

Securing 5G: Network Slicing Phase 1 Test Report *Q1 2023*

Table of Contents

Introduction	3
Scope of Report	5
Background	5
Network Slicing	5
Network Slicing Test Overview	6
Summary of Process and Findings	6
5G Standalone Test Configuration	8
Network Slicing	12
IPsec Configuration	12
Detailed Test Procedure	13
5G Security Test Bed Network Slicing Test Results	14
Test Case 1, TC-NetSlic-01	14
Test Case 2, TC-NetSlic-02	20
Test Case 3, TC-NetSlic-03	26
Conclusions and Next Steps	35
Appendix: Acronyms	37
References	

Introduction

The 5G Security Test Bed Is the Latest Industry Initiative to Advance 5G Security

The wireless industry prioritizes stronger security and reliability with every generation of its mobile networks. With 5G in particular, secure connectivity is the foundation that supports and enhances the many benefits these networks provide. The wireless industry devotes significant resources to 5G security and has expanded its efforts through the 5G Security Test Bed.

Formally launched in 2022, the 5G Security Test Bed is a unique collaborative endeavor between wireless providers, equipment manufacturers, cybersecurity experts, and academia, created with a sole focus on testing and validating 5G security recommendations and use cases from government agencies, standards bodies, wireless operators, and others. It is the only initiative that uses commercial-grade network equipment and facilities to demonstrate and validate how 5G security standards recommendations will work in practical, real-world conditions.

The 5G Security Test Bed reflects the industry's collaborative approach to 5G security—it was created by the Cybersecurity Working Group (CSWG), an industry initiative that convenes the world's leading telecom and tech companies to assess and address the present and future of cybersecurity. The Test Bed further works with a broad array of government agencies, policymakers, international standards bodies, thought leaders, and partners in the telecommunications and information technology sectors. These groups include the 3rd Generation Partnership Project (3GPP), the International Telecommunication Union (ITU), the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the FCC, among others.

The 5G Security Test Bed Uses Real-World Equipment, Validating Real-World Applications

One of the 5G Security Test Bed's core values lies in its ability to validate 5G security use cases in a real-world environment, using an actual 5G network architecture. Leveraging a significant investment and in-kind contributions, the 5G STB's founding members built this state-of-the-art, private 5G network from scratch for the singular purpose of evaluating 5G network security.

The 5G Security Test Bed's initial focus was to validate the recommendations of the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) advisory group, for both 5G non-standalone (5G NSA) and 5G standalone (5G SA) network configurations. The first report in this series focused on the validation of CSRIC recommendations for optional 5G NSA network security features. This second report focuses on a set of network slicing use cases,

validating 3GPP technical specifications for 5G security components. The 5G Security Test Bed will continue evaluating additional recommendations and use cases from CSRIC and other entities in future tests. It is not set up to be a platform for identifying vulnerabilities or conducting penetration testing of networks or equipment.

Real-World Testing

The 5G Security Test Bed advances wireless security by:

- Conducting real-world tests in a rigorous, transparent, and replicable manner that can assess and validate theoretical and policy concerns and overcome hypothetical laboratory testing limitations.
- Drawing on the expertise of government, wireless providers, and equipment manufactures to evaluate specific use cases and support new equipment development.
- Testing security functionality in different scenarios, enabling industry and government to identify, mitigate, and respond to evolving threats while protecting consumers, businesses, and government agencies.

Real-World Applications

The 5G Security Test Bed's tests and outcomes support several applications that can drive new technology and transform cities, government, and industries. Use cases include government and enterprise applications, general network security protections, and smart city applications such as:

• Government and Enterprise Applications

- o Building private 5G networks for enterprises and government.
- Developing dynamic supply-chain verification technologies for uses such as logistics management.
- Creating automated, reconfigurable factories and other automated factory processes.
- Developing immersive extended reality (XR) applications, including augmented reality (AR), virtual reality (VR), and mixed reality (MR), for both consumers and enterprises.

• General Network Security Protections

- Enhancing protections against international mobile subscriber identity (IMSI) catchers and "rogue" base stations used by cyber criminals.
- o Enabling automatic, rapid threat detection and response.
- Implementing a unified authentication framework that supports security across multiple network types (e.g., cellular and Wi-Fi).

- Smart City Applications
 - o Enabling video for unmanned aerial systems (e.g., drones).
 - Providing support for autonomous vehicles and related technology (e.g. connected cars and C-V2X standards).
 - o Enabling high-resolution video surveillance systems using fixed cameras.

The 5G standalone architecture and network slicing capability tested for in this report are key components of these applications because they enable service to be customized to diverse needs and requirements. The test cases outlined here show how these new and evolving uses can successfully adopt enhanced security capabilities while improving performance and capability.

Scope of Report

This 5G Security Test Bed report's scope is to evaluate and verify 3GPP technical specifications for network slicing, by investigating the security features associated with 5G network infrastructure and the devices that can access a 5G standalone network.

Background

Network Slicing

Network slicing enables operators to provide fine-grained, customizable, and differentiated services to meet the diverse needs of a variety of customers and applications, such as in public safety, transportation, security, and many other contexts.

Often, network slices are discussed in the context of leading commercial applications, such as the three wireless network service types defined by 3GPP: eMBB (Enhanced Mobile Broadband), URLLC (Ultra-Reliable Low-Latency Communication), and mMTC (Massive Machine-Type Communication). In addition, network slices for specific uses, such as vehicle-to-infrastructure, or a specific company's industrial control system are also considered for application of the network slicing concept.

Network slices can be viewed as logical networks sharing a common physical infrastructure. The security for network slicing will be critical to certain segments of commercial customers. Regarding network slice security, because network slices leverage network function virtualization and a service-oriented architecture, the main focus for slice security has been to ensure isolation among different slices. Specifically, there are two aspects of isolation: resource provision/isolation and security isolation. Security isolation not only requires slice-specific access control and security measures, but also ensures that potential problems in one slice will not spill over to other slices.

Network Slicing Test Overview

This document presents the dry run test results tests based on novel capabilities and concerns with network slicing implementations in 5G standalone systems. The tests are based on those described in the high-level test case document, *Test Plan for 5G Security Test Bed (5G STB) Network Slicing Use Cases, V1.0,* dated August 9, 2022 [1].

The objectives of this first phase of network slicing tests focus on the security isolation among slices, both demonstrating that network addresses are not visible across slices and that extra layers of encryption do not overly impact the user experience. Three test cases were executed, incrementally increasing the level of security from basic slice isolation to addition of an encrypted tunnel for greater security on one slice to addition of an end-to-end virtual private network (VPN) over the secure slice.

Summary of Process and Findings

The three Phase 1 test cases are described in Table 1. The test cases then led to detailed test plans that include step-by-step procedures to follow for setting up and executing tests, including defining specific test points, means of generating and capturing traffic, etc. While the test results are provided in detail in a later section, Table 2 previews the high-level findings here.

TLP:CLEAR:5GSTB

Table 1: 5G STB Network Slicing Phase 1 High-Level Test Cases

Test Case ID	Test Case Title	Objective
TC-NetSlic-01	Network Slice Authentication and Segmentation Security	The test confirms proper authentication and network slice segmentation/isolation. It confirms proper dynamic authentication using 5G Authentication and Key Agreement (5G-AKA) based on user equipment (UE) subscription data in the core and the dynamic assignment to the correct slice for the UEs using dynamic signaling.
TC-NetSlic-02	Ipsec Transport Protection for Highly Secure Slices	The test confirms proper authentication and network slice segmentation and isolation when Ipsec encryption is used in the transport network.
TC-NetSlic-03	Adding Multiple Layers of VPN Encryption within a Network Slice for a Second and Third Layer of Confidentiality	The purpose of this test is to ensure that adding another two layers of encryption on top of the 5G network encryption does not have a negative impact on user application throughput. It confirms that the security overlay does not cause significant packet fragmentation that cannot be alleviated.

Table 2: 5G STB Network Slicing Phase 1 Test Case Result Summary

Test Case Name	Conclusion	Rationale
Network Slice Authentication and Segmentation Security	Success	No IP addresses in the address space of Slice 1 were reachable from Slice 2. No IP addresses in the address space of Slice 2 were reachable from Slice 1.
Ipsec Transport Protection for Highly Secure Slices	Success	The Ipsec tunnel is shown to be enabled. No IP addresses in the address space of Slice 1 were reachable from Slice 2. No IP addresses in the address space of Slice 2 were reachable from Slice 1.
Adding Multiple Layers of VPN Encryption within a Network Slice for a Second and Third Layer of Confidentiality	Success	 The Ipsec tunnel statistics indicated no packet drops. The Ipsec tunnel statistics indicated no packet fragmentations beyond a few at the initiation of the VPN tunnel. The DMC Health Check statistics showed insignificant packet drops during the test. The DMC Metric Viewer recorded no packet drops during the test.

5G Standalone Test Configuration

The configuration used for these tests comprises radio access network (RAN) equipment hosted at the University of Maryland (UMD) and an Ericsson 5G Core hosted at the MITRE Corporation. The Ericsson 5G Core is provided as a dual-mode core (DMC), PCC version 1.19, which provides both 4G/LTE and 5G functionality. The connection between the RAN at UMD and the DMC at MITRE goes over the internet and, for the scenarios considered here, is treated as an untrusted link.¹ Figure 1 shows the relevant components of the Test Bed, including available test points (TP). Not all of the test points shown were used for these tests, which are network slicing-focused.



Figure 1:5G STB Lab Component Block Diagram and Test Points

The routers shown at each location are Ericsson 6672 routers (referred to as R6672 or R6K for short). The switches shown are each Pluribus Freedom 9372-X switches. For the tests implemented here, the two switches are considered part of the "untrusted" backhaul link. The core is configured to support two network slices. The first slice, referred to as Slice 1 in this report, is considered the default eMBB, or Enhanced Mobile Broadband, network slice. The second slice, Slice 2, emulates a private network and includes the ability to form an IPsec tunnel to create a highly secure slice. The IPsec tunnel is configured with one endpoint at the baseband unit (BBU) and the other at the core-side R6672 router.

