5G SECURITY™ TEST BED

Securing 5G:

Network Slicing Phase 1 Test Report

Q1 2023

Table of Contents

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
  - 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.
  - 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
    - 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).
    - 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.

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.

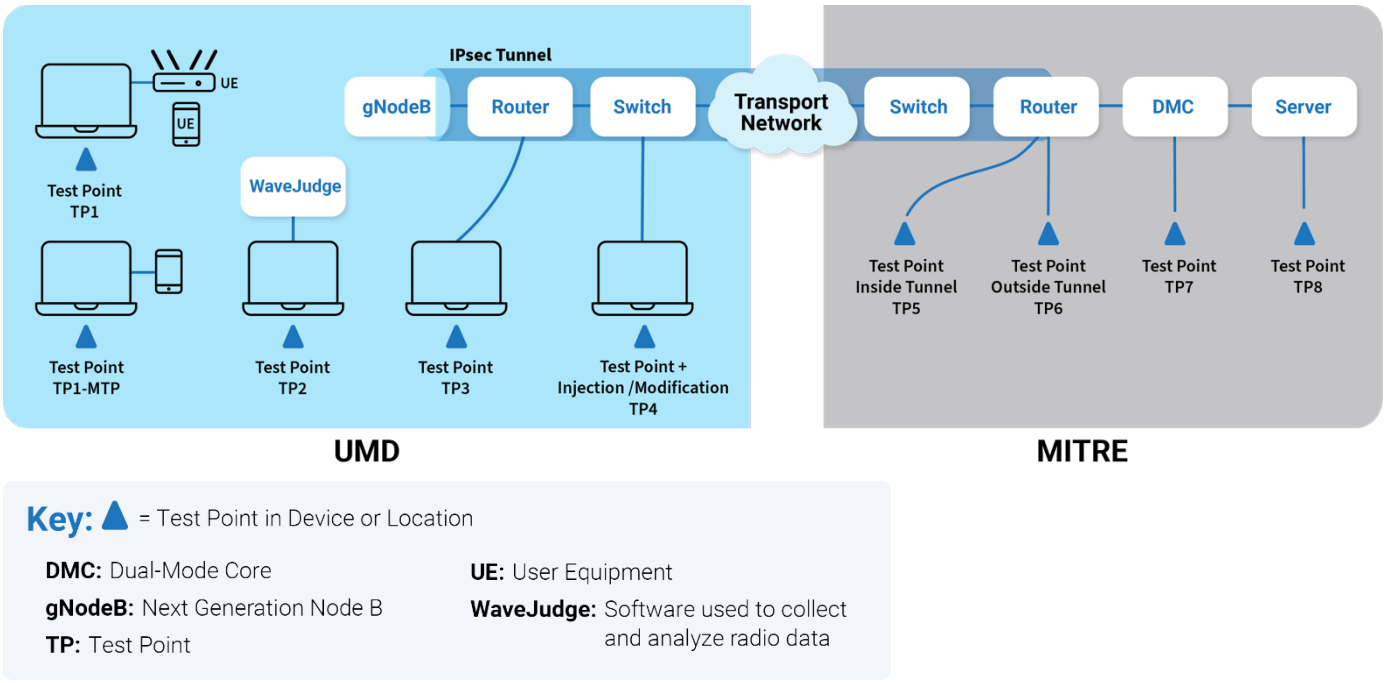
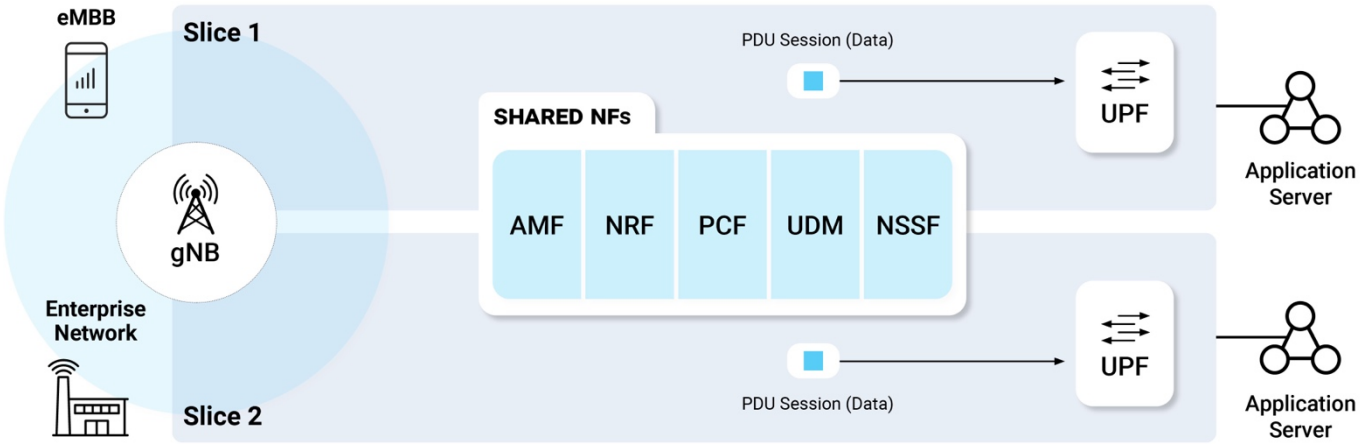


Figure 1: 5G STB Lab Component Block Diagram and Test Points

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.

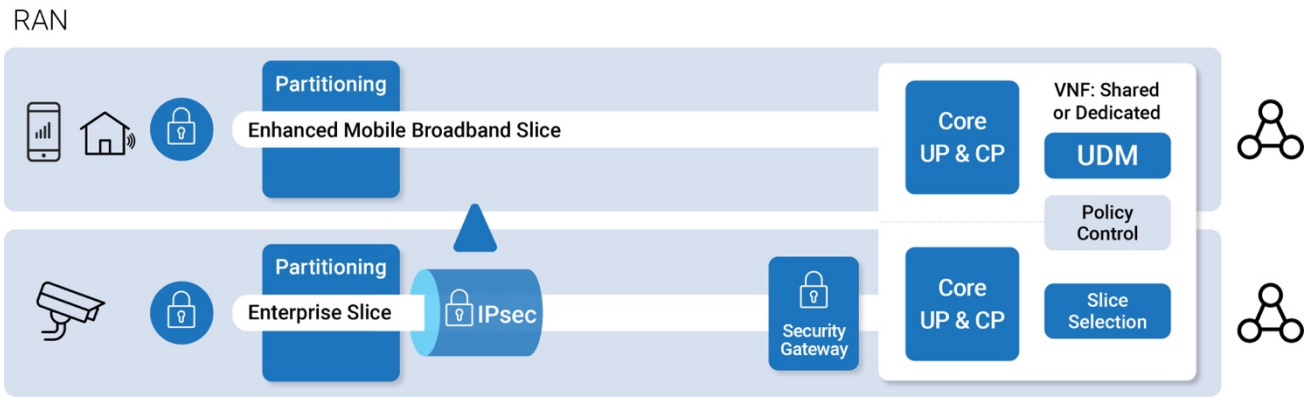
On the server on the core side, there are two virtual web servers instantiated, one for each slice, and isolated from each other. The slice configuration and IPsec tunnel location are illustrated in Figure 2 and Figure 3.



Key:

AMF: Access & Mobility Management Function
eMBB: Enhanced Mobile Broadband
gNB: gNodeB
NF: Network Function
NR Cell: New Radio Cell
NRF: Network Repository Function
NSSF: Network Slice Selection Function
PCF: Policy Control Function
PDU: Protocol Data Unit
SMF: Session Management Function
UDM: Unified Data Management
UPF: User Plane Function

Figure 2: Network Slice Configuration for Phase 1 Tests



Key: ▲ = Test Point in Device or Location

CP: Control Plane
eMBB: Enhanced Mobile Broadband
IPsec: IP security (encrypted tunnel)
UDM: Unified Data Management
UP: User Plane
VNF: Virtualized Network Function

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.

