IPsec Support for IPv6

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product (s) or Functional Area	5G-UPF
Applicable Platforms	VPC-SI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G UPF Configuration and Administration Guide*

Revision History

Table 2: Revision History

Revision Details	Release
First introduced	2021.04.0

Feature Description

IPsec is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPsec provides confidentiality, data integrity, access control, and data source authentication to IP datagrams.

IPsec AH and ESP

Authentication Header (AH) and Encapsulating Security Payload (ESP) are the two main wire-level protocols that are used by IPsec. They authenticate (AH) and encrypt-plus-authenticate (ESP) the data flowing over that connection.

- AH is used to authenticate – but not encrypt – IP traffic. Authentication is performed by computing cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which may be modified in transit, such as TTL or the header checksum), and stores this in a newly added AH header that is sent to the other end. This AH header is injected between the original IP header and the payload.
- ESP provides encryption and optional authentication. It includes header and trailer fields to support the encryption and optional authentication. Encryption for the IP payload is supported in transport mode and for the entire packet in the tunnel mode. Authentication applies to the ESP header and the encrypted data.

IPsec Transport and Tunnel Mode

Transport Mode provides a secure connection between two endpoints as it encapsulates the IP payload. The Tunnel Mode encapsulates the entire IP packet to provide a virtual secure hop between two gateways.

Tunnel Mode forms the more familiar VPN functionality, where entire IP packets are encapsulated inside another and delivered to the destination. It encapsulates the full IP header and the payload.

Note The UPF:UPF ICSR over IPsec works only with Tunnel Mode. Transport Mode is not supported.

IPsec Terminology

Crypto Access Control List

Access Control Lists define rules, usually permissions, for handling subscriber data packets that meet certain criteria. Crypto ACLs, however, define the criteria that must be met for a subscriber data packet to be routed over an IPsec tunnel.

Unlike other ACLs that are applied to interfaces, contexts, or one or more subscribers, crypto ACLs are matched with crypto maps. In addition, crypto ACLs contain only a single rule while other ACL types can consist of multiple rules.

Before routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria that are specified in the crypto ACL, the system initiates the IPsec policy that is dictated by the crypto map.

Transform Set

Transform Sets are used to define IPsec security associations (SAs). IPsec SAs specify the IPsec protocols to use to protect packets.

Transform sets are used during Phase 2 of IPsec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPsec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

ISAKMP Policy

Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (such as which encryption parameters to use, how to authenticate the remote peer, and so on) between the system and a peer security gateway.

During Phase 1 of IPsec establishment, the system and a peer security gateway negotiate IKE SAs. These SAs are used to protect subsequent communications between the peers including the IPsec SA negotiation process.

Crypto Map

Crypto Maps define the tunnel policies that determine how IPsec is implemented for subscriber data packets.

There are several types of crypto maps that are supported in 5G-UPF. They are:

- Manual crypto maps
- IKEv2 crypto maps
- Dynamic crypto maps

Crypto Template

A Crypto Template configures an IKEv2 IPsec policy. It includes most of the IPsec parameters and IKEv2 dynamic parameters for cryptographic, and authentication algorithms. Security gateway service cannot function without a configured crypto template.

Only one crypto template can be configured per service.

Supported Algorithms

IPsec in 5G-UPF supports the protocols in the following table, which are specified in RFC 5996.

Protocol	Type	Supported Options (with VPP)
Internet Key	IKEv2 Encryption	

Protocol	Type	Supported Options (with VPP)
Exchange version 2	IKEv2 Pseudo Random Function	PRF-HMAC-SHA1, PRF-HMAC-MD5, AES-XCBC-PRF-128
	IKEv2 Integrity	HMAC-SHA1-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192. HMAC-SHA2-512-256, HMAC-MD5-96, AES-XCBC-96
	IKEv2 Diffie-Hellman Group	Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit)
IP Security	IPsec Encapsulating Security Payload Encryption	NULL, DES-CBC, 3DES-CBC, AES-CBC-192, AES-CBC-128, AES-CBC-256, AES-128-GCM-128, AES-128-GCM-64, AES-128-GCM-96, AES-192-GCM, AES-256-GCM-128, AES-256-GCM-64, AES-256-GCM-96
	Extended Sequence Number	Value of 0 or off is supported (ESN itself is not supported)
	IPsec Integrity	NULL, HMAC-SHA1-96, HMAC-MD5-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 **Important** HMAC-SHA2-384-192 and HMAC-SHA2-512-256 are not supported on VPC-DI and VPC-SI platforms if the hardware does not have a crypto hardware.

Limitations and Restrictions

Following are the limitations and restrictions for this feature:

- The feature does not support modification of application ToS.
- If the reordering of packets occurs in an SA, the receiver may discard packets because of anti replay mechanism.
- IPv4 traffic cannot pass through the IPv6 tunnels as this configuration is not allowed. However, IPv4 and IPv6 traffic need IPv4 and IPv6 tunnels respectively.

Example Configurations

Sample Configuration

```
context ipsec-s
ipv6 access-list foo6
permit ip host 2002::1 host 2001::1
#exit
ipsec transform-set B-foo6
#exit
```

```
ikev2-ikesa transform-set ikesa-foo6
#exit
crypto map foo6 ikev2-ipv6
match address foo6
authentication local pre-shared-key encrypted key <encrypted_key>
authentication remote pre-shared-key encrypted key <encrypted_key>
ikev2-ikesa max-retransmission 3
ikev2-ikesa retransmission-timeout 15000
ikev2-ikesa transform-set list ikesa-foo6
ikev2-ikesa rekey
payload foo6-sa0 match ipv6
ipsec transform-set list B-foo6
rekey keepalive
#exit
peer fd4d:5643:2886:6e::7c:1
ikev2-ikesa policy error-notification
#exit
interface ike
ipv6 address fd4d:5643:2886:6e:6b::1/64
crypto-map foo6
#exit
interface loop1 loopback
ipv6 address 2002::1/128
#exit
subscriber default
exit
aaa group default
#exit
ipv6 route 2001::1/128 next-hop fd4d:5643:2886:6e::7c:1 interface ike
#exit
#exit
end
```

Monitoring and Troubleshooting

This section describes the CLI commands available to monitor and troubleshoot the IPsec support for the IPv6 feature.

Show Commands

This section provides information about show commands and their outputs in support of this feature.

- **show crypto map**
- **show crypto map tag** *map_name*: Use this command to verify the map status.
- **show crypto map summary**
- **show crypto ikev2-ikesa security-associations**
- **show crypto ikev2-ikesa security-associations tag** *map_name*
- **show crypto ikev2-ikesa security association summary**: Use this command to verify if the IKEv2 SAs are initiated.
- **show crypto ipsec security associations**: Use this command to verify if the IPsec SAs are stabilized.
- **show crypto ipsec security-associations tag** *map_name*

- **show crypto ipsec security-associations peer** *Peer IP Address*
- **show crypto ipsec security-associations summary**
- **show crypto statistics**
- **clear crypto ike-all** — Clear IKEv1 SA / IKEv2 SA of a map based on given criteria.
- **clear crypto managers** — Clear crypto managers.
- **clear crypto statistics** — Clear crypto statistics for this context.
- **clear crypto ikev2 { local-gateway | peer | tag }**
- **clear crypto security-associations { all | counters | local-gateway | peer | tag }**