¹ In the actual implementation, there are additional security measures implemented, including an IPsec tunnel between the UMD and MITRE campus/corporate networks. For the purposes of these tests, this tunnel is considered part of the untrusted link and therefore, any encryption implemented for the tests is in addition to these measures.

On the server on the core side, there are two virtual web servers instantiated, one for each slice, and isolated from each other. The slice configuration and IPsec tunnel location are illustrated in

Figure 2 and

Figure 3.



Figure 2: Network Slice Configuration for Phase 1 Tests



RAN

TLP:CLEAR:5GSTB

Figure 3: Network Slice Configuration with IPsec Tunnel on Slice 2

Tests were run with band N41 for the new radio (NR) using a Sierra Wireless EM9190 card connected to a laptop by USB as a cellular modem, as well as a Qualcomm Mobile Test Platform (MTP) device. For the purposes here, we will refer to the combination of that laptop and the cellular modem as the user equipment, or UE.

For the tests described here, packets were captured on a subset of the identified test points in Figure 1: at the UE(s) (TP1), on the RAN-side R6K router (TP3), on the core-side R6K router (TP6), from the DMC between the the AMF and UDM (using CNOM PCC, TP7), and at the Slice 1 and Slice 2 DN Servers (TP8). These test points are identified with numbers as shown in the figure and described in more detail in Table 3.

Test Point	Description and Use
TP1-SW	Laptop connected to Sierra Wireless card; Wireshark captures packets originating at and destined to UE laptop;
TP1-MTP	Laptop connected to Qualcomm MTP
TP2	WaveJudge interface to capture raw data over-the-air
ТР3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC; and command-line interface for IPsec tunnel statistics
TP7	CNOM tool accessing DMC messages
TP8	Applications running on application server in MITRE facility

Table 3: Test Point Descriptions

Network Slicing

The network is configured with two slices, with corresponding IP address space and other associated parameters as shown in Table 4.

Table 4: Network Slice Test Parameters

		SIM			
Slice	IP pool	LABEL	IMSI	DNN	DN SERVERS
Slice 1	172.24.0.0/24	N1	310014791791001	dnn-embb-stb1.mitre.net	192.168.59.130/28
Slice 2	172.24.1.0/24	N21	310014791791021	dnn-embb-stb2.mitre.net	192.168.59.146/28

IPsec Configuration

3GPP TS 33.401 requires IPsec, when used, to support ESP and IKEv2 with certificate-based authentication [2]. The SEG is optional to use. The following requirements are from 33.401, section 12, Backhaul link user plane protection:

In order to protect the S1 and X2 user plane as required by clause 5.3.4, it is required to implement IPsec ESP according to RFC 4303 [3] as profiled by TS 33.210 [4], with confidentiality, integrity and replay protection.

Tunnel mode IPsec is mandatory to implement on the gNodeB for X2-U and S1-U.

On the X2-U and S1-U, transport mode IPsec is optional for implementation. NOTE 1: Transport mode can be used for reducing the protocol overhead added by IPsec.

On the core network side, a SEG may be used to terminate the IPsec tunnel.

For both S1 and X2 user plane, IKEv2 with certificate-based authentication shall be implemented. The certificates shall be implemented according to the profile described by TS 33.310 [5]. IKEv2 shall be implemented conforming to the IKEv2 profile described in TS 33.310 [5].

3GPP TS 33.501 retains these IPsec requirements for 5G SA and NSA, when IPsec is used [6]. The CSRIC VII Working Group (WG) 3 5G SA Report recommends IPsec on untrusted links to provide confidentiality and integrity protection, and management interfaces [7].

IPsec is implemented on Slice 2, with tunnel endpoints at the RAN and at the core-side R6K.

Detailed Test Procedure

For each test, the UEs were enclosed in the RF-shielded enclosure, with the door sealed. The UE used for Slice 1 was the Qualcomm Mobile Test Platform (MTP), which was connected remotely through a laptop. Controlling the MTP—turning its signal on/off (Airplane Mode) and running its applications—were done via the Vysor program. The UE for Slice 2 was the Sierra Wireless Modem which was connected and controlled by a laptop outside the shielded enclosure. The UEs were initially powered off for each test and the UE context was deleted from the core. At the start of each test, Wireshark and tcpdump were started at each relevant test point.

For network scanning tests, we used the Fing tool on the MTP UE and the Angry IP scanning tool on the Windows laptop connected to the Sierra Wireless device. A network mapper, Nmap, was used to scan ports from the two virtual servers.

The IPsec tunnel state was queried and its statistics were reset and queried by command line interface after logging into the core-side router.

For tests using the VPN, an OpenVPN server was installed on the server for Slice 2 and an OpenVPN application was installed on the laptop connected to the Sierra Wireless device. Prior to execution of these tests, it was determined that the largest maximum transmission unit (MTU) that would result in no fragmentation of packets with the OpenVPN tunnel, Slice 2 IPsec tunnel, and other tunnels implemented in the system was 1121. As a result, for the VPN tests, we used an MTU of 1100. At the start of each test with OpenVPN, we confirmed that the laptop was using the correct MTU over the cellular interface.

5G Security Test Bed Network Slicing Test Results

This section presents the detailed results for each of the network slicing test cases. Test Case 1 and Test Case 2 were run on November 14, 2022. Test Case 3 was executed on February 13, 2023.

Test Case 1, TC-NetSlic-01

The test confirms proper authentication and network slice segmentation/isolation. It confirms proper dynamic authentication using 5G-AKA via the AMF based on UE subscription data in the core and the dynamic assignment to the correct slice for the UEs using dynamic signaling. Slice 1 is the default Enhanced Mobile Broadband network slice with the Single Network Slice Selection Assistance Information (S-NSSAI) comprising the Slice/Service Type (SST) set to 1 and the Slice Differentiator (SD) set to 1. The second slice is set as SST=1 and SD=2.

There are two components to this first test case: (1) confirming the UEs register to the correct slices; and (2) testing that no ports associated with one slice are reachable from the other slice. For reference on packet capture figures, Table 5 lists the files whose data are shown in the figures along with a description of the contents. The network mapping tools Nmap, Fing, and Angry IP are used to confirm that the UE of Slice 1 cannot access any application servers within Slice 2 and vice versa.

Table 5: Test Case 1 Raw Data Files and Content Descriptions

File Name	Contents
slicingtest_01_11-14- 22_2020_UMD_r6k_v1.pcapng	Log captured on the RAN-side R6K router, TP3
B20221114.2050-0500-20221114.2055-0500- AMF.mtrdmcamf01.FIV11_ue_trace.810	UE trace captured at DMC, TP7

Used	Test Point	Description and Use
Х	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
Х	TP1-MTP	Laptop connected to Qualcomm MTP
	TP2	WaveJudge interface
x	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC; and command-line interface for IPsec tunnel statistics
Х	TP7	CNOM tool accessing DMC messages
Х	TP8	Applications running on application server in MITRE facility

Test points used:

MUMD02/	AVW>	st ip	sec																			
221114	-19:5	58:14	169.	254.2	2.2 2	2.0h	MSRBS	_NODE	_MODE	L_22	.Q2_	_566	.281	25.1	16_3	317	sto	opfi	le=/	/tmp/	21049	942
Ргоху	Adm	State	:==== :	ор.	Stat	===== e	===== MO	=====	=====	====	====	====	====	====		====		====	=			
======	=====							=====		====	====		====	====		====			=			
Total:	0 MC)s																				
Figure 4.	Confi	realize a	Deee	la a ativ	10																	

Figure 4: Confirming IPsec Inactive

This test is run with IPsec off. Figure 4 confirms that the IPsec tunnel is not activated for the test.

Figure 5 shows a screen capture of the Wireshark session reading the log captured on the RANside R6K router. Highlighted is the initial context setup request from the UE used for Slice 1 and shown in the lower left are the details indicating the UE is configured for Slice 1 with SST=1 and SD=1. Figure 6 shows the response from the core accepting the registration request and acknowledging SST=1 and SD=1. Figure 7 shows a message from the AMF to the SMF indicating also that the UE is assigned to Slice 1, with SST=1 and SD=1. Highlighted in the figure are the IMSI, the assigned IP address in the IP address space associated with Slice 1, and the data network name (DNN) assigned to the slice for Slice 1 (see Table 4).

TLP:CLEAR:5GSTB

<pre>slicingtest_01_11-14-22_2020_UMD_r6k_v1.p</pre>	capng				- 🗆 ×			
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help								
🛯 🔳 🖉 🙁 🚞 🛅 🖹 🏹 🔍 👄 🔿 🖺	E 🛧 👲 📃 📃 🔍	Q. Q. 🎹						
ngap					+			
lo. Time	Source	Destination	Protocol	Length Info	2) DownlinkNASTnancoc			
4730 2022-11-14 20:02:47.233698 4732 2022-11-14 20:02:47.233698 4732 2022-11-14 20:02:47.353554 4735 2022-11-14 20:02:47.36214 4736 2022-11-14 20:02:47.368545 4742 2022-11-14 20:02:47.682697 4744 2022-11-14 20:02:47.684697 4745 2022-11-14 20:02:47.684697	10.220.67.18 10.220.67.18 10.205.67.204 10.220.67.18 10.205.67.204 10.220.67.18 10.205.67.204 10.220.67.18 10.220.67.18 10.220.67.18	10.205.67.204 10.205.67.204 10.205.67.204 10.205.67.204 10.220.67.18 10.205.67.204 10.220.67.18 10.205.67.204 10.205.67.204	NGAP / NAS - 5GS NGAP / NAS - 5GS NGAP / NAS - 5GS NGAP / NAS - 5GS NGAP / NAS - 5GS NGAP NGAP NGAP NGAP	142 UplinkNASTransport, Ider 142 UplinkNASTransport, Ider 138 DownlinkNASTransport, Aut 130 SACK (Ack=3, Arwnd=32768 206 SACK (Ack=3, Arwnd=16384 178 InitialContextSetupReque 1026 UERadioCapabilityInfoInc 90 InitialContextSetupRespc 146 DownlinkNASTransport	(i), journalist and a spectral spectra			
<pre>4747 2022-11-14 20:02:47.696719</pre>	10.205.67.204 eld wedNSSAI (0) :: reject (0) SSAI: 1 item 0 LowedNSSAI-Item s-NSSAI sST: 01 sD: 000001 urityCapabilities eld curityCapabilities	(119)	NGAP/NAS-5GS	166 DownlinkNASTransport. Re 0000 0010 0020 0040 0050 0050 0050 0050 0050 005	eristration accept 66 0e 94 bc 80 4a b4 0c 00 a4 f5 f0 00 00 33 84 43 12 96 0c 96 0c 02 69 00 82 01 10 77 f2 00 08 00 6e 00 00 08 00 0a 00 55 00 05 c0 01 00 31 f0 ff 00 8d 00 00 00 00 50 1c 00 0e 00 00 00 00 00 aa d2 f9 ce 89 aa e8 e8 e4 48 f7 fc 62 b1 f2 0a 20 13 00 41 00 13 00			