Table 3: Test Point Descriptions

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
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
TP7	CNOM tool accessing DMC messages
TP8	Applications running on application server in MITRE facility

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

Slice	IP pool	SIM 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.FIV1._1_ue_trace.810	UE trace captured at DMC, TP7

Test points used:

Used	Test Point	Description and Use
X	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
X	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
X	TP7	CNOM tool accessing DMC messages
X	TP8	Applications running on application server in MITRE facility

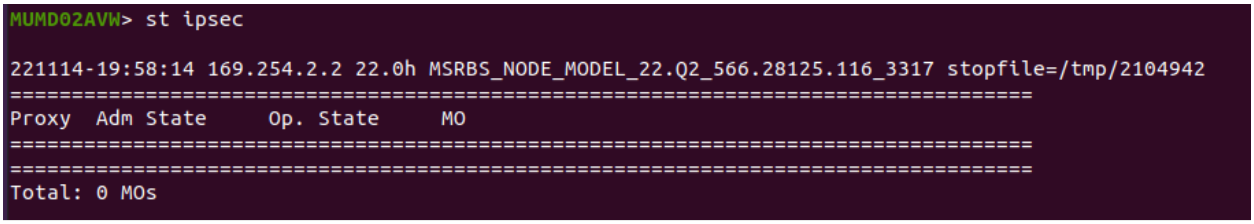


Figure 4: Confirming IPsec Inactive

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 RAN-side 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).

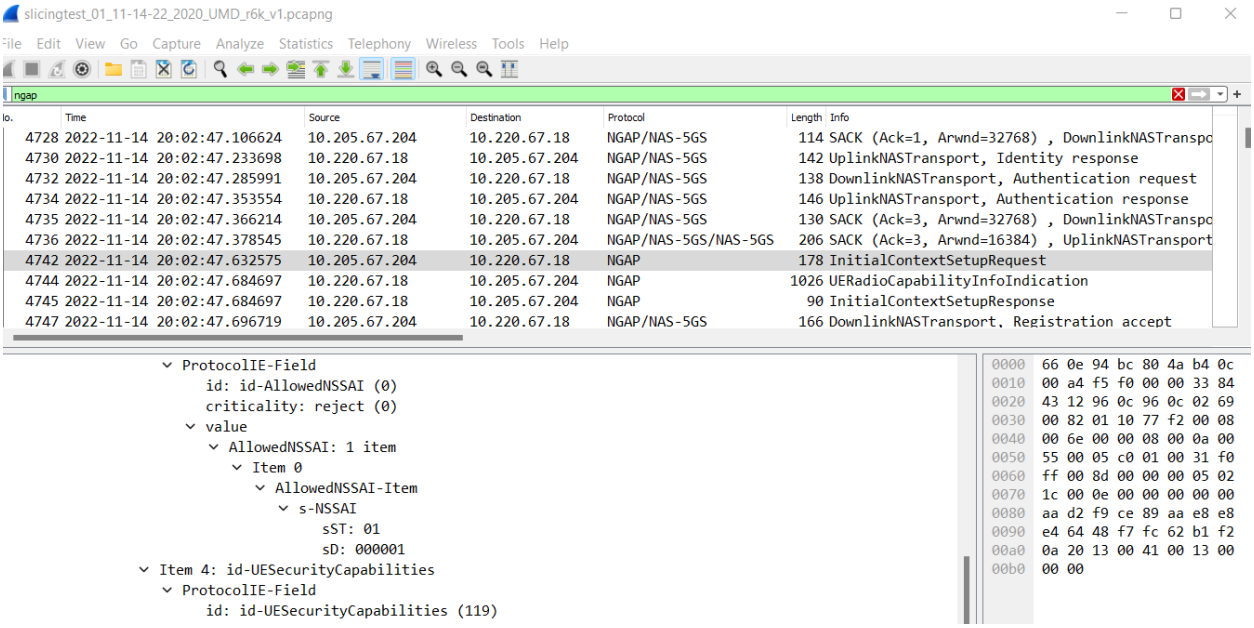


Figure 5: Wireshark capture showing UE1 allowed NSSAI

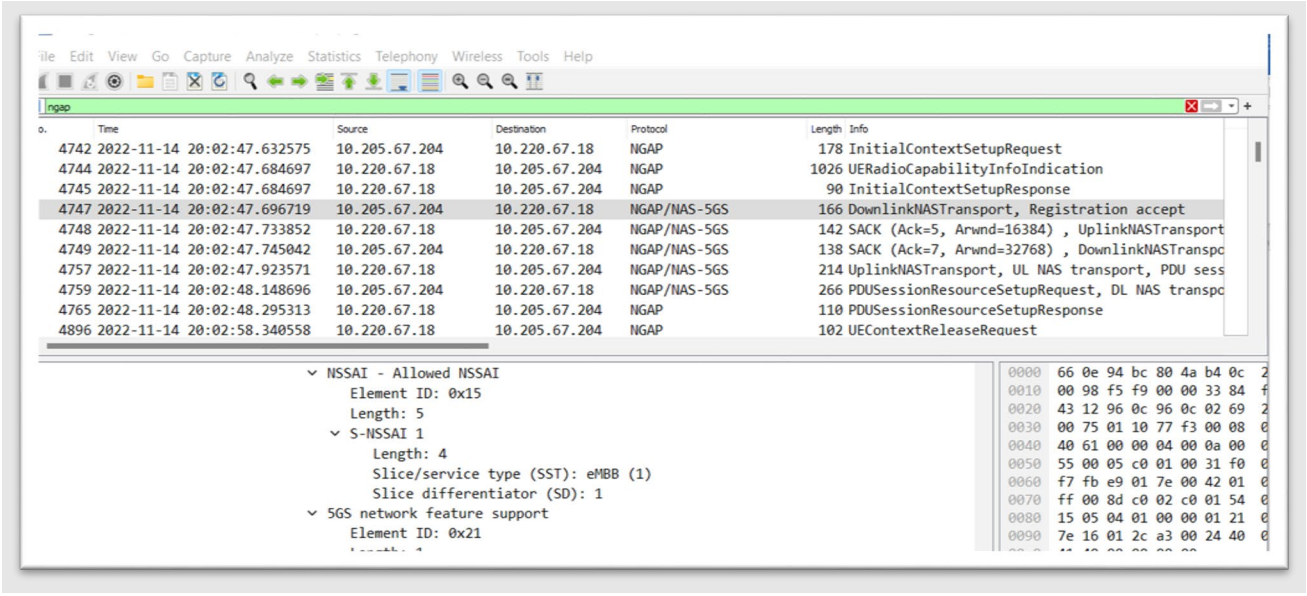


Figure 6: Wireshark capture of Downlink NAS Registration accept indicating NSSAI for UE1

