सत्यमेव जयते

अनंतिम परीक्षण निर्देशिका
टीईसी २११४१:२०२६

PROVISIONAL TEST GUIDE
TEC 21141:2026

फिक्स्ड वायरलेस एक्सेस ग्राहक परिसर उपकरण
Fixed Wireless Access Customer Premises Equipment

(**जीआर सं**: टीईसी २११४०:२०२६)

(**GR No.:** TEC 21140:2026)

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
दूरसंचार विभाग, संचार मंत्रालय, भारत सरकार
खुर्शीदलाल भवन, जनपथ, नई दिल्ली – ११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE
DEPARTMENT OF TELECOMMUNICATIONS, MINISTRY OF COMMUNICATIONS
GOVERNMENT OF INDIA, KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI-110001, INDIA
www.tec.gov.in

Release : ______ 2026

FORWARD

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Standards for Generic Requirements (GR), Interface Requirements (IR) and Service Requirements (SR) as well as Test guides for Telecom Products and Services;
- Issue of Technical regulations in the form of essential Requirements (ER);
- Field evaluation of products and Systems;
- National Fundamental Plans;
- Support to DOT on technology issues;
- Testing & Certification of Telecom products; and
- Designation of Conformance Assessment Bodies (CABs) for testing.

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document enumerates detailed test schedule and procedure for evaluating conformance / functionality / requirements / performance of Fixed Wireless Access Customer Premises Equipment as per GR/IR/Applicant’s spec. No GR No.: TEC: 21140:2026.

CONTENTS

A. HISTORY SHEET

Sl. No.	TSTP No.	Equipment/Interface	Issue
1.	TEST GUIDE No.: TEC 21141:2026	Fixed Wireless Access Customer Premises Equipment	Release 1

B. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance / functionality / requirements / performance of Fixed Wireless Access Customer Premises Equipment as per GR/IR/Applicant’s spec. No GR No.: TEC: 21140:2026.

C. General information:

Sn.	General Information [	Details *(to be filled by testing team)*	
1	Name and Address of the Applicant		
2	Date of Registration		
3	Name and No. of GR/IR/Applicant's Spec. against which the approval sought		
4	Details of Equipment		
	Type of Equipment	Model No.	Serial No.
(i)			
(ii)			
5	Any other relevant Information: -		

D. Testing team: *(to be filled by testing team)*

Sno.	Name	Designation	Organization	Signature
1.				
2.				

E. List of the Test Instruments:

Sno.	Name of the test instrument	Make /Model *(to be filled by testing team)*	Validity of calibration *(to be filled by testing team)*
1			dd/mm/yyy
2			
3			
4			
5			
6			
7			
8			

F. Equipment Configuration Offered: (to be filled by testing team)

(a) < Equipment/product name> Configuration:

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

(b) < Other equipment name> Configuration:

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

G. Equipment/System Manuals: *(to be filled by testing team)*

Availability of Maintenance manuals, Installation manual, Repair manual & User Manual etc. (Y/N)

H. Clause-wise Test Type and Test No.:

Clause No	Clause Description	Type of Test / Test No. etc. *
1	**Introduction**	
1.1	**Scope** This document is the standard for Generic Requirements (GR) of Fixed Wireless Access Customer Premises Equipment (FWA CPE), covering common features across 4G, 5G Non-Standalone (NSA), and 5G Standalone (SA) technologies. It also includes specific requirements that apply only to certain technologies. The requirements are grouped into important areas such as Radio/RRC/NAS, support for multiple APNs to separate different services, Quality of Service, Voice Services, Networking Features, Wi-Fi, IDU/ODU Interworking and Resilience, Device Management, and Security. For each area, it is clearly mentioned whether the requirement applies to Indoor FWA devices, Outdoor FWA devices, or both.	1. Submit the FWA CPE system datasheet and complete network architecture diagram clearly depicting all supported interfaces applicable to the equipment.
1.2	**Overview** Fixed Wireless Access (FWA) has emerged as a widely adopted and cost-effective solution for providing ultrabroadband Internet, especially in areas where wireline infrastructure like FTTx has not been deployed. FWA uses wireless radio links to connect customers to a service provider’s mobile	Explanatory Only

	network using standardized 4G/4G+/5G technologies. A typical FWA setup includes either an indoor unit (1-box) or a combination of an indoor and outdoor unit (2-box solution). These devices offer end-users high-speed internet through Wi-Fi, Ethernet ports, and voice connectivity via FXS ports for analog phones. While the radio interface (4G/5G) is standardized, several other critical features of FWA devices remain unstandardized. For example, remote management practices vary, with some operators using BBF TR-069/TR-369 and ACS platforms, while others rely on proprietary solutions. Voice service is another complex area—many FWA devices use VoLTE (IR.92 stack)/VoNR Stack, which is ideal for mobile phones but often lacks features needed for PSTN-like landline services. As a result, many operators deploy VoIP stacks, which require custom design, integration, and testing, increasing complexity and cost. In 2-box FWA setups, the Outdoor Unit (ODU) connects to the mobile network, while the Indoor Unit (IDU) provides Wi-Fi, Ethernet, and voice services. These units	

	typically connect via a Gigabit Ethernet cable with Power-over-Ethernet (PoE) to power the ODU. However, there is no open standard for the interface between IDU and ODU. Often, both units come from the same vendor and use proprietary protocols, limiting interoperability. Many operators now advocate for an open and standardized IDU-ODU interface to allow mixing and matching devices based on specific needs—such as consumer or enterprise use cases—thereby enabling greater flexibility and innovation.	
1.3	Architecture A FWA Device offers the typical features of a Home Router (also known as Residential Gateway) and connects to a 3GPP-based network via a Radio Interface. The two architectural models considered in this document are: indoor FWA solution and outdoor FWA solution. In the indoor FWA solution, a single box comprises all the functions and interfaces needed to deliver the Ultrabroadband Internet services to the end user. In the outdoor FWA solution, the functions are split between an Outdoor Unit (ODU), which connects to the mobile network with the	Explanatory Only

	radio interface, and an Indoor Unit (IDU), which offers all the functions and interfaces for the LAN network: Wi-Fi access point, Voice interface, networking functions (e.g. port mapping, Firewall), etc. While the indoor solution is clearly a single-tenant solution, different architectural alternatives are possible for outdoor FWA solutions. In particular, outdoor solutions can be single-tenant or multi-tenant: in a single-tenant solution, an Outdoor Unit is dedicated to a single customer and is connected with a point-to-point link with an Indoor Unit. In a multi-tenant solution, an Outdoor Unit serves multiple customers, and several Indoor Units are connected to it. Another possible option of the architecture of outdoor solutions is the interface between ODU and IDU. This document defines an open, standard interface between ODU and IDU; therefore, ODUs and IDUs from different manufacturers can be matched and combined.	
1.3.1	**Indoor FWA Solution**	Explanatory Only
1.3.2	**Outdoor FWA Solution**	Explanatory Only
2.	**Functional Requirements (Common)**	
2.1	**Radio/RRC/NAS common requirements**	

2.1.1	The FWA device shall support one (1) SIM/USIM. FWA Devices with multiple SIMs are outside the scope of this document.	GR_TSTP_2.1.1
2.1.2	The FWA device may be equipped with one (1) eSIM, instead of a physical SIM.	GR_TSTP_2.1.2
2.1.3	The Indoor FWA Device (1-box solution) shall support the establishment of at least 3 PDNs/PDUs (e.g. for data/remote management, video, and voice services).	GR_TSTP_2.1.3
2.1.4	The Outdoor Unit of an Outdoor FWA Solution (2-box) shall support the establishment of at least 4 PDNs/PDUs (e.g. for remote management of ODU, data/remote management of IDU, video, and voice services).	GR_TSTP_2.1.4
2.1.5	The FWA Device shall allow configurable associations between PDN/PDU connections and services/applications (e.g. voice, video; VLAN settings via Web UI).	GR_TSTP_2.1.5
2.1.6	The FWA device should support the establishment of at least 6 PDNs/PDUs.	GR_TSTP_2.1.6

2.1.7	For each PDNs/PDUs, the FWA Device shall allow to configure:
	a. Protocol stack (IPv4, IPv6, IPv4/v6);
	b. Authentication option (PAP/CHAP);
	c. MTU/MSS
		GR_TSTP_2.1.7

2.2	**Quality of Service**	
2.2.1	The FWA Device shall comply with the 3GPP standards 3GPP TS 23.207 and 3GPP TS 23.203, regardless of deployment scenario (e.g., 4G, 5G NSA, 5G SA).	GR_TSTP_2.2.1
2.2.2	If a wireless service provider utilizes customized QoS for specific category of subscribers including mission critical organizations, government entities and enterprise customers, the FWA device should comply with the wireless service provider's requirements and mandates.	GR_TSTP_2.2.2
2.3	**Voice Service (Optional)** Voice Service requirements apply to the Indoor FWA Device and to the Indoor Unit of an Outdoor FWA Solution (optional as per procurer requirements).	
2.3.1	Indoor FWA Device (1-box solution) shall support voice service either by means of VoLTE /VoNR technology or VoIP technology.	GR_TSTP_2.3.1
2.3.2	The Indoor Unit of an Outdoor FWA Solution (2-box) shall support voice service uniquely by means of VoIP technology.	GR_TSTP_2.3.2
2.3.3	In case of VoLTE/VoNR Technology, the FWA Device shall be compliant to GSMA IR.92 profile.	GR_TSTP_2.3.3
2.3.4	In case of VoNR Technology, the FWA Device shall be compliant to	GR_TSTP_2.3.4

	GSMA NG.114 profile.	
2.3.5	In case of VoIP technology, the FWA Device shall be compliant to 3GPP specification 24.229, with the profile defined in the following sections 3.3.2, 3.3.3 and, optionally, 3.3.5 of GSMA TS.64 FWA Devices Architecture and Requirements Version 1.0.	GR_TSTP_2.3.5
2.3.6	In case of VoIP technology, the FWA Device shall request a dedicated PDN Connection. The PDN Connection for VoIP traffic may be characterized with a dedicated QCI. Note: Voice Traffic includes SIP, RTP, RTCP and DNS traffic used to resolve the P-CSCF FQDN in order to get the P-CSCF addresses.	GR_TSTP_2.3.6
2.3.7	It shall be possible to disable all voice features.	GR_TSTP_2.3.7
2.3.8	The FWA Device shall be customizable in order not to have any FXS port or other voice interfaces	GR_TSTP_2.3.8
2.4	**Networking Features**	
2.4.1	**Interfaces**	
2.4.1.1	The indoor FWA Device and the Indoor Unit of an Outdoor FWA Solution shall support at least two Gigabit Ethernet LAN ports, compliant to IEEE 802.3ab standard.	GR_TSTP_2.4.1.1
2.4.1.2	For the physical interfaces for LAN Ethernet, the 10 100 1000BASE-T electrical interface should be used.	GR_TSTP_2.4.1.2

2.4.1.3	Different physical interfaces for LAN Ethernet, compliant to the standards, e.g. 10 100 1000BASE-TX, may be used in alternative to 10 100 1000BASE-T, depending on market and procurer needs.	GR_TSTP_2.4.1.3
2.4.1.4	The Indoor Unit and the Outdoor Unit of an Outdoor FWA Solution shall have a connection coherent with the LAN-WAN capability of the Device.	GR_TSTP_2.4.1.4
2.4.1.5	For the physical interfaces for the IDU-ODU, if Ethernet is used, the BASE-T electrical interface should be used.	GR_TSTP_2.4.1.5
2.4.1.6	If Ethernet is used for the IDU-ODU connection, different physical interfaces, compliant to the standards, e.g. 1000BASE-TX, may be used in place of BASE-T, depending on market and procurer needs.	GR_TSTP_2.4.1.6
2.4.2	**Performance**	
2.4.2.1	The 4G FWA Device shall offer an aggregate throughput of at least 1 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.	GR_TSTP_2.4.2.1

2.4.2.2	The 4G FWA Device should offer an aggregate throughput of at least 2.5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.	GR_TSTP_2.4.2.2
2.4.2.3	The 5G FWA Device shall offer an aggregate throughput of at least 2.5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.	GR_TSTP_2.4.2.3
2.4.2.4	The 5G FWA Device should offer an aggregate throughput of at least 5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.	GR_TSTP_2.4.2.4
2.4.2.5	The 4G FWA Device shall offer a throughput LAN-WAN coherent with the LTE UE Category of the Device, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length and not affected by the local LAN-LAN throughput.	GR_TSTP_2.4.2.5
2.4.2.6	The 5G FWA Device shall offer a throughput LAN-WAN coherent with 5G cellular bandwidth of the FWA Device, irrespective of IPv4 or IPv6 protocol, irrespective of Packet	GR_TSTP_2.4.2.6

	Length and not affected by the local LAN-LAN throughput.	
2.4.3	**Protocols**	
2.4.3.1	The FWA Device shall support Internet Protocol version 4 (IPv4), defined in IETF RFC 791.	GR_TSTP_2.4.3.1
2.4.3.2	The FWA Device shall support Internet Protocol version 6 (IPv6), defined in IETF RFC 8200 and further amendments defined by IETF.	GR_TSTP_2.4.3.2
2.4.3.3	The FWA Device shall support Address Resolution Protocol (ARP), defined in IETF RFC 826 and further amendments (IETF RFC 5227, IETF RFC 5494).	GR_TSTP_2.4.3.3
2.4.3.4	The FWA Device shall support Network Discovery Protocol for IPv6 (NDP) defined in IETF RFC 4861 and further amendments defined by IETF.	GR_TSTP_2.4.3.4
2.4.3.5	The FWA Device shall support Internet Control Message Protocol (ICMP) defined in IETF RFC 792 and further amendments defined by IETF (RFC 950, RFC 4884, RFC 6633, RFC 6918).	GR_TSTP_2.4.3.5
2.4.3.6	The FWA Device shall support Internet Control Message Protocol version 6 for IPv6 (ICMPv6) defined in IETF RFC 4443.	GR_TSTP_2.4.3.6

2.4.3.7	The FWA Device shall implement a Network Time Protocol (NTP) client as defined in IETF RFC 5905 and further amendments.	GR_TSTP_2.4.3.7
2.4.3.8	The FWA Device shall support Internet Group Management Protocol, version 3 (IGMPv3), defined in IETF RFC 3376.	GR_TSTP_2.4.3.8
2.4.3.9	The FWA Device shall support IGMP Proxy as defined in IETF RFC 4605.	GR_TSTP_2.4.3.9
2.4.3.10	The FWA Device shall support QoS Treatment both at level 2 (p-bits of 802.1q VLAN Tag) and at level 3 (Differentiated Services Code Point of the IP header).	GR_TSTP_2.4.3.10
2.4.3.11	The FWA Device shall support the Differentiated Services (DiffServ) architecture and behaviors defined in RFC 2474, 2475, 2597, 3246 and 3260.	GR_TSTP_2.4.3.11
2.4.3.12	The behaviors of traffic classification, marking, remarking, queuing, scheduling, policing, shaping shall be applicable both to internally generated traffic and to traffic coming from LAN and destined to the WAN.	GR_TSTP_2.4.3.12
2.4.3.13	At least four queues shall be supported on the WAN interface, of which one with Strict Priority scheduling, and the others with configurable scheduling mechanisms (e.g. Weighted Fair Queuing, Weighted	GR_TSTP_2.4.3.13

	Round Robin).	
2.4.3.14	The FWA Device should support a secondary IPv4 addressing on LAN, in order to enable the assignment of public IP addresses to hosts in LAN.	GR_TSTP_2.4.3.14
2.4.3.15	The FWA Device shall support VLAN Tagging, compliant to IEEE 802.1q standard.	GR_TSTP_2.4.3.15
2.4.4	**DHCP**	
2.4.4.1	The FWA Device shall support Dynamic Host Configuration Protocol (DHCP) defined in IETF RFC 2131.	GR_TSTP_2.4.4.1
2.4.4.2	The FWA Device shall support DHCP Options defined in IETF RFC 2132.	GR_TSTP_2.4.4.2
2.4.4.3	The FWA device may implement DHCP options 60 and 43 for automatic provision of ACS parameters.	GR_TSTP_2.4.4.3
2.4.4.4	In case of multiple connections from the same FWA device, FWA device shall implement DHCP option 82 and 37 for client identifications and policy enforcement.	GR_TSTP_2.4.4.4
2.4.4.5	The DHCP Server implemented by the FWA Device shall manage at least 254 addresses.	GR_TSTP_2.4.4.5
2.4.4.6	It shall be possible to define any IPv4 Unicast subnet for the private LAN and DHCP	GR_TSTP_2.4.4.6

	pool.	
2.4.4.7	The DHCP Server implemented by the FWA Device shall support Duplicate Address Detection (DAD) functionality.	GR_TSTP_2.4.4.7
2.4.4.8	The DHCP Server implemented by the FWA Device shall provide a mechanism for IP reservation on MAC Address basis, assigning the same IP address (if available) at the same MAC Address.	GR_TSTP_2.4.4.8
2.4.4.9	The FWA Device shall support hostnames presented by the hosts (DHCP clients) with DHCP Option 12.	GR_TSTP_2.4.4.9
2.4.4.10	The FWA Device shall properly manage the cases of overlapping hostnames and hostnames not presented by clients, by assigning to client's unambiguous hostnames by means of Option 12.	GR_TSTP_2.4.4.10
2.4.4.11	The FWA Device shall support Dynamic Host Configuration Protocol for IPv6 (DHCPv6) defined in IETF RFC 8415.	GR_TSTP_2.4.4.11
2.4.4.12	The FWA Device shall support Prefix Delegation for IPv6 (DHCPv6) defined in IETF RFC 8415.	GR_TSTP_2.4.4.12
2.4.4.13	The FWA Device shall support Prefix Exclude for IPv6 (DHCPv6) defined in IETF RFC 8415.	GR_TSTP_2.4.4.13

2.4.5	**NAT & Bridge operation**	
2.4.5.1	The FWA Device shall support IP Network Address Translator (NAT) as defined in IETF RFC 3022.	GR_TSTP_2.4.5.1
2.4.5.2	The Network Address Translator functionality implemented by the FWA Device shall be compliant to the behaviors defined in IETF RFC 4787.	GR_TSTP_2.4.5.2
2.4.5.3	The FWA Device shall implement a configurable Port Mapping/Virtual Server functionality, allowing the creation of entries for mapping protocols/ports on the WAN side of the FWA Device to an IP address and protocols/ports on the private LAN.	GR_TSTP_2.4.5.3
2.4.5.4	It shall be possible to configure at least 32 Port Mapping entries.	GR_TSTP_2.4.5.4
2.4.5.5	The FWA Device shall support Customer-side Translator (CLAT) functionality according to IETF RFC 6145	GR_TSTP_2.4.5.5
2.4.5.6	The FWA Device shall support operation in Bridge Mode. In this configuration both DHCP and NAT operations are provided by the network being bridged to.	GR_TSTP_2.4.5.6
2.4.5.7	The FWA Device shall implement a configurable Application Layer Gateway functionality (ALG), as	GR_TSTP_2.4.5.7

	defined in IETF RFC 2663, at least for the following protocols: SIP, IPSec, PPTP, L2TP.	
2.4.6	**MTU**	
2.4.6.1	The FWA Device shall support a default MTU size of 1380 bytes.	GR_TSTP_2.4.6.1
2.4.6.2	The FWA Device shall support network override of the default MTU size in IPv4 operation via Protocol Configuration Options (3GPP TS 24.008).	GR_TSTP_2.4.6.2
2.4.6.3	The FWA Device shall support network override of the default MTU size in IPv6 operation via Router Advertisement.	GR_TSTP_2.4.6.3
2.4.7	**DNS**	
2.4.7.1	The FWA Device shall support Domain Name System (DNS) compliant to IETF RFC 1034, RFC 1035 and further amendments defined by IETF	GR_TSTP_2.4.7.1
2.4.7.2	The FWA Device shall be able, on a configuration basis, to act as DNS Server for the Hosts in LAN.	GR_TSTP_2.4.7.2
2.4.7.3	The FWA Device shall be able to advertise the DNS server(s) to the Hosts in LAN via DHCP protocol. On a configuration basis, the advertised DNS server(s) can be: a. The FWA Device itself, if it’s	GR_TSTP_2.4.7.3

	configured to act as a DNS Server; b. The DNS server addresses received from the network, if the FWA Device is not configured to act as a DNS Server; c. Optionally, other DNS Server addresses configured on the FWA Device.	
2.4.7.4	The FWA Device shall support a configurable Dynamic DNS (DDNS) Service, allowing the FWA Device to be addressable from the Internet with an FQDN.	GR_TSTP_2.4.7.4
2.4.7.5	For the Dynamic DNS service, the FWA Device shall send updates to the DDNS server not periodically, but only whenever an IP address change is detected on the Data WAN Interface.	GR_TSTP_2.4.7.5
2.4.7.6	For Static DNS operation the FWA Device shall support Recursive DNS and not Iterative DNS.	GR_TSTP_2.4.7.6
2.4.7.7	The FWA Device shall support unencrypted DNS access.	GR_TSTP_2.4.7.7
2.4.7.8	The FWA Device shall support DNS access via HTTPS (IETF RFC 8484).	GR_TSTP_2.4.7.8
2.4.7.9	The FWA Device shall support DNS access via TLS.	GR_TSTP_2.4.7.9
2.4.7.10	The FWA device shall be protected against DNS Rebind	GR_TSTP_2.4.7.10

	Vulnerability.	
2.4.7.11	To prevent DNS spoofing, source ports and Transaction-IDs shall be selected randomly by the CPE.	GR_TSTP_2.4.7.11
2.4.8	**Security**	
2.4.8.1	The FWA Device shall implement a configurable DeMilitarized Zone (DMZ) functionality, allowing an internal host in LAN to be fully exposed on WAN.	GR_TSTP_2.4.8.1
2.4.8.2	The FWA Device shall implement a configurable Port Binding functionality, allowing binding of the WAN connections to none, one or more LAN interfaces (including Wi-Fi SSIDs).	GR_TSTP_2.4.8.2
2.4.8.3	The FWA Device shall implement a configurable Filtering functionality, allowing the creation of entries for blocking/allowing the communication of MAC Addresses on LAN towards specific IP address/range, on specific protocols/ports/port range.	GR_TSTP_2.4.8.3
2.4.8.4	It shall be possible to configure at least 32 Filtering entries.	GR_TSTP_2.4.8.4
2.4.8.5	The FWA Device should implement a configurable (on/off) UPnP Discovery functionality, compliant with the UPnP Forum's Device Architecture and Device Control Protocols standards.	GR_TSTP_2.4.8.5