Figure 5: Wireshark capture showing UE1 allowed NSSAI

igap				• • • • • • • • • • • • • • • • • • •			
Time	Source	Destination	Protocol	Length Info			
4742 2022-11-14 20:02:47.632575	10.205.67.204	10.220.67.18	NGAP	178 InitialContextSetupRequest			
4744 2022-11-14 20:02:47.684697	10.220.67.18	10.205.67.204	NGAP	1026 UERadioCapabilityInfoIndication			
4745 2022-11-14 20:02:47.684697	10.220.67.18	10.205.67.204	NGAP	90 InitialContextSetupResponse			
4747 2022-11-14 20:02:47.696719	10.205.67.204	10.220.67.18	NGAP/NAS-5GS	166 DownlinkNASTransport, Registration accept			
4748 2022-11-14 20:02:47.733852	10.220.67.18	10.205.67.204	NGAP/NAS-5GS	142 SACK (Ack=5, Arwnd=16384) , UplinkNASTransport			
4749 2022-11-14 20:02:47.745042	10.205.67.204	10.220.67.18	NGAP/NAS-5GS	138 SACK (Ack=7, Arwnd=32768) , DownlinkNASTranspc			
4757 2022-11-14 20:02:47.923571	10.220.67.18	10.205.67.204	NGAP/NAS-5GS	214 UplinkNASTransport, UL NAS transport, PDU sess			
4759 2022-11-14 20:02:48.148696	10.205.67.204	10.220.67.18	NGAP/NAS-5GS	266 PDUSessionResourceSetupRequest, DL NAS transpo			
4765 2022-11-14 20:02:48.295313	10.220.67.18	10.205.67.204	NGAP	110 PDUSessionResourceSetupResponse			
4896 2022-11-14 20:02:58.340558	10.220.67.18	10.205.67.204	NGAP	102 UEContextReleaseRequest			
~	NSSAI - Allowed N	SSAI					
~	NSSAI - Allowed N Element ID: 0x	ISSAI 15		0010 00 98 f5 f9 00 00 33 8			
v	NSSAI - Allowed N Element ID: 0x Length: 5	ISSAI 15		0010 00 98 f5 f9 00 00 33 g 0020 43 12 96 0c 96 0c 02 f			
~	NSSAI - Allowed N Element ID: 0x: Length: 5 ~ S-NSSAI 1	ISSAI 15		0010 00 09 94 00 00 33 0 0020 43 12 96 0c 96 0c 02 0 0030 00 75 01 10 77 73 00 0			
v	NSSAI - Allowed N Element ID: 0x: Length: 5 V S-NSSAI 1 Length: 4	ISSAI 15		0000 0000 94 0000 34 04 04 0000 33 0000 33 0000 33 0000 34 04			
v	NSSAI - Allowed N Element ID: 0x. Length: 5 V S-NSSAI 1 Length: 4 Slice/service	ISSAI 15 ce type (SST): eMBA	3 (1)	0000 00 00 94 00 00 34 04 04 06 03 34 04 06 03 34 04 06 03 34 04 04 03 34 04 06 03 34 04 06 03 34 04 06 03 34 04 06 03 00 07 01 10 77 73 06 06 04 06 06 04 06 06 06 05 05 00 05 05 00 06 04 06 0			
v	NSSAI - Allowed N Element ID: 0x Length: 5 V S-NSSAI 1 Length: 4 Slice/servic Slice differ	ISSAI 15 ce type (SST): eMBH rentiator (SD): 1	3 (1)	$\begin{array}{cccccccccccccccccccccccccccccccccccc$			

Figure 6: Wireshark capture of Downlink NAS Registration accept indicating NSSAI for UE1



Figure 7: UE trace showing AMF-SMF message indicating UE 1 assigned to Slice 1



Figure 8: UE trace showing AMF-SMF message indicating UE 2 assigned to Slice 2

Figure 8 shows a message from the AMF to the SMF indicating also that the second UE is assigned to Slice 2, with SST=1 and SD=2. In the information displayed in row 6, we can see the IMSI for the UE for Slice 2 (see Table 4).

Figure 9 through Figure 14 show the results of scanning the network from each UE and each virtual server. Figure 9 corresponds to the UE on Slice 1. On the left side of the figure are the results for scanning the IP address range of the Slice 1 gateway and DNN (192.168.59.130/28). We see successful pings to the DNN gateway (192.168.59.129) and the web server (192.168.59.130) and no other addresses in use. On the right side of the figure are the results for scanning the IP address range of the Slice 2 gateway and DNN (192.168.59.146/28). We see no successful pings to any addresses in that IP address space. Figure 10 and Figure 11 show the results of the Nmap scan from the virtual server on Slice 1 for the UEs on Slices 1 and 2, respectively. Figure 10 shows that Nmap on Slice 1, scanning the Slice 1 IP pool (172.14.0.0/24), could see an active device on Slice 1 with the IP address shown in Figure 7 as that assigned to the UE on Slice 1, 172.24.0.3. Figure 11 shows that Nmap on Slice 1 did not find an active UE on Slice 2.

Taro for_arm64 🔹 🛤 🗛 🕄 🌩 8:05 🕾 🌑 🔜	e	_ □ ×) 5G ∡í 🖸
← Subnet scanner		:
Manual configuration	*	SCAN
Scan subnet		
First 192.168.59.129		
Last 192.168.59.143		
Threads count - 15		
192.168.59.129		
192.168.59.129		
Ping: success		
Refused: 80		
192.168.59.130		
192.168.59.130		
Ping: success		
Opened ports: 80		
Scan statistics:		
Scanned 15, found online 2		

The scan on the MTP identified open ports only for hosts on the IP pool assigned for Slice 1

5 0 ⊖ 5G ∡i 🖡 Subnet scanner nual configuration SCAN an subnet st 192.168.59.145 st 192.168.59.158 reads count - 14 an statistics: anned 14, found online 0

ports for hosts on Slice 2.

Figure 9: Network scan from the UE on Slice 1 using Fing

Network scan did not find any IP and open

TLP:CLEAR:5GSTB



Figure 11: Network scan from the virtual server on Slice 1 for UE addresses assigned to Slice 2 using Nmap

Similar to the scan for the UE on Slice 1,

[dndiki@fgp-dmc-dnstb1 ~]\$

Figure 12 corresponds to the UE on Slice 2. On the left side of the figure are the results for scanning the IP address range of the Slice 2 gateway (192.168.59.145) and DNN (192.168.59.146/28). We see successful pings to the DNN gateway (192.168.59.145) and the web server (192.168.59.146) and no other addresses in use. On the right side of the figure are the results for scanning the IP address range of the Slice 1 gateway (192.168.59.129) and DNN (192.168.59.130/28). We see no successful pings to any addresses in that IP address space. Figure 13 and Figure 14 show the results of the Nmap scan from the virtual server on Slice 2 for the UEs on Slices 2 and 1, respectively. Figure 13 shows that Nmap on Slice 2, scanning the Slice 2 IP pool (172.168.1.2/24), produced one active host/open port on Slice 2 and Figure 14 shows that Nmap on Slice 2 produced no live hosts or open ports on Slice 1 (from the IP pool 172.14.0.0/24).

🏈 IP Range - Angry IP Scanner								
Scan Go t	o Comr	nands Fa	avorites Tools Help)				
IP Range: 192.168.59.145 to 192.168.59.154								
Hostname:	ISRLTAVW1322 IPt Netmask ~							
IP		Ping	Hostname	Ports [3+]				
🔵 192.168.5	59.145	0 ms	[n/a]	[n/a]				
€ 192.168.5	59.146	0 ms	[n/a]	80				
0192.168.5	59.147	[n/a]	[n/s]	[n/s]				
0192.168.5	59.148	[n/a]	[n/s]	[n/s]				
0192.168.5	59.149	[n/a]	[n/s]	[n/s]				
0192.168.5	59.150	[n/a]	[n/s]	[n/s]				
0192.168.5	59.151	[n/a]	[n/s]	[n/s]				
0192.168.5	59.152	[n/a]	[n/s]	[n/s]				
0192.168.5	59.153	[n/a]	[n/s]	[n/s]				
0192.168.5	59.154	[n/a]	[n/s]	[n/s]				

🎲 IP Range - Angry IP Scanner

Scan Go to Comr	mands F	avorites Tools Help	c
IP Range: 192.168	.59.129	to 192.168.59.1	42 I
Hostname: ISRLTAV	W1322	IP† Netmask	~
IP	Ping	Hostname	Ports [3+]
0192.168.59.129	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.130	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.131	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.132	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.133	[n/a]	[n/s]	[n/s]
9192.168.59.134	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.135	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.136	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.137	[n/a]	[n/s]	[n/s]
🔵 192.168.59.138	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.139	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.140	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.141	[n/a]	[n/s]	[n/s]
\varTheta 192.168.59.142	[n/a]	[n/s]	[n/s]

Figure 12: Network scan from the UE on Slice 2 using Angry IP Scanner

Starting Nmap 6.40 (http://nmap.org) at 2022-11-14 21:14 EST Nmap scan report for 172.24.1.2 Host is up (0.055s latency). Nmap done: 256 IP addresses (1 host up) scanned in 10.97 seconds [dndiki@fgp-dmc-dnstb2 ~]\$

Figure 13: Network scan from the virtual server on Slice 2 for UE addresses assigned to Slice 2 using Nmap

Starting Nmap 6.40 (http://nmap.org) at 2022-11-14 21:34 EST Nmap done: 256 IP addresses (0 hosts up) scanned in 2.41 seconds [dndiki@fgp-dmc-dnstb2 ~]\$

Figure 14: Network scan from the virtual server on Slice 2 for UE addresses assigned to Slice 1 using Nmap

Table 6 summarizes the hosts that were detected on each slice.