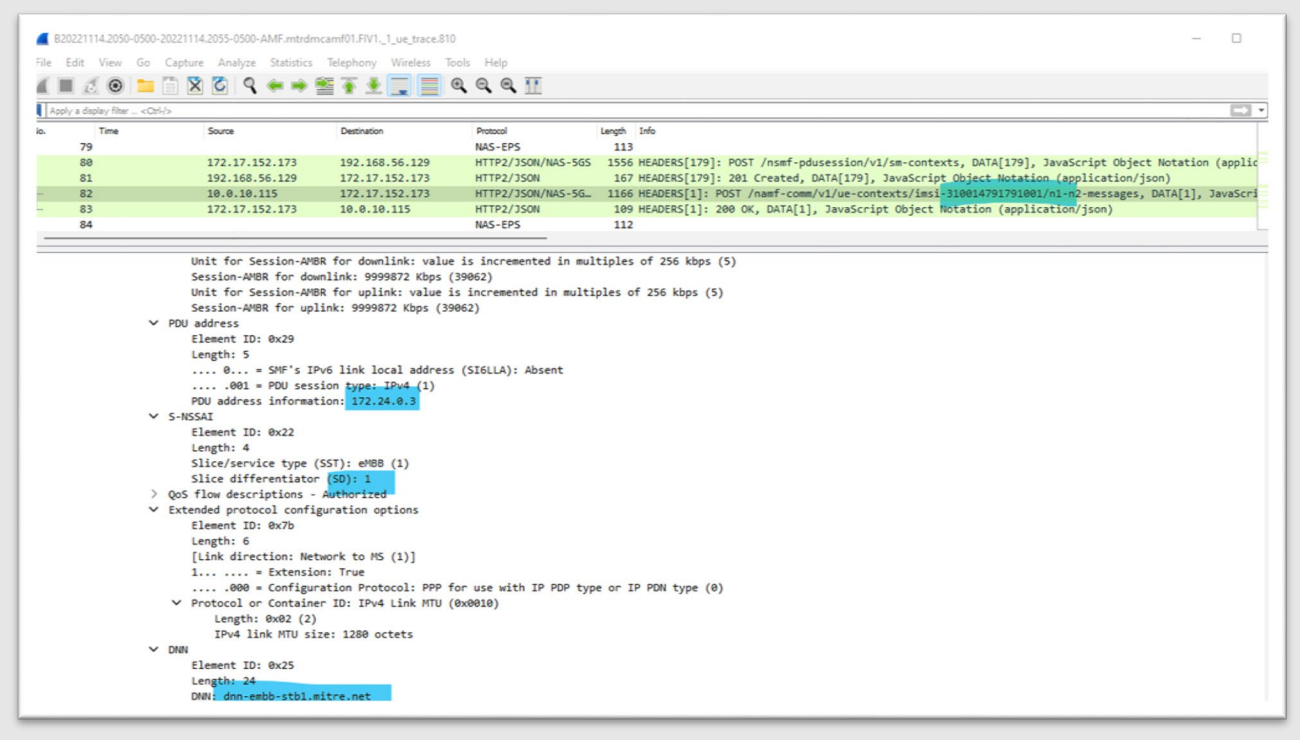


Figure 7: UE trace showing AMF-SMF message indicating UE 1 assigned to Slice 1

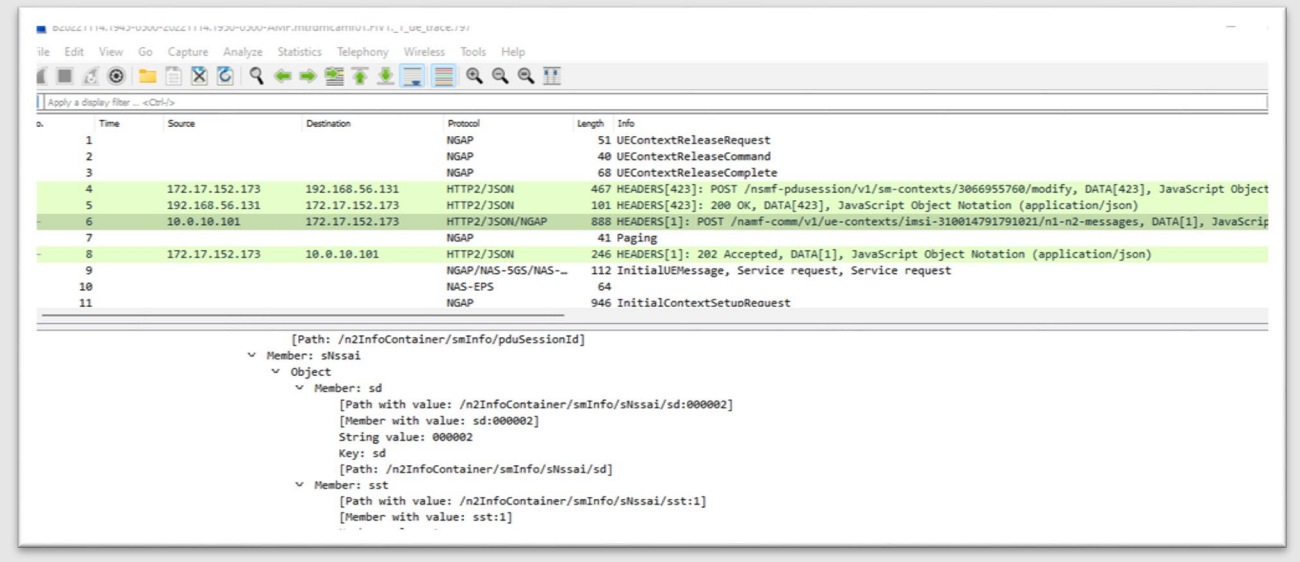
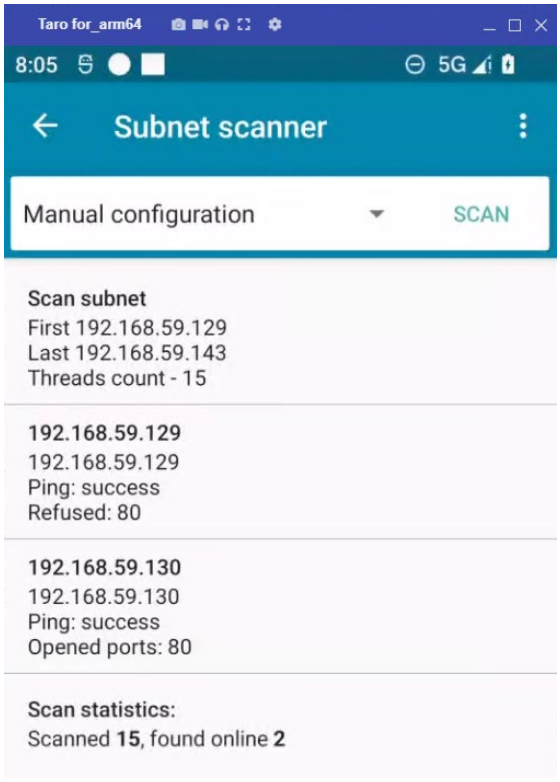


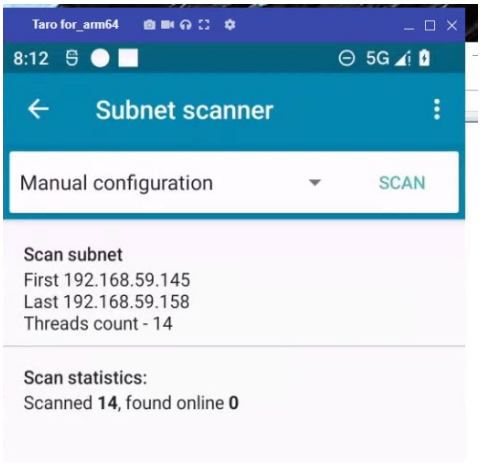
Figure 8: UE trace showing AMF-SMF message indicating UE 2 assigned to Slice 2

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.



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



Network scan did not find any IP and open ports for hosts on Slice 2.

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

```
[dndiki@fgp-dmc-dnstb1 ~]$ nmap -T4  172.24.0.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2022-11-03 18:24 EDT
Nmap scan report for 172.24.0.3
Host is up (0.026s latency).
All 1000 scanned ports on 172.24.0.3 are closed

Nmap done: 256 IP addresses (1 host up) scanned in 5.44 seconds
[dndiki@fgp-dmc-dnstb1 ~]$
```

Figure 10: Network scan from the virtual server on Slice 1 for UE addresses assigned to Slice 1 using Nmap

```
Starting Nmap 6.40 ( http://nmap.org ) at 2022-11-14 20:11 EST
Nmap done: 256 IP addresses (0 hosts up) scanned in 2.41 seconds
[dndiki@fgp-dmc-dnstb1 ~]$
```

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, 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).

