LX2160ASFSIBPB

LX2160-based Application Specific Fastpath for Small Cell IPsec Backhaul Product Brief

Rev. 0 — 3 February 2023 Product brief

Document information

Information	Content
Keywords	LX2160ASFSIBPB, Application Specific Fastpath (ASF), Small Cell IPsec Backhaul (SIB) DPAA2, LX2160 processor, ASF IPsec acceleration, Linux networking applications, performance setup, performance values
Abstract	This document describes ASF IPsec acceleration implementation on LX2160 processor. It also lists the use cases, performance setup, and performance values obtained for this processor.

1 Introduction

NXP Application Specific Fastpath (ASF) is a software-based fast path module to accelerate common Linux networking applications such as IPsec, firewall, QoS, NAT, and similar ones. It is supported and optimized to run on Layerscape DPAA2 (Data Path Acceleration Architecture Gen2) family of processors provided by NXP. The ASF leverages DPAA hardware acceleration elements for obtaining maximum performance.

The Linux kernel implements ASF. ASF acts as a fast path processing module, allowing repetitive packet processing to be conducted outside the networking stack. Therefore, ASF implementation enables significant saving of CPU cycles.

This document features the advantages of using ASF IPsec acceleration for Smallcell IPsec Backhaul (SIB) connectivity. It also lists the ASF SIB use cases, performance setup, and performance values on LX2160 processor-based platform.

2 Overview

ASF integrates with the various network control modules of Linux to extract state information for fast path processing.

Following are the main advantages of using ASF:

- Provides seamless integration with Linux Network stack
- Uses standard Linux tools for configuration
- Uses existing notification mechanisms
- Control module adds logic for offload
- ASF API abstracts actual fast-path implementation.

Figure 1 demonstrates how the ASF module fits in the overall Linux system.

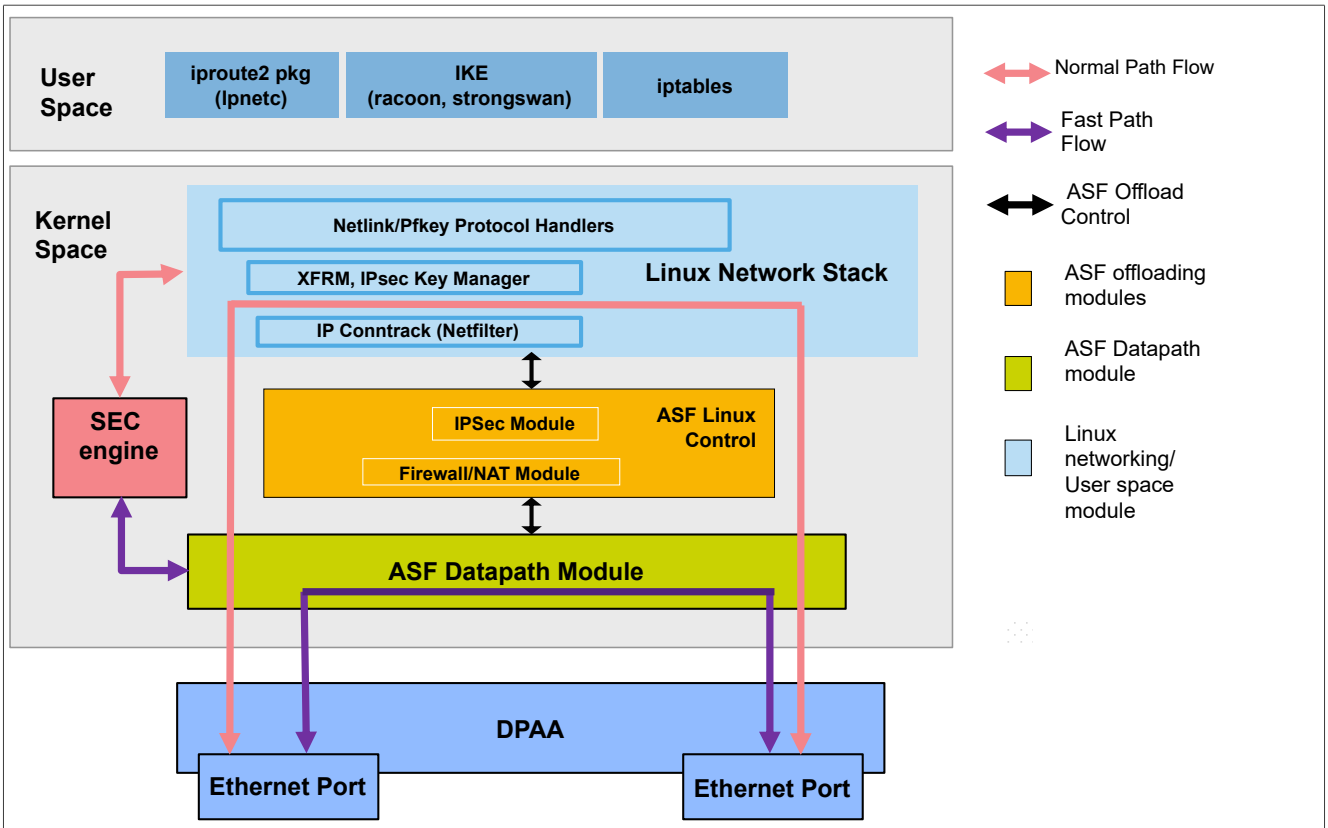

Figure 1. ASF Linux subsystem interaction

3 Features

ASF SIB supports various general and IPsec features as described in this section.