Table 6: Test Case 1 Network Scan Results

Scan source (slice, UE/Server)	Hosts/Ports found	Allowed?
Slice 1 UE	192.168.59.129, 192.168.59.130	Y
Slice 1 DNN Server	174.24.0.3	Y
Slice 2 UE	192.168.59.145, 192.168.59.146	Y
Slice 2 DNN Server	172.24.1.2	Y

Test Result

Success: Packet captures confirm each UE is associated with the correct slice. Use of network scanning tools on both servers and UEs show that only allowed ports are visible on each slice.

Condition	Status
UE on Slice 1 connected to SST 1, SD 1	Success
UE on Slice 2 connected to SST 1, SD 2	Success
Ports from Slice 2 hidden from Slice 1	Success
Ports from Slice 1 hidden from Slice 2	Success
Overall Test Case 1	Success

Test Case 2, TC-NetSlic-02

Utilizing the same configuration setup as Test Case 1, this test case adds transport IPsec protection for Slice 2 from the RAN to the Router/Security Gateway 6672 as a high security slice across the backhaul. In commercial networks, slice orchestration and IPsec encryption are

performed at the same time. In the transport network used for this test case, the IPsec encryption was configured after slice orchestration. Here, we are using a static configuration of the network elements. IPsec in the backhaul is then stitched into the network slice configuration by the same tools. The Test Case 1 procedure is rerun to confirm proper authentication and network slice segmentation and isolation.

	Test points us	ed:
Used	Test Point	Description and Use
х	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
Х	TP1-MTP	Laptop connected to Qualcomm MTP
	TP2	WaveJudge interface
х	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
х	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC; and command-line interface for IPsec tunnel statistics
Х	TP7	CNOM tool accessing DMC messages
Х	TP8	Applications running on application server in MITRE facility

This test activates the IPsec tunnel on Slice 2. Figure 15 confirms that IPsec is enabled on the gNodeB. Figure 16 shows the IKE and IPsec configuration settings. And Figure 17 shows the IPsec statistics at the beginning of the test.

MUMD02	AVW>	st ip	sec			
221114	-18:0	97:33	169.	254.2	.2 22.0h	MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317
Ргоху	Adm	State	2	Ор.	State	мо
14290				1 (E	NABLED)	Transport=1,Router=NRCUCP,IpsecTunnel=1
Total:	1 MC	======)s			=======	

Figure 15: IPsec state for Test Case 2

[dmc_ran]R6672-IP-1-1#show configuration ike Building configurationBuilding configurationCurrent configuration:!context dmc_ran ike2 policy ike_policy_UMD description ike_policy_UMD connection-type responder-only authentication rsa-signature identity local dn dpd interval 60 lifetime seconds 86400 identity remote dn "*" seq 1 proposal ike_proposal_UMD !!!** End Context ** ike2 proposal ike_proposal_UMD description ike_proposal_UMD authentication algorithm hmac-md5-96 encryption algorithm aes-128-cbc pseudo-random-function hmac-sha1 dh-group 14 !	R6K configuration dump:	[dmc_ran]R6672-IP-1-1#show configuration ipsec
Building configurationCurrent configurationCurrent configuration:!context dmc_ranipsec access-list IPSec-ACL-UMDike2 policy ike_policy_UMDdescription IPSec-ACL-UMD-CPdescription ike_policy_UMDdescription IPSec-ACL-UMDconnection-type responder-onlyauthentication rsa-signatureidentity local dnipsec proposal ipsec_proposal_UMDdpd interval 60lifetime seconds 86400lifetime seconds 86400esp encryption aes-128-cbcidentity remote dn "*"!seq 1 proposal ike_proposal_UMD!! ** End Context **!ike2 proposal ike_proposal_UMDlifetime seconds 86400secription ike_proposal_UMDauthentication algorithm hmac-md5-96encryption algorithm aes-128-cbcendpseudo-random-function hmac-sha1!!!	[dmc_ran]R6672-IP-1-1#show configuration ike	Building configuration
Current configuration:!!context dmc_ranike2 policy ike_policy_UMDipsec access-list IPSec-ACL-UMDdescription ike_policy_UMDdescription IPSec-ACL-UMD-CPconnection-type responder-only!authentication rsa-signature!identity local dnipsec proposal ipsec_proposal_UMDdpd interval 60escription ipsec-proposal-UMDlifetime seconds 86400esp encryption aes-128-cbcidentity remote dn "*"esp authentication ipsec-policy_UMD!!!* End Context **!ike2 proposal ike_proposal_UMD!!ipsec policy ipsec_policy_UMDdescription ike_proposal_UMDauthentication algorithm hmac-md5-96encryption algorithm aes-128-cbc!pseudo-random-function hmac-sha1!!!	Building configuration	Current configuration:
!context dmc_ranike2 policy ike_policy_UMDipsec access-list IPSec-ACL-UMDdescription ike_policy_UMDdescription IPSec-ACL-UMD-CPconnection-type responder-only1authentication rsa-signature1identity local dnipsec proposal ipsec_proposal_UMDdestription ike_polosal ike_proposal_UMDipsec proposal ipsec_polocy_UMDidentity remote dn "*"esp encryption aes-128-cbcseq 1 proposal ike_proposal_UMDipsec policy ipsec_policy_UMDike2 proposal ike_proposal_UMDipsec policy ipsec_policy_UMDike2 proposal ike_proposal_UMDanti-replay-window 128ike2 proposal ike_proposal_UMDseq 1 proposal ipsec_proposal_UMDauthentication algorithm hmac-md5-96iencryption algorithm aes-128-cbcendpseudo-random-function hmac-sha1idh-group 14i	Current configuration:	!
!	Current configuration Current configuration: context dmc_ran ike2 policy ike_policy_UMD description ike_policy_UMD connection-type responder-only authentication rsa-signature identity local dn dpd interval 60 lifetime seconds 86400 identity remote dn "*" seq 1 proposal ike_proposal_UMD ** End Context ** ike2 proposal ike_proposal_UMD description ike_proposal_UMD authentication algorithm hmac-md5-96 encryption algorithm aes-128-cbc pseudo-random-function hmac-sha1 dh-group 14	Current configuration: ! context dmc_ran ipsec access-list IPSec-ACL-UMD description IPSec-ACL-UMD-CP seq 1 10.205.67.192/26 10.220.67.19/32 ! ! ** End Context ** ! ipsec proposal ipsec_proposal_UMD description ipsec-proposal-UMD esp encryption aes-128-cbc esp authentication hmac-sha1-96 ! ipsec policy ipsec_policy_UMD description ipsec-policy-UMD anti-replay-window 128 lifetime seconds 86400 seq 1 proposal ipsec_proposal_UMD ! end
end	end	

Figure 16: IKE and IPsec configuration parameters

```
local]R6672-IP-1-1#show ipsec statistics global
PSec Global Packet Processing Stats:
Packets Received for Inbound Processing : 1621318
Packets Processed by Inbound Processing : 1621318
Packets Received for Outbound Processing : 7920530
Packets Processed by Outbound Processing : 7920530
Inbound UDP Encapsulated Packets : 0
Invalid IP Header Length : 0
Packet Length is less than Minimum ESP Header Length : 0
Dropping the Packet, No Inbound SA Found : 0
Unable to Allocate memory for Packet Queue Node : 0
Dropping the Packet, Late Packets Received : 0
local1R6672-IP-1-1#
```

Figure 17: IPsec statistics at beginning of Test Case 2

Table 7 lists the parameters for the two UEs used in this test, including the assigned IP addresses. Figure 18 shows the view of the traffic at the RAN-side R6K router (TP3) where Slice 2 traffic is inside the IPsec tunnel but Slice 1 traffic is not. We can see ping traffic from the Slice 1 UE (IP address 172.24.0.2) to 192.168.59.130, the Slice 1 web server, but all other traffic is encrypted as ESP traffic, showing source and destination addresses as the endpoints of the IPsec tunnel.