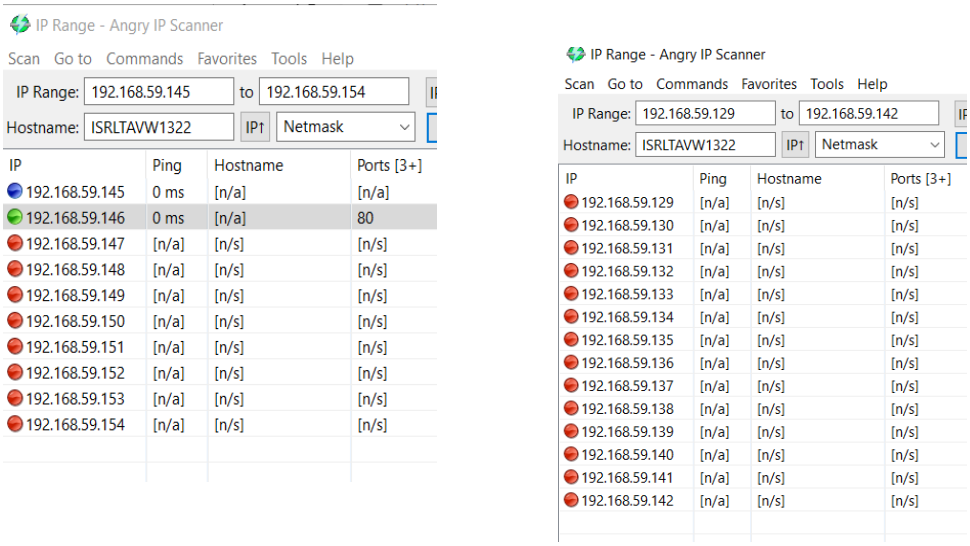


Figure 12: Network scan from the UE on Slice 2 using Angry IP Scanner

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

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 used:

Used	Test Point	Description and Use
X	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
X	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”
X	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
X	TP7	CNOM tool accessing DMC messages
X	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.

```
MUMD02AVW> st ipsec

221114-18:07:33 169.254.2.2 22.0h MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/2104942
================================================================================
Proxy  Adm State     Op. State     MO
================================================================================
14290                1 (ENABLED)   Transport=1,Router=NRCUCP,IpsecTunnel=1
================================================================================
Total: 1 MOs
```

Figure 15: IPsec state for Test Case 2

R6K configuration dump:

```
[dmc_ran]R6672-IP-1-1#show configuration ike
Building 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
!
end
```

```
[dmc_ran]R6672-IP-1-1#show configuration ipsec
Building configuration...
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
```

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
local]R6672-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.

Table 7: UE parameters for Test Case NetSlic-02

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

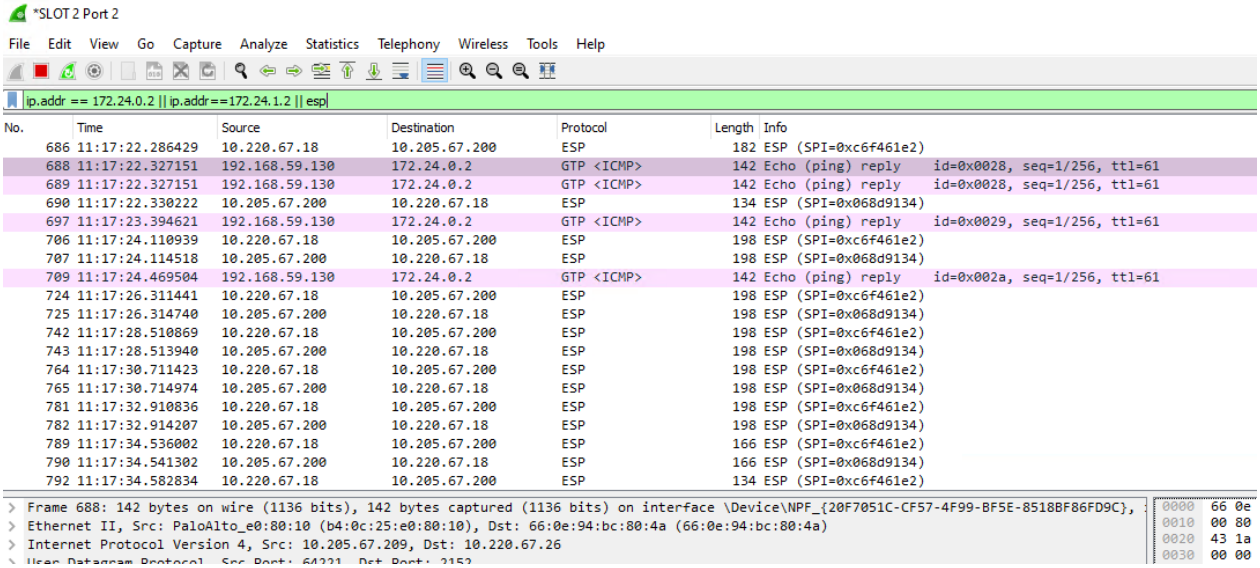


Figure 18: Test Case NetSlic-02 traffic at RAN-side R6K router (TP3)

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.