General features of ASF SIB include the following:

- IPv4 and IPv6 forwarding
- Network Address Translation (NAT)
- Virtual Local Area Network (VLAN)

SIB ASF supports IPsec features as listed in Table 1.

Table 1. ASF IPsec supported features

Parameter	Supported features
Protocols	ESP (Encapsulation Security Payload)
Algorithms	DES, 3DES, AES (CBS, CTR, XCBC), HMA-SHA1, HMAC-MD5
Mode	Acceleration for Tunnel mode, Transport mode in normal path
HW acceleration	Integrated with NXP security engine for protocol and crypto acceleration
Features	Supports route based and policy-based VPN
	NAT traversal
	Extended sequence number
	Red-side and black-side fragmentation

Table 1. ASF IPsec supported features*...continued*

Parameter	Supported features
	Security Association (SA) based on DSCP values
	Populate From Packet (PFP)
	Copy/Set/Clear DF and DSCP/QoS bits in outer header
	Persistent tunnels
	Random IV generation for each packet
	IPv4, IPv6 support
	PMTU discovery
	Anti-replay mechanism
	SA lifetime – time and volume
	PMTU handling during fragmentation
	Inbound policy verification
	Stats at policy, SA, and global level
	Internet Key Exchange (IKE) v1 and v2

4 Packet flow path with ASF

This section describes the uplink and downlink packet flow path of ASF SIB product.

4.1 Downlink Packet Flow (network to modem)

Figure 2 illustrates the Downlink Packet Flow.

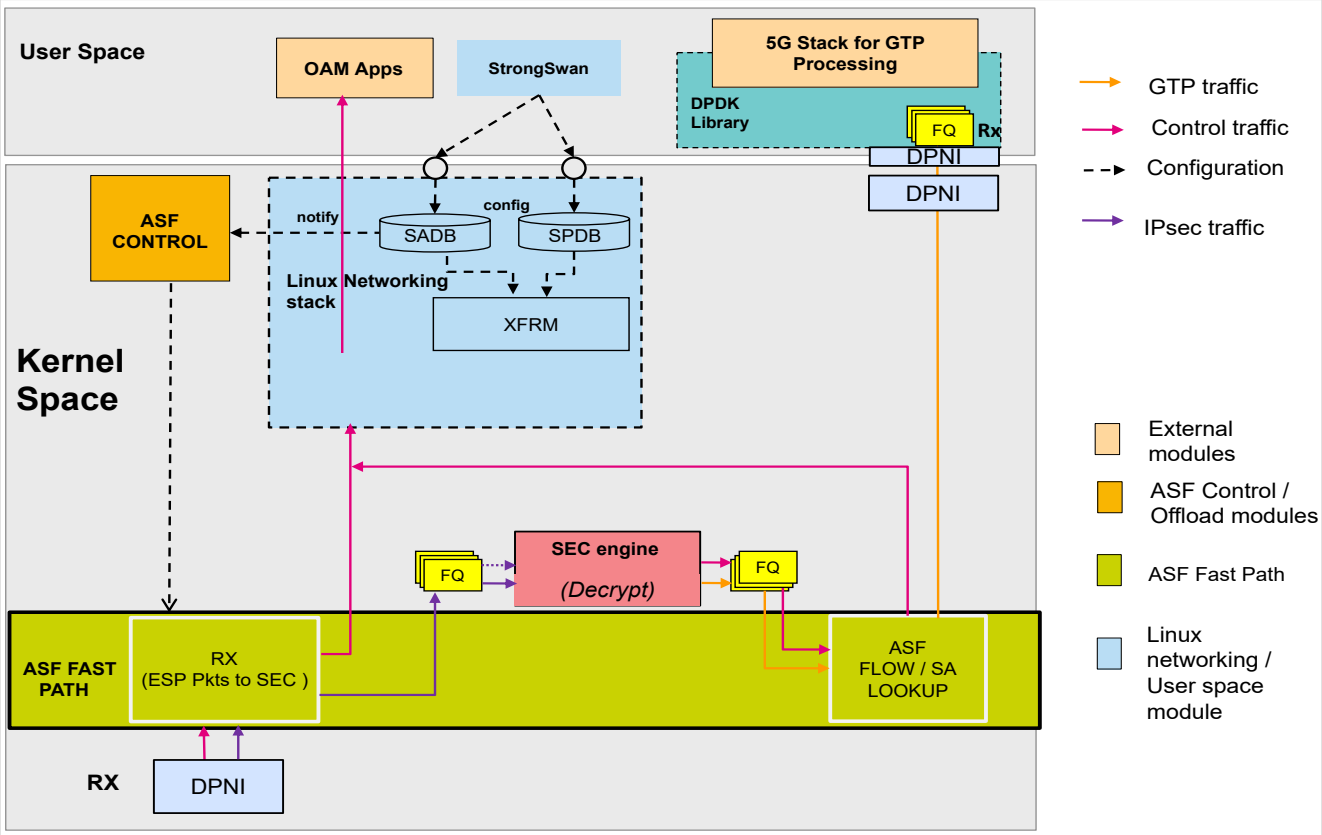

Figure 2. Downlink packet flow using ASF SIB

Downlink packet flow process using ASF SIB is as follows.

ASF kernel module receives ESP encapsulated GTP packets from the backhaul Ethernet port and checks for a matching entry in the ESP table.