UE	IMSI	SST	SD	IP address
MTP	310014791791001	1	1	172.24.0.2
Sierra Wireless	310014791791021	1	2	172.24.1.2

Table 7: UE parameters for Test Case NetSlic-02

💰 *SLOT 2 Port 3	2
------------------	---

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
1	6		1 🖪	8 6	Q (= =	a 🖘 🚡	A = =	⊕ ⊖ (a 🎫	

📕 ip.add	r == 172.24.0.2 ip.addr:	==172.24.1.2 esp			
No.	Time	Source	Destination	Protocol I	ength Info
68	6 11:17:22.286429	10.220.67.18	10.205.67.200	ESP	182 ESP (SPI=0xc6f461e2)
68	8 11:17:22.327151	192.168.59.130	172.24.0.2	GTP <icmp></icmp>	142 Echo (ping) reply id=0x0028, seq=1/256, ttl=61
68	9 11:17:22.327151	192.168.59.130	172.24.0.2	GTP <icmp></icmp>	142 Echo (ping) reply id=0x0028, seq=1/256, ttl=61
69	0 11:17:22.330222	10.205.67.200	10.220.67.18	ESP	134 ESP (SPI=0x068d9134)
69	7 11:17:23.394621	192.168.59.130	172.24.0.2	GTP <icmp></icmp>	142 Echo (ping) reply id=0x0029, seq=1/256, ttl=61
70	6 11:17:24.110939	10.220.67.18	10.205.67.200	ESP	198 ESP (SPI=0xc6f461e2)
70	7 11:17:24.114518	10.205.67.200	10.220.67.18	ESP	198 ESP (SPI=0x068d9134)
70	9 11:17:24.469504	192.168.59.130	172.24.0.2	GTP <icmp></icmp>	142 Echo (ping) reply id=0x002a, seq=1/256, ttl=61
72	4 11:17:26.311441	10.220.67.18	10.205.67.200	ESP	198 ESP (SPI=0xc6f461e2)
72	5 11:17:26.314740	10.205.67.200	10.220.67.18	ESP	198 ESP (SPI=0x068d9134)
74	2 11:17:28.510869	10.220.67.18	10.205.67.200	ESP	198 ESP (SPI=0xc6f461e2)
74	3 11:17:28.513940	10.205.67.200	10.220.67.18	ESP	198 ESP (SPI=0x068d9134)
76	4 11:17:30.711423	10.220.67.18	10.205.67.200	ESP	198 ESP (SPI=0xc6f461e2)
76	5 11:17:30.714974	10.205.67.200	10.220.67.18	ESP	198 ESP (SPI=0x068d9134)
78	1 11:17:32.910836	10.220.67.18	10.205.67.200	ESP	198 ESP (SPI=0xc6f461e2)
78	2 11:17:32.914207	10.205.67.200	10.220.67.18	ESP	198 ESP (SPI=0x068d9134)
78	9 11:17:34.536002	10.220.67.18	10.205.67.200	ESP	166 ESP (SPI=0xc6f461e2)
79	0 11:17:34.541302	10.205.67.200	10.220.67.18	ESP	166 ESP (SPI=0x068d9134)
79	2 11:17:34.582834	10.220.67.18	10.205.67.200	ESP	134 ESP (SPI=0xc6f461e2)
> Frame	e 688: 142 bytes on	wire (1136 bits), 1	142 bytes captured	(1136 bits) on interface	\Device\NPF_{20F7051C-CF57-4F99-BF5E-8518BF86FD9C}, 0000 66 0

> Frame 688: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{20F7051C-CF57-4F99-BF5E-8518BF86FD9C}, | 0000 66 0e 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0010 00 80 0000 43 18 0000 60

Figure 18: Test Case NetSlic-02 traffic at RAN-side R6K router (TP3)

The next part of the test confirms isolation between the slices. Similar to Test Case NetSlic-01, Figure 19 through Figure 22 show the results of scanning the network from each UE and each virtual server. Figure 19 corresponds to the UE on Slice 1. On the left side of the figure are the results for scanning the IP address range of the Slice 1 gateway and DNN (192.168.59.130/28). We see a successful ping to the web server (192.168.59.130) and no other addresses in use. On the right side of the figure are the results for scanning the IP address range of Slice 2 gateway and DNN (192.168.59.146/28). We see no successful pings to any addresses in that IP address space. Figure 20 and Figure 21 show the results of the Nmap scan from the virtual server on Slice 1 for the UEs on Slices 1 and 2, respectively. Figure 20 shows that the Nmap on Slice 1, scanning the Slice 1 IP pool (172.14.0.0/24), could see an active device on Slice 1 (corresponding to the UE IP address, 172.24.0.2) and Figure 21 shows that the Nmap on Slice 1 did not find an active UE on Slice 2.

TLP:CLEAR:5GSTB



Figure 19: Network scan from the UE on Slice 1 for Test Case 2

[dndiki@fgp-dmc-dnstb1 ~]\$ nmap -sn 172.24.0.0/24 Starting Nmap 6.40 (http://nmap.org) at 2022-11-14 19:36 EST Nmap scan report for 172.24.0.2 Host is up (0.064s latency). Nmap done: 256 IP addresses (1 host up) scanned in 10.32 seconds [dndiki@fgp-dmc-dnstb1 ~]\$ ■

Figure 20: Network scan from the virtual server on Slice 1 for UE addresses on Slice 1 for Test Case 2

[dndiki@fgp-dmc-dnstb1 ~]\$ nmap -sn 172.24.1.0/24

Starting Nmap 6.40 (http://nmap.org) at 2022-11-14 19:39 EST Nmap done: 256 IP addresses (0 hosts up) scanned in 2.51 seconds [dndiki@fgp-dmc-dnstb1 ~]\$

Figure 21: Network scan from the virtual server on Slice 1 for UE addresses on Slice 2 for Test Case 2

Figure 22 corresponds to the UE on Slice 2. On the left side of the figure are the results for scanning the IP address range of the Slice 2 gateway (192.168.59.145) and DNN (192.168.59.146/28). We see successful pings to the DNN gateway (192.168.59.145) and the web server (192.168.59.146) and no other addresses in use. On the right side of the figure are the results for scanning the IP address range of Slice 1 gateway (192.168.59.129) and DNN (192.168.59.130/28). We see no successful pings to any addresses in that IP address space.

🎸 IP Range - Angr	y IP Scan	ner		IP Range - Ang	ry IP Scan	iner	
, J J	-			Scan Go to Com	mands	Favorites Tools	Help
Scan Go to Com	mands F	avorites Tools Hel	р	IP Range: 192.16	8.59.129	to 192.168.5	59.142 IF
IP Range: 192.168	3.59.145	to 192.168.59.1	154 IF	Hostname: ISRLTA	VW1322	IPt Netma	ask 🗸
Hostname: ISRITAV	/W1322	IPt Netmask	~	IP	Ping	Hostname	Ports [3+]
				🔵 192.168.59.129	[n/a]	[n/s]	[n/s]
IP	Ping	Hostname	Ports [3+]	\varTheta 192.168.59.130	[n/a]	[n/s]	[n/s]
9 192 168 59 145	0 ms	[n/a]	[n/a]	🔵 192.168.59.131	[n/a]	[n/s]	[n/s]
0 102 100 50 145	0	[[]]]	[[], 0]	🔵 192.168.59.132	[n/a]	[n/s]	[n/s]
♥ 192.168.59.146	0 ms	[n/a]	80	\varTheta 192.168.59.133	[n/a]	[n/s]	[n/s]
0192.168.59.147	[n/a]	[n/s]	[n/s]	\varTheta 192.168.59.134	[n/a]	[n/s]	[n/s]
0192.168.59.148	[n/a]	[n/s]	[n/s]	0192.168.59.135	[n/a]	[n/s]	[n/s]
	[n/a]	[n/c]	[n/c]	🔵 192.168.59.136	[n/a]	[n/s]	[n/s]
0 192.100.39.149	[1]/a]		[1/3]	0192.168.59.137	[n/a]	[n/s]	[n/s]
9192.168.59.150	[n/a]	[n/s]	[n/s]	0192.168.59.138	[n/a]	[n/s]	[n/s]
🔵 192.168.59.151	[n/a]	[n/s]	[n/s]	0192.168.59.139	[n/a]	[n/s]	[n/s]
192.168.59.152	[n/a]	[n/s]	[n/s]	0192.168.59.140	[n/a]	[n/s]	[n/s]
	[n/a]	[n/c]	[n/c]	0192.168.59.141	[n/a]	[n/s]	[n/s]
0 192.100.39.133	[1]/a]	[1/5]	[1/3]	0192.168.59.142	[n/a]	[n/s]	[n/s]
9192.168.59.154	[n/a]	[n/s]	[n/s]				
				1			

Figure 22: Network scan from the UE on Slice 2 using Angry IP Scanner for Test Case 2

Table 8: Test Case 2 Network Scan Results

Scan source (slice, UE/Server)	Hosts/Ports found	Allowed?
Slice 1 UE	192.168.59.129, 192.168.59.130	Y
Slice 1 DNN Server	174.24.0.2	γ
Slice 2 UE	192.168.59.145, 192.168.59.146	Y
Slice 2 DNN Server	172.24.1.2	Y

Test Result

Success: The IPsec tunnel is shown to be enabled. Packet captures confirm each UE is associated with the correct slice and that traffic is encrypted over the transport link. Use of network scanning tools on both servers and UEs show that only allowed ports are visible on each slice.

Condition	Status
Ports from Slice 2 hidden from Slice 1	Success
Ports from Slice 1 hidden from Slice 2	Success
IPsec up with no errors or warnings	Success
IPsec encrypts all Slice 2 traffic	Success

Overall Test Case 2	Success
Test Case 3, TC-NetSlic-03	

This test case builds on Test Case 2 and demonstrates the efficacy of end-to-end encryption over the 5G standalone network. Specifically, this test ensures that overlaying another two layers of encryption on top of the 5G network encryption does not have a significant impact on user application throughput and cause packet fragmentation that cannot be alleviated. MTU settings issues on the various network paths need to be configured correctly, for example.

Using a Remote Access VPN solution from OpenVPN, the VPN client was installed on the UE on Slice 2 and the headend VPN gateway was installed on the virtual server off the slice UPF for Slice 2. As a result, for Slice 2 there are three layers of encryption: Transport layer security (TLS) for the application, the VPN encryption, and the network layer encryption done by 5G over the air (both encryption and integrity) and IPsec for the air interface and transport network respectively. The UE for Slice 2 connects over the slice to the headend gateway and then accesses the application servers. A large file is downloaded, as well as a sequence of images, in order to stress the file size and download speed.

	reerpenne ae	
Used	Test Point	Description and Use
Х	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
х	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC; and command-line interface for IPsec tunnel statistics
Х	TP7	CNOM tool accessing DMC messages
Х	TP8	Applications running on application server in MITRE facility

Test points used:

This test comprises both observing UE registration to Slice 2 and collecting packet fragmentation and drop statistics for layered encryption over the VPN and IPsec backhaul tunnels. All parts use Slice 2 with IPsec security applied across the 5G SA transport channel.

