobility Management Function of the core network, the response including a Registration Reject message including a cause value indicating that access to the core network over the untrusted access network is not allowed; and

generating the IKE response message with the NAS payload including a message type indicating that the connection establishment over the untrusted access network is not allowed by the core network.

4. The N3IWF of claim 2, wherein the processing device is further configured to cause the N3IWF to generate the IKE response message by either:

generating the IKE response message with a notify payload including a private notify message type indicating a failure reason; or

generating the IKE response message with the notify payload including the private notify message type indicating that the connection establishment over the untrusted access network is not allowed by the core network.

5. The N3IWF of any preceding claim, wherein the processing device is further configured to cause the N3IWF to perform:

transmitting the response message to the UE, wherein the response message indicates that the connection establishment over the untrusted access network is not allowed by the core network; and

in response to receiving the stop message from the UE, generating a failure message to the UE.

6. The N3IWF of any preceding claim, wherein the processing device is further configured to cause the N3IWF to perform:

processing the stop message from the UE, wherein the stop message includes a 5G-Stop message format having a message identifier field, and wherein the message identifier field includes a 5G-Stop identifier.

7. The N3IWF of any preceding claim, wherein the request for the connection establishment from the UE in the untrusted access network includes an IKE request message to initiate an IPsec Security Association (SA) with the core network.

8. The N3IWF of any preceding claim, wherein the core network is a fifth-generation core network (5GCN) and the untrusted access network is an untrusted non-third-generation partnership project (non-3GPP) access network.

9. An Access and Mobility management Function (AMF) device for handling a network connection request to a core network received from an interworking function node (N3IWF), the AMF device comprising:

a network interface configured to communicate with the N3IWF and an authentication function in the core network; and

a processing device configured to cause the AMF device to perform at least:

receiving, from the N3IWF, over the network interface, an authentication and secure connection establishment request, the authentication and secure connection establishment request being associated with a request for connection establishment with the core network received by the N3IWF, from a user equipment (UE), over an untrusted access network;

in response to receiving the authentication and secure connection establishment request, providing a request for authentication and subscription check towards an Authentication Server Function (AUSF) of the core network;

in response to determining that the authentication and subscription check by the AUSF has failed, generating a response message to the authentication and secure connection establishment request received from the N3IWF by encapsulating in the response message a cause value indicating that secure access to the core network is not allowed to be requested or established over untrusted access networks; and

providing the response message to the N3IWF.

10. The AMF device of claim 9, wherein the processing device is further configured to cause the AMF device to perform:

encapsulating in the response message a Registration Reject message that includes the cause value, wherein the cause value includes a cause value indicating access to the core network over the untrusted access network is not allowed by the core network.

11. The AMF device of claim 10, wherein the processing device is further configured to cause the AMF device to perform:

generating an Extensible Authentication Protocol (EAP) failure indication in the response message.

12. The AMF device of any one of claims 9 to 11, wherein the untrusted access network is an untrusted non-third-generation partnership project (non-3GPP) access network and the core network is a fifth-generation core network (5GCN).

13. A user equipment (UE) comprising:

a network interface configured to communicate with an interworking function node (N3IWF) of a core network over an untrusted access network; and

a processing device configured to cause the UE to perform at least:

generating a registration request for secure session establishment to the core network;

sending, over the untrusted access network, to the N3IWF of the core network, the registration request;

receiving, in response to the registration request, from the N3IWF of the core network, a response message, the response message comprising an indication of whether access to the core network over untrusted access networks is allowed by the core network;

determining, from the response message, that secure session establishment with the core network over untrusted access networks is not allowed by the core network; and

in an instance in which secure session establishment with the core network over untrusted access networks is not allowed by the core network, providing, to the N3IWF, a stop message to terminate the request for the secure session establishment with the core network.

14. The UE of claim 13, wherein the processing device is further configured to cause the UE to perform:

generating the stop message, the stop message indicating an end to the registration request for secure session establishment to the core network.

15. The UE of claim 14, wherein the processing device is further configured to cause the UE to perform:

generating the stop message as an Extensible Authentication Protocol (EAP)-Response formatted message including a message identifier field set to 5G-Stop.

16. The UE of claim 15, wherein the processing device is further configured to cause the UE to perform:

processing an EAP failure message from the N3IWF; and

performing a security association (SA) deletion procedure.

17. The UE of any one of claims 13 to 16, wherein the untrusted access network is an untrusted non-third-generation partnership project (non-3GPP) access network and the core network is a fifth-generation core network (5GCN).