2.4.8.6	UPnP functionality shall be blocked on the WAN side.	GR_TSTP_2.4.8.6
2.4.8.7	If the FWA Device supports UPnP, it should be disabled in Factory default configuration.	GR_TSTP_2.4.8.7
2.4.8.8	If the FWA Device supports UPnP, rules created for one client device shall apply only to that device and not to other LAN clients (also for the FWA Device itself).	GR_TSTP_2.4.8.8
2.4.8.9	The FWA Device should implement a configurable VPN functionality, both as a VPN-client and a VPN-server, with L2TP/IPSec PSK or PPTP.	GR_TSTP_2.4.8.9
2.4.8.10	The FWA Device shall implement a Parental Control functionality, letting the user to configure a list of URLs which access must be denied to all (or a configurable subset of) LAN hosts.	GR_TSTP_2.4.8.10
2.4.8.11	The FWA Device shall implement a per-user device configurable Internet access control functionality, letting the user to configure, for a selected user device, which days of the week/which hours of the day or how many hours per day the Internet access must be allowed/denied.	GR_TSTP_2.4.8.11
2.4.8.12	The FWA Device shall implement a configurable (at least with on/off behaviors) stateful IPv4 Firewall.	GR_TSTP_2.4.8.12

2.4.8.13	The FWA Device shall implement Denial of Service (DoS) protection functionality.	GR_TSTP_2.4.8.13
2.4.8.14	The DoS functionality shall remain enabled even when the Firewall has been disabled by user configuration.	GR_TSTP_2.4.8.14
2.4.8.15	The behavior of the FWA Device to ICMP messages coming from WAN interface shall be configurable.	GR_TSTP_2.4.8.15
2.4.8.16	The FWA Device shall implement a configurable (at least with on/off behaviors) stateful IPv6 Firewall.	GR_TSTP_2.4.8.16
2.4.8.17	The IPv6 and IPv4 firewall shall be independently configurable.	GR_TSTP_2.4.8.17
2.4.8.18	The IPv6 and IPv4 firewall status shall be presented independently.	GR_TSTP_2.4.8.18
2.4.8.19	The FWA Device shall NOT allow outgoing traffic originated from a LAN IP address outside the range defined by the FWA Device itself.	GR_TSTP_2.4.8.19
2.4.8.20	In Factory Reset condition, the status of the firewall shall be enabled	GR_TSTP_2.4.8.20
2.4.8.21	The FWA CPE device shall comply to the security requirements mentioned in the applicable Indian Telecommunication Security Assurance Requirements (ITSAR) as and when notified by National Centre for	Security Certificate issued by NCCS may be submitted.

	communication Security (NCCS).	
2.4.9	**Customisation**	
2.4.9.1	It shall be possible for a procurer to customize a FWA Device in addition to the requirements mentioned.	GR_TSTP_2.4.9.1
2.4.10	**USB Port (optional)**	
2.4.10.1	The FWA Device shall support a Universal Serial Bus (USB) interface.	GR_TSTP_2.4.10.1
2.4.10.2	The USB interface shall be compliant to the Universal Serial Bus Specification version 3.1 or higher.	GR_TSTP_2.4.10.2
2.4.10.3	The USB Interface receptacle shall be any of Type-A, Type-Micro B or Type-C.	GR_TSTP_2.4.10.3
2.4.10.4	The USB Interface shall supply a current of at least 1.5A.	GR_TSTP_2.4.10.4
2.4.10.5	The FWA Device should use SMBv2 (or higher) protocol to enable the sharing of an USB Mass Storage Hard Disk Devices between LAN hosts.	GR_TSTP_2.4.10.5
2.4.10.6	The FWA Device should use SMBv2 (or higher) protocol to enable the print sharing between the LAN hosts, supporting the standard error messages via SMB	GR_TSTP_2.4.10.6

	protocol.	
2.4.10.7	The FWA Device shall NOT support SMBv1 protocol.	GR_TSTP_2.4.10.7
2.4.10.8	The USB Interface shall block firmware upgrade, logging, tracing and similar local management and troubleshooting activities on the FWA Device.	GR_TSTP_2.4.10.8
2.5	**WIFI (Optional)**	
2.5.1.	**Standards**	
2.5.1.1	The FWA Device shall integrate a Wi-Fi 4 (IEEE 802.11n) Access Point (AP), or later standards, operating on 2.4 GHz bands.	GR_TSTP_2.5.1.1
2.5.1.2	The FWA Device shall integrate a Wi-Fi 5 (IEEE 802.11ac) Access Point (AP), or later standards, operating on 5 GHz bands.	GR_TSTP_2.5.1.2
2.5.1.3	The FWA Device should integrate a Wi-Fi 6 (IEEE 802.11ax) Access Point (AP), or later standards, operating on both 2.4 and 5 GHz bands.	GR_TSTP_2.5.1.3
2.5.1.4	The FWA Device may integrate a Wi-Fi 6E (IEEE 802.11ax) Access Point (AP), or later standards, operating on 2.4, 5 and 6 GHz bands.	GR_TSTP_2.5.1.4
2.5.1.5	The FWA Device may integrate a Wi-Fi 7 (IEEE 802.11be) Access Point (AP), or later standards,	GR_TSTP_2.5.1.5

	operating on 2.4,5 and 6 GHz bands.	
2.5.1.6	The Wi-Fi AP of a FWA Device shall comply to the TEC ER of WiFi Access Point and CPE.	MTCTE Certificate issued by TEC may be submitted.
2.5.1.7	The FWA Device shall comply to WPA3 and Wi-Fi Protected Setup (PBC).	GR_TSTP_2.5.1.7
2.5.2	**MIMO Capabilities, Bandwidth, Modulation and Coding schemes**	
2.5.2.1	The Wi-Fi AP of a FWA Device shall support at least MIMO 2x2 on all supported frequency bands.	GR_TSTP_2.5.2.1
2.5.2.2	The Wi-Fi AP of a FWA Device should support MIMO 4x4 on all supported frequency bands.	GR_TSTP_2.5.2.2
2.5.2.3	The Wi-Fi AP of a FWA Device may support MIMO higher than 4x4 on some or all supported frequency bands.	GR_TSTP_2.5.2.3
2.5.2.4	An 802.11n AP of a FWA Device shall support a bandwidth of 40 MHz.	GR_TSTP_2.5.2.4
2.5.2.5	An 802.11ac AP of a FWA Device shall support a bandwidth of 80 MHz in the 5 GHz band.	GR_TSTP_2.5.2.5
2.5.2.6	An 802.11ax AP of a FWA Device shall support a bandwidth of 40 MHz in the 2.4 GHz band.	GR_TSTP_2.5.2.6
2.5.2.7	An 802.11ax AP of a FWA Device shall support a bandwidth of 80 MHz in the 5 GHz band.	GR_TSTP_2.5.2.7

2.5.2.8	An 802.11ax AP of a FWA Device should support a bandwidth of 160 MHz in the 5 GHz band.	GR_TSTP_2.5.2.8
2.5.2.9	An 802.11ax (Wi-Fi 6E) AP of a FWA Device should support a bandwidth of 160 MHz in the 6 GHz band.	GR_TSTP_2.5.2.9
2.5.2.10	An 802.11be (Wi-Fi 7) AP of a FWA Device should support a bandwidth of 320 MHz in the 6 GHz band.	GR_TSTP_2.5.2.10
2.5.2.11	An 802.11n AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 64-QAM with coding 5/6.	GR_TSTP_2.5.2.11
2.5.2.12	An 802.11ac AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 256-QAM with coding 5/6.	GR_TSTP_2.5.2.12
2.5.2.13	An 802.11ax/be AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 1024-QAM with coding 5/6.	GR_TSTP_2.5.2.13
2.5.3	**Performance**	
2.5.3.1	The AP of a FWA Device shall offer a throughput coherent with the theoretical maximum physical bit rate attainable by the AP characteristics, at least 70% of Maximum Physical Speed with TCP and UDP traffic in a “clean” environment.	GR_TSTP_2.5.3.1

2.5.3.2	All the Wi-Fi interfaces shall NOT exceed the regulatory limits as defined by WPC regards output power level (EIRP).	GR_TSTP_2.5.3.2
2.5.3.3	FWA device shall have the capability to perform the speedTest or other equivalent measures of initiating throughput tests by the Service Provider.	GR_TSTP_2.5.3.3
2.5.4	**Service Set Identifier (SSID)**	
2.5.4.1	The AP of a FWA Device shall permit the configuration of one main SSID for each supported band.	GR_TSTP_2.5.4.1
2.5.4.2	The AP of a FWA Device shall permit the configuration of at least one guest SSID.	GR_TSTP_2.5.4.2
2.5.4.3	The guest SSID(s) shall NOT permit the access to the configuration of the FWA Device.	GR_TSTP_2.5.4.3
2.5.4.4	The guest SSID(s) shall NOT permit traffic between hosts in LAN.	GR_TSTP_2.5.4.4
2.5.4.5	Each SSID shall be configurable to operate on one or more frequency bands.	GR_TSTP_2.5.4.5
2.5.4.6	Each SSID shall be configurable as regards the Authentication and Security mechanisms adopted.	GR_TSTP_2.5.4.6
2.5.4.7	Each SSID shall be configurable as regards the SSID broadcasting.	GR_TSTP_2.5.4.7
2.5.4.8	The default configuration of the FWA Device shall be	GR_TSTP_2.5.4.8

	with the same SSID for all supported bands.	
2.5.4.9	Based on procurer requirements, in the default configuration, the SSIDs may have an unambiguous, not-repeating value for each deployed FWA Device and not contain any information that consist of or are derived from data or parts of data that depend on the FWA device model itself.	GR_TSTP_2.5.4.9
2.5.5	**Channel and Bandwidth Selection**	
2.5.5.1	The AP of a FWA Device shall permit the manual channel selection on all supported bands.	GR_TSTP_2.5.5.1
2.5.5.2	The AP of a FWA Device shall support Automatic Channel Selection on all supported bands, in order to select the less interfered channels.	GR_TSTP_2.5.5.2
2.5.5.3	If enabled, the Automatic Channel Selection shall be performed every time the AP is turned on.	GR_TSTP_2.5.5.3
2.5.5.4	The AP of a FWA Device shall support Periodic Automatic Channel Selection.	GR_TSTP_2.5.5.4
2.5.5.5	The default value for Periodic Automatic Channel Selection should be 24 hours.	GR_TSTP_2.5.5.5
2.5.5.6	The Periodic Automatic Channel Selection shall be configurable by the procurer through customization.	GR_TSTP_2.5.5.6

2.5.5.7	The AP of a FWA Device shall permit the manual Bandwidth selection on all supported bands.	GR_TSTP_2.5.5.7
2.5.5.8	The AP of a FWA Device shall support Automatic Bandwidth Selection on all supported bands.	GR_TSTP_2.5.5.8
2.5.6	**Clients**	
2.5.6.1	The AP of a FWA Device shall support at least 64 clients.	GR_TSTP_2.5.6.1
2.5.7	**Security** The Security related requirements for the WiFi Access point shall comply with ITSAR Number: ITSAR702042504 (Group-IV Devices Common Security Requirements ITSAR) which covers Wi-Fi CPE (Customer Premises Equipment) device.	Security certificate by NCCS to be submitted by manufacturer.
2.5.8	The AP of a FWA Device may support WPS with Push Button mode in order to facilitate the association between clients and the AP of the FWA Device. If present, WPS shall be disabled by default and enabled only with full awareness of risks and only when physical access is strictly controlled.	GR_TSTP_2.5.8
2.5.9	The AP of a FWA Device shall support IEEE 802.11k industry standard for radio resource measurement	GR_TSTP_2.5.9

2.5.10	The AP of a FWA Device shall support Band Steering to steer clients from the more congested 2.4 GHz band to the less congested bands (5 GHz, and 6GHz if supported).	GR_TSTP_2.5.10
2.5.11	The Band Steering feature shall be manually configurable (ON/OFF selection).	GR_TSTP_2.5.11
2.5.12	The AP of a FWA Device shall support RF Mesh functionality.	GR_TSTP_2.5.12
2.5.13	The Wi-Fi Diagnostic solution shall collect data also from the other APs connected in mesh, as well as from the clients connected to those APs.	GR_TSTP_2.5.13
2.5.14	The AP of a FWA Device should support multimedia extensions in order to prioritize traffic in the Wireless Network according to Access Categories.	GR_TSTP_2.5.14
2.5.15	If multimedia extensions is supported; the FWA Device shall provide the mechanism to enable/disable the feature and to configure the mappings (Access Categories vs DSCP).	GR_TSTP_2.5.15
2.5.16	It shall be possible for a procurer to customize the settings of a FWA Device as regards Wi-Fi region/country of operation, enabled bands and channels, power transmission limits, SSIDs,	GR_TSTP_2.5.16

	passphrases.	
2.6	**IDU/ODU Interworking and Resilience**	
2.6.1	**Common requirements to bridge and routed modes of operation**	
2.6.1.1	The outdoor Unit (ODU) in an Outdoor FWA Solution, shall be able to map the traffic received on each PDN Connection / PDU Session, on different VLANs over the interface with the Indoor Unit (IDU), and vice versa.	GR_TSTP_2.6.1.1
2.6.1.2	The IDU shall be able to map the different traffic generated by the IDU itself or by hosts in LAN, and destined to the WAN, on different VLANs over the interface with the ODU, based on Service/VLAN mapping rules defined on the IDU.	GR_TSTP_2.6.1.2
2.6.1.3	The ODU shall be configurable in order to operate on each VLAN, either in bridged mode or in routed mode.	GR_TSTP_2.6.1.3
2.6.1.4	The ODU shall allow to configure one PDN connection / PDU session to be locally terminated in the ODU itself, that is to operate in routed mode without being mapped on a VLAN with the IDU. Note: for example, this connection may be dedicated to ODU Remote	GR_TSTP_2.6.1.4

	Management.	
2.6.2	**ODU Bridge Mode Operation**	
2.6.2.1	The Outdoor Unit (ODU) shall be able to operate in bridged mode, over one or more PDNs-PDUs/VLANs.	GR_TSTP_2.6.2.1
2.6.2.2	In bridged mode operation, the ODU shall use DHCP/DHCPv6 to assign to the IDU, on each VLAN, the network parameters received from the mobile network over a PDN/PDU a. IP Address b. DNS Servers IP Addresses (DHCP Option 6) Therefore, in bridge mode operation, the IP Address received on each PDN/PDU from the network, is not retained on the ODU itself, but is assigned to the IDU on the VLAN corresponding to that PDN/PDU	GR_TSTP_2.6.2.2
2.6.2.3	The ODU shall define, for each VLAN, the following parameters: a. Subnet Mask b. Default Gateway c. and assign them to the IDU by means of DHCP/DHCPv6. Note 1: this is needed because the mobile network does not provide a UE (specifically, the ODU) with	GR_TSTP_2.6.2.3

	such parameters over a PDN/PDU, while they are needed to properly configure the IDU with DHCP/DHCPv6. Note 2: Subnet Mask is DHCP Option 1, Default Gateway is DHCP Option 3 (Router).	
2.6.2.4	The ODU may define: a. For the Subnet Mask, a /30 (255.255.255.252) b. For the Default Gateway, the IP Address immediately after or before the one assigned to the IDU on each VLAN, following the rules of the Classless Inter-Domain Routing (CIDR).	GR_TSTP_2.6.2.4
2.6.3	**Reliability of IDU-ODU operation**	
2.6.3.1	If an APN is configured in bridged mode, the ODU shall guarantee that the IDU IP configuration will always be the same of the WAN (mobile) IP configuration.	GR_TSTP_2.6.3.1
2.6.3.2	As soon as the WAN (mobile) IP connection state changes, the ODU shall trigger the IDU IP Address renewal by means of a reset of the physical interface with the IDU.	GR_TSTP_2.6.3.2
2.6.4	**ODU Routed mode operation**	
2.6.4.1	The Outdoor Unit (ODU) shall be able to operate in routed mode, over one or more PDNs-PDUs/VLANs.	GR_TSTP_2.6.4.1

2.6.4.2	In routed mode operation, the ODU shall retain for itself the IP Address received from the mobile network over a APN/DNN.	GR_TSTP_2.6.4.2
2.6.4.3	In routed mode operation, the ODU shall be able to configure the IP Address of the IDU, on each VLAN configured in routed mode, by means of DHCP, using a private IP address pool.	GR_TSTP_2.6.4.3
2.6.4.4	In routed mode operation, if DHCP is used, then ODU shall provide via DHCP also: a. The DNS Server IP Address(es), which can be either the ODU itself or the Servers received from network; b. The Default Gateway (Router), which is the IP Address of the ODU over the IDU-ODU connection.	GR_TSTP_2.6.4.4
2.6.4.5	In routed mode operation, the ODU shall be able to manage statically configured addresses for: a.The IP Address of the IDU over the IDU-ODU connection: this is a directly connected interface b. The LAN of the IDU: this will be a subnet routed through the IP Address of the IDU. Note: Static IP Addressing, for the IDU-ODU connection, can be used as an alternative to DHCP.	GR_TSTP_2.6.4.5

2.6.4.6	In routed mode operation, the ODU shall perform NAT of traffic coming from the IDU and destined to the Network.	GR_TSTP_2.6.4.6
2.6.5	**Tunnels / VPNs**	
2.6.5.1	The IDU shall be able to establish, through the ODU, one or more Tunnels or VPN connections, based on IPSec or PPTP or GRE, over one or more VLANs, towards Tunnel/VPN Terminators in the network.	GR_TSTP_2.6.5.1
3	**Specific Functional Requirements**	
3.1	**For 5G NSA FWA Devices**	
3.1.1	The FWA device shall support standardized QCIs as specified in 3GPP TS 23.203.	GR_TSTP_3.1.1
3.1.2	The FWA device should support operator-specific QCIs as specified in 3GPP TS 23.203.	GR_TSTP_3.1.2
3.1.3	The FWA device shall be compliant with 3GPP E-UTRAN and NR Access Stratum Release 16 baseline or later.	GR_TSTP_3.1.3
3.1.4	The FWA device shall support periodical ANR measurements for reporting via the 4G network the Strongest NR Cells and related CGI (Cell Global	GR_TSTP_3.1.4

	Identity) when in ENDC operation.	
3.1.5	The FWA device should support periodical inter-RAT ANR measurements for reporting via the 4G network the Strongest NR Cells and related CGI (Cell Global Identity) when not in ENDC operation.	GR_TSTP_3.1.5
3.1.6	The FWA device shall support periodical inter-RAT ANR measurements for reporting via the NR network the Strongest 4G Cells and related CGI (Cell Global Identity).	GR_TSTP_3.1.6
3.1.7	The FWA device shall support periodical intra-RAT ANR measurements for reporting via the NR network the Strongest NR Cells and related CGI (Cell Global Identity).	GR_TSTP_3.1.7
3.1.8	The FWA device may be compliant to GSMA TS.24 for Antenna Performance acceptance values.	GR_TSTP_3.1.8
3.1.9	**Radio/RRC/NAS specific requirements for 5G-FR1 NSA FWA devices**	
3.1.9.1	The FWA device shall support EN-DC (Option 3x).	GR_TSTP_3.1.9.1
3.1.9.2	The FWA device shall support DSS technology.	GR_TSTP_3.1.9.2
3.1.9.3	The FWA device shall support rateMatchingResrcSetSemi -Static Information element	GR_TSTP_3.1.9.3

	in the Capability Information message.	
3.1.9.4	The FWA device shall support rateMatchingResrcSetDynamic Information element in the Capability Information message.	GR_TSTP_3.1.9.4
3.1.9.5	The FWA device shall support rateMatchingLTE-CRS Information element at least for one FDD mid-band (e.g. n1, n3) in the Capability Information message.	GR_TSTP_3.1.9.5
3.1.9.6	FWA device should support AdditionalDMRS-DL-Alt Information element in the Capability Information message.	GR_TSTP_3.1.9.6
3.1.9.7	The FWA device shall support NR SRS antenna switching 1T4R in 5G NR TDD high-bands (e.g. n77/n78).	GR_TSTP_3.1.9.7
3.1.9.8	The FWA device shall support NR SRS antenna switching 1T2R in 5G NR TDD mid- and low-bands.	GR_TSTP_3.1.9.8
3.1.9.9	The FWA device should support 2DL NR Inter-Band Carrier Aggregation.	GR_TSTP_3.1.9.9
3.1.9.10	The FWA device shall support UL split bearer to transmit concurrently on LTE and NR.	GR_TSTP_3.1.9.10
3.1.9.11	The FWA device shall support MIMO 4x4 DL capability on NR mid-bands	GR_TSTP_3.1.9.11

	(e.g. NR bands n77/n78).	
3.1.9.12	The FWA device shall support 4Rx diversity on NR bands.	GR_TSTP_3.1.9.12
3.1.9.13	The FWA device should support 8Rx diversity on NR bands.	GR_TSTP_3.1.9.13
3.1.9.14	The FWA device may support more than 8Rx diversity on NR bands.	GR_TSTP_3.1.9.14
3.1.9.15	The FWA device shall support 256QAM modulation for downlink.	GR_TSTP_3.1.9.15
3.1.9.16	The FWA device shall support 64QAM modulation for uplink.	GR_TSTP_3.1.9.16
3.1.9.17	The FWA device should support 256QAM modulation for uplink.	GR_TSTP_3.1.9.17
3.1.9.18	The FWA device shall support power class 3 (23 dBm).	GR_TSTP_3.1.9.18
3.1.9.19	The FWA device should support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1	GR_TSTP_3.1.9.19
3.1.9.20	The FWA device should support power class 1.5 (29 dBm) in compliance with 3GPP TS 38.101-1	GR_TSTP_3.1.9.20
3.1.9.21	The FWA device shall support 15 kHz Sub-Carrier Spacing in FR1 NR bands.	GR_TSTP_3.1.9.21
3.1.9.22	The FWA device shall support 30 kHz Sub-Carrier Spacing in FR1 NR bands.	GR_TSTP_3.1.9.22
3.1.9.23	The FWA device Should support all 3GPP Channel Bandwidths.	GR_TSTP_3.1.9.23
3.1.10	**Radio/RRC/NAS specific requirements for 5G-FR2 NSA FWA devices**	

3.1.10.1	The FWA device shall support EN-DC (Option 3x)	GR_TSTP_3.1.10.1
3.1.10.2	The FWA device shall support 2DL contiguous NR Carrier Aggregation.	GR_TSTP_3.1.10.2
3.1.10.3	The FWA device should support 2UL contiguous NR Carrier Aggregation	GR_TSTP_3.1.10.3
3.1.10.4	The FWA device shall support UL split bearer to transmit concurrently on LTE and NR.	GR_TSTP_3.1.10.4
3.1.10.5	The FWA device shall support MIMO 2 x 2 DL capabilities on NR FR2 bands (e.g., NR bands n257/n258).	GR_TSTP_3.1.10.5
3.1.10.6	The FWA device should support MIMO 4 x 4 DL capabilities on NR FR2 bands (e.g., NR bands n257/n258).	GR_TSTP_3.1.10.6
3.1.10.7	The FWA device shall support 64QAM modulation for downlink	GR_TSTP_3.1.10.7
3.1.10.8	The FWA device should support 256QAM modulation for downlink.	GR_TSTP_3.1.10.8
3.1.10.9	The FWA device shall support 64QAM modulation for uplink.	GR_TSTP_3.1.10.9
3.1.10.10	The FWA device should support 256QAM modulation for uplink.	GR_TSTP_3.1.10.10
3.1.10.11	The FWA device shall support power class 3 (23 dBm).	GR_TSTP_3.1.10.11
3.1.10.12	The FWA device should support power class 2 (26 dBm).	GR_TSTP_3.1.10.12
3.1.10.13	The FWA device should support power class 1 (31 dBm).	GR_TSTP_3.1.10.13
3.1.10.14	The FWA device shall support 100 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.1.10.14
3.1.10.15	The FWA device should support 200 MHz channel bandwidth in FR2 NR TDD	GR_TSTP_3.1.10.15

	bands (e.g., n257/n258).	
3.1.10.16	The FWA device should support 400 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.1.10.16
3.1.10.17	The FWA device shall support Cell Carriers with ax50Mhz + bx100MHz channel bandwidth in FR2 NR TDD bands (i.e N258 , N257) , where a & b represents integer numbers	GR_TSTP_3.1.10.17
3.1.10.18	The FWA device shall support 60 KHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.1.10.18
3.1.10.19	The FWA device shall support 120 KHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.1.10.19
3.1.11	**Antenna Performance Acceptance Values for 5G NSA FWA devices**	
3.1.11.1	The FWA device may be compliant to TS.24 for Antenna Performance acceptance values	GR_TSTP_3.1.11.1
3.2	**For 5G FWA Devices**	
3.2.1	The FWA device shall support Option 2 SA deployment option	GR_TSTP_3.2.1
3.2.2	The FWA device should support Option 4 NSA deployment option.	GR_TSTP_3.2.2
3.2.3	The FWA device shall be compliant with 3GPP NR Access Stratum Release 16 baseline or later	GR_TSTP_3.2.3