Figure 23 shows the status of the IPsec tunnel at the core-side R6K router, confirming the tunnel is up. At the start of the test, prior to restarting the UE and connecting the VPN, the IPsec statistics were cleared on the core-side router. Figure 24 and Figure 25 show the IPsec statistics following resetting counters.

MUMD02	AVW> st ipsec		
230213	-16:15:25 169.	254.2.2 22.0h 1	MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317
====== Ргоху	Adm State	Op. State	MO
14293		1 (ENABLED)	Transport=1,Router=NRCUCP,IpsecTunnel=1
Total:	1 MOs		

Figure 23: Test Case 3 IPsec Tunnel Status

```
[local]R6672-IP-1-1#sh ipsec statistics global
IPSec Global Packet Processing Stats:
# Packets Received for Inbound Processing : 33
# Packets Processed by Inbound Processing : 33
# Packets Received for Outbound Processing : 33
# Packets Processed by Outbound Processing : 33
# Inbound UDP Encapsulated Packets : 0
# Invalid IP Header Length : 0
# Packet Length is less than Minimum ESP Header Length : 0
# Dropping the Packet, No Inbound SA Found : 0
# Unable to Allocate memory for Packet Queue Node : 0
# Dropping the Packet, Late Packets Received : 0
```

Figure 24: Test Case 3 Initial IPsec Global Statistics

[local]R6672-IP-1-1#sh tunnel ipsec	name	іp	sec_tunnel_UMD statistics	detail	
Remote IP : 10.220.67.18 Local IP	: 1	0.	205.67.200		
# IN Packets Received:	52	#	IN Bytes Received:		9152
# OUT Packets Received:	52	#	OUT Bytes Received:		10608
<pre># Packets Fragmented Tx:</pre>	0	#	Bytes Fragmented Tx:		Θ
Errors					
Incoming packets dropped due to the	follo	wi	.ng reasons:		
<pre># Authentication errors:</pre>	0	#	Decryption errors:		Θ
# Anti-replay check failure:	0	#	No matching SA:		Θ
IPsec acl name #: IPSec-ACL-UMD					
SA #: Inbound ESP					
5PI : 0xc189a0c7					
# Packets sent:	0	#	Packets received:		52
# Bytes sent:	0	#	Bytes received:		9152
<pre># Packets Fragmented Rx:</pre>	0	#	Packets Fragmented Tx:		Θ
# Bytes Fragmented Rx:	0	#	Bytes Fragmented Tx:		Θ
Errors					
Incoming packets dropped due to the	follo	wi	.ng reasons:		
# Authentication errors:	0	#	Decryption errors:		Θ
# Anti-replay check failure:	0				
IPsec acl name #: IPSec-ACL-UMD					
SA #: Outbound ESP					
SPI : 0x586ab14f					
# Packets sent:	52	#	Packets received:		Θ
# Bytes sent:	10608	#	Bytes received:		Θ
<pre># Packets Fragmented Rx:</pre>	0	#	Packets Fragmented Tx:		Θ
# Bytes Fragmented Rx:	Θ	#	Bytes Fragmented Tx:		Θ

Figure 25: Test Case 3 Initial IPsec Statistics Details

Figure 26 shows the MTU for the UE, Cellular 52, interface set to 1100, which was determined as approximately the highest value that does not cause packet fragmentations when the VPN is enabled.

C:\User	s\sysadmin≻netsh	interface i	pv4 show su	binterface
MTU	MediaSenseState	Bytes In	Bytes Out	Interface
4294967	295	1	0 20607	'316 Loopback Pseudo-Interface 1
1100	5	0	0	OpenVPN Wintun
1500	2	213608	303766	Wi-Fi
1100	5	0	0	OpenVPN TAP-Windows6
1500	2	276806306	5900020	Local Area Connection
1500	5	0	0	Bluetooth Network Connection
1500	5	0	0	Local Area Connection* 13
1500	1	0	75336	vEthernet (Default Switch)
1100	1	0	10766	Cellular 52

Figure 26: Test Case 3 UE MTU Setting

Also recorded were the initial packet drop rates (in packets per million, ppm) for sections "Access Throughput KPIs" and "Core Throughput KPIs" from the CNOM Health Check View as shown in Figure 27. Note there is a baseline non-zero packet drop rate for each of these statistic sets. A screenshot of ip_received_packet drop statistics from the CNOM Metric Viewer is shown in Figure 28.

TLP:CLEAR:5GSTB

Access_Thro	ughput_K	Pls_20232	13-161129	9-588									
Now	1h ago	3h ago	6h ago	12h ago	24h ago	Name	Core_Throu	ghput_Ki	'ls_202321	L3-161136	-136	24b ago	Namo
-	()	0 () () (GTP T-PDU in (bps)	NOW		Sil ago	on ago		2411 ago	GTD T DDU in (boc)
-	()	0 () () (GTP T-PDU out (bps)							GTP T-PDU out (bps)
-	()	0 () () (IP in (bps)) () () (0	IP in (bps)
-	()	0 () () (IP out (bps)	() () () () (0	IP out (bps)
-	()	0 () () (GTP T-PDU in (pps)	() () () () (0	GTP T-PDU in (pps)
-	()	0 () () (GTP T-PDU out (pps)	() () () () (0	GTP T-PDU out (pps)
-	()	0 () () (IP in (pps)	0) () () () (0	IP in (pps)
-	()	0 () () (IP out (pps)	() () () () (0	IP out (pps)
6.7	1 6.71	6.71	6.71	6.71	6.71	Packet Drop Ratio (ppr	106.66	106.66	106.66	106.66	106.66	106.66	Packet Drop Ratio (p

Figure 27: Test Case 3 Initial Packet Drop Rates from Access Throughput KPIs and Core Throughput KPIs

(up-c	Irop-counters			
	Metri	25			
	Filt	er: Metric			Refresh table
	k	Metric 🗘	Absolute 💠	Delta (2 min) 💠	Rate (2 min) 💠
	\checkmark	pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="no_host"}	4333	0	0.00
	\checkmark	pc_up_udp_received_packets_total{action="drop",reason="no_socket"}	4333	0	0.00
	\checkmark	pc_up_gtp_received_packets_total{action="drop",reason="local_teid_lookup_fail"}	4	0	0.00
	\checkmark	pc_up_pktio_dropped_packets_total{reason="packet_buffer_allocation_failed"}	0	0	0.00
		pc_up_pktio_dropped_packets_total{reason="packet_buffer_too_small"}	0	0	0.00
		pc_up_pktio_dropped_packets_total{reason="route_lookup_failed"}	0	0	0.00
		pc_up_pktio_dropped_packets_total{reason="pktsock_set_ipcontext"}	0	0	0.00
		pc_up_pktio_dropped_packets_total{reason="pktsock_set_fwd_meta"}	0	0	0.00
		pc_up_pktio_dropped_packets_total{reason="pktsock_set_papid"}	0	0	0.00

Figure 28: Test Case 3 Initial ip_received_packet drop

Upon restarting the UE, the OpenVPN tunnel connects as shown in Figure 29.

OpenVPN Connect	- ×	slicing_test	03_01-30-23_1440pm	- Word		Sign in	图 —
Profiles	٩	Capturing from Cellular ile Edit View Go Cap	52 iture Analyze Statis	tics Telephony Wi	eless Tools H	Help	
	1		ି 🍳 🔶 🛎	¥ 📃 📃 Q	ର୍ ର୍ 🎹		
CONNECTED		Apply a display filter < Ctrl-	>				
	No	o. Time	Source	Destination	Protocol Len	ngth Info	
OpenVPN Profile		- 10.000000	172.24.1.2	224.0.0.251	MDNS	490 Standard q	uery response
192.168.16.82 [dmc-dr	12-vpn-	2 0.839792	1/2.24.1.2	192.168.16.82	OpenVPN	756 MessageTyp	e: P_DATA_V2
UDP4-1194-umd-conf	fig]	3 10.213006	172.24.1.2	192.168.16.82	OpenVPN	192 Messageryp	e: P_DATA_V2
		5 10 1/18/2	102 168 16 82	172 24 1 2	OpenVPN	68 MessageTyp	A D DATA V2
		6 20 214387	172 24 1 2	192 168 16 82	OpenVPN	68 MessageTyp	e: P DATA V2
		7 30, 217248	172.24.1.2	192.168.16.82	OpenVPN	68 MessageTyp	e: P DATA V2
CONNECTION STATS 3.7KB/s 0B/s							
O KB/S	BYTES OUT 0 KB/S						
DURATION PACKET R	ECEIVED						
03:11:16 17 sec ag	JO						
	<						

Figure 29: Test Case 3 OpenVPN tunnel establishment

Figure 30 through Figure 32 show Wireshark windows of the UE trace in which the UE tells the core its allowable network slice and subsequent messages within the core indicating the UE has been assigned to Slice 2 (STT=1, SD=2). In particular, Figure 30 shows core messages showing the correct slice is assigned to the appropriate UE, as indicated by its IMSI.