- In case a matching ESP entry is not found (few initial packets):
  - The packet is sent to Linux kernel for processing.
  - The Linux kernel checks for a matching configuration (iptable rules, StrongSwan IPsec) and creates a connection tracking entry. It then submits the packet to the SEC hardware engine for applying IPsec. ASF control path taps the SA information and programs to the ASF kernel module.
  - SEC hardware engine decrypts the ESP packet and enqueues to ASF.
- In case a matching ESP entry is found in ASF:
  - Packets are submitted to SEC hardware engine for IPsec processing.
  - After IPsec processing, packets are received back in ASF.
  - If the decrypted packets are fragments, packets are reassembled in ASF.
- ASF classifies the decrypted plain traffic and sends GTP traffic to DPDK application for GTP processing
- DPDK application processes GTP traffic.
- Non-GTP traffic such as OAM is sent to the Linux network stack for respective application processing.

4.2 Uplink Packet Flow (modem to network)

Figure 3 illustrates the Uplink Packet Flow.

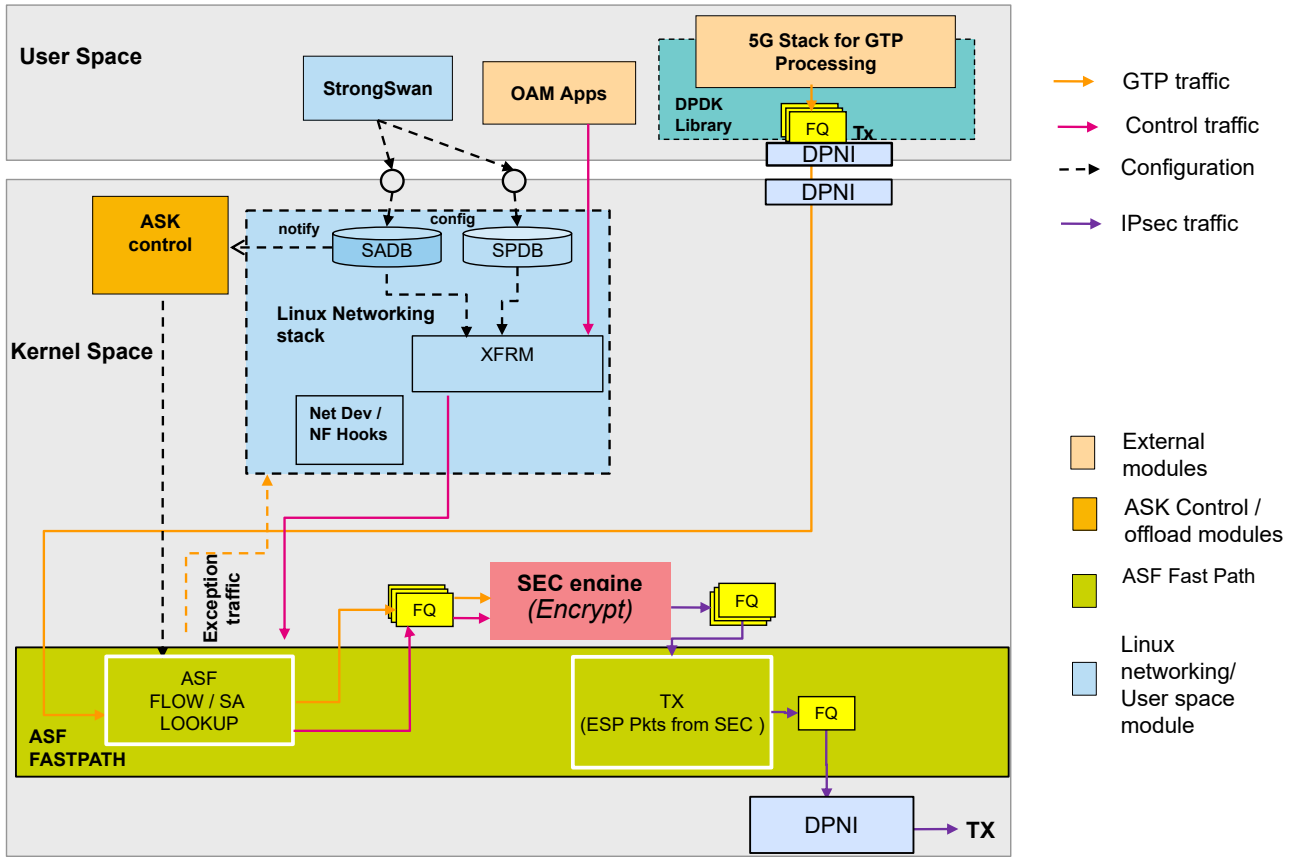

Figure 3. Uplink packet flow using ASF SIB

Uplink packet flow process using ASF SIB is as follows.

The DPDK GTP application enqueues packets to ASF. ASF checks for matching flow.

- If a matching UDP flow is not found (few initial packets):
  - The packet is sent to Linux kernel for processing.
  - The Linux kernel checks for a matching configuration (iptable rules, StrongSwan IPsec) and creates a connection tracking entry. It submits the packet to the SEC hardware engine for applying IPsec. The ASF control path taps SA info and programs to ASF kernel module.
  - SEC hardware engine encrypts and encapsulates the packet in ESP header and enqueues to ASF.
- If a matching 5-tuple UDP flow is found:
  - SA information corresponding to this flow is extracted and the packet is submitted to SEC hardware engine.
  - SEC hardware engine encrypts and encapsulates the packet in ESP header, then enqueues the ESP packet back to ASF.
- ASF then checks the ESP table and transmits the packet on backhaul port. If the packets require to be fragmented, ASF does the fragmentation, and then transmits on backhaul Ethernet port.