3.2.4	The FWA device shall support standardized 5QIs as specified in 3GPP TS 23.501	GR_TSTP_3.2.4
3.2.5	The FWA CPE shall comply with 5G NR security requirements as specified in 3GPP TS 33.501, including support for mandatory NR encryption, integrity protection, authentication algorithms, and SUCI-based registration as applicable to the UE category. Optional algorithms defined therein may be supported.	GR_TSTP_3.2.5
3.2.6	The FWA device shall support Initial 5GC Registration with SUCI, as per 3GPP TS 24.501. The FWA device may support 5G Slicing User Equipment Route Selection Policy (URSP) parameters.	GR_TSTP_3.2.6
3.2.7	The FWA device may be compliant to GSMA TS.24 for Antenna Performance acceptance values	GR_TSTP_3.2.7
3.2.8	The FWA device may support 5G Slicing Network Slice Selection Assistance Information (NSSAI) parameters, as per 3GPP TS 24.501	GR_TSTP_3.2.8
3.2.9	The FWA device may support SST (Slice/Service Type) and SD (Slice Differentiator) parameters.	GR_TSTP_3.2.9
3.2.10	The FWA device may support standardized SST	GR_TSTP_3.2.10

	values, as specified in 3GPP TS 23.501	
3.2.11	The FWA device should support all 3GPP Channel Bandwidths.	GR_TSTP_3.2.11
3.2.12	**Radio/RRC/NAS specific requirements for 5G-FR1 SA FWA devices.**	
3.2.12.1	The FWA device shall support SA option of connectivity to 5GC with Option-2 Architecture	GR_TSTP_3.2.12.1
3.2.12.2	The FWA device shall support 2DL NR Carrier Aggregation.	GR_TSTP_3.2.12.2
3.2.12.3	The FWA Device shall support all combinations of FDD and TDD duplexing (i.e., 2F, 2T, F+T and T+F) in 2DL NR Carrier Aggregation.	GR_TSTP_3.2.12.3
3.2.12.4	The FWA device should support 3DL NR Carrier Aggregation.	GR_TSTP_3.2.12.4
3.2.12.5	The FWA device may support 4DL NR Carrier Aggregation or higher order.	GR_TSTP_3.2.12.5
3.2.12.6	The FWA device should support 2UL NR Carrier Aggregation	GR_TSTP_3.2.12.6
3.2.12.7	The FWA device shall support 15 kHz Sub-Carrier Spacing in FR1 NR bands.	GR_TSTP_3.2.12.7
3.2.12.8	The FWA device shall support 30 kHz Sub-Carrier Spacing in FR1 NR bands.	GR_TSTP_3.2.12.8
3.2.12.9	The FWA device shall support MIMO 4x4 DL capability on NR high-bands (e.g. NR bands n77/n78).	GR_TSTP_3.2.12.9
3.2.12.10	The FWA device shall support MIMO 2x2 UL capability on NR high-bands (e.g. NR bands n77/n78).	GR_TSTP_3.2.12.10
3.2.12.11	The FWA device shall support 4Rx diversity on NR	GR_TSTP_3.2.12.11

	bands.	
3.2.12.12	The FWA device should support 8Rx diversity on NR bands	GR_TSTP_3.2.12.12
3.2.12.13	The FWA device may support more than 8Rx diversity on NR bands	GR_TSTP_3.2.12.13
3.2.12.14	The FWA device shall support 256QAM modulation for downlink.	GR_TSTP_3.2.12.14
3.2.12.15	The FWA device may support 1024QAM modulation for downlink on NR TDD FR1 high-bands (e.g. n77/n78).	GR_TSTP_3.2.12.15
3.2.12.16	The FWA device shall support 64QAM modulation for uplink.	GR_TSTP_3.2.12.16
3.2.12.17	The FWA device should support 256QAM modulation for uplink	GR_TSTP_3.2.12.17
3.2.12.18	The FWA device shall support power class 3 (23 dBm).	GR_TSTP_3.2.12.18
3.2.12.19	The FWA device should support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1	GR_TSTP_3.2.12.19
3.2.12.20	The FWA device should support power class 1.5 (29 dBm) or class 1 (31 dBm) in compliance with 3GPP TS 38.101-1.	GR_TSTP_3.2.12.20
3.2.13	**Radio/RRC/NAS specific requirements for 5G-FR2 SA FWA devices**	
3.2.13.1	The FWA device shall support SA option of connectivity to 5GC with Option-2 Architecture	GR_TSTP_3.2.13.1
3.2.13.2	The FWA device shall support 2DL intra-band contiguous NR Carrier Aggregation	GR_TSTP_3.2.13.2
3.2.13.3	The FWA device should support 4DL intra-band contiguous NR Carrier Aggregation	GR_TSTP_3.2.13.3

3.2.13.4	The FWA device may 8DL intra-band contiguous NR Carrier Aggregation	GR_TSTP_3.2.13.4
3.2.13.5	The FWA device should support 2UL intra-band contiguous NR Carrier Aggregation	GR_TSTP_3.2.13.5
3.2.13.6	The FWA device may support 4UL intra-band contiguous NR Carrier Aggregation	GR_TSTP_3.2.13.6
3.2.13.7	The FWA device shall support 100 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.2.13.7
3.2.13.8	The FWA device should support 200 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.2.13.8
3.2.13.9	The FWA device may support 400 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.2.13.9
3.2.13.10	The FWA device shall support Cell Carriers with [a x 50Mhz + b x100MHz] channel bandwidth in FR2 NR TDD bands (i.e N258 , N257) , where a & b represents integer numbers.	GR_TSTP_3.2.13.10
3.2.13.11	The FWA device shall support 60 kHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.2.13.11
3.2.13.12	The FWA device shall support 120 kHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).	GR_TSTP_3.2.13.12
3.2.13.13	The FWA device shall support MIMO 2x2 DL capability on NR FR2 bands (e.g., NR bands n257/n258)	GR_TSTP_3.2.13.13

3.2.13.14	The FWA device should support MIMO 4x4 DL capability on NR FR2 bands (e.g., NR bands n257/n258).	GR_TSTP_3.2.13.14
3.2.13.15	The FWA device shall support 64QAM modulation for downlink	GR_TSTP_3.2.13.15
3.2.13.16	The FWA device should support 256QAM modulation for downlink	GR_TSTP_3.2.13.16
3.2.13.17	The FWA device shall support 64QAM modulation for uplink	GR_TSTP_3.2.13.17
3.2.13.18	The FWA device should support 256QAM modulation for uplink	GR_TSTP_3.2.13.18
3.2.13.19	The FWA device shall support power class 3.	GR_TSTP_3.2.13.19
3.2.13.20	The FWA device should support power class 2 or class 1 in compliance with 3GPP TS 38.101-2.	GR_TSTP_3.2.13.20
3.3	**For 4G FWA Devices**	
3.3.1	**Radio/RRC/NAS specific requirements for 4G FWA devices**	
3.3.1.1	The FWA device shall be complaint with 3GPP E-UTRAN Access Stratum Release 12 baseline or later	GR_TSTP_3.3.1.1
3.3.1.2	The FWA CPE shall comply with EPS (LTE/EPC) security requirements as specified in 3GPP TS 33.401, including support for mandatory EPS encryption, integrity protection, and authentication algorithms applicable to the UE category. Optional EPS algorithms defined therein may be supported.	GR_TSTP_3.3.1.2
3.3.1.3	RRC, User Plane, and NAS security procedures shall be	GR_TSTP_3.3.1.3

	implemented in accordance with 3GPP TS 36.323 and TS 24.301	
3.3.1.4	In order to support the transmission techniques reported above, the FWA device shall support ue-CategoryDL 11 and ue-CategoryUL 5 or higher and all fallback configurations foreseen by the standard.	GR_TSTP_3.3.1.4
3.3.1.5	The FWA device should support ue-CategoryDL 12 and ue-CategoryUL 13 (Uplink CA support) or higher and all fallback configurations foreseen by the standard.	GR_TSTP_3.3.1.5
3.3.1.6	The FWA device shall support at least 3DL LTE Carrier Aggregation capability	GR_TSTP_3.3.1.6
3.3.1.7	The FWA device should support 2UL LTE Carrier Aggregation capability	GR_TSTP_3.3.1.7
3.3.1.8	The FWA device shall support MIMO 4x4 capability at least on one LTE mid-band (e.g., LTE B3 for Europe/Asia or B2 for US)	GR_TSTP_3.3.1.8
3.3.1.9	The FWA device shall support 256QAM modulation for downlink	GR_TSTP_3.3.1.9
3.3.1.10	The FWA device shall support 64QAM modulation for uplink.	GR_TSTP_3.3.1.10
3.3.1.11	The FWA device should support 256QAM modulation for uplink	GR_TSTP_3.3.1.11
3.3.1.12	The FWA device shall support standardized QCIs as specified in 3GPP TS 23.203	GR_TSTP_3.3.1.12
3.3.1.13	The FWA device should support operator specific QCIs as specified in 3GPP TS 23.203.	GR_TSTP_3.3.1.13

3.3.1.14	The FWA device shall support periodical intra-frequency ANR measurements for reporting to the network the Strongest Cells and related CGI (Cell Global Identity).	GR_TSTP_3.3.1.14
3.3.1.15	The FWA device shall support periodical inter-frequency ANR measurements for reporting to the network the Strongest Cells and related CGI (Cell Global Identity).	GR_TSTP_3.3.1.15
3.4	**Operating Frequency & Channel Bandwidth**	
3.4.1	Operating frequency and Channel bandwidth shall be as per the applicable National Frequency Allocation Plan.	GR_TSTP_3.4.1
3.4.2	The equipment shall be capable of operating in at least one of the frequency bands as per the applicable National Frequency Allocation Plan.	GR_TSTP_3.4.2
3.5	**Transmitter & Receiver Specifications**	
3.5.1	Transmitter Specifications for FWA CPE (4G & 5G)	
	Maximum Output Power	GR_TSTP_3.5.1.1
	Power Control	GR_TSTP_3.5.1.2
	Minimum Output Power	GR_TSTP_3.5.1.3
	Transmit OFF Power	GR_TSTP_3.5.1.4
	Frequency Error	GR_TSTP_3.5.1.5
	Error Vector Magnitude (EVM)	GR_TSTP_3.5.1.6

	Time Alignment Error	GR_TSTP_3.5.1.7
	Occupied Bandwidth	GR_TSTP_3.5.1.8
	Adjacent Channel Leakage Ratio	GR_TSTP_3.5.1.9
	Carrier Leakage & In-band emissions	GR_TSTP_3.5.1.10
	Spurious Emissions	GR_TSTP_3.5.1.11
	Transmitter Intermodulation	GR_TSTP_3.5.1.12
	Spectrum Emission Mask	GR_TSTP_3.5.1.13
3.5.2	Receiver Specifications for FWA CPE (4G & 5G UE)	
	Reference Sensitivity	GR_TSTP_3.5.2.1
	Adjacent Channel Selectivity	GR_TSTP_3.5.2.2
	Blocking	GR_TSTP_3.5.2.3
	Spurious Response	GR_TSTP_3.5.2.4
	Intermodulation	GR_TSTP_3.5.2.5
	Spurious Emission	GR_TSTP_3.5.2.6
4	**Hardware, Safety, EMC requirements and environment operating conditions**	
4.1	**Quality Requirements**	
4.1.1	The supplier/manufacturer shall conform to ISO 9001:2015 certifications. A quality plan describing the quality assurance system followed by the manufacturer shall be required to be submitted.	ISO Certificate to be submitted by the manufacturer
4.1.2	The failure of any component/ sub-system in the system may not result in the failure of complete	GR_TSTP_4.1.2

	system.	
4.1.3	Provision shall be made for continuous testing of the system to allow both system qualities check and fault indication as a fault arises.	GR_TSTP_4.1.3
4.1.4	In case a fault is detected requiring reloading of the program, this shall be carried out automatically. In case of manual re-loading, it shall be possible to stop and start at any particular point in the program	GR_TSTP_4.1.4
4.1.5	The components used shall be available from multiple sources with adequate qualification. Number of proprietary components used shall be minimum. List of such components shall be indicated.	Declaration and List to be submitted by manufacturer.
4.1.6	All the equipment shall have a tropical finish and coated to protect against saline atmosphere.	Declaration to be submitted by manufacturer.
4.1.7	The FWA Device shall comply with the eco-design and energy efficiency regulations of the market where it is meant to be used.	GR_TSTP_4.1.7
4.1.8	The FWA Device shall comply to the restrictions of use of hazardous materials and waste management regulations of the market where it is meant to be used	GR_TSTP_4.1.8

4.1.9	The FWA Device shall have a MTBF (Mean Time Between Failure) not shorter than 7 years at 30 °C.	Declaration to be submitted by manufacturer.
4.2	**Device Management (Common for IDU and ODU)**	
4.2.1	The System shall support following methods: a. RPC methods b. Data model structure c. Security d. Performance monitoring e. Data model parameters	GR_TSTP_4.2.1
4.3	**Stability**	
4.3.1	In case of loss of power, when the power is restored the FWA Device shall return automatically to the operational state, with all services (e.g., data, voice) restored according to the configuration of the device prior the power interruption.	GR_TSTP_4.3.1
4.3.2	In case of loss of radio signal(s), when the radio signal is restored the FWA Device shall return automatically to the operational state, with all services (e.g., data, voice) restored according to the configuration of the device prior the radio signal interruption.	GR_TSTP_4.3.2
4.3.3	For data service, in normal operating conditions, the FWA Device shall offer a service availability equal or greater than 99.95%.	Declaration to be submitted by manufacturer.

	Note: this objective considers only the availability of the Device itself, not the availability of the network.	
4.3.4	In normal operating conditions, the FWA Device shall offer a service availability for voice service of at least 99.5%.	Declaration to be submitted by manufacturer.
4.3.5	If voice service is supported, the FWA Device shall maintain uninterrupted voice (SIP protocol) registration for at least 72 consecutive hours, during which the Device is idle for Voic	GR_TSTP_4.3.5
4.3.6	If voice service is supported, the FWA Device shall be able to receive and make phone calls regularly, as well as to transmit and receive IP data user packets regularly.	GR_TSTP_4.3.6
4.3.7	If voice service is supported, the FWA Device shall be able to support long-lasting voice calls (1.5 hours at least).	GR_TSTP_4.3.7
4.4	**User Interface**	
4.4.1	The FWA Device shall offer a Web UI to the end user for customizing the configuration of the FWA Device	GR_TSTP_4.4.1
4.4.2	The Web UI should permit the configuration of all the service features relevant for the end user.	GR_TSTP_4.4.2
4.4.3	The Web UI shall be customizable based on	GR_TSTP_4.4.3

	procurer requirements.	
4.5	**Safety Requirements** The equipment shall conform to relevant safety requirements as per (IS/IEC 62368-1:2018 or Latest & IS 10437: 2019/IEC 60215: 2016) as prescribed under Table no. 1 of the TEC document ‘SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT”: TEC10009: 2024. These requirements are applicable for purposely built hardware or a physical entity only.	Test report from accredited laboratory
4.6	**Electromagnetic Compatiblity (ECM)** These requirements are applicable for purposely built hardware or a physical entity only. (These requirements shall be as per TEC Standard No. TEC11016:2016 as modified/ amended from time to time)	Test report from accredited laboratory
4.7	**System Radio Opearting Environments**	
4.7.1	**Availability** a.The facility shall be available for introduction of centralized Operation and Maintenance Control (OMC). b. The maintenance spares supplies shall take in to account the MTBF and MTTR.	GR_TSTP_4.7.1

4.7.2	**Diagnostic Capability** a. The diagnostic capability of the system shall be such as to minimize the human efforts required. The diagnostic programs which are normally resident in the on-line program shall be indicated. Details of the off-line diagnostic programs shall be given. The procedure for invoking such programs shall be described. The procedure for consulting fault dictionary for diagnostic programs shall be made available. b.The system shall provide facility for automatic restart under severe fault conditions. Where automatic restart fails to restore system sanity, facility shall be provided for manual restart of the system.	GR_TSTP_4.7.2
4.7.3	**Environmental Test Conditions:** a.Indoor entity : Category A SD: QM-333 b.Outdoor entity: Category D SD: QM-333 and IP65	Test report from accredited laboratory
4.8	**General Requirements**	
4.8.1	**General**	
4.8.1.1	The operation of the equipment shall be in the frequency band allotted.	GR_TSTP_4.8.1.1

4.8.1.2	Support of Multiple Equipment Vendors as per tender requirement	GR_TSTP_4.8.1.2
4.8.1.3	The system shall support the possibility of using equipment and sub-systems of different vendors as per defined industry standards, wherever relevant.	GR_TSTP_4.8.1.3
4.8.2	**Hardware**	
4.8.2.1	The system hardware shall be modular in design and shall permit growth in steps. The arrangement shall be such that failure/ deterioration of service shall not occur when implementing the growth.	GR_TSTP_4.8.2.1
4.8.2.2	Design precautions shall be taken to minimize the possibility of equipment damage arising from the insertion of an electronic package into the wrong connector or the removal of any package from any connector.	GR_TSTP_4.8.2.2
4.8.2.3	The system hardware shall not pose any problem, due to changes in date and time caused by events such as changeover of leap year etc., in the normal functioning of the system.	GR_TSTP_4.8.2.3
4.8.3	**Processors**	

4.8.3.1	Provision shall be made to prevent the loss/alteration of memory contents due to power failures, improper operating procedures and the procedure for restoring the system to its normal state, etc.	GR_TSTP_4.8.3.1
4.8.4	**Input-Output Devices**	
4.8.4.1	The communication facilities provided for exchange of information between the elements of FWA device and the maintenance and operating personnel shall include facilities for a system test, control and alarm indication at OMC.	GR_TSTP_4.8.4.1
4.8.4.2	Input / output terminals shall be capable of transmitting/ receiving characters of a subset of the ITU-T T.50 alphabet. The printing/display device shall print/display different graphic symbols for the digit zero and the capital letter O. The input/output terminal shall have the English Keyboard.	GR_TSTP_4.8.4.2
4.8.4.3	Adequate number of man-machine interfaces shall be available.	GR_TSTP_4.8.4.3

4.8.4.4	If provision is made for monitoring from a remote terminal, it shall be ensured that the data links conform to the ITU-T Recommendation Q.513. Care shall be taken that the reliability of the data links towards remote terminal does not, in any way, affect the reliability of the device. Special provision shall also be made for storage of failure event even when the system is unable to transmit an output message	GR_TSTP_4.8.4.4
4.8.4.5	A suitable alarm and display system at OMC shall be provided for a continuous indication of the system status.	GR_TSTP_4.8.4.5
4.8.5	**Equipement Practice**	
4.8.5.1	It shall be indicated whether printed board connectors are of edge-type or plug-and-socket type. They shall not be easily damaged during replacements and removals. The contact particulars as well as life test performance on contact resistance for each type of connector shall be supplied.	GR_TSTP_4.8.5.1

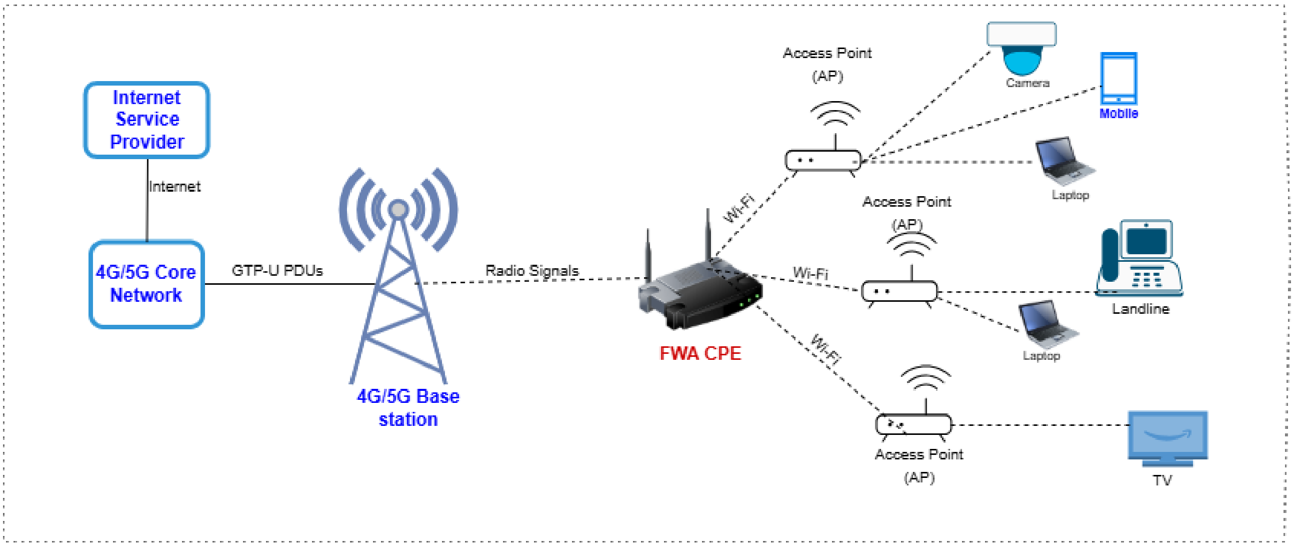
4.8.5.2	All components and material used in the equipment shall be non-inflammable or in absence of it, self-extinguishable. They shall be fully tropicalized.	GR_TSTP_4.8.5.2
4.8.5.3	The method used for connection of permanent wiring outside the printed cards shall be indicated.	GR_TSTP_4.8.5.3
4.8.5.4	The buses, if any, shall be suitably protected against electrical and magnetic interference from neighbouring systems (like electromechanical systems, fluorescent tubes, motors, etc.).	GR_TSTP_4.8.5.4
4.8.5.5	The different plug-in cards shall have suitable mechanical safeguards to prevent damage due to accidental interchange of cards.	GR_TSTP_4.8.5.5
4.8.5.6	The requirement at the external interface against induced voltages and currents due to lightning, high power system, etc. shall be indicated.	GR_TSTP_4.8.5.6
4.8.5.7	The system shall provide for human isolation and protection from accidental high voltage power contact.	GR_TSTP_4.8.5.7
4.9	**Software**	

4.9.1	The software shall be written in a High-Level Language. The software shall be modular and structured.	GR_TSTP_4.9.1
4.9.2	The software shall include the following characteristics: a.The design of the software shall be such that the system is easy to handle both during installation and normal operations as well as during extensions. b.The functional modularity of the software shall permit introduction of changes wherever necessary with least impact on other modules. c.It shall be open-ended to allow addition of new features. d.Adequate flexibility shall be available to easily adopt changes in service features & facilities and technological evolution in hardware. e. The design shall be such that propagation of software faults is contained. f. Test programs shall include fault tracing for	GR_TSTP_4.9.2

	detection and localization of system faults.	
4.9.3	**Software Maintenance**	
4.9.3.1	All software updates, for a period as specified, shall be supplied on continuing basis. These updates shall include new features and services and other maintenance updates.	GR_TSTP_4.9.3.1
4.9.3.2	Integration of software updates without posing any problem to the existing functionality shall be possible.	GR_TSTP_4.9.3.2
5	INFORMATION FOR THE PROCURER/VENDOR OF PRODUCT Interfaces and features which are optional needs to be examined by the procurer and suitably specified in the tender conditions as per their requirement based on the deployment scenario specific to the procurer. Below is table of recommended and optional features form the GR where in as per terminology 'Should' and 'may' has been used.	Optional information to be specified by procurer during procurement.