• •	•	🚄 B	20230213.1605-050	0-20230213.161	0-0500-AM	F.mtrdmcar	nf01.FIV	11_ue_trace	.572.pc	ар							
		o 🗴 🗂 🗖	Q 🌰 🔿 🗪	👅 🕹 🗖		ΞQ	Ð										
						-、-、	-•										
App	ly a display filter	. <郑/>														· ·	٠
No.	2 I ime	Source	Destination	NGAP	Length 40	UEContext	Release	Command									
	3			NGAP	68	UEContext	Release	eComplete									
	4	172.17.95.197	192.168.56.131	HTTP2/JSON	467	HEADERS [3]: POST	/nsmf-pdus	ession/	v1/sm	-conte	xts/3	06701	8832/1	nodify		
	5	192.168.56.131	172.17.95.197	HTTP2/JSON	101	HEADERS [3]: 200	OK, DATA[3]	, Javas	Script	Objec	t Nota	ation	(app)	licati	.or	
	6	192.168.57.201	172.17.27.33	HTTP2/JSON/	. 888	HEADERS [1]: POST	「∕namf-comm	/v1/ue-	-conte	xt/im	si-31	00147	917910	021/ 1	-r	
	7			NGAP	41	Paging											
L	8	172.17.27.33	192.168.57.201	HTTP2/JSON	246	HEADERS [1]: 202	Accepted, D	ATA[1],	Java	Script	0bje	ct No	tatio	n (app	li	
	9			NGAP/NAS-5G.	. 116	InitialUE	Message	e, Service r	equest,	Serv	ice re	quest					
	10			NAS-EPS	68												
	11			NGAP	946	InitialCo	ntextSe	etupRequest									
	12			NGAP	38	InitialCo	ntextSe	etupResponse									
	13	172.17.27.33	192.168.56.131	HTTP2/JSON	431	HEADERS [3]: POST	Γ /nsmf-pdus	ession/	v1/sm	-conte	xts/3	06701	.8832/r	nodify		
	14	192.168.56.131	172.17.27.33	HTTP2/JSON/.	. 594	HEADERS [3]: 200	OK, DATA[3]	, Javas	Script	Objec	t Nota	ation	(app)	licati	.or	
	15			NGAP	114	PDUSessio	nResour	rceSetupRequ	est								
	16			NAS-EPS	35												_
		Key: pduSessi	Lon1d					000	0 00	0c 00	08 68	74 74	70	32 00	00 0	00	14
		[Path: /n2Inf	foContainer/smInfo,	/pduSessionId]				001	0 c0	a8 39	c9 00	15 00	04	ac 11	1b 2	L 00	00
		∨ Member: sNssai						002	0 00	00 b5	01 04	00 00 6d 2f	00	01 86 21 2f	44 3	12f	6e
		∨ Object					-	003	0 74	20 03 65 78	74 73	2f 69	6d	73 69	2d 3	3 31	30
		Member: sd						005	0 34	37 39	31 37	39 31	30	32 31	2f 6	31	2d
		[Path wi	ith value: /n2Info	Container/smIn	fo/sNssai	/sd:000002	1	006	0 2d	6d 65	73 73	61 67	65	73 83	41 3	5 6d	74
		[Member	with value: sd:000	0002]				007	0 6d	63 61	6d 66	30 31	2e	61 6d	66 2	35	67
		String	/alue: 000002					008	0 6d	be 63	30 31	34 2e	60 70	63 63 65 20	33 3 6f 7	L 30	2e
		Key: sd						003	0 38	30 5f	35 6d	75 6c	74	69 70	61 7	2 74	2f
		[Path: /	/n2InfoContainer/s	mInfo/sNssai/s	d]			 ØØb 	0 6c	61 74	65 64	3b 20	62	6f 75	6e 6	4 61	72
		Member: ss	t					000	0 4d	75 6c	74 69	70 61	72	74 44	61 7	1 61	4c
		[Path wi	ith value: /n2Info	Container/smIn	fo/sNssai	/sst:1]		000	0 74	42 6f	75 6e	64 61	72	79 5c	03 3	7 31	30
		[Member	with value: sst:1]				006	0 91	00 01	61 74	00 01	2d	2d 4d	75 6	5 74 F 75	69
		Number v	/alue: 1					010	0 72	79 Ød	0a 43	6f 6e	74	65 6e	74 2	1 54	79
		Key: sst	t					011	0 3a	20 61	70 70	6c 69	63	61 74	69 6	f 6e	2f
		[Path: /	/n2InfoContainer/s	mInfo/sNssai/s	stj			012	0 6f	6e Ød	0a 0d	0a 7b	22	6e 31	6e 3	2 46	61
		Key: sNssai						013	0 75	72 65	54 78	66 4e	6f	74 69	66 5	5 52	49
		[Path: /n2Inf	foContainer/smInfo,	/sNssai]				014	22	b8 74	74 70	3a 2f	21	31 39	32 2	8 31	36
		Key: smInfo						Fram	ne (888 by	Dec	ompress	ed Head	er (28	2 by E	litstring	tvb (4	by.

Figure 30: Test Case 3 Wireshark capture showing assigned NSSAI

TLP:CLEAR:5GSTB

5G STB – Phase 1 Network Slicing Test Report

•••	•	🚄 В	20230213.1605-050	0-20230213.1610	0-0500-AMF	F.mtrdmcan	nf01.FIV1.	_1_ue_t	trace.57	2.pcap	p								
	1	🖿 🗋 🗙 🙆	۹ 🔶 🍝 😫	🟹 👲 🗌			Q T	C.											
	v a display filter .	<%/>																Ψ,	+
No.	Time	Source	Destination	Protocol	Length	Info											_	_	-
	4	172.17.95.197	192.168.56.131	HTTP2/JSON	467	HEADERS [3]: POST	/nsmf-	pduses	sion/v	1/sm	-cont	exts	/30676	1883	2/moc	lify,		
	5	192.168.56.131	172.17.95.197	HTTP2/JSON	101	HEADERS [3]: 200 0	K, DAT	A[3],	JavaSc	ript	0bje	ct N	otatio	on (a	pplic	atio	or	
	6	192.168.57.201	172.17.27.33	HTTP2/JSON/	888	HEADERS [1]: POST	/namf-	comm/v	1/ue-c	onte	xts/i	msi-	310014	7917	91021	l/n1-	-r	
	7			NGAP	41	Paging													-11
	8	172.17.27.33	192.168.57.201	HTTP2/JSON	246	HEADERS [1]: 202 A	ccepte	d, DAT	A[1],	Java	Scrip	t Ob	ject N	lotat	ion (appl	i.	
	9			NGAP/NAS-5G	116	InitialUE	Message,	Servi	ce req	uest,	Serv	ice r	eque	st					-11
	10			NAS-EPS	68			_											
	11			NGAP	946	InitialCo	ntextSet	upReque	est										
	12	470 47 07 00	400 400 50 404	NGAP	38	InitialCo	ntextSet	upResp	onse					(2067)	4000	• (• • • •			
	13	1/2.1/.2/.33	192.108.00.131	HTTP2/JSUN	431	HEADERS [3	1: PUSI	/nsmi-	A [2]	510n/v	1/Sm	-cont	exts	/300/0	1883	2/ 000	11TY,		Ŭ
	14	192.108.50.131	1/2.1/.2/.33	NGAP	114	PDUSessio		Setup	A[3],		птрс	obje	CUN	otatio	n (a	pptic	allo	7	
	16			NAS-EPS	35	100363310	intesourc	esecupi	neques										
	17			NGAP/NAS-56S	75	DownlinkN	ASTransp	ort											
	18			NAS-EPS	42														
		id, id DDUCossionD	acourceCoturi ictCl	Deg (74)	0				0000	00 00	. 00	04 60	e 67	61 70	00	00 0	0 0 0	00	1d (
		criticality, reject	+ (a)	Red (74)					0010	00 00	0 04	00 00	a 00	06 80	03	19 5	5 83	b2	00 5
		value	(0)						0020	05 c0	0 01	00 37	7 f4	00 4a	00	38 0	00 6	01	40 2
		 PDIISessionResource 	ceSetuplistSURea:	1 item					0030	00 02 3h 9a	2 21	00 00	0 04 0 8h	00 82 00 0a	00	0a 0	a cd	9a 43	ca (
		v Item 0	cese cupers cookeq.	I ICC.					0050	07 38	3 00	86 00	0 01	00 00	88	00 0	7 00	09	00 0
		V PDUSession	ResourceSetupItemS	URea					0060	2c 00	00 0	6e 40	0 0 C	10 02	54	0b e	4 00	40	02 5
		pDUSessi	onID: 1						0070	e4 00	9								
		s-NSSAI																	
		sST:	01																
		sD: 0	00002					0											
		v pDUSessi	onResourceSetupRe	questTransfer:	000004008	2000a0c3b	9aca0030	3b9aca											
		v PDUSe:	ssionResourceSetup	RequestTransfe	r														
		✓ pro	tocolIEs: 4 items																
		~	Item 0: id-PDUSess	ionAggregateMa	ximumBitRa	ate													
			 ProtocolIE-Fiel 	d															
			id: id-PDUSes	sionAggregate№	laximumBitF	Rate (130))												
			criticality:	reject (0)															
			✓ value ✓ PDUSession	AggregateMaxim	umBitRate				Frame (14 byt	Unal	ligned	OCTET	STRING	(1 b	Bitst	ring tv	b (4	byt

Figure 31: Test Case 3 Wireshark Capture Showing UE NSSAI in PDU Setup Request



Figure 32: Test Case 3 Wireshark capture showing PDU session resource setup request NSSAI

After connecting to the VPN, we downloaded a large file as well as connected to a continual random image downloader as shown in Figure 33.



Figure 33: Test Case 3 bulk file and continual random image download

[local]R6672-IP-1-1#sh tunnel ipsec name ipsec_tunnel_UMD statistics detail Remote IP : 10.220.67.18 Local IP : 10.205.67.200 # IN Packets Received: 666447 # IN Bytes Received: # OUT Packets Received: 1214108 # OUT Bytes Received: 107250965 1543271328 # Packets Fragmented Tx: 24 # Bytes Fragmented Tx: 14880 Errors Incoming packets dropped due to the following reasons: # Authentication errors: 0 # Decryption errors: 0 # Anti-replay check failure: 0 # No matching SA: 0 IPsec acl name #: IPSec-ACL-UMD SA #: Inbound ESP SPI : 0xc189a0c7 # Packets sent: 0 # Packets received: 666447 0 # Bytes received: # Bytes sent: 107250965 0 # Packets Fragmented Tx: # Packets Fragmented Rx: 0 # Bytes Fragmented Rx: 0 # Bytes Fragmented Tx: 0 Errors Incoming packets dropped due to the following reasons: # Authentication errors: 0 # Decryption errors: 0 # Anti-replay check failure: 0 IPsec acl name #: IPSec-ACL-UMD SA #: Outbound ESP SPI : 0x586ab14f 1214109 # Packets received: # Packets sent: 0 1543272604 # Bytes received: # Bytes sent: 0 # Packets Fragmented Rx: 0 # Packets Fragmented Tx: 0 # Bytes Fragmented Rx: 0 # Bytes Fragmented Tx: 0

Figure 34: Test Case 3 final IPsec statistics details

After downloading these large files, we rechecked the IPsec statistics as shown in Figure 34. Comparing to Figure 25, we see the total number of packets sent have increased by 666,395 on the input and 1,214,056 on the output. The number of fragmented packets increased to 24, representing 0.002%. These packet fragmentations occur during the initialization of the OpenVPN session. Also, no errors are shown, and no fragmented packets appear within the access control list (ACL) both for the inbound and outbound ESPs.