5 SIB deployment use cases

The 5G/LTE Integrated Small Cell (ISC) is a typical small cell deployment IPsec use case. This use case utilizes an encrypted (IPsec) link for backhaul to the core network in both Non-Standalone Architecture (NSA) and Standalone Architecture (SA) deployment modes. The deployment uses LX2160 processor to host the 3GPP/5G stack. The processor optionally interfaces with an LTE module that is connected to it over Ethernet.

Figure 4 shows an example deployment use case for an NSA system based on LX2160.

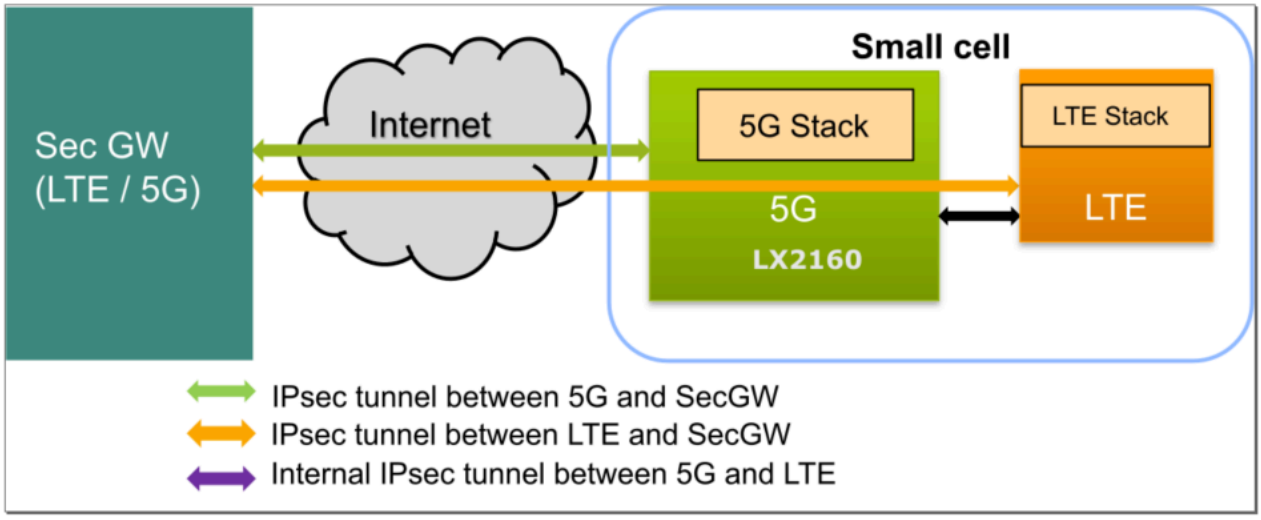

Figure 4. A sample deployment use case for an NSA system based on LX2160

For performance optimization reasons, 5G stacks are typically implemented as DPDK applications in Linux user-space. Leveraging the user-space has the advantage that the ASK solution delivers packets directly ('zero-copy') to the GTP stack in the user-space, bypassing the Linux kernel. The process provides for near-zero communication overhead for backhaul traffic. The typical deployment use cases of NSA mode ISC solution are as listed below:

1. Dedicated IPsec tunnels for LTE and New Radio (NR) modem with Tunnel for LTE using NAT.
2. Dedicated IPsec tunnels for LTE and NR modem with tunnels terminating on NR.
3. Single IPsec Tunnel carrying data for both NR and LTE.
4. Single IPsec Tunnel carrying data for both NR and LTE (with the same inner IP address or inner IP address same as backhaul IP address).

For the first three use cases, backhaul assigns different inner IP addresses for LTE and NR modems using few procedures that are not in the scope of this document. However, one of these procedures is through `IKEv2 ModeCfg`, which is mentioned in the below sections.

For the last use case, consider that backhaul is not aware of the IP addresses assigned to internal ports of LTE and NR modems. In such a case, backhaul assigns a single internal IP address for both LTE and NR modems.

Note: *In this deployment model, control-plane traffic is still delivered to the Linux kernel stack.*

5.1 Dedicated IPsec tunnels for LTE and 5G NR modem, LTE IPsec tunnel using NAT

In this deployment, 5G NR and LTE communicate with the backhaul network using two different inner IP addresses and two different IPsec tunnels:

- One IPsec tunnel between 5G NR and Security gateway, to secure 5G NR traffic.
- Another IPsec tunnel between LTE and Security gateway, to secure LTE traffic. 5G NR applies NAT to LTE traffic while routing to Internet. Due of NAT configuration, LTE uses UDP encapsulated ESP tunneling.

One way to receive these inner IP addresses is through `IKEv2 ModeCfg` configuration where the VPN server issues virtual IP addresses in IKEv2 negotiation.

The tunnels are configured separately on LTE and 5G NR modems with additional NAT rule configured on 5G NR. Figure 5 illustrates this use case.