I. Test Setup & Procedures

TEST SETUP X



Fixed wireless access setup

Test No.	**GR_TSTP_2.1.1**
Test Details	To verify that FWA device shall support one (1) SIM/USIM. FWA Devices with multiple SIMs are outside the scope of this document.
Test Instruments Required	FWA CPE, one (1) SIM/USIM, Power supply unit
Test Setup	TEST SETUP X
Test Procedure	1. Insert one (1) SIM/USIM into the FWA CPE. 2. Power ON the FWA CPE. 3. Verify that the FWA CPE detects the inserted SIM/USIM and operates normally. 4. Verify that the FWA CPE does not support operation with more than one SIM/USIM.
Test Limits	NA
Expected Results	FWA device shall support **only one (1) SIM/USIM**. FWA Devices with multiple SIMs shall not be supported.

Test No.	**GR_TSTP_2.1.2**
Test Details	To verify that the FWA device may be equipped with one (1) eSIM, instead of a physical SIM.
Test Instruments Required	FWA CPE with eSIM capability, Power supply unit
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA CPE equipped with one (1) eSIM. 2. Verify that the eSIM is available and recognized by the FWA CPE. 3. Verify that the FWA CPE operates normally using the eSIM without a physical SIM.
Test Limits	NA
Expected Results	FWA device shall be able to operate with one (1) eSIM instead of a physical SIM.

Test No.	**GR_TSTP_2.1.3**
Test Details	To verify that the Indoor FWA Device (1-box solution) shall support the establishment of at least 3 PDNs/PDUs (e.g. for data/remote management, video, and voice services).
Test Instruments Required	Indoor FWA CPE (1-box solution), Power supply unit, Network connectivity for service establishment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Indoor FWA Device (1-box solution). 2. Configure the device to establish multiple PDNs/PDUs. 3. Establish the first PDN/PDU for data/remote management services. 4. Establish the second PDN/PDU for video services. 5. Establish the third PDN/PDU for voice services. 6. Verify that all established PDNs/PDUs remain active simultaneously.
Test Limits	NA
Expected Results	Indoor FWA Device (1-box solution) shall successfully support the establishment of at least three (3) PDNs/PDUs simultaneously.

Test No.	**GR_TSTP_2.1.4**
Test Details	To verify that the Outdoor Unit of an Outdoor FWA Solution (2-box) shall support the establishment of at least 4 PDNs/PDUs (e.g. for remote management of ODU, data/remote management of IDU, video, and voice services).
Test Instruments Required	Outdoor Unit (ODU), Indoor Unit (IDU), Power supply unit, Network connectivity for service establishment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Outdoor Unit (ODU) and Indoor Unit (IDU). 2. Establish connectivity between the ODU and IDU. 3. Configure the ODU to establish multiple PDNs/PDUs. 4. Establish a PDN/PDU for remote management of ODU. 5. Establish a PDN/PDU for data/remote management of IDU. 6. Establish a PDN/PDU for video services. 7. Establish a PDN/PDU for voice services. 8. Verify that all established PDNs/PDUs remain active simultaneously.
Test Limits	NA
Expected Results	Outdoor Unit (ODU) of the Outdoor FWA Solution (2-box) shall successfully support the establishment of at least four (4) PDNs/PDUs simultaneously.

Test No.	**GR_TSTP_2.1.5**
Test Details	To verify that FWA Device shall allow configurable associations between PDN/PDU connections and services/applications (e.g. voice, video; VLAN settings via Web UI).
Test Instruments Required	FWA CPE, Power supply unit, LAN/Wi-Fi client (PC/Laptop) for Web UI access
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the Web UI of the FWA Device from a connected LAN/Wi-Fi client. 3. Configure PDN/PDU connections for different services/applications. 4. Associate a PDN/PDU connection with voice service. 5. Associate a PDN/PDU connection with video service. 6. Configure VLAN settings via the Web UI and associate them with the corresponding PDN/PDU connections. 7. Verify that the configured associations are applied correctly.
Test Limits	NA
Expected Results	FWA Device shall allow configurable associations between PDN/PDU connections and services/applications, including VLAN configuration via Web UI.

Test No.	**GR_TSTP_2.1.6**
Test Details	To verify that FWA device should support the establishment of at least 6 PDNs/PDUs.
Test Instruments Required	FWA CPE, Power supply unit, Network connectivity for PDN/PDU establishment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Configure the device to establish multiple PDNs/PDUs. 3. Establish PDN/PDU connections sequentially until at least six (6) PDNs/PDUs are active. 4. Verify that all established PDNs/PDUs remain active simultaneously.
Test Limits	NA
Expected Results	FWA device shall successfully support the establishment of at least six (6) PDNs/PDUs.

Test No.	**GR_TSTP_2.1.7**

Test Details	To verify that for each PDNs/PDUs, the FWA Device shall allow to configure:
	a. Protocol stack (IPv4, IPv6, IPv4/v6);
	b. Authentication option (PAP/CHAP);
	c. MTU/MSS

Test Instruments Required	FWA CPE, Power supply unit, LAN/Wi-Fi client (PC/Laptop) for configuration access
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Select a configured PDN/PDU. 4. Configure the protocol stack as IPv4. 5. Configure the authentication option as PAP or CHAP. 6. Configure the MTU/MSS values. 7. Repeat steps 3 to 6 for other PDNs/PDUs using IPv6 and IPv4/v6 protocol stacks. 8. Verify that the configured parameters are applied independently for each PDN/PDU.
Test Limits	NA
Expected Results	For each PDN/PDU, the FWA Device shall allow configuration of protocol stack, authentication option, and MTU/MSS as specified.

Test No.	**GR_TSTP_2.2.1**
Test Details	The FWA Device shall comply with the 3GPP standards 3GPP TS 23.207 and 3GPP TS 23.203, regardless of deployment scenario (e.g., 4G, 5G NSA, 5G SA).
Test Instruments Required	Outdoor Unit (ODU), Indoor Unit (IDU), Power supply unit, 4G/5G Network Simulator (EPC/5GC with PCRF/PCF functionality), Traffic Generator & Analyzer, Protocol Analyzer (for QoS bearer verification)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device (ODU/IDU as applicable). 2. Attach the FWA Device to LTE or 5G network. 3. Establish default bearer (LTE) or default PDU session (5G). 4. Trigger establishment of dedicated bearer / QoS Flow with different QCI (LTE) or 5QI (5G). 5. Generate differentiated traffic streams: a. Voice (low latency) b. Video (high throughput) c. Best-effort data 6. Capture signaling messages to verify: a. Correct QoS parameters (QCI / 5QI) b. GBR / Non-GBR handling c. ARP parameters 7. Verify that traffic is treated according to assigned QoS parameters.
Test Limits	NA
Expected Results	Verify that traffic is treated according to assigned QoS parameters.

Test No.	**GR_TSTP_2.2.2**
Test Details	To verify that if a wireless service provider utilizes customized QoS for specific category of subscribers including mission critical organizations, government entities and enterprise customers, the FWA device should comply with the wireless service provider's requirements and mandates.
Test Instruments Required	FWA CPE, Power supply unit, LAN/Wi-Fi client (PC/Laptop) for service usage and configuration verification
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Provision the FWA device with a subscription/profile associated with customized QoS requirements as defined by the wireless service provider. 3. Establish service connectivity using the provisioned profile. 4. Generate traffic corresponding to the configured service category (e.g. enterprise or mission-critical service). 5. Verify that the FWA device applies and adheres to the customized QoS parameters as mandated by the service provider.
Test Limits	NA
Expected Results	The FWA device shall comply with the customized QoS requirements and mandates defined by the wireless service provider for the specified subscriber category.

Test No.	**GR_TSTP_2.3.1**
Test Details	To verify the Indoor FWA Device (1-box solution) shall support voice service either by means of VoLTE /VoNR technology or VoIP technology.
Test Instruments Required	Indoor FWA CPE (1-box solution), Power supply unit, Telephone handset / VoIP client (as applicable)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Indoor FWA Device (1-box solution). 2. Configure the device for voice service using VoLTE / VoNR or VoIP, as applicable. 3. Register the voice service on the device. 4. Initiate an outgoing voice call and verify call establishment. 5. Receive an incoming voice call and verify call establishment.
Test Limits	NA
Expected Results	Indoor FWA Device (1-box solution) shall successfully support voice service using VoLTE / VoNR or VoIP technology.

Test No.	**GR_TSTP_2.3.2**
Test Details	To verify the Indoor Unit of an Outdoor FWA Solution (2-box) shall support voice service uniquely by means of VoIP technology.
Test Instruments Required	Indoor Unit (IDU), Outdoor Unit (ODU), Power supply unit, Telephone handset / VoIP client (as applicable)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Outdoor Unit (ODU) and Indoor Unit (IDU). 2. Establish connectivity between the ODU and IDU. 3. Configure the Indoor Unit (IDU) for VoIP-based voice service. 4. Register the VoIP service on the IDU. 5. Initiate an outgoing VoIP call and verify call establishment. 6. Receive an incoming VoIP call and verify call establishment.
Test Limits	NA
Expected Results	Indoor Unit (IDU) of the Outdoor FWA Solution (2-box) shall support voice service only through VoIP technology.

Test No.	**GR_TSTP_2.3.3**
Test Details	To verify that in case of VoLTE/VoNR Technology, the FWA Device shall be compliant to GSMA IR.92 profile.
Test Instruments Required	FWA CPE, Power supply unit, Voice service subscription supporting VoLTE / VoNR, Telephone handset / voice client (as applicable)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure the device for VoLTE / VoNR-based voice service. 3. Register the voice service on the network. 4. Verify that the voice service parameters are aligned with GSMA IR.92 profile requirements. 5. Initiate an outgoing voice call and verify successful call establishment. 6. Receive an incoming voice call and verify successful call establishment.
Test Limits	NA
Expected Results	The FWA Device shall be compliant with the GSMA IR.92 profile when operating with VoLTE / VoNR technology.

Test No.	**GR_TSTP_2.3.4**
Test Details	To verify that in case of VoNR Technology, the FWA Device shall be compliant to GSMA NG.114 profile.
Test Instruments Required	FWA CPE, Power supply unit, Voice service subscription supporting VoNR, Telephone handset / voice client (as applicable)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure the device for VoNR-based voice service. 3. Register the VoNR service on the network. 4. Verify that the VoNR service parameters comply with GSMA NG.114 profile requirements. 5. Initiate an outgoing VoNR call and verify successful call establishment. 6. Receive an incoming VoNR call and verify successful call establishment.
Test Limits	NA
Expected Results	The FWA Device shall be compliant with the GSMA NG.114 profile when operating with VoNR technology.

Test No.	**GR_TSTP_2.3.5**
Test Details	To verify that in case of VoIP technology, the FWA Device shall be compliant to 3GPP specification 24.229, with the profile defined in the following sections 3.3.2, 3.3.3 and, optionally, 3.3.5 of GSMA TS.64 FWA Devices Architecture and Requirements Version 1.0.
Test Instruments Required	FWA CPE, Power supply unit, VoIP service configuration parameters, Telephone handset / VoIP client (as applicable)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure the device for VoIP-based voice service. 3. Configure VoIP parameters in accordance with 3GPP TS 24.229. 4. Verify that the VoIP profile complies with the requirements specified in Sections 3.3.2 and 3.3.3, and optionally Section 3.3.5, of GSMA TS.64 Version 1.0. 5. Register the VoIP service on the network. 6. Initiate an outgoing VoIP call and verify successful call establishment. 7. Receive an incoming VoIP call and verify successful call establishment.
Test Limits	NA
Expected Results	The FWA Device shall be compliant with 3GPP TS 24.229 and the applicable VoIP profile defined in GSMA TS.64 Version 1.0 when operating with VoIP technology.

Test No.	**GR_TSTP_2.3.6**
Test Details	To verify that in case of VoIP technology, the FWA Device shall request a dedicated PDN Connection. The PDN Connection for VoIP traffic may be characterized with a dedicated QCI. Note: Voice Traffic includes SIP, RTP, RTCP and DNS traffic used to resolve the P-CSCF FQDN in order to get the P-CSCF addresses.
Test Instruments Required	FWA CPE, Power supply unit, VoIP service configuration parameters, Network monitoring / protocol analysis tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure the device for VoIP-based voice service. 3. Initiate VoIP service registration. 4. Observe that the FWA Device requests a dedicated PDN Connection for VoIP traffic. 5. Verify that the PDN Connection used for VoIP traffic is associated with a dedicated QCI, if configured. 6. Verify that SIP, RTP, RTCP and DNS traffic related to VoIP service is carried over the dedicated PDN Connection.
Test Limits	NA
Expected Results	In case of VoIP technology, the FWA Device shall request and use a dedicated PDN Connection for VoIP traffic, and the connection may be characterized with a dedicated QCI.

Test No.	**GR_TSTP_2.3.7**
Test Details	To verify that it shall be possible to disable all voice features.
Test Instruments Required	FWA CPE, Power supply unit, LAN/Wi-Fi client (PC/Laptop) for configuration access
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Locate the voice service configuration settings. 4. Disable all voice-related features on the device. 5. Apply and save the configuration.
Test Limits	NA
Expected Results	It shall be possible to disable all voice features on the FWA Device, and no voice services shall be operational after disabling.

Test No.	**GR_TSTP_2.3.8**
Test Details	To verify that FWA Device shall be customizable in order not to have any FXS port or other voice interfaces.
Test Instruments Required	FWA CPE, Power supply unit, LAN/Wi-Fi client (PC/Laptop) for configuration verification
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the device configuration interface (e.g. Web UI). 3. Verify the customization options related to voice interfaces. 4. Configure the FWA Device to operate without FXS port or any other voice interface, if supported. 5. Apply and save the configuration. 6. Verify that no FXS port or voice interface is available or active on the FWA Device.
Test Limits	NA
Expected Results	FWA Device shall be customizable to operate without any FXS port or other voice interfaces.

Test No.	**GR_TSTP_2.4.1.1**
Test Details	To verify the indoor FWA Device and the Indoor Unit of an Outdoor FWA Solution shall support at least two Gigabit Ethernet LAN ports, compliant to IEEE 802.3ab standard.
Test Instruments Required	Indoor FWA Device or Indoor Unit (IDU), Power supply unit, Two (2) Ethernet cables, Two (2) Ethernet-capable LAN clients (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Indoor FWA Device or Indoor Unit (IDU). 2. Connect two LAN clients to the available Ethernet LAN ports using Ethernet cables. 3. Verify that at least two Gigabit Ethernet LAN ports are present. 4. Verify that each connected LAN client establishes a link at Gigabit Ethernet speed (1000BASE-T). 5. Verify normal data connectivity on both LAN ports simultaneously.
Test Limits	NA
Expected Results	The Indoor FWA Device and the Indoor Unit (IDU) of an Outdoor FWA Solution shall support at least two (2) Gigabit Ethernet LAN ports, compliant with IEEE 802.3ab standard.

Test No.	**GR_TSTP_2.4.1.2**
Test Details	To verify that for the physical interfaces for LAN Ethernet, the 10 100 1000BASE-T electrical interface should be used.
Test Instruments Required	Indoor FWA Device or Indoor Unit (IDU), Power supply unit, Ethernet cables, LAN client (PC/Laptop) with 10/100/1000 Mbps Ethernet support
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Indoor FWA Device or Indoor Unit (IDU). 2. Connect a LAN client to the Ethernet port using an Ethernet cable. 3. Verify that the Ethernet interface supports 10 Mbps, 100 Mbps, and 1000 Mbps link speeds. 4. Configure the LAN client to operate at 10 Mbps, 100 Mbps, and 1000 Mbps sequentially, if supported. 5. Verify successful link establishment and data connectivity at each supported speed.
Test Limits	NA
Expected Results	The physical LAN Ethernet interfaces shall support 10/100/1000BASE-T electrical interface operation.

Test No.	**GR_TSTP_2.4.1.3**
Test Details	To verify the different physical interfaces for LAN Ethernet, compliant to the standards, e.g. 10 100 1000BASE-TX, may be used in alternative to 10 100 1000BASE-T, depending on market and procurer needs.
Test Instruments Required	Indoor FWA Device or Indoor Unit (IDU), Power supply unit, Ethernet cables compatible with the supported interfaces, LAN client (PC/Laptop) compatible with the applicable Ethernet standards
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Indoor FWA Device or Indoor Unit (IDU). 2. Identify the available LAN Ethernet physical interfaces on the device. 3. Connect a LAN client using an Ethernet cable compatible with the supported interface (e.g. 10/100/1000BASE-TX). 4. Verify successful link establishment and data connectivity. 5. Confirm that the implemented LAN Ethernet interface complies with the applicable standard and meets market/procurer requirements.
Test Limits	NA
Expected Results	The Indoor FWA Device or Indoor Unit (IDU) shall support alternative standard-compliant LAN Ethernet physical interfaces (e.g. 10/100/1000BASE-TX) in place of 10/100/1000BASE-T, as per market and procurer needs.

Test No.	**GR_TSTP_2.4.1.4**
Test Details	To verify the Indoor Unit and the Outdoor Unit of an Outdoor FWA Solution shall have a connection coherent with the LAN-WAN capability of the Device.
Test Instruments Required	Indoor Unit (IDU), Outdoor Unit (ODU), Power supply units, Ethernet cable(s) for IDU–ODU interconnection, LAN client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Outdoor Unit (ODU) and Indoor Unit (IDU). 2. Establish the physical connection between the ODU and IDU. 3. Verify that the IDU–ODU connection type and capacity are coherent with the LAN–WAN capability of the device. 4. Connect a LAN client to the IDU. 5. Verify end-to-end data connectivity through the IDU–ODU connection.
Test Limits	NA
Expected Results	The Indoor Unit (IDU) and Outdoor Unit (ODU) of the Outdoor FWA Solution shall have a connection coherent with the LAN–WAN capability of the device.

Test No.	**GR_TSTP_2.4.1.5**
Test Details	To verify that for the physical interfaces for the IDU-ODU, if Ethernet is used, the BASE-T electrical interface should be used.
Test Instruments Required	Indoor Unit (IDU), Outdoor Unit (ODU), Power supply units, Ethernet cable(s) compliant with BASE-T interface
Test Setup	TEST SETUP
Test Procedure	1. Power ON the Outdoor Unit (ODU) and Indoor Unit (IDU). 2. Connect the IDU and ODU using an Ethernet interface. 3. Verify that the Ethernet physical interface used for the IDU–ODU connection is based on the BASE-T electrical interface. 4. Verify successful link establishment between the IDU and ODU. 5. Verify normal data connectivity through the IDU–ODU Ethernet link.
Test Limits	NA
Expected Results	For the IDU–ODU physical interface, when Ethernet is used, the BASE-T electrical interface shall be supported.

Test No.	**GR_TSTP_2.4.1.6**
Test Details	To verify that if Ethernet is used for the IDU-ODU connection, different physical interfaces, compliant to the standards, e.g. 1000BASE-TX, may be used in place of BASE-T, depending on market and procurer needs.
Test Instruments Required	Indoor Unit (IDU), Outdoor Unit (ODU), Power supply units, Ethernet cable(s) compatible with the supported physical interface
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Outdoor Unit (ODU) and Indoor Unit (IDU). 2. Connect the IDU and ODU using an Ethernet interface compliant with an alternative standard (e.g. 1000BASE-TX). 3. Verify successful link establishment between the IDU and ODU. 4. Verify that the physical interface used is standard-compliant and suitable for the intended market/procurer requirements. 5. Verify normal data connectivity through the IDU–ODU Ethernet connection.
Test Limits	NA
Expected Results	When Ethernet is used for the IDU–ODU connection, the device shall support alternative standard-compliant physical interfaces (e.g. 1000BASE-TX) in place of BASE-T, as per market and procurer needs.

Test No.	**GR_TSTP_2.4.2.1**
Test Details	To verify the 4G FWA Device shall offer an aggregate throughput of at least 1 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.
Test Instruments Required	4G FWA Device, Power supply unit, LAN clients (PC/Laptop) with Gigabit Ethernet and/or Wi-Fi capability, Network performance measurement tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 4G FWA Device. 2. Connect LAN clients to the device using Ethernet and/or Wi-Fi interfaces. 3. Configure traffic generation tools on the LAN clients. 4. Generate bidirectional traffic between LAN interfaces using IPv4. 5. Measure and record the aggregate throughput. 6. Repeat the test using IPv6. 7. Repeat the measurements using different packet lengths. 8. Verify the aggregate bidirectional throughput in all test conditions.
Test Limits	NA
Expected Results	The 4G FWA Device shall provide an aggregate bidirectional throughput of at least 1 Gb/s between LAN interfaces, irrespective of protocol (IPv4/IPv6) and packet length.

Test No.	**GR_TSTP_2.4.2.2**
Test Details	To verify that the 4G FWA Device should offer an aggregate throughput of at least 2.5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.
Test Instruments Required	4G FWA Device, Power supply unit, LAN clients (PC/Laptop) with multi-Gigabit Ethernet and/or high-performance Wi-Fi capability, Network performance measurement tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 4G FWA Device. 2. Connect LAN clients to the device using Ethernet and/or Wi-Fi interfaces. 3. Configure traffic generation tools on the LAN clients. 4. Generate bidirectional traffic between LAN interfaces using IPv4. 5. Measure and record the aggregate throughput. 6. Repeat the test using IPv6. 7. Repeat the measurements using different packet lengths. 8. Verify the aggregate bidirectional throughput under all test conditions.
Test Limits	NA
Expected Results	The 4G FWA Device shall provide an aggregate bidirectional throughput of at least 2.5 Gb/s between LAN interfaces, irrespective of protocol (IPv4/IPv6) and packet length.