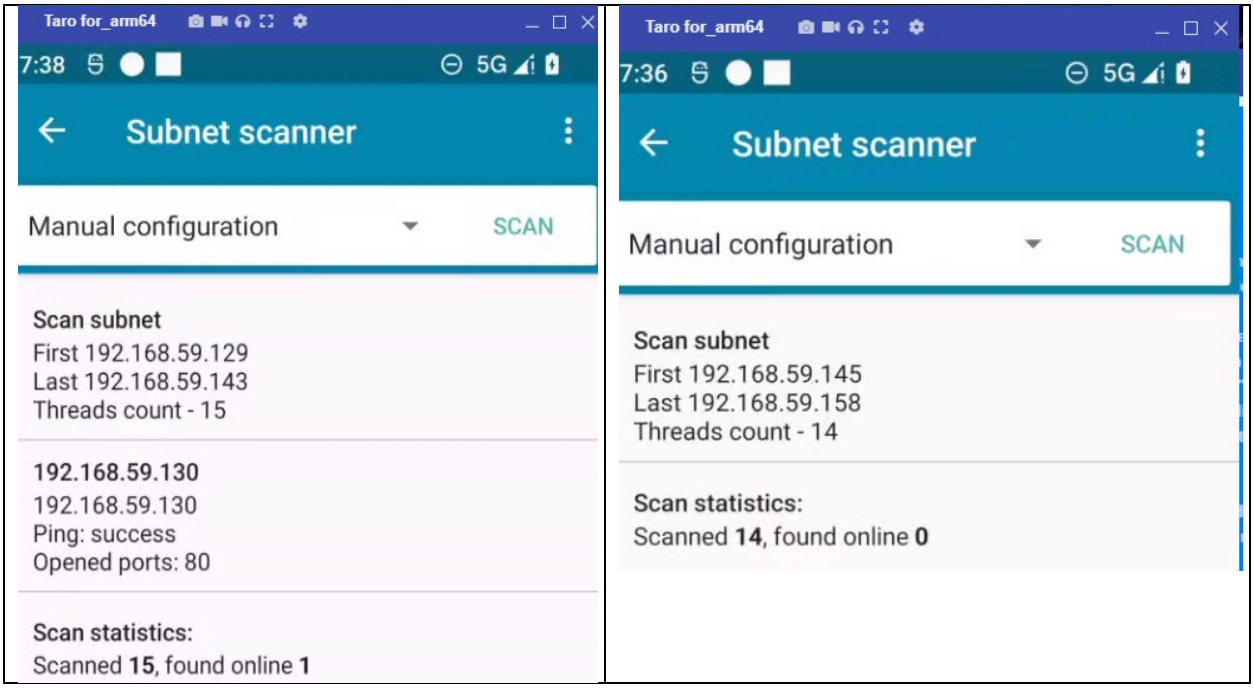


Figure 19: Network scan from the UE on Slice 1 for Test Case 2

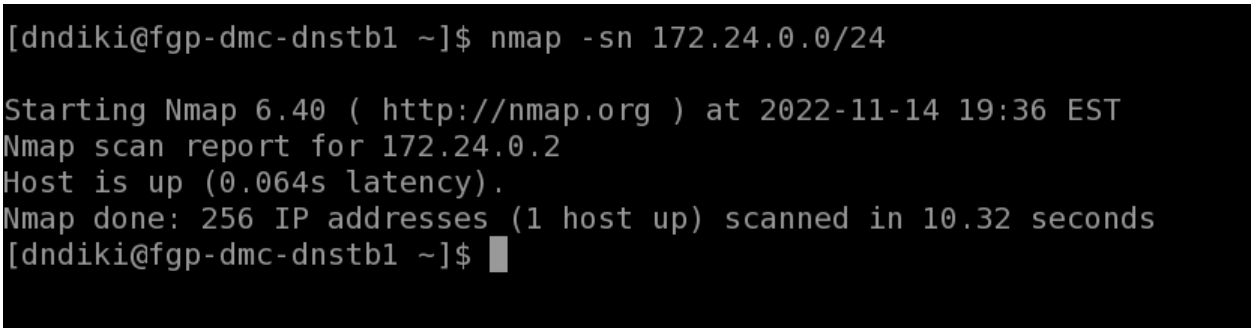


Figure 20: Network scan from the virtual server on Slice 1 for UE addresses on Slice 1 for Test Case 2

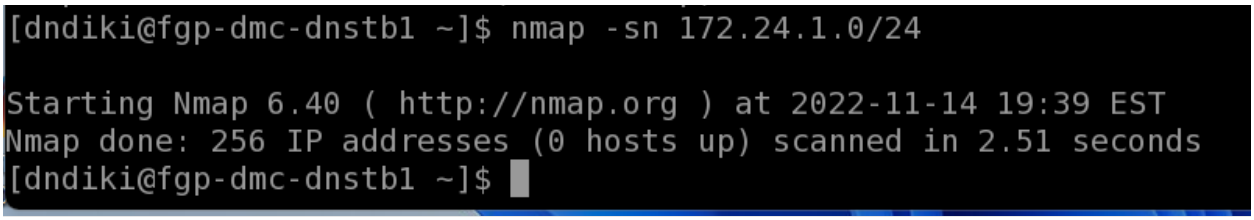


Figure 21: Network scan from the virtual server on Slice 1 for UE addresses on Slice 2 for Test Case 2

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.

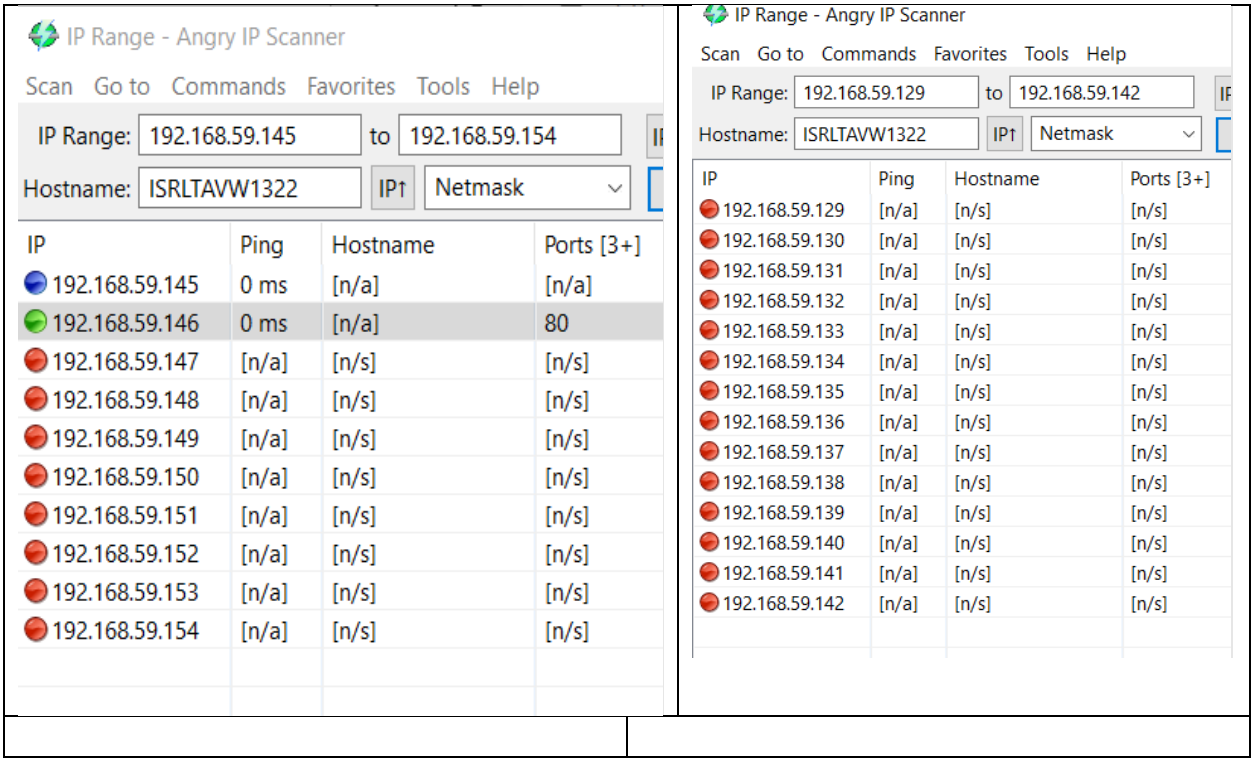


Figure 22: Network scan from the UE on Slice 2 using Angry IP Scanner for Test Case 2

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	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: 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.

Test points used:

Used	Test Point	Description and Use
X	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”
X	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
X	TP7	CNOM tool accessing DMC messages
X	TP8	Applications running on application server in MITRE facility

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.

```
MUMD02AVW> st ipsec

230213-16:15:25 169.254.2.2 22.0h MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/1577469
================================================================================
Proxy  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 ipsec_tunnel_UMD statistics detail
Remote IP : 10.220.67.18  Local IP    : 10.205.67.200
# IN Packets Received:                52 # IN Bytes Received:               9152
# OUT Packets Received:               52 # OUT Bytes Received:              10608
# Packets Fragmented Tx:               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 # No matching SA:                      0

IPsec acl name #: IPSec-ACL-UMD
SA #: Inbound ESP
-----------------------------------
SPI : 0xc189a0c7
# Packets sent:                       0 # Packets received:                  52
# Bytes sent:                         0 # Bytes received:                  9152
# Packets Fragmented Rx:              0 # Packets Fragmented Tx:               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
# Packets sent:                      52 # Packets received:                   0
# Bytes sent:                     10608 # Bytes received:                     0
# Packets Fragmented Rx:              0 # Packets Fragmented Tx:               0
# Bytes Fragmented Rx:                0 # Bytes Fragmented Tx:                0
```

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:\Users\sysadmin>netsh interface ipv4 show subinterface

   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
4294967295                1          0   20607316  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.