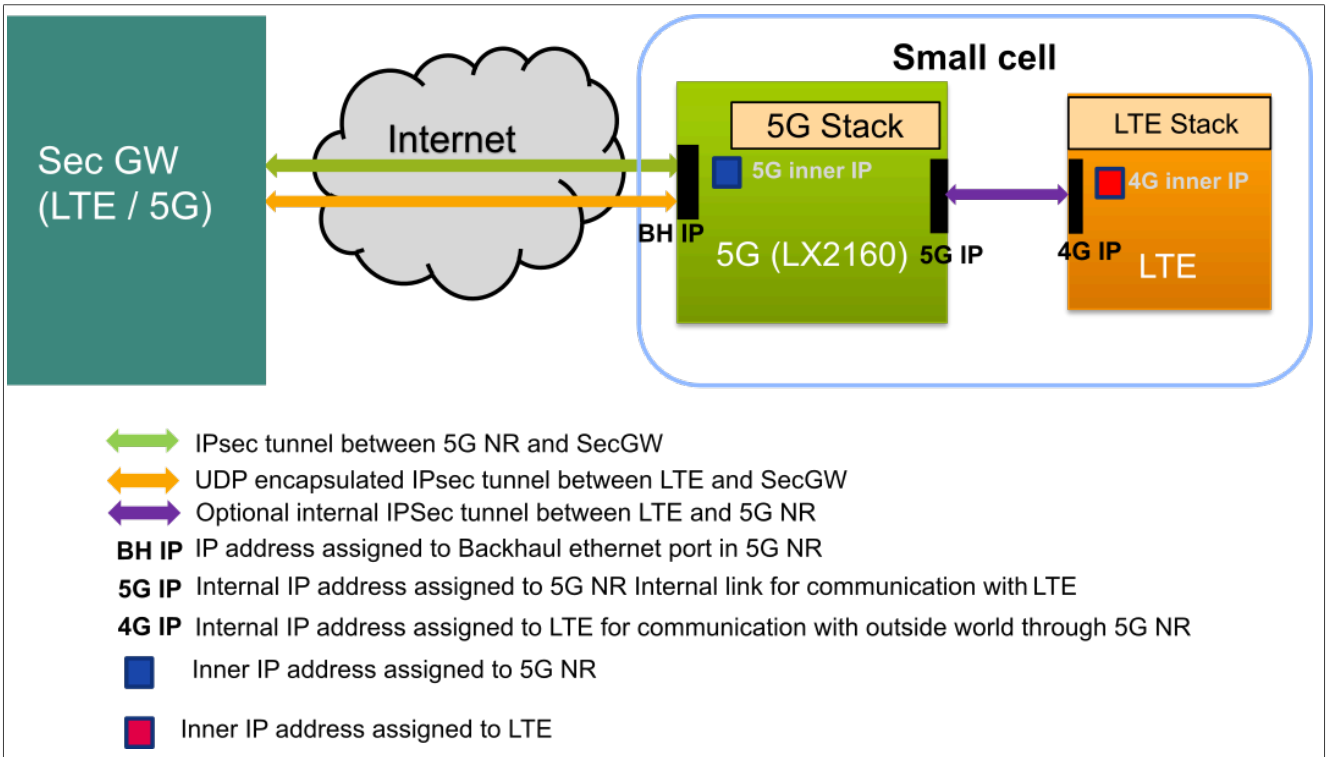

Figure 5. Use case 1: IPsec tunnels for 5G and LTE using NAT

Note: *Internally, depending on implementation, 5G stack and/or LTE stack can use static private IP addresses for GTP traffic. In such cases, NAT should be configured to change static private IP address to inner IP address before IPsec encapsulation.*

5.2 Dedicated IPsec tunnels for LTE and 5G NR modem, LTE tunnel terminating on 5G NR

In this deployment, 5G NR establishes 2 IPsec tunnels;

- One each IPsec tunnel to secure 5G NR and LTE traffic.

In this case, the two inner IP addresses are assigned separately, one for 5G NR and another for LTE.

The LTE IPsec tunnel is terminated on 5G NR. This termination is required in deployments in either of the two scenarios:

- LTE module does not have IPsec.
- LTE requires to communicate with 5G NR only, which can be secure or non-secure.

When using `IKEv2 ModeCfg` configuration for receiving inner IP addresses, 5G NR receives two inner IP addresses as it establishes another IPsec tunnel for LTE traffic. Inner IP address received for LTE IPsec tunnel should be communicated to LTE for publishing its IP address to core network.

Figure 6 illustrates this use case.