Test No.	**GR_TSTP_2.4.2.3**
Test Details	To verify the 5G FWA Device shall offer an aggregate throughput of at least 2.5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.
Test Instruments Required	5G FWA Device, Power supply unit, LAN clients (PC/Laptop) with multi-Gigabit Ethernet and/or high-performance Wi-Fi capability, Network performance measurement tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 5G FWA Device. 2. Connect LAN clients to the device using Ethernet and/or Wi-Fi interfaces. 3. Configure traffic generation tools on the LAN clients. 4. Generate bidirectional traffic between LAN interfaces using IPv4. 5. Measure and record the aggregate throughput. 6. Repeat the test using IPv6. 7. Repeat the measurements using different packet lengths. 8. Verify the aggregate bidirectional throughput under all test conditions.
Test Limits	NA
Expected Results	The 5G FWA Device shall provide an aggregate bidirectional throughput of at least 2.5 Gb/s between LAN interfaces, irrespective of protocol (IPv4/IPv6) and packet length.

Test No.	**GR_TSTP_2.4.2.4**
Test Details	To verify the 5G FWA Device should offer an aggregate throughput of at least 5 Gb/s bidirectional between LAN interfaces, either Ethernet or WiFi, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length.
Test Instruments Required	5G FWA Device, Power supply unit, LAN clients (PC/Laptop) with multi-Gigabit Ethernet and/or high-performance Wi-Fi capability, Network performance measurement tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 5G FWA Device. 2. Connect LAN clients to the device using Ethernet and/or Wi-Fi interfaces. 3. Configure traffic generation tools on the LAN clients. 4. Generate bidirectional traffic between LAN interfaces using IPv4. 5. Measure and record the aggregate throughput. 6. Repeat the test using IPv6. 7. Repeat the measurements using different packet lengths. 8. Verify the aggregate bidirectional throughput under all test conditions.
Test Limits	NA
Expected Results	The 5G FWA Device shall provide an aggregate bidirectional throughput of at least 5 Gb/s between LAN interfaces, irrespective of protocol (IPv4/IPv6) and packet length.

Test No.	**GR_TSTP_2.4.2.5**
Test Details	To verify that 4G FWA Device shall offer a throughput LAN-WAN coherent with the LTE UE Category of the Device, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length and not affected by the local LAN-LAN throughput.
Test Instruments Required	4G FWA Device, Power supply unit, LAN client(s) (PC/Laptop) with Gigabit Ethernet and/or Wi-Fi capability, Network performance measurement tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 4G FWA Device. 2. Connect a LAN client to the device and establish WAN connectivity. 3. Generate LAN–WAN traffic using IPv4 and measure throughput. 4. Repeat the measurement using IPv6. 5. Repeat the measurements using different packet lengths. 6. In parallel, generate LAN–LAN traffic between local LAN interfaces. 7. Verify that the LAN–WAN throughput remains coherent with the LTE UE Category and is not impacted by the concurrent LAN–LAN traffic.
Test Limits	NA
Expected Results	The 4G FWA Device shall provide LAN–WAN throughput coherent with its LTE UE Category, irrespective of protocol (IPv4/IPv6) and packet length, and independent of local LAN–LAN throughput.

Test No.	**GR_TSTP_2.4.2.6**
Test Details	To verify that 5G FWA Device shall offer a throughput LAN-WAN coherent with 5G cellular bandwidth of the FWA Device, irrespective of IPv4 or IPv6 protocol, irrespective of Packet Length and not affected by the local LAN-LAN throughput.
Test Instruments Required	5G FWA Device, Power supply unit, LAN client(s) (PC/Laptop) with multi-Gigabit Ethernet and/or high-performance Wi-Fi capability, Network performance measurement tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 5G FWA Device. 2. Connect a LAN client to the device and establish WAN connectivity. 3. Generate LAN–WAN traffic using IPv4 and measure throughput. 4. Repeat the measurement using IPv6. 5. Repeat the measurements using different packet lengths. 6. In parallel, generate LAN–LAN traffic between local LAN interfaces. 7. Verify that the LAN–WAN throughput remains coherent with the 5G cellular bandwidth and is not impacted by the concurrent LAN–LAN traffic.
Test Limits	NA
Expected Results	The 5G FWA Device shall provide LAN–WAN throughput coherent with its 5G cellular bandwidth, irrespective of protocol (IPv4/IPv6) and packet length, and independent of local LAN–LAN throughput.

Test No.	**GR_TSTP_2.4.3.1**
Test Details	To verify that FWA Device shall support Internet Protocol version 4 (IPv4), defined in IETF RFC 791.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv4 capability
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure the LAN client to use IPv4 addressing. 4. Verify that the FWA Device assigns or supports an IPv4 address for the LAN client. 5. Verify successful IPv4-based data connectivity through the FWA Device.
Test Limits	NA
Expected Results	The FWA Device shall support IPv4 operation in accordance with IETF RFC 791, and IPv4-based communication shall be successful.

Test No.	**GR_TSTP_2.4.3.2**
Test Details	To verify that FWA Device shall support Internet Protocol version 6 (IPv6), defined in IETF RFC 8200 and further amendments defined by IETF.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv6 capability
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure the LAN client to use IPv6 addressing. 4. Verify that the FWA Device assigns or supports an IPv6 address for the LAN client. 5. Verify successful IPv6-based data connectivity through the FWA Device.
Test Limits	NA
Expected Results	The FWA Device shall support IPv6 operation in accordance with IETF RFC 8200 and applicable amendments, and IPv6-based communication shall be successful.

Test No.	**GR_TSTP_2.4.3.3**
Test Details	To verify that FWA Device shall support Address Resolution Protocol (ARP), defined in IETF RFC 826 and further amendments (IETF RFC 5227, IETF RFC 5494).
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure the LAN client for IPv4-based connectivity. 4. Generate traffic that triggers ARP request and response messages. 5. Capture and observe ARP packets using a network protocol analyzer. 6. Verify that ARP behavior is compliant with IETF RFC 826 and applicable amendments.
Test Limits	NA
Expected Results	The FWA Device shall correctly support Address Resolution Protocol (ARP) in accordance with IETF RFC 826, RFC 5227, and RFC 5494, and ARP-based address resolution shall be successful.

Test No.	**GR_TSTP_2.4.3.4**
Test Details	To verify that FWA Device shall support Network Discovery Protocol for IPv6 (NDP) defined in IETF RFC 4861 and further amendments defined by IETF.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv6 capability, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect an IPv6-capable LAN client to the FWA Device. 3. Configure the LAN client to operate using IPv6. 4. Generate IPv6 traffic that triggers NDP messages (e.g. Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement). 5. Capture and observe NDP packets using a network protocol analyzer. 6. Verify that NDP behavior is compliant with IETF RFC 4861 and applicable amendments.
Test Limits	NA
Expected Results	The FWA Device shall correctly support IPv6 Network Discovery Protocol (NDP) in accordance with IETF RFC 4861and applicable amendments, and IPv6 neighbor discovery shall function successfully.

Test No.	**GR_TSTP_2.4.3.5**
Test Details	To verify that FWA Device shall support Internet Control Message Protocol (ICMP) defined in IETF RFC 792 and further amendments defined by IETF (RFC 950, RFC 4884, RFC 6633, RFC 6918).
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure the LAN client for IP-based connectivity. 4. Generate ICMP traffic (e.g. Echo Request/Echo Reply). 5. Capture and observe ICMP packets using a network protocol analyzer. 6. Verify that ICMP behavior is compliant with IETF RFC 792 and applicable amendments.
Test Limits	NA
Expected Results	The FWA Device shall correctly support ICMP in accordance with IETF RFC 792 and applicable amendments, and ICMP-based communication shall be successful.

Test No.	**GR_TSTP_2.4.3.6**
Test Details	To verify that FWA Device shall support Internet Control Message Protocol version 6 for IPv6 (ICMPv6) defined in IETF RFC 4443.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv6 capability, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect an IPv6-capable LAN client to the FWA Device. 3. Configure the LAN client for IPv6-based connectivity. 4. Generate ICMPv6 traffic (e.g. Echo Request/Echo Reply). 5. Capture and observe ICMPv6 packets using a network protocol analyzer. 6. Verify that ICMPv6 behavior is compliant with IETF RFC 4443.
Test Limits	NA
Expected Results	The FWA Device shall correctly support ICMPv6 in accordance with IETF RFC 4443, and ICMPv6-based communication shall be successful.

Test No.	**GR_TSTP_2.4.3.7**
Test Details	To verify that FWA Device shall implement a Network Time Protocol (NTP) client as defined in IETF RFC 5905 and further amendments.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) for configuration access, NTP server (reachable over the network)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the device configuration interface (e.g. Web UI). 3. Configure the NTP server parameters on the FWA Device. 4. Enable the NTP client functionality. 5. Verify that the FWA Device synchronizes its system time with the configured NTP server. 6. Verify that time synchronization is maintained as per configuration.
Test Limits	NA
Expected Results	The FWA Device shall implement an NTP client compliant with IETF RFC 5905 and applicable amendments, and system time synchronization shall be successful.

Test No.	**GR_TSTP_2.4.3.8**
Test Details	To verify that FWA Device shall support Internet Group Management Protocol, version 3 (IGMPv3), defined in IETF RFC 3376.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with multicast capability, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure the LAN client to join and leave IPv4 multicast groups using IGMPv3. 4. Generate multicast traffic from the network. 5. Capture and observe IGMPv3 messages using a network protocol analyzer. 6. □ Verify that multicast group membership is handled correctly in accordance with IGMPv3 behavior.
Test Limits	NA
Expected Results	The FWA Device shall correctly support IGMPv3 in accordance with IETF RFC 3376, and IPv4 multicast group management shall function successfully.

Test No.	**GR_TSTP_2.4.3.9**
Test Details	To verify that FWA Device shall support IGMP Proxy as defined in IETF RFC 4605.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with multicast capability, Multicast source, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable IGMP Proxy functionality on the FWA Device, if configurable. 3. Connect a LAN client to the FWA Device. 4. Configure the LAN client to join an IPv4 multicast group. 5. Generate multicast traffic from the multicast source. 6. Capture and observe IGMP messages on the LAN and WAN interfaces using a network protocol analyzer. 7. Verify that the FWA Device correctly proxies IGMP messages between LAN and WAN interfaces in accordance with RFC 4605.
Test Limits	NA
Expected Results	The FWA Device shall correctly support IGMP Proxy functionality in accordance with IETF RFC 4605, and multicast traffic shall be forwarded appropriately.

Test No.	**GR_TSTP_2.4.3.10**
Test Details	To verify that FWA Device shall support QoS Treatment both at level 2 (p-bits of 802.1q VLAN Tag) and at level 3 (Differentiated Services Code Point of the IP header).
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) capable of VLAN and DSCP configuration, Network traffic generator, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure VLAN tagging on the LAN client with specific 802.1Q p-bits. 4. Generate traffic from the LAN client with configured Layer 2 p-bits. 5. Configure traffic with specific DSCP values in the IP header. 6. Capture and observe packets using a network protocol analyzer. 7. Verify that the FWA Device correctly recognizes and applies QoS treatment based on Layer 2 p-bits. 8. Verify that the FWA Device correctly recognizes and applies QoS treatment based on Layer 3 DSCP values.
Test Limits	NA
Expected Results	The FWA Device shall correctly support QoS treatment at both Layer 2 (802.1Q p-bits) and Layer 3 (DSCP) levels.

Test No.	**GR_TSTP_2.4.3.11**
Test Details	To verify that FWA Device shall support the Differentiated Services (DiffServ) architecture and behaviors defined in RFC 2474, 2475, 2597, 3246 and 3260.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) capable of DSCP configuration, Network traffic generator, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure traffic with different DSCP values corresponding to DiffServ classes (e.g. BE, AF, EF). 4. Generate traffic flows for the configured DiffServ classes. 5. Capture and observe packets using a network protocol analyzer. 6. Verify that the FWA Device applies DiffServ behaviors (classification, marking, and forwarding) in accordance with the defined RFCs.
Test Limits	NA
Expected Results	The FWA Device shall support the DiffServ architecture and behaviors as defined in RFC 2474, 2475, 2597, 3246, and 3260, and differentiated traffic handling shall function correctly.

Test No.	**GR_TSTP_2.4.3.12**
Test Details	To verify the behaviors of traffic classification, marking, remarking, queuing, scheduling, policing, shaping shall be applicable both to internally generated traffic and to traffic coming from LAN and destined to the WAN.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Network traffic generator, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure traffic management and QoS policies on the FWA Device. 3. Generate internally generated traffic from the FWA Device (e.g. management or control traffic). 4. Generate LAN-to-WAN traffic from a connected LAN client. 5. Apply traffic flows with different classifications and markings. 6. Capture and observe traffic using a network protocol analyzer. 7. □ Verify that classification, marking/remarking, queuing, scheduling, policing, and shaping behaviors are applied correctly to both traffic types.
Test Limits	NA
Expected Results	The FWA Device shall apply traffic classification, marking, remarking, queuing, scheduling, policing, and shapingconsistently to internally generated traffic and to LAN-to-WAN traffic, as configured.

Test No.	**GR_TSTP_2.4.3.13**
Test Details	To verify that at least four queues shall be supported on the WAN interface, of which one with Strict Priority scheduling, and the others with configurable scheduling mechanisms (e.g. Weighted Fair Queuing, Weighted Round Robin).
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Network traffic generator, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure WAN interface queuing and scheduling parameters on the FWA Device. 3. Configure at least four queues on the WAN interface. 4. Assign Strict Priority scheduling to one queue. 5. Assign configurable scheduling mechanisms (e.g. WFQ, WRR) to the remaining queues. 6. Generate traffic mapped to each configured queue. 7. Capture and observe traffic behavior using a network protocol analyzer. 8. Verify that traffic is handled according to the configured queue and scheduling policies.
Test Limits	NA
Expected Results	The FWA Device shall support at least four queues on the WAN interface, including one Strict Priority queue and other queues with configurable scheduling mechanisms such as WFQ and WRR.

Test No.	**GR_TSTP_2.4.3.14**
Test Details	To verify that FWA Device should support a secondary IPv4 addressing on LAN, in order to enable the assignment of public IP addresses to hosts in LAN.
Test Instruments Required	FWA CPE, Power supply unit, LAN client(s) (PC/Laptop), Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the device configuration interface (e.g. Web UI). 3. Configure a primary IPv4 address on the LAN interface. 4. Configure a secondary IPv4 address on the same LAN interface. 5. Connect one or more LAN hosts to the FWA Device. 6. Assign a public IPv4 address to a LAN host using the secondary IPv4 addressing. 7. Verify IPv4 connectivity for the LAN host using the assigned public IPv4 address.
Test Limits	NA
Expected Results	The FWA Device shall support secondary IPv4 addressing on the LAN interface, enabling the assignment of public IPv4 addresses to LAN hosts.

Test No.	**GR_TSTP_2.4.3.15**
Test Details	To verify that FWA Device shall support VLAN Tagging, compliant to IEEE 802.1q standard.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with VLAN configuration capability, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure VLAN tagging (IEEE 802.1Q) on the LAN client with a specific VLAN ID. 4. Generate traffic from the LAN client with the configured VLAN tag. 5. Capture and observe VLAN-tagged packets using a network protocol analyzer. 6. Verify that the FWA Device correctly supports and processes 802.1Q VLAN tags.
Test Limits	NA
Expected Results	The FWA Device shall correctly support VLAN tagging in accordance with IEEE 802.1Q standard.

Test No.	**GR_TSTP_2.4.4.1**
Test Details	To verify that the FWA Device shall support Dynamic Host Configuration Protocol (DHCP) defined in IETF RFC 2131.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable DHCP server functionality on the FWA Device, if configurable. 3. Connect a LAN client to the FWA Device. 4. Configure the LAN client to obtain an IP address automatically via DHCP. 5. Verify that the LAN client receives an IPv4 address and related network parameters from the FWA Device. 6. Verify successful IP-based connectivity for the LAN client.
Test Limits	NA
Expected Results	The FWA Device shall support DHCP in accordance with IETF RFC 2131, and LAN clients shall successfully obtain network configuration via DHCP.

Test No.	**GR_TSTP_2.4.4.2**
Test Details	To verify that FWA Device shall support DHCP Options defined in IETF RFC 2132.
Test Instruments Required	Power supply unit, LAN client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure DHCP server options on the FWA Device in accordance with RFC 2132. 3. Connect a LAN client to the FWA Device. 4. Configure the LAN client to obtain network parameters via DHCP. 5. Verify that the LAN client receives the configured DHCP options (e.g. default gateway, DNS server). 6. Verify correct application of the received DHCP options on the LAN client.
Test Limits	NA
Expected Results	The FWA Device shall support DHCP Options as defined in IETF RFC 2132, and LAN clients shall correctly receive and apply the provided options.

Test No.	**GR_TSTP_2.4.4.3**
Test Details	To verify that FWA device may implement DHCP options 60 and 43 for automatic provision of ACS parameters.
Test Instruments Required	FWA CPE, Power supply unit, DHCP server configured with Option 60 and Option 43, LAN/WAN connectivity for provisioning
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure the DHCP server to include Option 60 (Vendor Class Identifier) and Option 43 (Vendor-Specific Information) with valid ACS parameters. 3. Connect the FWA Device to the network with access to the configured DHCP server. 4. Allow the FWA Device to request network configuration via DHCP. 5. Verify that the FWA Device receives and processes DHCP Options 60 and 43. 6. Verify that the ACS parameters are automatically provisioned on the FWA Device.
Test Limits	NA
Expected Results	The FWA Device shall be able to implement DHCP Option 60 and DHCP Option 43 for automatic provisioning of ACS parameters, when supported and configured.

Test No.	**GR_TSTP_2.4.4.4**
Test Details	To verify that in case of multiple connections from the same FWA device, FWA device shall implement DHCP option 82 and 37 for client identifications and policy enforcement.
Test Instruments Required	FWA CPE, Power supply unit, DHCP server supporting Option 82 and Option 37, Multiple LAN clients or interfaces, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure the DHCP server to support Option 82 (Relay Agent Information) and Option 37 (Client Identifier). 3. Establish multiple simultaneous connections from the same FWA Device (e.g. multiple LAN ports or VLANs). 4. Allow each connection to request network configuration via DHCP. 5. Capture and observe DHCP messages using a network protocol analyzer. 6. Verify that DHCP Option 82 and DHCP Option 37 are included for each connection. 7. Verify that client identification and policy enforcement are applied correctly based on the DHCP options.
Test Limits	NA
Expected Results	In case of multiple connections from the same FWA Device, DHCP Option 82 and DHCP Option 37 shall be implemented for client identification and policy enforcement, as configured.

Test No.	**GR_TSTP_2.4.4.5**
Test Details	To verify that DHCP Server implemented by the FWA Device shall manage at least 254 addresses.
Test Instruments Required	FWA CPE with DHCP server functionality, Power supply unit, LAN clients (PC/Laptop) or DHCP client emulation tool capable of generating multiple DHCP requests
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure the DHCP Server on the FWA Device. 3. Configure the DHCP address pool to support at least 254 IP addresses. 4. Connect multiple LAN clients to the FWA Device or use a DHCP client emulation tool. 5. Initiate DHCP requests from the LAN clients. 6. Verify that IP addresses are successfully assigned to at least 254 clients. 7. Verify that no address conflicts occur during assignment.
Test Limits	NA
Expected Results	The DHCP Server implemented by the FWA Device shall successfully manage and assign at least 254 IP addresses to LAN clients.

Test No.	**GR_TSTP_2.4.4.6**
Test Details	To verify that it shall be possible to define any IPv4 Unicast subnet for the private LAN and DHCP pool.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the device configuration interface (e.g. Web UI). 3. Configure the private LAN IPv4 subnet using a valid IPv4 Unicast address range. 4. Configure the DHCP pool to match the defined IPv4 Unicast subnet. 5. Connect a LAN client to the FWA Device. 6. Configure the LAN client to obtain an IP address via DHCP. 7. Verify that the LAN client receives an IP address from the configured IPv4 Unicast subnet and has IP connectivity.
Test Limits	NA
Expected Results	It shall be possible to configure any IPv4 Unicast subnet for the private LAN and corresponding DHCP pool on the FWA Device, and LAN clients shall receive addresses accordingly.

Test No.	**GR_TSTP_2.4.4.7**
Test Details	To verify that DHCP Server implemented by the FWA Device shall support Duplicate Address Detection (DAD) functionality.
Test Instruments Required	FWA CPE with DHCP server functionality, Power supply unit, LAN clients (PC/Laptop), Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure the DHCP Server on the FWA Device. 3. Connect a LAN client to the FWA Device and allow it to obtain an IP address via DHCP. 4. Configure another LAN client with a manually assigned IPv4 address that duplicates an address within the DHCP pool. 5. Initiate DHCP address assignment for a new client. 6. Capture and observe DHCP and ARP traffic using a network protocol analyzer. 7. Verify that the DHCP Server detects the duplicate address and prevents assignment of the duplicated IP address.
Test Limits	NA
Expected Results	The DHCP Server implemented by the FWA Device shall support Duplicate Address Detection (DAD) and shall prevent assignment of duplicate IPv4 addresses within the DHCP pool.

Test No.	**GR_TSTP_2.4.4.8**
Test Details	To verify that DHCP Server implemented by the FWA Device shall provide a mechanism for IP reservation on MAC Address basis, assigning the same IP address (if available) at the same MAC Address.
Test Instruments Required	FWA CPE with DHCP server functionality, Power supply unit, LAN client (PC/Laptop), Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure the DHCP Server on the FWA Device. 3. Access the DHCP configuration interface and create an IP reservation mapped to a specific MAC address. 4. Connect the LAN client with the configured MAC address to the FWA Device. 5. Allow the LAN client to obtain an IP address via DHCP. 6. Verify that the LAN client is assigned the reserved IP address. 7. Release and renew the DHCP lease and verify that the same IP address is assigned again.
Test Limits	NA
Expected Results	The DHCP Server implemented by the FWA Device shall support IP address reservation based on MAC address, consistently assigning the same IP address to the same MAC address when available.

Test No.	**GR_TSTP_2.4.4.9**
Test Details	To verify that FWA Device shall support hostnames presented by the hosts (DHCP clients) with DHCP Option 12.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) capable of sending DHCP Option 12, Configuration access (e.g. Web UI) or network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure the DHCP Server on the FWA Device. 3. Configure the LAN client to include a hostname using DHCP Option 12. 4. Connect the LAN client to the FWA Device and initiate a DHCP request. 5. Verify that the FWA Device receives and processes the hostname information provided via DHCP Option 12. 6. Verify that the hostname is visible or usable in the device’s client list or management interface.
Test Limits	NA
Expected Results	The FWA Device shall support and correctly process hostnames provided by DHCP clients using Option 12, and the hostname information shall be available as expected.