The packet drop rate (in ppm) for sections "Access Throughput KPIs" and "Core Throughput KPIs" from the CNOM Health Check View after the test are shown in Figure 35. Figure 36 shows the ip_received_packet drop statistics from the CNOM Metric Viewer.

Access Throu	about KE	20232	13-17020.	.800			Core_Throu	ghput_KF	Pls_20232	13-17027	-929		
Now	1h ago	3h ago	6h ago	12h ago	24h ago	Name	Now	1h ago	3h ago	6h ago	12h ago	24h ago	Name
514,361.60)	0 (0	0	0 GTP T-PDU in (b	-	() ()	0 0) () GTP T-PDU in (
8,915,707.73	C)	0 (D	0	GTP T-PDU out	-	() ()	0 0) (GTP T-PDU out
-	C)	0 (D	0	D IP in (bps)	8,915,707.73	() ()	0 0) () IP in (bps)
-	C)	0 (D	0	D IP out (bps)	514,361.60	() ()	0 0) (D IP out (bps)
616.27	C)	0 (D	0	D GTP T-PDU in (p	-	() ()	0 0) (GTP T-PDU in
973.47	C)	0 (D	0	D GTP T-PDU out	-	() ()	0 0) (GTP T-PDU ou
-	C)	0 (D	0	D IP in (pps)	973.47	() ()	0 0) () IP in (pps)
-	C)	0 (D	0	0 IP out (pps)	616.27	(1	0 0		IP out (nns)
5.76	6.71	6.71	6.71	6.	6.71	Packet Drop Rat	01.25	106.66	106.66	106.66	106.66	106.66	Backot Drop P

Figure 35: Test Case 3 Final Packet Drop Rates from Access Throughput KPIs and Core Throughput KPIs

Comparing results in Figure 27 with those in Figure 35 (as well as the "1h ago" columns of Figure 35), we see the packet drop rate decreased from 6.71ppm to 5.76ppm for Access Throughput, and from 106.66 to 91.25ppm for Core Throughput. The reason that these statistics decrease is due to the increase in traffic through the system (affecting the denominator of the rate calculation) and a lower relative number of packet drops. Consequently, it is reasonable to conclude that the VPN tunnel did not contribute to any additional packet drops. Furthermore, there was no change for the ip_received_packet drops statistics from CNOM Metric Viewer as shown on the screenshot in Figure 36.

tttings Time interval [minutes]: 2			
up_ip_received_packets			Refresh
🗠 Metric 🗘	Absolute 🗢	Delta (2 min) 🗘	Rate (2 min)
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="no_host"}	4333	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="length"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="fragments"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="checksum"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="no_gateway"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="unsupported_protocol"}	0	0	0.
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="pmtu"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_internal"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_invalid_fragment"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_max_fragment_flow"	} 0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_no_memory"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_overflow"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_ttl"}	0	0	0.
pc_up_ip_received_packets_total{action="drop",protocol="ipv6",reason="length"}	0	0	0.0
pc_up_ip_received_packets_total{action="drop",protocol="ipv6",reason="fragments"}	0	0	0.0
pc up in received packets total/action="drop".protocol="inv6".reason="no host"}	0	0	0.

Figure 36: Test Case 3 CNOM Metric Viewer—final ip_received_packet drops statistics

Test Result

Success: The IPsec tunnel statistics indicated no packet drops and no packet fragmentations (other than 24 fragmented packets at the initiation of the VPN tunnel). The DMC Health Check statistics showed insignificant packet drops during the test. The DMC Metric Viewer recorded no packet drops during the test.

Condition	Status
IPsec tunnel error-free	Success
IPsec tunnel fragmentation-free	Success
Acceptable core packet drop rate	Success
Overall Test Case 3	Success

Conclusions and Next Steps

This round of testing successfully verified the feasibility and efficacy of employing security procedures for network slicing based on 3GPP Technical Specifications TS 33.401 and 33.501, including select measures recommended by the CSRIC VII WG3 report, while using commercial hardware in a commercially-relevant 5G standalone configuration.

Test Case 1 involved two main components: first, demonstrating authentication by confirming that the user equipment successfully registers to its assigned network slice, and second, assessing isolation and segmentation by verifying that the user equipment assigned to one network slice cannot access the applications in another network slice. In testing, packet capture software showed that the user equipment assigned to each slice successfully registered and acknowledged its slice assignment both by responding from the core, and also through a message from the Access and Mobility Function to the Session Management Function that confirmed the correct IP address and data network name. Using network scanning tools, testing also confirmed that each user device and associated server was not able to access the IP address space or find devices or ports in slices other than the slice it was assigned to.

Test Case 2 added transport protection using IPsec to one of the two test network slices. In the first part of the test, the RAN-side router view showed ping traffic from the network slice that did not use IPsec, while the other slice configured with IPsec showed encrypted traffic with the IPsec tunnel endpoints as the source and destination addresses. The second part of the test confirmed that the network slices were isolated from each other. As in Test Case 1, scans from the network equipment and web servers operating on one slice were able to access the web server on that slice only, but could not see or access IP addresses or devices on the other slice. Test Case 2 successfully enabled IPsec, confirmed user equipment was associated with the correct slice, and that traffic was encrypted over the IPsec link. It also used network scanning tools on both the servers and user equipment to confirm isolation by showing that only the ports associated with each network slice were visible from that slice.

Test Case 3 built on Test Cases 1 and 2 to add end-to-end encryption on top of the IPsec-enabled transport. The goal was to show that these additional layers of encryption do not have significant impacts on the throughput or cause packet fragmentation. This case used three layers of encryption: transport layer security (TLS) for application security, VPN encryption, and the 5G network layer encryption (both over the air, and through the IPsec tunnel for the transport network). Testing involved downloading a large file and then a series of images. The test verified that user equipment had registered to the network slice using IPsec and confirmed that the IPsec tunnel was active. The test set the Maximum Transmission Unit for the user equipment at 1100, the highest estimated value that would not cause packet fragmentation using a VPN. Testing showed that the packet drop rate was not significantly affected by the VPN tunnel, and packet

fragmentation was minimal, occurring only at the initialization of the VPN session. This test case shows that a highly secure configuration that uses multiple layers of encryption would not cause problematic levels of packet drops or fragmentation. This finding means that customers seeking additional security layers for their 5G applications are not likely to have to sacrifice performance for security.

Together, these three test cases proved the feasibility and efficacy of security procedures using network slicing in a 5G SA configuration. They show that network slices are isolated from each other, and that customers may select additional layers of security using encryption that will not significantly affect performance.

For future tests, the 5G Security Test Bed is exploring additional potential network slicing security concerns, such as the impact on slice isolation if a network function becomes compromised. The Test Bed is also in the process of developing test cases for false base station and roaming security use cases. The 5G Security Test Bed members and administrator welcome engagement from stakeholders with an interest in the Test Bed's mission, and we expect to develop more and diverse test cases along with new participants.

Appendix: Acronyms

3GPP	Third Generation Partnership Project
5GSTB	5G Security Test Bed
ACL	Access Control List
AKA	Authentication and Key Agreement
AMF	Access & Mobility Management Function
BBU	Baseband Unit
CNOM	Core Network Operations Manager
СР	Control Plane
CPE	Customer Premise Equipment
CSRIC	Communications Security, Reliability, and Interoperability Council
DMC	Dual-Mode Core
DN	Data Network
DNN	Data Network Name
eMBB	Enhanced Mobile Broadband
eNB/eNodeB	Evolved Node B
ENDC	E-UTRA New Radio – Dual Connectivity
EPG	Evolved Packet Gateway
ESP	Encapsulating Security Payload
	Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial
E-UTKA	Radio Access
FDD	Frequency Division Duplex
gNB/gNodeB	Next Generation Node B
HSS	Home Subscriber Server
IKEv2	Internet Key Exchange Protocol Version 2
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPSec	Internet Protocol Security
LTE	Long Term Evolution
MACsec	Media Access Control security
MBB	Mobile Broadband
MME	Mobility Management Entity
mMTC	Massive Machine-Type Communication
MNO	Mobile Network Operator
MTP	Mobile Test Platform
MTU	Maximum Transmission Unit
NMS	Network Management System
NR	New Radio
NRF	Network Repository Function

NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
PCF	Policy Control Function
PDU	Protocol Data Unit
PGW	Packet Data Network Gateway
ppm	Packets per million
R6K	Router 6672
RAN	Radio Access Network
RAT	Radio Access Technology
SA	Standalone
SD	Slice Differentiator
SDR	Software-Defined Radio
SEG	Security Gateway
SGW	Serving Gateway
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SST	Slice/Service Type
STB	Security Test bed
TAS	Telecom Application Server
ТС	Test Case
TDD	Time Division Duplex
TLS	Transport Layer Security
ТР	Test Point
UDM	Unified Data Management
UE	User Equipment
UMD	University of Maryland
UP	User Plane
UPF	User Plane Functions
URLLC	Ultra-Reliable Low-Latency Communication
VNF	Virtualized Network Function
VPN	Virtual Private Network
WG	Working Group

References

- [1] CTIA 5G STB, Test Plan for 5G Security Test Bed (5GSTB) Network Slicing Use Cases, V1.0, August 9, 2022
- [2] 3GPP TS 33.401
- [3] RFC 4303
- [4] TS 33.210
- [5] TS 33.310
- [6] 3GPP TS 33.501
- [7] Communications Security, Reliability, and Interoperability Council (CSRIC) VII Working Group 2 (WG2) Report 2.