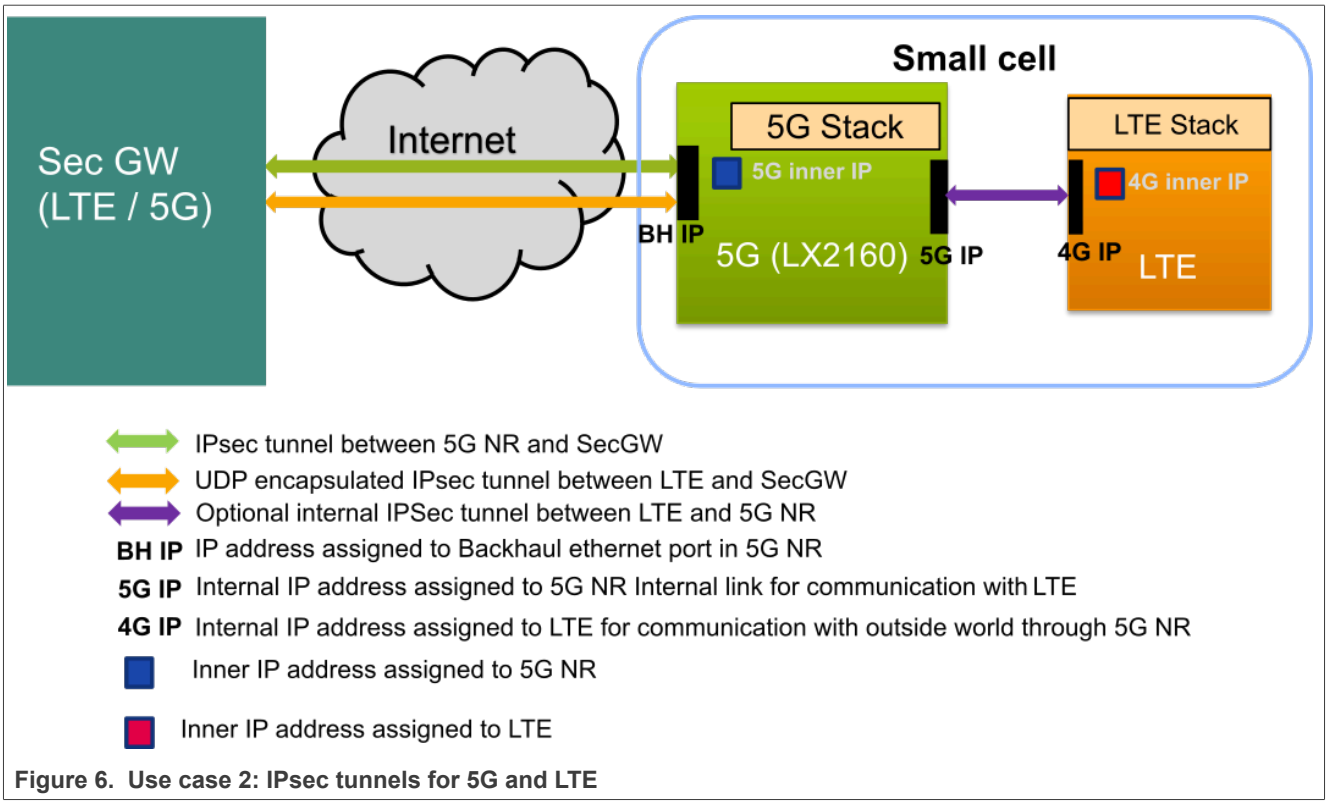

Figure 6. Use case 2: IPsec tunnels for 5G and LTE

For internal communication between 5G NR and LTE, IPsec can be configured to provide security.

Note: *Internally, depending on implementation, 5G stack and/or LTE stack can use static private IP addresses for GTP traffic. In such cases, NAT can be configured to change static private IP address to inner IP address before IPsec encapsulation.*

5.3 Single IPsec tunnel carrying data for both 5G NR and LTE

In this deployment, 5G NR establishes single IPsec tunnel for securing both 5G NR traffic and LTE traffic. Two inner IP addresses are assigned separately, one for 5G NR and another for LTE.

When using `IKEv2 ModeCfg` method of receiving inner IP addresses, 5G NR receives two inner IP addresses while establishing single IPsec tunnel. One Inner IP address should be used for 5G NR traffic. The other inner IP address should be communicated to LTE for publishing its IP address to core network.

Figure 7 illustrates this use case.