Test No.	**GR_TSTP_2.4.4.10**
Test Details	To verify that FWA Device shall properly manage the cases of overlapping hostnames and hostnames not presented by clients, by assigning to client's unambiguous hostnames by means of Option 12.
Test Instruments Required	FWA CPE, Power supply unit, Multiple LAN clients (PC/Laptop) with configurable hostnames, Configuration access (e.g. Web UI) or network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure the DHCP Server on the FWA Device. 3. Connect multiple LAN clients using identical hostnames via DHCP Option 12. 4. Connect one or more LAN clients without providing a hostname in the DHCP request. 5. Allow all clients to obtain IP addresses via DHCP. 6. Verify that the FWA Device assigns unique and unambiguous hostnames to each client. 7. Verify that no hostname conflicts exist in the device's client list or management interface.
Test Limits	NA
Expected Results	The FWA Device shall correctly manage overlapping or missing hostnames by assigning unambiguous hostnames to DHCP clients using Option 12.

Test No.	**GR_TSTP_2.4.4.11**
Test Details	To verify that FWA Device shall support Dynamic Host Configuration Protocol for IPv6 (DHCPv6) defined in IETF RFC 8415.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv6 capability
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure DHCPv6 functionality on the FWA Device. 3. Connect an IPv6-capable LAN client to the FWA Device. 4. Configure the LAN client to obtain IPv6 parameters via DHCPv6. 5. Verify that the LAN client receives IPv6 address and related configuration information. 6. Verify successful IPv6-based connectivity for the LAN client.
Test Limits	NA
Expected Results	The FWA Device shall support DHCPv6 in accordance with IETF RFC 8415, and IPv6 clients shall successfully obtain configuration via DHCPv6.

Test No.	**GR_TSTP_2.4.4.12**
Test Details	To verify that FWA Device shall support Prefix Delegation for IPv6 (DHCPv6) defined in IETF RFC 8415.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv6 capability, IPv6 network with DHCPv6 Prefix Delegation support
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure DHCPv6 Prefix Delegation on the FWA Device. 3. Connect the FWA Device to an IPv6 network providing prefix delegation. 4. Allow the FWA Device to request an IPv6 prefix via DHCPv6. 5. Verify that the delegated IPv6 prefix is assigned to the LAN interface(s). 6. Connect an IPv6-capable LAN client to the FWA Device. 7. Verify that the LAN client receives an IPv6 address derived from the delegated prefix. 8. Verify successful IPv6 connectivity for the LAN client.
Test Limits	NA
Expected Results	The FWA Device shall support IPv6 Prefix Delegation via DHCPv6 in accordance with IETF RFC 8415, and delegated prefixes shall be correctly applied to LAN interfaces.

Test No.	**GR_TSTP_2.4.4.13**
Test Details	To verify that FWA Device shall support Prefix Exclude for IPv6 (DHCPv6) defined in IETF RFC 8415.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv6 capability, IPv6 network with DHCPv6 Prefix Delegation and Prefix Exclude support
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure DHCPv6 Prefix Delegation with Prefix Exclude option on the FWA Device. 3. Connect the FWA Device to an IPv6 network providing delegated prefix with excluded sub-prefix. 4. Allow the FWA Device to receive the delegated prefix and excluded prefix information via DHCPv6. 5. Verify that the FWA Device correctly applies the Prefix Exclude information. 6. Assign IPv6 addresses to LAN interfaces excluding the specified sub-prefix. 7. Connect an IPv6-capable LAN client to the FWA Device. 8. Verify that the LAN client receives an IPv6 address outside the excluded prefix range. 9. Verify successful IPv6 connectivity for the LAN client.
Test Limits	NA
Expected Results	The FWA Device shall support IPv6 Prefix Exclude via DHCPv6 in accordance with IETF RFC 8415, and excluded prefixes shall not be used for LAN address assignment.

Test No.	**GR_TSTP_2.4.5.1**
Test Details	To verify that FWA Device shall support IP Network Address Translator (NAT) as defined in IETF RFC 3022.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), External network or WAN connectivity, Network protocol analyzer (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure NAT functionality on the FWA Device. 3. Connect a LAN client to the FWA Device. 4. Configure the LAN client with a private IPv4 address. 5. Generate traffic from the LAN client towards the WAN. 6. Verify that the FWA Device performs address translation from private to public IP address. 7. Optionally capture and observe translated packets using a network protocol analyzer.
Test Limits	NA
Expected Results	The FWA Device shall support NAT in accordance with IETF RFC 3022, and private-to-public IP address translation shall function correctly.

Test No.	**GR_TSTP_2.4.5.2**
Test Details	To verify that Network Address Translator functionality implemented by the FWA Device shall be compliant to the behaviors defined in IETF RFC 4787.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), External WAN connectivity, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure NAT functionality on the FWA Device. 3. Connect a LAN client to the FWA Device with a private IPv4 address. 4. Establish multiple outbound connections from the LAN client towards the WAN. 5. Generate inbound traffic scenarios as applicable. 6. Capture and observe NAT behavior using a network protocol analyzer. 7. Verify that the NAT behavior (mapping, filtering, hairpinning if applicable) complies with the requirements defined in IETF RFC 4787.
Test Limits	NA
Expected Results	The NAT functionality implemented by the FWA Device shall be compliant with the behaviors defined in IETF RFC 4787, and address translation behavior shall be correct and consistent.

Test No.	**GR_TSTP_2.4.5.3**
Test Details	To verify that The FWA Device shall implement a configurable Port Mapping/Virtual Server functionality, allowing the creation of entries for mapping protocols/ports on the WAN side of the FWA Device to an IP address and protocols/ports on the private LAN.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), External WAN client or service, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable and configure Port Mapping / Virtual Server functionality. 4. Create a port mapping entry specifying WAN protocol and port. 5. Map the WAN protocol and port to a specific private LAN IP address and port. 6. From the external WAN side, initiate traffic towards the configured WAN port. 7. Verify that the traffic is correctly forwarded to the mapped LAN host and port.
Test Limits	NA
Expected Results	The FWA Device shall support configurable Port Mapping / Virtual Server functionality, and traffic received on the configured WAN protocol and port shall be correctly forwarded to the specified private LAN IP address and port.

Test No.	**GR_TSTP_2.4.5.4**
Test Details	To verify that it shall be possible to configure at least 32 Port Mapping entries.
Test Instruments Required	FWA CPE, Power supply unit, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable Port Mapping / Virtual Server functionality. 4. Create multiple Port Mapping entries sequentially. 5. Continue creating entries until at least 32 Port Mapping entries are configured. 6. Verify that all configured entries are saved and active.
Test Limits	NA
Expected Results	It shall be possible to configure at least 32 Port Mapping entries on the FWA Device, and all entries shall be retained and functional.

Test No.	**GR_TSTP_2.4.5.5**
Test Details	To verify that FWA Device shall support Customer-side Translator (CLAT) functionality according to IETF RFC 6145
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), IPv6-only network with NAT64 support, Network protocol analyzer (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable and configure CLAT functionality on the FWA Device. 3. Connect the FWA Device to an IPv6-only network providing NAT64 service. 4. Connect a LAN client configured for IPv4-only connectivity to the FWA Device. 5. Generate IPv4 traffic from the LAN client towards an IPv4 destination. 6. Verify that the FWA Device translates IPv4 traffic to IPv6 using CLAT. 7. Verify successful end-to-end connectivity through the NAT64 infrastructure.
Test Limits	NA
Expected Results	The FWA Device shall support CLAT functionality in accordance with IETF RFC 6145, enabling IPv4-only LAN clients to communicate over an IPv6-only network.

Test No.	**GR_TSTP_2.4.5.6**
Test Details	To verify that FWA Device shall support operation in Bridge Mode. In this configuration both DHCP and NAT operations are provided by the network being bridged to.
Test Instruments Required	FWA CPE, Power supply unit, External network providing DHCP and NAT, LAN client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the device configuration interface (e.g. Web UI). 3. Configure the FWA Device to operate in Bridge Mode. 4. Connect the FWA Device to an external network that provides DHCP and NAT. 5. Connect a LAN client to the FWA Device. 6. Verify that the LAN client obtains IP address information from the external network DHCP server. 7. Verify that NAT operations are performed by the external network and not by the FWA Device.
Test Limits	NA
Expected Results	The FWA Device shall support Bridge Mode operation, with DHCP and NAT functions provided by the bridged network, and LAN clients shall operate accordingly.

Test No.	**GR_TSTP_2.4.5.7**
Test Details	To verify that FWA Device shall implement a configurable Application Layer Gateway functionality (ALG), as defined in IETF RFC 2663, at least for the following protocols: SIP, IPSec, PPTP, L2TP.
Test Instruments Required	FWA CPE, Power supply unit, LAN client(s) supporting SIP, IPSec, PPTP, and L2TP, External WAN connectivity, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable and configure ALG functionality. 4. Enable ALG support for SIP, IPSec, PPTP, and L2TP protocols. 5. Generate protocol-specific traffic from the LAN client towards the WAN for each supported protocol. 6. Verify that the FWA Device correctly processes and allows traffic for each protocol with ALG enabled. 7. Disable ALG functionality (if configurable) and verify behavior as per configuration.
Test Limits	NA
Expected Results	The FWA Device shall support a configurable ALG functionality in accordance with IETF RFC 2663, for at least SIP, IPSec, PPTP, and L2TP protocols.

Test No.	**GR_TSTP_2.4.6.1**
Test Details	To verify that FWA Device shall support a default MTU size of 1380 bytes.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Network traffic generation tool or packet capture tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Verify the default MTU configuration on the FWA Device. 4. Generate IP traffic from the LAN client with packet sizes approaching and exceeding 1380 bytes. 5. Observe packet transmission behavior using a packet capture or traffic analysis tool. 6. Verify that the default MTU value is 1380 bytes and that traffic is handled accordingly.
Test Limits	NA
Expected Results	The FWA Device shall support a default MTU size of 1380 bytes, and traffic handling shall be consistent with this MTU setting.

Test No.	**GR_TSTP_2.4.6.2**
Test Details	To verify that FWA Device shall support network override of the default MTU size in IPv4 operation via Protocol Configuration Options (3GPP TS 24.008).
Test Instruments Required	FWA CPE, Power supply unit, Network providing PCO-based MTU configuration, LAN client (PC/Laptop), Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect the FWA Device to a network capable of sending MTU override parameters via PCO. 3. Configure the network to provide a non-default MTU value through Protocol Configuration Options. 4. Establish IPv4 connectivity for the FWA Device. 5. Verify that the FWA Device receives the MTU override from the network. 6. Verify that the effective MTU on the FWA Device reflects the network-provided value. 7. Generate IPv4 traffic from a LAN client and verify packet handling according to the overridden MTU.
Test Limits	NA
Expected Results	The FWA Device shall support network override of the default MTU size via PCO, as defined in 3GPP TS 24.008, and shall correctly apply the overridden MTU during IPv4 operation.

Test No.	**GR_TSTP_2.4.6.3**
Test Details	To verify that FWA Device shall support network override of the default MTU size in IPv6 operation via Router Advertisement.
Test Instruments Required	FWA CPE, Power supply unit, IPv6 network providing Router Advertisement with MTU option, LAN client (PC/Laptop) with IPv6 capability, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect the FWA Device to an IPv6 network configured to send Router Advertisements with MTU information. 3. Establish IPv6 connectivity for the FWA Device. 4. Verify that the FWA Device receives the MTU value from the Router Advertisement. 5. Verify that the effective MTU on the FWA Device is updated according to the RA-provided MTU. 6. Generate IPv6 traffic from a LAN client and verify packet handling according to the overridden MTU.
Test Limits	NA
Expected Results	The FWA Device shall support network override of the default MTU size via IPv6 Router Advertisement, and shall correctly apply the overridden MTU during IPv6 operation.

Test No.	**GR_TSTP_2.4.7.1**
Test Details	To verify that FWA Device shall support Domain Name System (DNS) compliant to IETF RFC 1034, RFC 1035 and further amendments defined by IETF
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Reachable DNS server, Network protocol analyzer (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure DNS parameters on the FWA Device (automatic or manual). 3. Connect a LAN client to the FWA Device. 4. Configure the LAN client to use DNS service via the FWA Device. 5. Perform DNS name resolution for valid domain names from the LAN client. 6. Verify successful resolution of domain names to IP addresses. 7. Optionally capture and observe DNS query and response messages.
Test Limits	NA
Expected Results	The FWA Device shall support DNS functionality in accordance with IETF RFC 1034 and RFC 1035, and DNS name resolution shall function correctly.

Test No.	**GR_TSTP_2.4.7.2**
Test Details	To verify that FWA Device shall be able, on a configuration basis, to act as DNS Server for the Hosts in LAN.
Test Instruments Required	FWA CPE, Power supply unit, LAN client(s) (PC/Laptop), Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the device configuration interface (e.g. Web UI). 3. Enable the DNS Server functionality on the FWA Device. 4. Connect one or more LAN hosts to the FWA Device. 5. Configure the LAN hosts to use the FWA Device as DNS Server. 6. Perform DNS queries from the LAN hosts. 7. Verify that the FWA Device correctly resolves or forwards DNS queries for the LAN hosts.
Test Limits	NA
Expected Results	The FWA Device shall be configurable to act as a DNS Server for LAN hosts, and DNS resolution shall function correctly when enabled.

Test No.	**GR_TSTP_2.4.7.3**
Test Details	To verify that FWA Device shall be able to advertise the DNS server(s) to the Hosts in LAN via DHCP protocol. On a configuration basis, the advertised DNS server(s) can be: a. The FWA Device itself, if it’s configured to act as a DNS Server; b. The DNS server addresses received from the network, if the FWA Device is not configured to act as a DNS Server. c. Optionally, other DNS Server addresses configured on the FWA Device.
Test Instruments Required	FWA CPE, Power supply unit, LAN client(s) (PC/Laptop), Configuration access (e.g. Web UI), Network providing DNS server addresses
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Configure the FWA Device to act as a DNS Server, if applicable. 4. Configure the FWA Device to obtain DNS server addresses from the network, if applicable. 5. Optionally configure custom DNS server addresses on the FWA Device. 6. Enable DHCP service on the FWA Device. 7. Connect LAN hosts and allow them to obtain network configuration via DHCP. 8. Verify that the LAN hosts receive the correct DNS server address(es) according to the configured option.
Test Limits	NA
Expected Results	The FWA Device shall correctly advertise DNS server address(es) via DHCP to LAN hosts, based on the configured mode: self, network-provided, or user-configured DNS servers.

Test No.	**GR_TSTP_2.4.7.4**
Test Details	To verify that FWA Device shall support a configurable Dynamic DNS (DDNS) Service, allowing the FWA Device to be addressable from the Internet with an FQDN.
Test Instruments Required	FWA CPE, Power supply unit, DDNS service provider account, Internet/WAN connectivity, LAN client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Configure Dynamic DNS (DDNS) parameters using valid DDNS service credentials. 4. Enable the DDNS service on the FWA Device. 5. Verify that the FWA Device registers and updates its public IP address with the DDNS service. 6. From an external network, attempt to access the FWA Device using the configured FQDN. 7. Verify successful name resolution and reachability of the FWA Device via the FQDN.
Test Limits	NA
Expected Results	The FWA Device shall support configurable Dynamic DNS (DDNS) functionality and shall be reachable from the Internet using an FQDN, with correct and timely IP address updates.

Test No.	**GR_TSTP_2.4.7.5**
Test Details	To verify that Dynamic DNS service, the FWA Device shall send updates to the DDNS server not periodically, but only whenever an IP address change is detected on the Data WAN Interface.
Test Instruments Required	FWA CPE, Power supply unit, DDNS service provider account, Internet/WAN connectivity, LAN client (PC/Laptop), Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Configure and enable the Dynamic DNS (DDNS) service using valid credentials. 4. Verify that no DDNS update is sent without an IP address change. 5. Trigger a change of the WAN IP address (e.g. reconnect WAN interface). 6. Verify that the FWA Device sends a DDNS update immediately after detecting the IP address change. 7. Verify that no periodic DDNS updates are sent in the absence of IP address changes.
Test Limits	NA
Expected Results	The FWA Device shall send DDNS updates only upon detection of a WAN IP address change, and shall not send periodic updates when the IP address remains unchanged.

Test No.	**GR_TSTP_2.4.7.6**
Test Details	To verify that for Static DNS operation the FWA Device shall support Recursive DNS and not Iterative DNS.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Static DNS server configuration
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Configure the FWA Device for Static DNS operation. 4. Configure one or more static DNS server addresses on the FWA Device. 5. Connect a LAN client to the FWA Device. 6. Perform DNS queries from the LAN client. 7. Capture and observe DNS query behavior, if required. 8. Verify that the FWA Device performs recursive DNS resolution and does not perform iterative DNS queries.
Test Limits	NA
Expected Results	For Static DNS operation, the FWA Device shall support Recursive DNS resolution only, and Iterative DNS behavior shall not be observed.

Test No.	**GR_TSTP_2.4.7.7**
Test Details	To verify that FWA Device shall support unencrypted DNS access.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Reachable DNS server, Network protocol analyzer (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Configure DNS parameters on the FWA Device for standard (unencrypted) DNS operation. 3. Connect a LAN client to the FWA Device. 4. Configure the LAN client to use DNS service via the FWA Device. 5. Perform DNS queries (e.g. A/AAAA record lookups) from the LAN client. 6. Optionally capture DNS traffic and verify that DNS queries and responses are sent without encryption.
Test Limits	NA
Expected Results	The FWA Device shall support unencrypted DNS access, and standard DNS queries and responses shall function correctly.

Test No.	**GR_TSTP_2.4.7.8**
Test Details	To verify that The FWA Device shall support DNS access via HTTPS (IETF RFC 8484).
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with DoH capability, Reachable DNS over HTTPS (DoH) server, Network protocol analyzer (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Enable and configure DNS over HTTPS (DoH) functionality, if applicable. 4. Connect a LAN client to the FWA Device. 5. Configure the LAN client to perform DNS queries via DoH. 6. Perform DNS resolution for valid domain names. 7. Verify successful DNS resolution using HTTPS-based DNS queries.
Test Limits	NA
Expected Results	The FWA Device shall support DNS over HTTPS (DoH) in accordance with IETF RFC 8484, and DNS resolution over HTTPS shall function correctly.

Test No.	**GR_TSTP_2.4.7.9**
Test Details	To verify that the FWA Device shall support DNS access via TLS.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with DNS over TLS capability, Reachable DNS over TLS (DoT) server, Network protocol analyzer (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Enable and configure DNS over TLS (DoT) functionality, if applicable. 4. Connect a LAN client to the FWA Device. 5. Configure the LAN client to perform DNS queries using TLS-based DNS. 6. Perform DNS resolution for valid domain names. 7. Verify successful DNS resolution using DNS over TLS.
Test Limits	NA
Expected Results	The FWA Device shall support DNS access via TLS, and DNS queries and responses over a TLS-secured connection shall function correctly.

Test No.	**GR_TSTP_2.4.7.10**
Test Details	To verify that FWA device shall be protected against DNS Rebind Vulnerability.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), DNS server capable of simulating DNS rebinding scenarios, Web server or test service for rebinding validation
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable default security settings related to DNS Rebinding protection, if configurable. 3. Connect a LAN client to the FWA Device. 4. Configure or use a DNS server to perform a DNS rebinding test (changing DNS resolution of the same domain to different IP addresses). 5. Access the rebinding test domain from the LAN client. 6. Verify that the FWA Device blocks or mitigates the DNS rebinding attempt. 7. Verify that access to internal network resources is not allowed via DNS rebinding.
Test Limits	NA
Expected Results	The FWA Device shall be protected against DNS Rebinding attacks, and DNS rebinding attempts shall be blocked or mitigated as per device security mechanisms.

Test No.	**GR_TSTP_2.4.7.11**
Test Details	To verify that to prevent DNS spoofing, source ports and Transaction-IDs shall be selected randomly by the CPE.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Reachable DNS server, Network protocol analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a LAN client to the FWA Device. 3. Configure the LAN client to use DNS service via the FWA Device. 4. Generate multiple DNS queries from the LAN client in quick succession. 5. Capture DNS query packets using a network protocol analyzer. 6. Observe the UDP source ports used for DNS queries. 7. Observe the DNS Transaction IDs in the captured packets. 8. Verify that both source ports and Transaction IDs are randomized across multiple DNS queries.
Test Limits	NA
Expected Results	The FWA Device shall randomly select DNS source ports and Transaction IDs, thereby reducing susceptibility to DNS spoofing attacks.

Test No.	**GR_TSTP_2.4.8.1**
Test Details	To verify that FWA Device shall implement a configurable DeMilitarized Zone (DMZ) functionality, allowing an internal host in LAN to be fully exposed on WAN.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) to act as DMZ host, External WAN client or test service, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable DMZ functionality on the FWA Device. 4. Configure a specific LAN host IP address as the DMZ host. 5. Connect the configured DMZ host to the LAN. 6. From the WAN side, initiate inbound traffic towards the FWA Device. 7. Verify that inbound traffic is forwarded to the configured DMZ host. 8. Verify that the DMZ host is reachable from the WAN without port-specific restrictions.
Test Limits	NA
Expected Results	The FWA Device shall support configurable DMZ functionality, and the configured LAN host shall be fully exposed on the WAN as per DMZ configuration.

Test No.	**GR_TSTP_2.4.8.2**
Test Details	To verify tha the FWA Device shall implement a configurable Port Binding functionality, allowing binding of the WAN connections to none, one or more LAN interfaces (including Wi-Fi SSIDs).
Test Instruments Required	FWA CPE, Power supply unit, LAN client(s) (PC/Laptop), Wi-Fi client(s), Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Enable Port Binding functionality. 4. Configure WAN connection binding to: a. No LAN interface; b. A single LAN interface; c. Multiple LAN interfaces and/or Wi-Fi SSIDs. 5. Connect LAN and Wi-Fi clients to the respective interfaces. 6. Verify connectivity behavior for each binding configuration. 7. Verify that traffic is allowed or blocked according to the configured WAN–LAN binding rules.
Test Limits	NA
Expected Results	The FWA Device shall support configurable Port Binding, allowing WAN connections to be bound to none, one, or multiple LAN interfaces, including Wi-Fi SSIDs, as configured.

Test No.	**GR_TSTP_2.4.8.3**
Test Details	To verify that FWA Device shall implement a configurable Filtering functionality, allowing the creation of entries for blocking/allowing the communication of MAC Addresses on LAN towards specific IP address/range, on specific protocols/ports/port range.
Test Instruments Required	FWA CPE, Power supply unit, LAN client(s) (PC/Laptop) with known MAC addresses, External network or WAN connectivity, Configuration access (e.g. Web UI)\
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Enable Filtering functionality. 4. Create a filtering rule to allow or block traffic from a specific MAC address. 5. Define the rule with destination IP address or IP range. 6. Configure protocol, port, or port range parameters for the rule. 7. Generate traffic from the LAN client matching the rule criteria. 8. Verify that traffic is allowed or blocked according to the configured filtering rule. 9. Modify the rule and re-verify behavior.
Test Limits	NA
Expected Results	The FWA Device shall support configurable filtering rules based on MAC address, destination IP/IP range, protocol, and port/port range, and traffic shall be correctly allowed or blocked as configured.