Access_Throughput_KPIs_2023213-161129-588

Now	1h ago	3h ago	6h ago	12h ago	24h ago	Name
-	0	0	0	0	0	GTP T-PDU in (bps)
-	0	0	0	0	0	GTP T-PDU out (bps)
-	0	0	0	0	0	IP in (bps)
-	0	0	0	0	0	IP out (bps)
-	0	0	0	0	0	GTP T-PDU in (pps)
-	0	0	0	0	0	GTP T-PDU out (pps)
-	0	0	0	0	0	IP in (pps)
-	0	0	0	0	0	IP out (pps)
6.71	6.71	6.71	6.71	6.71	6.71	Packet Drop Ratio (ppr

Core_Throughput_KPIs_2023213-161136-136

Now	1h ago	3h ago	6h ago	12h ago	24h ago	Name
0	0	0	0	0	0	GTP T-PDU in (bps)
0	0	0	0	0	0	GTP T-PDU out (bps)
0	0	0	0	0	0	IP in (bps)
0	0	0	0	0	0	IP out (bps)
0	0	0	0	0	0	GTP T-PDU in (pps)
0	0	0	0	0	0	GTP T-PDU out (pps)
0	0	0	0	0	0	IP in (pps)
0	0	0	0	0	0	IP out (pps)
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

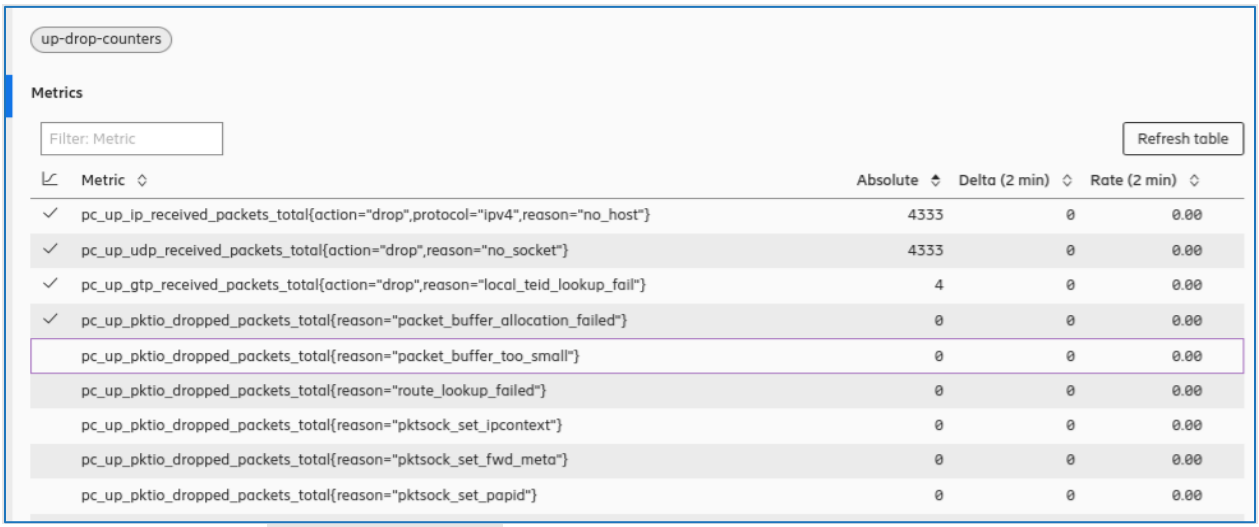


Figure 28: Test Case 3 Initial ip_received_packet drop

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

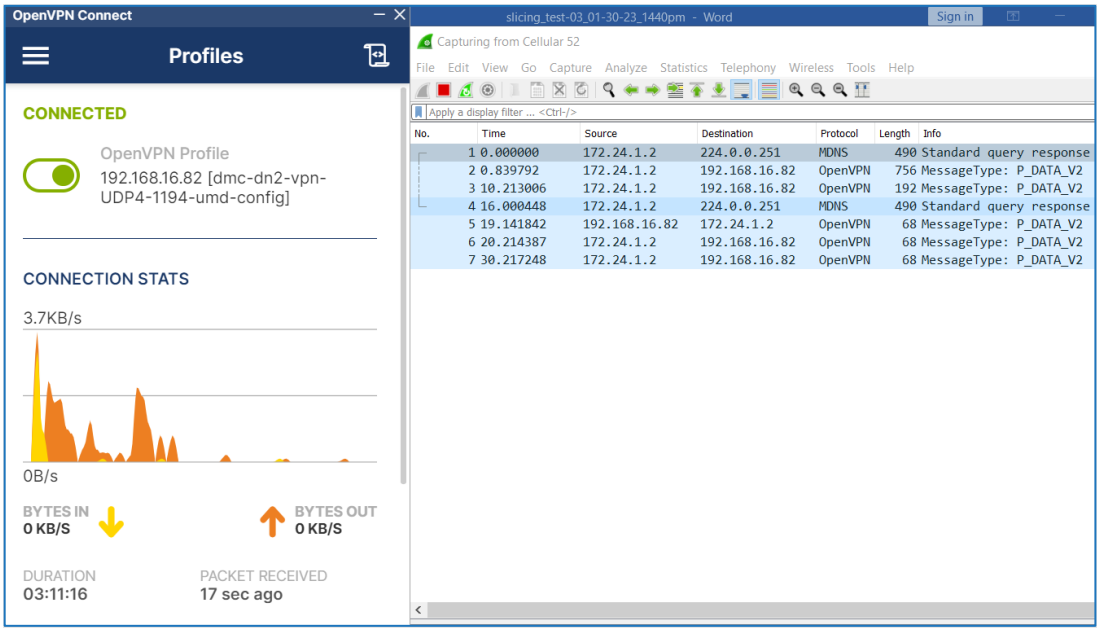


Figure 29: Test Case 3 OpenVPN tunnel establishment

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.