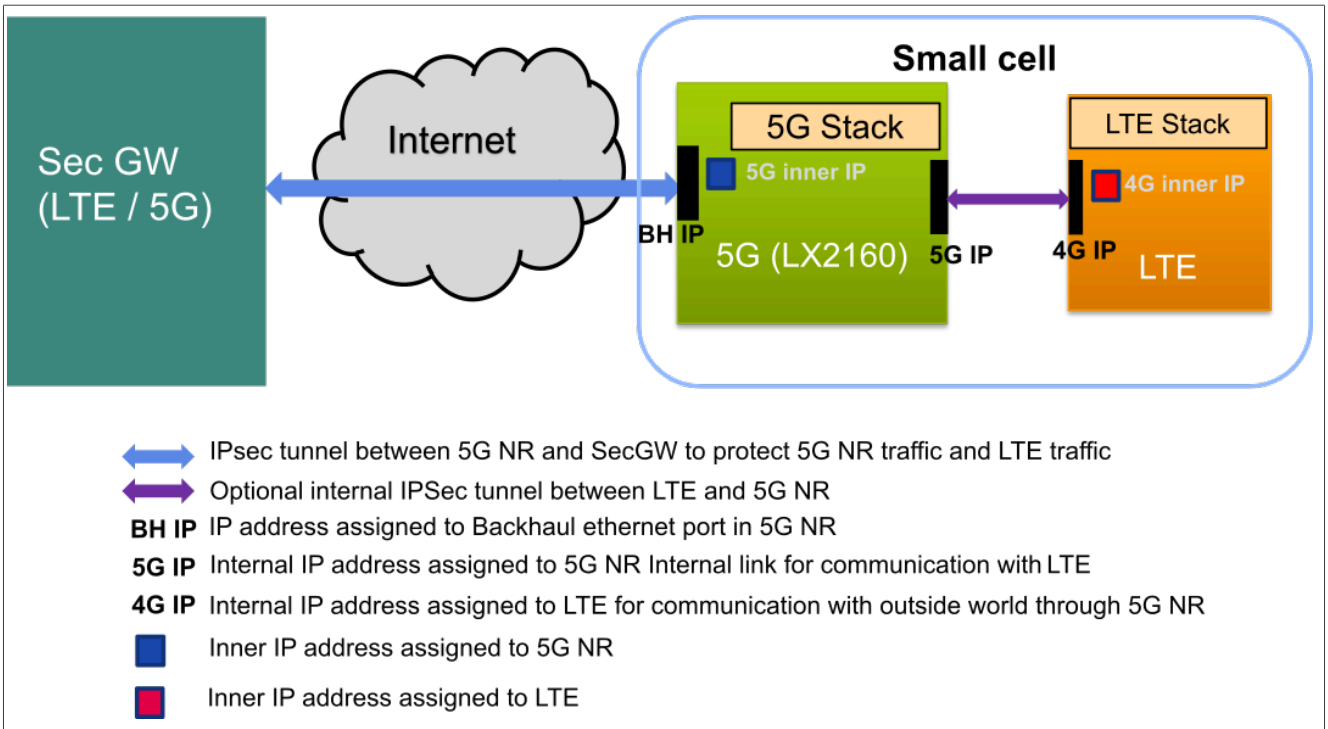

Figure 7. Use case 3: Single IPsec tunnel for 5G and LTE

Note: *Internally, depending on implementation, 5G stack and/or LTE stack can use static private IP addresses for GTP traffic. In such cases, NAT can be configured to change static private IP address to inner IP address before IPsec encapsulation.*

5.4 Single IPsec tunnel carrying data for both 5G NR and LTE and with single inner IP

In this deployment, 5G NR establishes single IPsec tunnel for securing both 5G NR traffic and LTE traffic with single inner IP address. This single inner IP address can be same as Backhaul port (BH) IP address.

The internal ports are managed within ISC, backhaul is not aware of LTE and NR internal port IPs.

Figure 8 illustrates this use case.

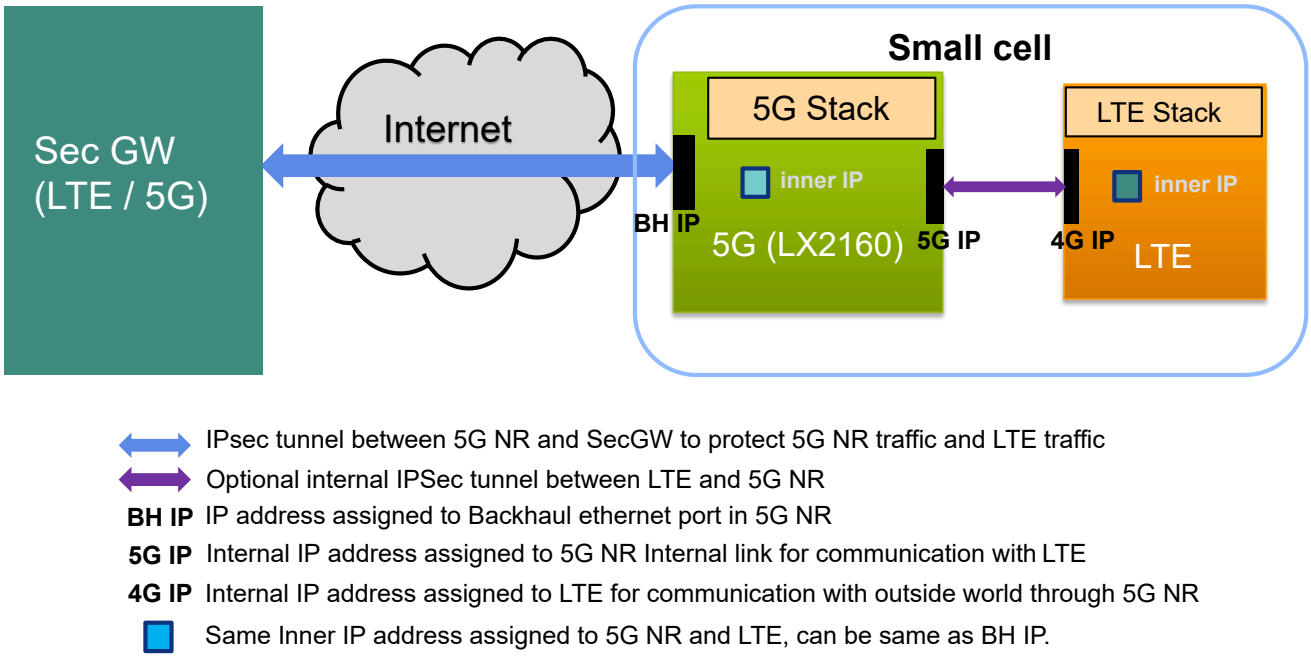

Figure 8. Use case 4: Single IPsec tunnel for 5G and LTE with single inner IP

Note:

ASF SIB does not support this deployment currently. It might be supported in future.

6 IPsec performance with ASF on LX2160 platform

The following sections describe the test setup and performance details for ASF implemented on a sample LX2160 platform operating at 1.8 GHz.

6.1 Test setup for ASF

Figure 9 shows the test setup with LX2160 hardware platform.