Test No.	**GR_TSTP_2.4.8.4**
Test Details	To verify that it shall be possible to configure at least 32 Filtering entries.
Test Instruments Required	FWA CPE, Power supply unit, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable Filtering functionality. 4. Create filtering rules sequentially. 5. Continue adding rules until at least 32 filtering entries are configured. 6. Verify that all configured filtering entries are saved and active.
Test Limits	NA
Expected Results	The FWA Device shall allow configuration of at least 32 filtering entries, and all entries shall be stored and applied correctly.

Test No.	**GR_TSTP_2.4.8.5**
Test Details	To verify that FWA Device should implement a configurable (on/off) UPnP Discovery functionality, compliant with the UPnP Forum's Device Architecture and Device Control Protocols standards.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with UPnP capability, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable UPnP Discovery functionality. 4. Connect a UPnP-capable LAN client to the FWA Device. 5. Verify that the FWA Device is discoverable via UPnP from the LAN client. 6. Disable UPnP Discovery functionality. 7. Verify that the FWA Device is no longer discoverable via UPnP.
Test Limits	NA
Expected Results	The FWA Device shall support configurable UPnP Discovery (ON/OFF) functionality, compliant with UPnP Forum standards, and discovery behavior shall reflect the configured state.

Test No.	**GR_TSTP_2.4.8.6**
Test Details	To verify that UPnP functionality shall be blocked on the WAN side.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with UPnP capability, External WAN-side client or test tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Enable UPnP functionality on the LAN side, if configurable. 4. Connect a LAN client and verify that UPnP discovery and control work correctly on the LAN side. 5. From the WAN side, attempt to discover or access the FWA Device using UPnP protocols. 6. Observe the behavior for any UPnP discovery or control attempts from the WAN side.
Test Limits	NA
Expected Results	The FWA Device shall block UPnP functionality on the WAN side, and no UPnP discovery or control shall be possible from the WAN interface, while LAN-side behavior remains unaffected.

Test No.	**GR_TSTP_2.4.8.7**
Test Details	To verify that if the FWA Device supports UPnP, it should be disabled in Factory default configuration.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with UPnP capability, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Perform a factory reset of the FWA Device to restore default settings. 2. Power ON the FWA Device after factory reset. 3. Access the device configuration interface (e.g. Web UI). 4. Check the status of UPnP functionality in the default configuration. 5. From a LAN client, attempt to discover the FWA Device using UPnP discovery. 6. Observe whether UPnP discovery or control is possible.
Test Limits	NA
Expected Results	If UPnP is supported by the FWA Device, it shall be disabled by default in the factory configuration, and no UPnP discovery or control shall be possible unless explicitly enabled by the user.

Test No.	**GR_TSTP_2.4.8.8**
Test Details	To verify that If the FWA Device supports UPnP, rules created for one client device shall apply only to that device and not to other LAN clients (also for the FWA Device itself).
Test Instruments Required	FWA CPE, Power supply unit, Multiple LAN client devices (PC/Laptop) with UPnP capability, Configuration access (e.g. Web UI), External WAN connectivity
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable UPnP functionality on the FWA Device. 3. Connect multiple LAN clients to the FWA Device. 4. From one specific LAN client, create a UPnP rule (e.g. port mapping). 5. Verify that the UPnP rule is active and functional for the originating client. 6. From other LAN clients, attempt to use or access the same UPnP-created rule. 7. Verify that the UPnP rule does not apply to other LAN clients or to the FWA Device itself.
Test Limits	NA
Expected Results	If UPnP is supported, the UPnP rules created by one LAN client shall be applied exclusively to that client and shall not affect other LAN clients or the FWA Device itself.

Test No.	**GR_TSTP_2.4.8.9**
Test Details	To verify that FWA Device should implement a configurable VPN functionality, both as a VPN-client and a VPN-server, with L2TP/IPSec PSK or PPTP.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Remote VPN server / VPN client, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Configure the FWA Device as a VPN Client using L2TP/IPSec PSK or PPTP. 4. Establish a VPN connection to a remote VPN Server and verify successful connection. 5. Configure the FWA Device as a VPN Server using L2TP/IPSec PSK or PPTP. 6. From a remote VPN client, initiate a VPN connection to the FWA Device. 7. Verify successful VPN tunnel establishment and data connectivity in both scenarios.
Test Limits	NA
Expected Results	The FWA Device shall support configurable VPN functionality operating as both a VPN Client and a VPN Server, with support for L2TP/IPSec PSK or PPTP, and VPN connectivity shall function correctly.

Test No.	**GR_TSTP_2.4.8.10**
Test Details	To verify that FWA Device shall implement a Parental Control functionality, letting the user to configure a list of URLs which access must be denied to all (or a configurable subset of) LAN hosts.
Test Instruments Required	FWA CPE, Power supply unit, LAN client(s) (PC/Laptop), Internet/WAN connectivity, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP 1
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable Parental Control functionality. 4. Configure a URL blacklist with one or more domain names or URLs. 5. Apply the restriction to all LAN hosts or to a selected subset of LAN hosts, as configured. 6. From the restricted LAN client(s), attempt to access the blocked URLs. 7. From non-restricted LAN client(s), attempt to access the same URLs (if applicable). 8. Verify access behavior according to the configured parental control rules.
Test Limits	NA
Expected Results	The FWA Device shall support Parental Control functionality, and access to configured blocked URLs shall be denied for the specified LAN hosts while remaining accessible to non-restricted hosts, as per configuration.

Test No.	**GR_TSTP_2.4.8.11**
Test Details	To verify that FWA Device shall implement a per-user device configurable Internet access control functionality, letting the user to configure, for a selected user device, which days of the week/which hours of the day or how many hours per day the Internet access must be allowed/denied.
Test Instruments Required	FWA CPE, Power supply unit, Multiple LAN client devices (PC/Laptop) with identifiable MAC addresses, Internet/WAN connectivity, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable per-device Internet access control functionality. 4. Select a specific user device (identified by MAC address or hostname). 5. Configure Internet access rules for the selected device based on: a. Days of the week; b. Time slots (hours of the day); and/or c. Maximum allowed Internet usage hours per day. 6. Apply the configuration. 7. Verify Internet access from the selected device during allowed periods. 8. Verify Internet access is blocked during denied periods. 9. Verify that other LAN devices are not affected by the configured rules.
Test Limits	NA
Expected Results	The FWA Device shall support per-user device Internet access control, allowing Internet access to be allowed or denied based on configured schedules or usage limits, without impacting other LAN devices.

Test No.	**GR_TSTP_2.4.8.12**
Test Details	To verify that FWA Device shall implement a configurable (at least with on/off behaviors) stateful IPv4 Firewall.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), External WAN client or test service, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Verify that stateful IPv4 Firewall functionality is available. 4. Enable the IPv4 Firewall and apply the configuration. 5. Generate inbound and outbound IPv4 traffic between LAN and WAN. 6. Verify that the firewall allows or blocks traffic based on stateful inspection rules. 7. Disable the IPv4 Firewall. 8. Repeat traffic tests and verify the change in behavior.
Test Limits	NA
Expected Results	The FWA Device shall support a configurable stateful IPv4 Firewall with ON/OFF control, and firewall behavior shall change appropriately based on configuration.

Test No.	**GR_TSTP_2.4.8.13**
Test Details	To verify that The FWA Device shall implement Denial of Service (DoS) protection functionality.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), External WAN-side traffic generation tool (DoS simulation), Network monitoring / protocol analysis tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Verify that DoS protection functionality is available and enabled by default or configurable. 4. Establish normal LAN–WAN connectivity and verify baseline traffic flow. 5. Generate high-rate or malformed traffic patterns from the WAN side simulating DoS attack scenarios (e.g. SYN flood, UDP flood). 6. Monitor the behavior of the FWA Device during the attack simulation. 7. Verify that legitimate traffic is still handled appropriately and that the device remains responsive. 8. Verify that attack traffic is detected, limited, or blocked by the DoS protection mechanism.
Test Limits	NA
Expected Results	The FWA Device shall implement DoS protection functionality, and simulated DoS attack traffic shall be detected and mitigated, while maintaining stable operation for legitimate traffic.

Test No.	**GR_TSTP_2.4.8.14**
Test Details	To verify that DoS functionality shall remain enabled even when the Firewall has been disabled by user configuration.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), External WAN-side traffic generation tool (DoS simulation), Configuration access (e.g. Web UI), Network monitoring / protocol analysis tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Disable the stateful firewall functionality via user configuration. 4. Verify normal LAN–WAN connectivity after firewall is disabled. 5. Generate DoS attack traffic patterns from the WAN side (e.g. SYN flood, malformed packets). 6. Monitor the behavior of the FWA Device during the attack simulation. 7. Verify that DoS protection mechanisms remain active despite the firewall being disabled. 8. Verify that the device remains stable and responsive, and that attack traffic is mitigated.
Test Limits	NA
Expected Results	The FWA Device shall maintain DoS protection functionality even when the firewall is disabled by user configuration, and DoS attacks shall continue to be detected and mitigated.

Test No.	**GR_TSTP_2.4.8.15**
Test Details	To verify that behavior of the FWA Device to ICMP messages coming from WAN interface shall be configurable.
Test Instruments Required	FWA CPE, Power supply unit, External WAN-side client or test tool capable of generating ICMP traffic, LAN client (PC/Laptop), Configuration access (e.g. Web UI), Network protocol analyzer (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Locate the configuration settings related to ICMP handling on the WAN interface. 4. Configure the FWA Device to allow ICMP messages from the WAN interface. 5. From the WAN side, send ICMP Echo Request messages towards the FWA Device. 6. Verify that the FWA Device responds according to the configured behavior. 7. Reconfigure the FWA Device to block ICMP messages from the WAN interface. 8. Repeat the ICMP tests from the WAN side. 9. Verify that ICMP messages are handled in accordance with the updated configuration.
Test Limits	NA
Expected Results	The FWA Device shall support configurable handling of ICMP messages received from the WAN interface, and ICMP behavior shall change according to user configuration.

Test No.	**GR_TSTP_2.4.8.16**
Test Details	To verify that FWA Device shall implement a configurable (at least with on/off behaviors) stateful IPv6 Firewall.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv6 capability, External WAN-side client or test service, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Verify that stateful IPv6 Firewall functionality is available. 4. Enable the IPv6 Firewall and apply the configuration. 5. Generate inbound and outbound IPv6 traffic between LAN and WAN. 6. Verify that the firewall allows or blocks traffic based on stateful inspection rules. 7. Disable the IPv6 Firewall. 8. Repeat IPv6 traffic tests and verify the change in behavior.
Test Limits	NA
Expected Results	The FWA Device shall support a configurable stateful IPv6 Firewall with ON/OFF control, and firewall behavior shall change appropriately based on configuration.

Test No.	**GR_TSTP_2.4.8.17**
Test Details	To verify that The IPv6 and IPv4 firewall shall be independently configurable.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with IPv4 and IPv6 capability, External WAN-side client or test service, Configuration access (e.g. Web UI)
Test Setup	TEST SETU X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Enable the IPv4 firewall and disable the IPv6 firewall. 4. Generate IPv4 traffic between LAN and WAN and verify firewall behavior. 5. Generate IPv6 traffic between LAN and WAN and verify firewall behavior. 6. Reconfigure the FWA Device to disable the IPv4 firewall and enable the IPv6 firewall. 7. Repeat IPv4 and IPv6 traffic tests. 8. Verify that firewall behavior for IPv4 and IPv6 traffic follows their independent configuration settings
Test Limits	NA
Expected Results	The FWA Device shall support independent configuration of IPv4 and IPv6 firewalls, and each firewall shall operate according to its respective configuration without impacting the other.

Test No.	**GR_TSTP_2.4.8.18**
Test Details	To verify that IPv6 and IPv4 firewall status shall be presented independently.
Test Instruments Required	FWA CPE, Power supply unit, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration or status interface (e.g. Web UI) of the FWA Device. 3. Locate the firewall status display for IPv4 and IPv6. 4. Verify that the IPv4 firewall status (e.g. Enabled/Disabled) is displayed separately. 5. Verify that the IPv6 firewall status (e.g. Enabled/Disabled) is displayed separately. 6. Change the configuration of the IPv4 firewall and observe its status indication. 7. Change the configuration of the IPv6 firewall and observe its status indication. 8. Verify that changes to one firewall do not affect the status display of the other.
Test Limits	NA
Expected Results	The FWA Device shall present IPv4 and IPv6 firewall status independently, and each firewall's status shall accurately reflect its respective configuration.

Test No.	**GR_TSTP_2.4.8.19**
Test Details	To verify that FWA Device shall NOT allow outgoing traffic originated from a LAN IP address outside the range defined by the FWA Device itself.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) with manual IP configuration capability, External WAN connectivity, Network protocol analyzer (optional)
Test Setup	TEST SETUP 1
Test Procedure	1. Power ON the FWA Device. 2. Configure the LAN IP address range and DHCP pool on the FWA Device. 3. Connect a LAN client to the FWA Device. 4. Manually configure the LAN client with an IPv4 address outside the configured LAN IP range. 5. Attempt to generate outgoing traffic from the LAN client towards the WAN. 6. Observe traffic behavior using connectivity tests or a network protocol analyzer. 7. Verify that outgoing traffic from the out-of-range IP address is blocked or dropped. 8. Reconfigure the LAN client with a valid IP address within the defined range and verify normal connectivity.
Test Limits	NA
Expected Results	The FWA Device shall block outgoing traffic originating from LAN IP addresses outside the configured LAN IP address range, and shall allow traffic only from valid, device-defined LAN IP ranges.

Test No.	**GR_TSTP_2.4.8.20**
Test Details	To verify that In Factory Reset condition, the status of the firewall shall be enabled
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop), Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Perform a factory reset of the FWA Device. 2. Power ON the FWA Device after factory reset. 3. Connect a LAN client to the FWA Device. 4. Access the device configuration or status interface (e.g. Web UI). 5. Check the firewall status immediately after factory reset. 6. Verify that the firewall is enabled by default.
Test Limits	NA
Expected Results	After factory reset, the firewall on the FWA Device shall be enabled by default, ensuring baseline security without user configuration.

Test No.	**GR_TSTP_2.4.9.1**
Test Details	To verify that it shall be possible for a procurer to customize a FWA Device in addition to the requirements mentioned.
Test Instruments Required	FWA CPE, Power supply unit, Customization profile / requirements provided by procurer, Configuration access (e.g. Web UI / CLI), Documentation of supported customization options
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Review the customization requirements specified by the procurer. 3. Access the configuration or customization interface of the FWA Device. 4. Apply procurer-specific customizations (e.g. feature enable/disable, branding, default configuration parameters). 5. Save and apply the customized configuration. 6. Reboot the FWA Device, if required. 7. Verify that the applied customizations are retained and operational. Verify that the customized device continues to meet all baseline functional requirements.
Test Limits	NA
Expected Results	The FWA Device shall support procurer-specific customization beyond the baseline requirements, and all applied customizations shall function correctly without impacting mandatory features.

Test No.	**GR_TSTP_2.4.10.1**
Test Details	To verify that FWA Device shall support a Universal Serial Bus (USB) interface.
Test Instruments Required	FWA CPE, Power supply unit, USB peripheral device (e.g. USB storage or USB modem), Configuration access (e.g. Web UI), LAN client (PC/Laptop)
Test Setup	TEST SETUP 1
Test Procedure	1. Power ON the FWA Device. 2. Connect a USB peripheral device to the USB port of the FWA Device. 3. Verify that the FWA Device detects the USB interface and the connected peripheral. 4. Access the device management interface to confirm USB interface status. 5. Verify that the USB interface operates according to the supported functionality (e.g. device recognition, power supply).
Test Limits	NA
Expected Results	The FWA Device shall support a USB interface, and connected USB peripherals shall be detected and recognized as per the device capabilities.

Test No.	**GR_TSTP_2.4.10.2**
Test Details	To verify that USB interface shall be compliant to the Universal Serial Bus Specification version 3.1 or higher.
Test Instruments Required	FWA CPE, Power supply unit, USB 3.1 or higher compliant peripheral device, USB specification compliance documentation (if available)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a USB 3.1 or higher compliant USB peripheral to the USB port of the FWA Device. 3. Verify that the USB interface negotiates SuperSpeed (or higher) operation. 4. Check the device management interface or status indicators for USB version compliance. 5. Verify normal operation of the connected USB peripheral.
Test Limits	NA
Expected Results	The USB interface of the FWA Device shall be compliant with USB Specification version 3.1 or higher, and connected peripherals shall operate accordingly.

Test No.	**GR_TSTP_2.4.10.3**
Test Details	To verify that the USB Interface receptacle shall be any of Type-A, Type-Micro B or Type-C.
Test Instruments Required	FWA CPE, Power supply unit, Visual inspection tools (as required), USB Type-A / Type-Micro-B / Type-C cable or connector
Test Setup	TEST SETUP X
Test Procedure	1. Power OFF the FWA Device. 2. Visually inspect the USB interface receptacle provided on the FWA Device. 3. Identify the physical USB connector type present on the device. 4. Verify that the connector type matches USB Type-A, Type-Micro-B, or Type-C. 5. Optionally connect a compatible USB cable to confirm mechanical compatibility
Test Limits	NA
Expected Results	The USB interface receptacle of the FWA Device shall be Type-A, Type-Micro-B, or Type-C, compliant with the specified requirement.

Test No.	**GR_TSTP_2.4.10.4**
Test Details	To verify that the USB Interface shall supply a current of at least 1.5A.
Test Instruments Required	FWA CPE, Power supply unit, USB load device or USB power meter (capable of measuring current), USB cable compatible with the FWA Device USB interface
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a USB power meter or a USB load device to the USB interface of the FWA Device. 3. Gradually apply load through the USB load device. 4. Measure the output current supplied by the USB interface. 5. Verify that the USB interface is capable of supplying at least 1.5 A without interruption or shutdown. 6. Observe stability of voltage and current during the test.
Test Limits	NA
Expected Results	The USB interface of the FWA Device shall supply a current of at least 1.5 A, and the interface shall remain stable while delivering the required current.

Test No.	**GR_TSTP_2.4.10.5**
Test Details	To verify that the FWA Device should use SMBv2 (or higher) protocol to enable the sharing of an USB Mass Storage Hard Disk Devices between LAN hosts.
Test Instruments Required	FWA CPE, Power supply unit, USB Mass Storage hard disk device, LAN client(s) (PC/Laptop) with SMBv2 or higher support, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a USB Mass Storage hard disk device to the USB port of the FWA Device. 3. Access the configuration interface of the FWA Device. 4. Enable USB storage sharing functionality. 5. Verify that the file sharing protocol used is SMBv2 or higher. 6. Connect one or more LAN hosts to the FWA Device. 7. From LAN hosts, access the shared USB storage device. 8. Verify read/write access to the shared storage. 9. Confirm that the connection uses SMBv2 or higher (e.g. via client settings or protocol information).
Test Limits	NA
Expected Results	The FWA Device shall use SMBv2 or higher protocol for sharing USB Mass Storage devices among LAN hosts, and shared storage shall be accessible and functional.

Test No.	**GR_TSTP_2.4.10.6**
Test Details	To verify that FWA Device should use SMBv2 (or higher) protocol to enable the print sharing between the LAN hosts, supporting the standard error messages via SMB protocol.
Test Instruments Required	FWA CPE, Power supply unit, USB printer or network printer connected to FWA Device, LAN client(s) (PC/Laptop) with SMBv2 or higher support, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a printer to the FWA Device (USB or supported interface). 3. Access the configuration interface of the FWA Device. 4. Enable print sharing functionality on the FWA Device. 5. Verify that the print sharing service uses SMBv2 or higher protocol. 6. Connect one or more LAN hosts to the FWA Device. 7. From LAN hosts, add the shared printer and initiate a print job. 8. Verify successful printing from multiple LAN hosts. 9. Trigger an error condition (e.g. printer offline, paper out). 10. Verify that standard SMB error messages are correctly delivered to the LAN hosts.
Test Limits	NA
Expected Results	The FWA Device shall use SMBv2 or higher protocol for print sharing among LAN hosts, and standard SMB error messages shall be correctly supported and presented.

Test No.	**GR_TSTP_2.4.10.7**
Test Details	To verify that FWA Device shall NOT support SMBv1 protocol.
Test Instruments Required	FWA CPE, Power supply unit, LAN client (PC/Laptop) capable of initiating SMBv1 connection attempts, Configuration access (e.g. Web UI), Network protocol analyzer (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface of the FWA Device. 3. Verify available file/print sharing protocol settings. 4. Ensure that SMBv1 is not enabled or selectable in the configuration. 5. Connect a LAN client to the FWA Device. 6. From the LAN client, attempt to establish a file or print sharing session using SMBv1. 7. Observe the connection behavior and any error messages. 8. Optionally capture traffic using a network protocol analyzer to verify protocol usage
Test Limits	NA
Expected Results	The FWA Device shall not support SMBv1 protocol, and any attempt to establish SMBv1-based communication shall be rejected or blocked, ensuring improved security.

Test No.	**GR_TSTP_2.4.10.8**
Test Details	To verify that USB Interface shall block firmware upgrade, logging, tracing and similar local management and troubleshooting activities on the FWA Device.
Test Instruments Required	FWA CPE, Power supply unit, USB storage device, LAN client (PC/Laptop), Configuration / management access (e.g. Web UI or CLI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Connect a USB storage device to the USB interface of the FWA Device. 3. Access the management interface of the FWA Device. 4. Attempt to perform firmware upgrade using the USB interface. 5. Attempt to access or enable logging, tracing, or diagnostic functions via the USB interface. 6. Observe whether any local management or troubleshooting actions can be initiated through USB. 7. Verify normal management and troubleshooting operations remain accessible only through authorized interfaces (e.g. Web UI, network-based management).
Test Limits	NA
Expected Results	The USB Interface of the FWA Device shall block firmware upgrades, logging, tracing, and other local management or troubleshooting activities, ensuring that such operations are not permitted via USB.