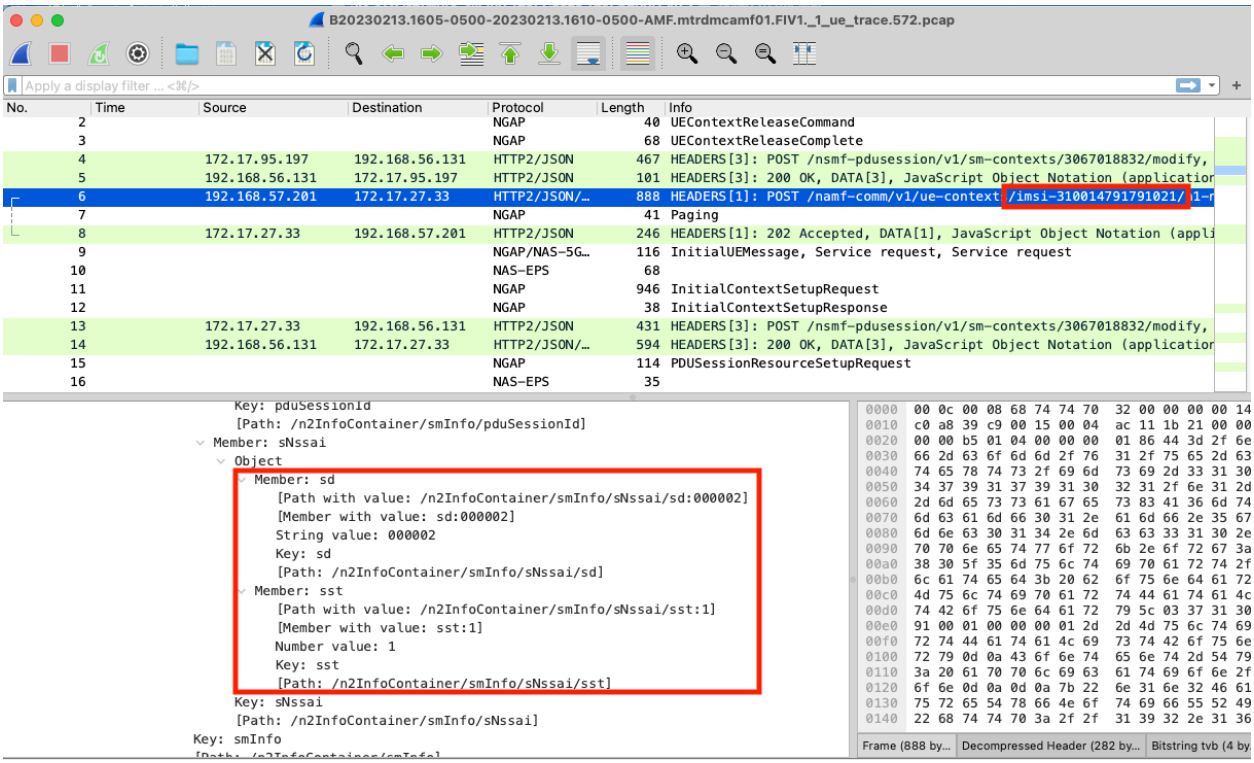


Figure 30: Test Case 3 Wireshark capture showing assigned NSSAI

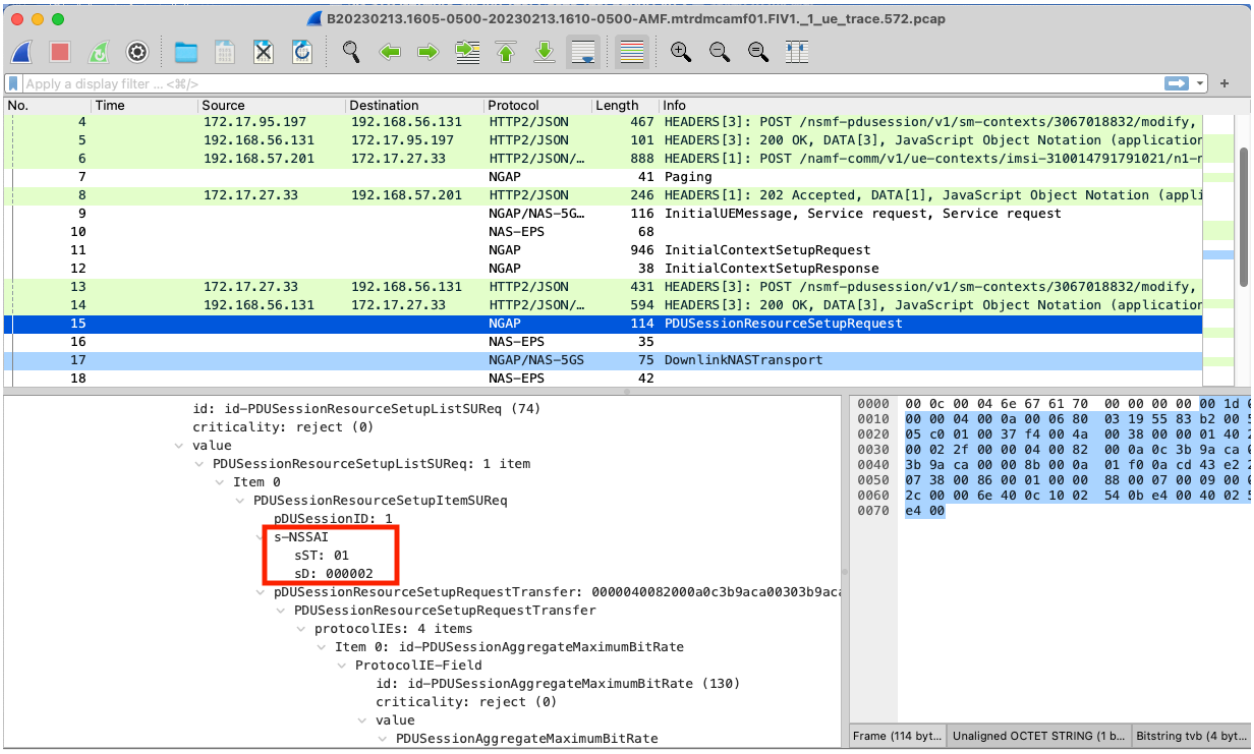


Figure 31: Test Case 3 Wireshark Capture Showing UE NSSAI in PDU Setup Request

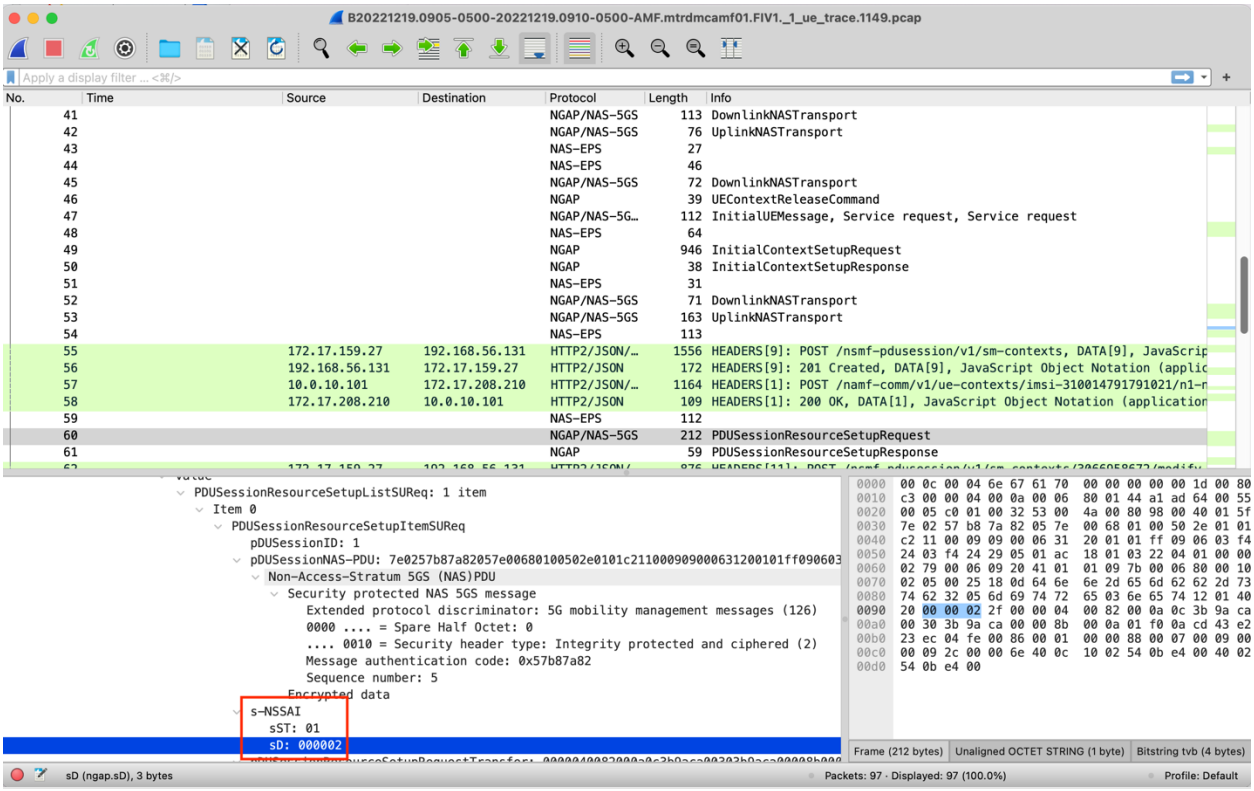


Figure 32: Test Case 3 Wireshark capture showing PDU session resource setup request NSSAI

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.