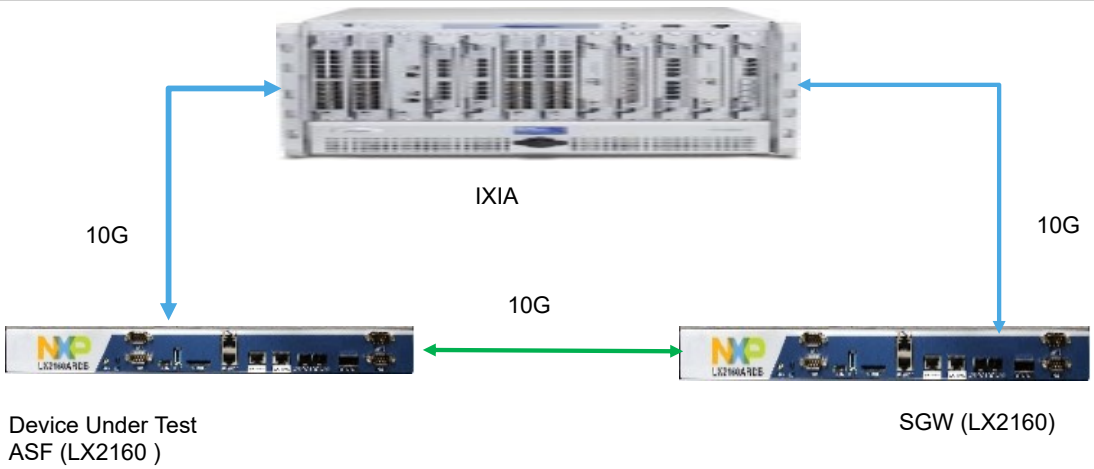

Figure 9. Test setup with LX2160

6.2 IPsec performance with ASF on LX2160 platform

Table 2 presents the IPsec performance with ASF on LX2160 platform operating at 1.8 GHz.

For this test, L2FWD application was run with 2 cores, which utilizes around 12.5% CPU for user space processing.

Note: *In the following table, the following conventions hold:*

1. *Mpps indicates Megapackets per second.*
2. *Reported CPU utilization refers to % of CPU cycles across the number of engaged cores (2,3, or 6) used during test.*
3. ** refers to line rate performance achieved on LX2160 device using 10G interface.*

LX2160A platform specifications *-> 16 cores; Clock @ 1.8 GHz, DDR 2600 MT/s, Bus 600 MHz*

Table 2. IPsec performance with ASF on LX2160 platform

S. No	Packet Size	ASF (LX2160) – L2FWD IPsec 1 Flows 1 Tunnel	ASF (LX2160) – L2FWD IPsec 2 Flows 2 Tunnels	ASF (LX2160) – L2FWD IPsec 4 Flows 4 Tunnels
		Uspace – Kspace communication (DPDK)	Uspace – Kspace communication (DPDK)	Uspace – Kspace communication (DPDK)
1	128	1.52 Mega packets per sec (Mpps) / 1.80 Gbit/s 2 cores with 89% CPU	1.60 Mpps / 1.90 Gbit/s 3 cores with 73% CPU	3.04 Mpps / 3.60 Gbit/s 6 cores with 71% CPU
2	512	1.69 Mpps / 7.20 Gbit/s 2 cores with 95% CPU	1.74 Mpps / 7.40 Gbit/s 3 cores with 73% CPU	3.28 Mpps / 14.0 Gbit/s 6 cores with 71% CPU
3	1024	1.74 Mpps / 14.60 Gbit/s 2 cores with 97% CPU	1.74 Mpps / 14.60 Gbit/s 3 cores with 73% CPU	2.39 Mpps / 19.9 Gbit/s* 6 cores with 61% CPU
4	1400	1.75 Mpps / 19.9 Gbit/s* 2 cores with 96% CPU	1.75 Mpps / 19.9 Gbit/s* 3 cores with 66% CPU	1.75 Mpps / 19.9 Gbit/s* 6 cores with 49% CPU

7 Compliance with specifications

In this solution, the Linux module supports IPsec and the StrongSwan open source application supports Internet Key Exchange (IKE). Table 3 lists the RFCs that these modules support.

Table 3. Supported RFCs

Feature	Specification
IKE (OpenSource Strong Swan)	IKEv1: • RFC 2407 - Domain of interpretation • RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP) • RFC 2409 - The Internet Key Exchange • RFC 2412 - OAKLEY IKEv2: • RFC 7296 - Internet Key Exchange v2 Protocol • RFC 7427 – Signature Authentication in IKEv2
IPsec (Linux)	• RFC 2401 - General IP Security Protocol • RFC 2402 - Authentication Header Protocol • RFC 2403 - HMAC-MD5-96 • RFC 2404 - HMAC-SHAI-96 • RFC 2405 - DES-CBC Cipher algorithm

Table 3. Supported RFCs*...continued*

Feature	Specification
	• RFC 2406 - Encapsulation Security Payload Protocol • RFC 2407 - Domain of interpretation • RFC 2410 - The NULL Encryption Algorithm and its use with IPsec • RFC 5084 – Combined Mode Algorithms (AES-CCM and AES-GCM Authenticated Encryptions)

8 Product availability and commercial terms

ASF SIB is offered under source code license. NXP also offers commercial support and customization and enhancement services. ASF IPsec solution on LX2160 platform is available in Q1' 2023.

Contact your local NXP representative for timing, availability, and commercial terms.

9 Revision history

Table 4 summarizes revisions to this document.

Document revision history

Revision	Date	Topic cross-reference	Substantive change
0	03 February 2023	-	Initial release for LX2160 platform

10 Legal information

10.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

10.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

10.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile — are trademarks and/or registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved.

Layerscape — is a trademark of NXP B.V.

Contents

For more information, please visit: http://www.nxp.com

Date of release: 3 February 2023
Document identifier: LX2160ASFSIBPB