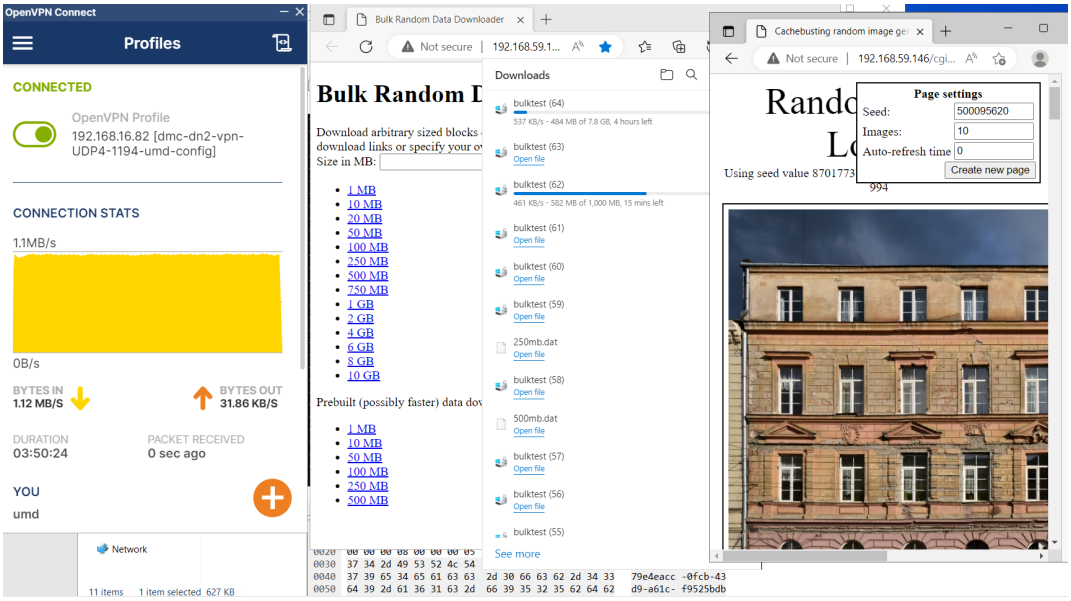


Figure 33: Test Case 3 bulk file and continual random image download

```
[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:          107250965
# OUT Packets Received:          1214108 # OUT Bytes Received:        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
# Bytes sent:                          0 # Bytes received:             107250965
# Packets Fragmented Rx:               0 # Packets Fragmented Tx:             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
# Packets sent:                  1214109 # Packets received:                   0
# Bytes sent:                 1543272604 # Bytes received:                   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_Throughput_KPIs_2023213-17020-800

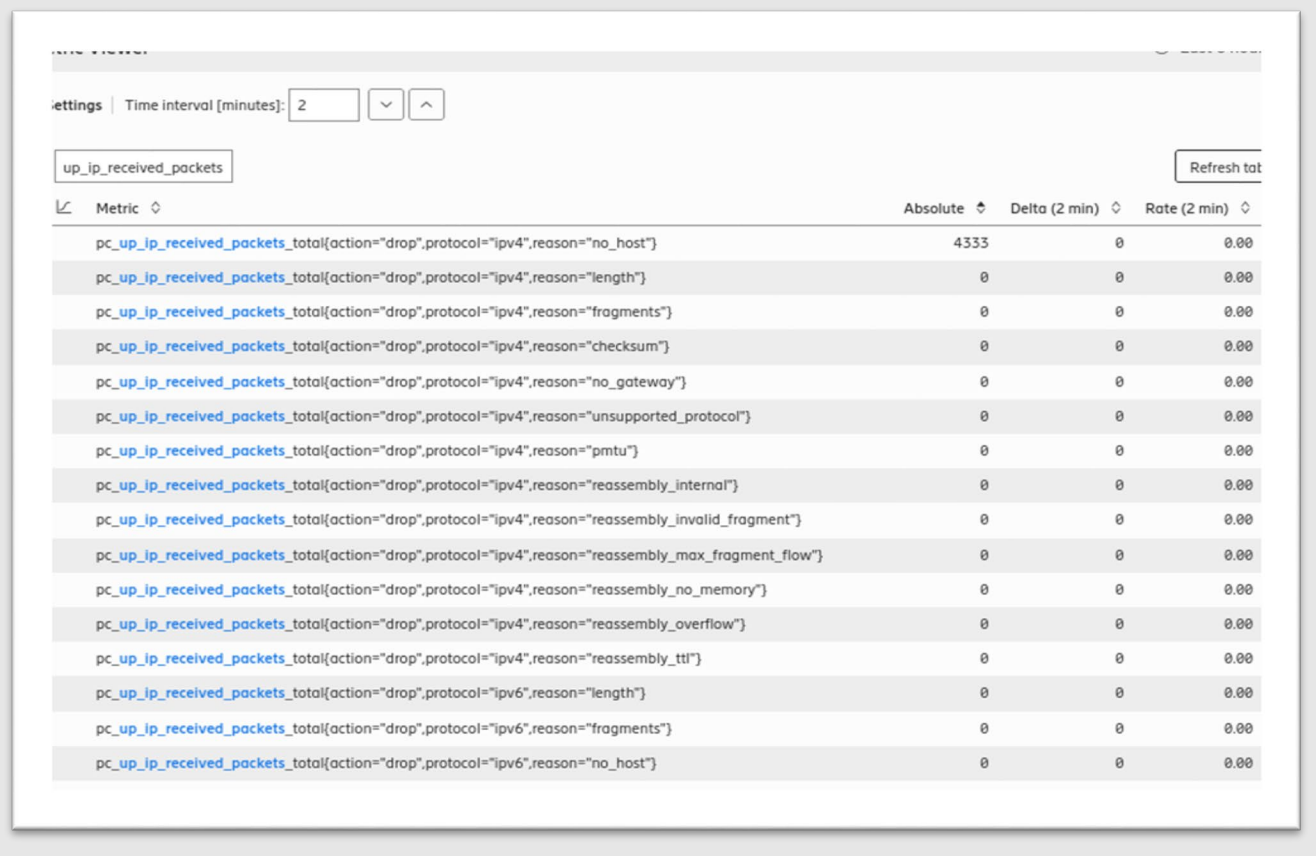
Now	1h ago	3h ago	6h ago	12h ago	24h ago	Name
514,361.60	0	0	0	0	0	GTP T-PDU in (b
8,915,707.73	0	0	0	0	0	GTP T-PDU out (
-	0	0	0	0	0	IP in (bps)
-	0	0	0	0	0	IP out (bps)
616.27	0	0	0	0	0	GTP T-PDU in (p
973.47	0	0	0	0	0	GTP T-PDU out (
-	0	0	0	0	0	IP in (pps)
-	0	0	0	0	0	IP out (pps)
5.76	6.71	6.71	6.71	6.71	6.71	Packet Drop Rat

Core_Throughput_KPIs_2023213-17027-929

Now	1h ago	3h ago	6h ago	12h ago	24h ago	Name
-	0	0	0	0	0	GTP T-PDU in (
-	0	0	0	0	0	GTP T-PDU out
8,915,707.73	0	0	0	0	0	IP in (bps)
514,361.60	0	0	0	0	0	IP out (bps)
-	0	0	0	0	0	GTP T-PDU in (
-	0	0	0	0	0	GTP T-PDU out
973.47	0	0	0	0	0	IP in (pps)
616.27	0	0	0	0	0	IP out (pps)
91.25	106.66	106.66	106.66	106.66	106.66	Packet Drop Ra

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.



ettings | Time interval [minutes]: 2

up_ip_received_packets

Refresh tat

Metric	Absolute	Delta (2 min)	Rate (2 min)
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="no_host"}	4333	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="length"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="fragments"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="checksum"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="no_gateway"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="unsupported_protocol"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="pmtu"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_internal"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_invalid_fragment"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_max_fragment_flow"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_no_memory"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_overflow"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv4",reason="reassembly_ttl"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv6",reason="length"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv6",reason="fragments"}	0	0	0.00
pc_up_ip_received_packets_total{action="drop",protocol="ipv6",reason="no_host"}	0	0	0.00

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
CP	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
E-UTRA	Evolved Universal Mobile Telecommunications System (UMTS) Terrestrial 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
TC	Test Case
TDD	Time Division Duplex
TLS	Transport Layer Security
TP	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.