Test No.	**GR_TSTP_2.5.1.1**
Test Details	To verify that FWA Device shall integrate a Wi-Fi 4 (IEEE 802.11n) Access Point (AP), or later standards, operating on 2.4 GHz bands.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11n or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that the 2.4 GHz Wi-Fi radio is enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11n or later). 6. Connect a Wi-Fi client device to the FWA Device using the 2.4 GHz band. 7. Verify successful Wi-Fi association and IP address assignment. 8. Optionally verify operational parameters (channel, bandwidth, mode) using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11n (Wi-Fi 4) or later standards, operating on the 2.4 GHz band, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.1.2**
Test Details	To verify that FWA Device shall integrate a Wi-Fi 5 (IEEE 802.11ac) Access Point (AP), or later standards, operating on 5 GHz bands.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ac or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that the 5 GHz Wi-Fi radio is enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11ac or later). 6. Connect a Wi-Fi client device to the FWA Device using the 5 GHz band. 7. Verify successful Wi-Fi association and IP address assignments. 8. Optionally verify operational parameters (channel, bandwidth, mode) using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11ac (Wi-Fi 5) or later standards, operating on the 5 GHz band, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.1.3**
Test Details	The FWA Device should integrate a Wi-Fi 6 (IEEE 802.11ax) Access Point (AP), or later standards, operating on both 2.4 and 5 GHz bands.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ax or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that both 2.4 and 5 GHz Wi-Fi radios are enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11ax or later). 6. Connect a Wi-Fi client device to the FWA Device using the 2.4 band and check for successful Wi-Fi association and IP address. 7. Repeat the step 6 with 5 GHz band. 8. Optionally verify operational parameters (channel, bandwidth, mode) using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11ax (Wi-Fi 6) or later standards, operating on the 2.4 and 5 GHz bands, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.1.4**
Test Details	To verify that FWA Device may integrate a Wi-Fi 6E (IEEE 802.11ax) Access Point (AP), or later standards, operating on 2.4, 5 and 6 GHz bands.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ax or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that 2.4, 5 and 6 GHz Wi-Fi radios are enabled. 5. From the configuration or status page, verify the supported Wi-Fi 6E standard (IEEE 802.11ax or later). 6. Connect a Wi-Fi client device to the FWA Device using the 2.4 band and check for successful Wi-Fi association and IP address. 7. Repeat the step 6 with 5 GHz band. 8. Repeat the step 6 with 6 GHz band. 9. Optionally verify operational parameters (channel, bandwidth, mode) using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11ax (Wi-Fi 6E) or later standards, operating on the 2.4, 5 and 6 GHz bands, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.1.5**
Test Details	To verify that FWA Device may integrate a Wi-Fi 7 (IEEE 802.11be) Access Point (AP), or later standards, operating on 2.4,5 and 6 GHz bands.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11be or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI).
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that the 2.4, 5 and 6 GHz Wi-Fi radios are enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11be or later). 6. Connect a Wi-Fi client device to the FWA Device using the 2.4 band and check for successful Wi-Fi association and IP address. 7. Repeat step 6 with 5 GHz band. 8. Repeat step 6 with 6 GHz band. 9. Optionally verify operational parameters (channel, bandwidth, mode) using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11be (Wi-Fi 7) or later standards, operating on the 2.4,5 and 6 GHz bands, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.1.7**
Test Details	To verify that FWA Device shall comply to WPA3 and Wi-Fi Protected Setup (PBC).
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) which Support WAP3 and PBC requirements. Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI).
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Identify the applicable WPA3 and PBC requirements of the FWA device. 3. Enable WPA3 mode via web UI on AP. Save and apply the configs. 4. Connect to the WPA3 capable client. 5. Verify successful association and IP address assignment. 6. Run ping test and verify packet encryption using WPA3. 7. Reconnect to the client device. 8. Verify that the client device is connected by pressing the WPS button on the AP and client device. 9. Check client device connected without entering password. 10. Optionally verify operational parameters.
Test Limits	NA
Expected Results	The FWA Device shall be compliant with WPA3 and PBC requirement, and no mandatory requirement shall be unmet.

Test No.	**GR_TSTP_2.5.2.1**
Test Details	To verify that the Wi-Fi AP of a FWA Device shall support at least MIMO 2x2 on all supported frequency bands.
Test Instruments Required	1. FWA and AP. 2. Wi-Fi client device supporting 2x2 MIMO (laptop / smartphone / Wi-Fi test adapter). 3. Wi-Fi Analyzer tool. 4. GUI of FWA.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Base Station, RU, and FWA Device. 2. Verify that FWA device is registered and in service. 3. Enable Wi-Fi on the FWA device for all supported bands. 4. Connect a 2x2 MIMO capable Wi-Fi client to the FWA AP on **2.4 GHz** band. 5. Using Wi-Fi analyzer tool or client adapter properties, verify. MIMO configuration = **2x2** 6. Repeat steps 4–5 for **5 GHz** bands.
Test Limits	NA
Expected Results	FWA Wi-Fi AP shall advertise and operate with **at least 2x2 MIMO** on all supported frequency bands.

Test No.	**GR_TSTP_2.5.2.2**
Test Details	To verify that the Wi-Fi AP of a FWA Device should support MIMO 4x4 on all supported frequency bands.
Test Instruments Required	1. FWA and AP. 2. Wi-Fi client device supports 4x4 MIMO (laptop / smartphone / Wi-Fi test adapter). 3. Wi-Fi Analyzer tool. 4. GUI of FWA.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Base Station, RU, and FWA Device. 2. Verify that FWA device is registered and in service. 3. Enable Wi-Fi on the FWA device for all supported bands. 4. Connect a 2x2 MIMO capable Wi-Fi client to the FWA AP on **2.4 GHz** band. 5. Using Wi-Fi analyzer tool or client adapter properties, verify. MIMO configuration = **4x4** 6. Repeat steps 4–5 for **5 GHz** bands.
Test Limits	NA
Expected Results	FWA Wi-Fi AP shall advertise and operate with **4x4 MIMO** on all supported frequency bands.

Test No.	**GR_TSTP_2.5.2.3**
Test Details	To verify that Wi-Fi AP of a FWA Device may support MIMO higher than 4x4 on some or all supported frequency bands.
Test Instruments Required	1. FWA and AP. 2. Wi-Fi client device supporting > 4x4 MIMO (laptop / smartphone / Wi-Fi test adapter). 3. Wi-Fi Analyzer tool. 4. GUI of FWA.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Base Station, RU, and FWA Device. 2. Verify that FWA device is registered and in service. 3. Enable Wi-Fi on the FWA device for all supported bands. 4. Connect a 2x2 MIMO capable Wi-Fi client to the FWA AP on **2.4 GHz** band. 5. Using Wi-Fi analyzer tool or client adapter properties, verify. MIMO configuration = **8x8.** 6. Repeat steps 4–5 for **5 GHz** bands.
Test Limits	NA
Expected Results	FWA Wi-Fi AP shall advertise and support MIMO configurations higher than 4x4 on supported frequency bands.

Test No.	**GR_TSTP_2.5.2.4**
Test Details	To verify that an 802.11n AP of a FWA Device shall support a bandwidth of 40 MHz.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11n or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11n or later). 5. Connect a Wi-Fi client device to the FWA Device. 6. Verify successful Wi-Fi association and IP address assignments. 7. Confirm that AP operates with a 40 MHz bandwidth using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11n, supports 40MHz bandwidth, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.2.5**
Test Details	To verify that an 802.11ac AP of a FWA Device shall support a bandwidth of 80 MHz in the 5 GHz band.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ac or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that the 5 GHz Wi-Fi radio is enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11ac or later). 6. Connect a Wi-Fi client device to the FWA Device using the 5 GHz band. 7. Verify successful Wi-Fi association and IP address assignments. 8. Confirm that AP operates with an 80 MHz bandwidth in the 5 GHz by using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11ac or later standards, operating on the 5 GHz band with an 80 MHz bandwidth, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.2.6**
Test Details	To verify that an 802.11ax AP of a FWA Device shall support a bandwidth of 40 MHz in the 2.4 GHz band.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ax or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that the 2.4 GHz Wi-Fi radio is enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11ax or later). 6. Connect a Wi-Fi client device to the FWA Device using the 2.4 GHz band. 7. Verify successful Wi-Fi association and IP address assignments. 8. Confirm that AP operates with a 40 MHz bandwidth in the 2.4 GHz using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11ax or later standards, operating on the 2.4 GHz band with a 40 MHz bandwidth, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.2.7**
Test Details	To verify that an 802.11ax AP of a FWA Device shall support a bandwidth of 80 MHz in the 5 GHz band.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ax or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that the 5 GHz Wi-Fi radio is enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11ax or later). 6. Connect a Wi-Fi client device to the FWA Device using the 5 GHz band. 7. Verify successful Wi-Fi association and IP address assignments. 8. Confirm that AP operates with an 80 MHz bandwidth in the 5 GHz by using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11ax or later standards, operating on the 5 GHz band with an 80 MHz bandwidth, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.2.8**
Test Details	To verify that An 802.11ax AP of a FWA Device should support a bandwidth of 160 MHz in the 5 GHz band.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ax or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Verify that the 5 GHz Wi-Fi radio is enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11ax or later). 6. Connect a Wi-Fi client device to the FWA Device using the 5 GHz band. 7. Verify successful Wi-Fi association and IP address assignments. 8. Confirm that AP operates with a160 MHz bandwidth in the 5 GHz by using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi Access Point supporting IEEE 802.11ax or later standards, operating on the 5 GHz band with a 160 MHz bandwidth, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.2.9**
Test Details	To verify that An 802.11ax (Wi-Fi 6E) AP of a FWA Device should support a bandwidth of 160 MHz in the 6 GHz band.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ac or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi 6E Access Point functionality. 4. Verify that the 5 GHz Wi-Fi 6E radio is enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11ax or later). 6. Connect a Wi-Fi client device to the FWA Device using the 6 GHz band. 7. Verify successful Wi-Fi 6E association and IP address assignments. 8. Confirm that AP operates with a160 MHz bandwidth in the 6 GHz using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi 6E Access Point supporting IEEE 802.11ax or later standards, operating on the 6 GHz band with a 160 MHz bandwidth, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.2.10**
Test Details	To verify that an 802.11be (Wi-Fi 7) AP of a FWA Device should support a bandwidth of 320 MHz in the 6 GHz band.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ac or higher, Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi 7 Access Point functionality. 4. Verify that the 6 GHz Wi-Fi 7 radio is enabled. 5. From the configuration or status page, verify the supported Wi-Fi standard (IEEE 802.11be or later). 6. Connect a Wi-Fi client device to the FWA Device using the 6 GHz band. 7. Verify successful Wi-Fi 7 association and IP address assignments. 8. Confirm that AP operates with a 320 MHz bandwidth in the 6 GHz using a Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall integrate a Wi-Fi 7 Access Point supporting IEEE 802.11be or later standards, operating on the 6 GHz band with a 320 MHz bandwidth, and Wi-Fi connectivity shall function correctly.

Test No.	**GR_TSTP_2.5.2.11**
Test Details	To verify that An 802.11n AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 64-QAM with coding 5/6.
Test Instruments Required	1. FWA and AP. 2. Wi-Fi client device supporting full 802.11n MCS set 3. FWA GUI. 4. Throughput validation tool (iperf3).
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Verify that FWA Device is operational, and Wi-Fi AP is enabled. 3. Configure Wi-Fi AP to **802.11n mode**. 4. Set channel bandwidth to **20 MHz**. 5. Using Wi-Fi test tools or AP capability reports, verify support for (BPSK, QPSK, 16QAM, 64QAM). 6. Verify coding rates including (½, 2/3, ¾, 5/6). 7. Optionally run throughput tests to confirm highest MCS is achievable under good RF conditions.
Test Limits	NA
Expected Results	The FWA Wi-Fi AP shall be capable of operating with all mandatory 802.11n MCS rates.

Test No.	**GR_TSTP_2.5.2.12**
Test Details	To verify that An 802.11ac AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 256-QAM with coding 5/6.
Test Instruments Required	1. FWA and AP. 2. Wi-Fi Analyzer. 3. FWA GUI. 4. Wi-Fi client device supporting full 802.11ac MCS set.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Verify that FWA Device is operational, and Wi-Fi AP is enabled. 3. Configure Wi-Fi AP to **802.11ac mode**. 4. Set channel bandwidth to **20 MHz**. 5. Using Wi-Fi test tools or AP capability reports, verify support for (BPSK, QPSK, 16QAM, 64QAM). 6. Verify coding rates including (½, 2/3, ¾, 5/6). 7. Optionally run throughput tests to confirm highest MCS is achievable under good RF conditions. 8. Verify operation for all supported spatial streams (e.g., 2x2, 3x3, 4x4).
Test Limits	NA
Expected Results	The FWA Wi-Fi AP shall implement and operate with all mandatory 802.11ac MCS rates.

Test No.	**GR_TSTP_2.5.2.13**
Test Details	An 802.11ax/be AP of a FWA Device shall support all the Modulation and coding schemes foreseen by the standard, up to 1024-QAM with coding 5/6.
Test Instruments Required	5. FWA and AP. 6. Wi-Fi Analyzer. 7. FWA GUI. 8. Wi-Fi client device supporting full 802.11ac MCS set.
Test Setup	TEST SETUP X
Test Procedure	9. Power ON the FWA Device. 10. Verify that FWA Device is operational, and Wi-Fi AP is enabled. 11. Configure Wi-Fi AP to **802.11ax/be mode**. 12. Set channel bandwidth to **20 MHz**. 13. Using Wi-Fi test tools or AP capability reports, verify support for (BPSK, QPSK, 16QAM, 64QAM, 256 QAM, 1024 QAM). 14. Verify coding rates including (½, 2/3, ¾, 5/6). 15. Optionally run throughput tests to confirm highest MCS is achievable under good RF conditions. 16. Verify operation for all supported spatial streams (e.g., 2x2, 3x3, 4x4).
Test Limits	NA
Expected Results	The FWA Wi-Fi AP shall implement and operate with all mandatory 802.11ac MCS rates.

Test No.	**GR_TSTP_2.5.3.1**
Test Details	To verify that the AP of a FWA Device shall offer a throughput coherent with the theoretical maximum physical bit rate attainable by the AP characteristics, at least 70% of Maximum Physical Speed with TCP and UDP traffic in a “clean” environment.
Test Instruments Required	FWA Device Access Point Power supply unit to FWA Device and AP Wi-Fi client device (PC/Laptop/Smartphone) supporting IEEE 802.11ac or higher, A computer running with Iperf3 server
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA and AP Device. 2. Connect two PC to same AP 2.4GHz or 5GHz 3. Run Iperf3 client on one PC and Iperf3 server on another PC 4. Verify UDP and TCP speed using iperf3 tool between two PCs 5. iperf3 TCP and UDP client and server commands
Test Limits	NA
Expected Results	The two PCs connected to same AP shall get more than 70% with 2.4GHz or 5GHz for UDP or TCP.

Test No.	**GR_TSTP_2.5.3.2**
Test Details	To verify that all the Wi-Fi interfaces shall NOT exceed the regulatory limits as defined by WPC regards output power level (EIRP).
Test Instruments Required	1. FWA. 2. Power Meter with suitable RF sensors. 3. Calibrated Wi-Fi test antenna(s). 4. RF shield box or anechoic chamber (recommended).
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Enable Wi-Fi AP on all supported frequency bands. 3. Configure Wi-Fi transmit power to maximum allowed by device settings. 4. Force continuous transmission using, iPerf traffic 5. Wi-Fi test mode / continuous wave (CW) if supported 6. Measure conducted output power at RF port (if available). 7. Measure radiated EIRP using antenna method (if radiated test is required).
Test Limits	NA
Expected Results	All Wi-Fi interfaces **shall operate within** WPC-defined maximum EIRP limits.

Test No.	**GR_TSTP_2.5.3.3**
Test Details	To verify that FWA device shall have the capability to perform the speed Test or other equivalent measures of initiating throughput tests by the Service Provider.
Test Instruments Required	FWA CPE Power supply Unit LAN client (PC / Laptop) Service Provider management system or test platform capable of: • Triggering speed/throughput tests • Collecting test results Throughput test server
Test Setup	TEST SETUP X
Test Procedure	1. FWA device powered ON and active network connectivity 2. No active user traffic that may significantly impact results 3. Verify Throughput Test Capability Exists by Selecting the target FWA device and check available diagnostics or performance test options. 4. Initiate the Downlink Throughput Test and observe test execution status. 5. Initiate Uplink Throughput Test 6. Verify Test Completion and Results and retrieve throughput results. 7. If above method of speedtesting is not an option, initiate iPerf based testing
Test Limits	NA
Expected Results	FWA device is able to initiate throughput and have provision on testing it.

Test No.	**GR_TSTP_2.5.4.1**
Test Details	To verify that The AP of a FWA Device shall permit the configuration of one main SSID for each supported band.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power On the FWA Device 2. Log in to the FWA AP management interface. 3. Navigate to Wi-Fi settings for Band-1 (e.g., 2.4 GHz, 5 GHz). 4. Select the first available band and configure one main SSID using a common prefix with a band identifier. 5. Save / apply the configuration for the selected band. 6. Repeat step 4 and step 5 to configure the remaining SSID and remaining supported band until all bands have one main SSID configured.
Test Limits	NA
Expected Results	Using a Wi-Fi client or analyzer, scan for available networks. Confirm that: • FWA_Main_24G is visible on the 2.4 GHz band. • FWA_Main_5G is visible on the 5 GHz band.

Test No.	**GR_TSTP_2.5.4.2**
Test Details	To verify that the AP of a FWA Device shall permit the configuration of at least one guest SSID.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power FWA and log in to the FWA AP management interface. 2. Navigate to Wi-Fi / Wireless Settings. 3. Verify the presence of a Guest Wi-Fi / Guest SSID configuration option. 4. Enable the Guest SSID feature. 5. Configure these parameters: SSID name, Enable SSID broadcast, Enable Guest Id isolation (if configurable) 6. Save and apply the configuration.
Test Limits	NA
Expected Results	1. A Guest SSID configuration option is available. 2. The Guest SSID configuration is accepted.

Test No.	**GR_TSTP_2.5.4.3**
Test Details	To verify that the guest SSID(s) shall NOT permit access to the configuration of the FWA Device.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. FWA device powered ON and operational 2. At least one Main SSID configured 3. At least one Guest SSID configured and enabled 4. Using a client device, connect to the Guest SSID. 5. From the guest-connected client, open a browser. 6. Attempt SSH or Telnet access to the FWA device IP.
Test Limits	NA
Expected Results	1. Access is denied, blocked, or unreachable. 2. Connection attempt fails.

Test No.	**GR_TSTP_2.5.4.4**
Test Details	To verify that the guest SSID(s) shall NOT permit traffic between hosts in LAN.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Connect client-1 to Main SSID. 2. Connect client-2 to wired LAN. 3. Connect client-3 to Guest SSID. 4. Connect client-4 to Guest SSID. 5. Try to communicate from Client-1 to Client-2 through ping. 6. From Client-3 attempt to ping client-1 7. From Client-3 attempt to ping Client-2 8. From Client-3 attempt to ping Client-4 9. Verify the test results.
Test Limits	NA
Expected Results	1. For step 5, LAN connectivity works normally for non-guest clients. 2. For step 6, All attempts fail (timeout, unreachable, or blocked). 3. For step 7, All attempts fail. 4. For step 8, Access to Guest client is blocked or restricted.

Test No.	**GR_TSTP_2.5.4.5**
Test Details	To verify that each SSID shall be configurable to operate on one or more frequency bands.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Log in to the FWA device management interface. 2. Create a new SSID named "FWA_Test_SSID". 3. In the SSID configuration, enable **2.4 GHz band**, disable **5 GHz,** Save and apply configuration. 4. Connect a Wi-Fi client to "FWA_Test_SSID". 5. Verify: Connection is established on 2.4 GHz; Client receives IP address. 6. Modify SSID configuration to disable 2.4 GHz and enable 5 GHz. 7. Scan Wi-Fi networks on both bands and connect the Client on 5 GHz. 8. Modify SSID configuration enable both 2.4 GHz and 5 GHz 9. Verify SSID appears on both bands by Connecting two different clients to 2.5 and 5 GHz respectively.
Test Limits	NA
Expected Results	1. After step 3 "FWA_Test_SSID" shall be visible on 2.4 GHz should not be visible on 5 GHz. 2. After setp 5 "FWA_Test_SSID" shall be visible on 5 GHz should not be visible on 2.5 GHz. 3. After step 8 SSID should be visible on both bands.

Test No.	**GR_TSTP_2.5.4.6**
Test Details	To verify that each SSID shall be configurable as regards the Authentication and Security mechanisms adopted.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Log in to the FWA management interface. 2. Create a new SSID or select an existing one (e.g., FWA_Secure_SSID). 3. Set authentication/security mode to open and disable encryption. 4. Connect a client to the SSID without entering a password. 5. Change SSID security to WPA2-PSK and Set a valid passphrase.
Test Limits	NA
Expected Results	1. After step 2, Client connects successfully without credentials. 2. After step 5, Connection fails with incorrect password but succeeds with correct password.

Test No.	**GR_TSTP_2.5.4.7**
Test Details	To verify that each SSID shall be configurable as regards the SSID broadcasting.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power on FWA and Log in to the FWA device management interface. 2. Create two SSIDs:“FWA_SSID_VISIBLE” and “FWA_SSID_HIDDEN”. 3. Enable SSID Broadcast for FWA_SSID_VISIBLE and disable for the other. 4. Use a Wi-Fi client or analyzer to scan available networks. 5. On the Wi-Fi client, manually add a network, SSID name: “FWA_SSID_HIDDEN” with correct credentials 6. Change broadcast settings for any one of the SSID and verify the broadcast setting for other SSID is unaffected
Test Limits	NA
Expected Results	1. FWA_SSID_VISIBLE appears in the scan list 2. FWA_SSID_HIDDEN does **not** appear in the scan list 3. Client successfully connects to the hidden SSID. 4. Verify that the broadcast setting of the other SSID is unaffected.

Test No.	**GR_TSTP_2.5.4.8**
Test Details	To verify that the default configuration of the FWA Device shall be with the same SSID for all supported bands.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device and perform a factory reset of the FWA device using the Reset button. 2. Wait until the device boots up. 3. Check device UI to confirm supported Wi-Fi bands. 4. Scan the available networks on 2.5 and 5GHz. 5. Verify the configured SSID for all supported bands.
Test Limits	NA
Expected Results	1. An SSID with the same name appears on each supported band.

Test No.	GR_TSTP_2.5.4.9
Test Details	To verify that based on procurer requirements, in the default configuration, the SSIDs may have an unambiguous, not-repeating value for each deployed FWA Device and not contain any information that consist of or are derived from data or parts of data that depend on the FWA device model itself.
Test Instruments Required	FWA CPE Power supply unit LAN Client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Perform a factory reset on FWA. 2. Power on FWA devices. 3. Using a Wi-Fi scanner, scan for available networks. 4. Confirm that each SSID can be clearly distinguished from other without ambiguity (no minor variations such as only band suffixes)
Test Limits	NA
Expected Results	1. Each FWA broadcasts at least one default SSID. 2. No two devices share the same SSID value.

Test No.	**GR_TSTP_2.5.5.1**
Test Details	To verify that AP of a FWA Device shall permit the manual channel selection on all supported bands.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone). Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Check the List of available channel bandwidths in all the supported bands. 4. Manually select the channel out of available channels in bands in AP settings/Configurations via UI. 5. Save and apply the configurations of AP. 6. Enable the Wi-Fi Access Point functionality. 7. Connect a Wi-Fi client device to the FWA Device. 8. Verify successful Wi-Fi association and IP address assignments. 9. Confirm that the AP is Operating on the manually selected Channel using Wi-Fi analyzer.
Test Limits	NA
Expected Results	The FWA Device shall permit manual selection of channels in the available bands with manually selected channels in a configured bandwidth.

Test No.	**GR_TSTP_2.5.5.2**
Test Details	To verify that the AP of a FWA Device shall support Automatic Channel Selection on all supported bands, in order to select the less interfered channels.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Interference generators (Signal generators/ another AP), Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Check the List of available channels in all the supported bands. 4. Check ACS is enabled for supported bands. If not enabled. 5. Save and apply the configurations of AP. 6. Enable the Wi-Fi Access Point functionality. 7. Connect a Wi-Fi client device to the FWA Device. 8. Verify successful Wi-Fi association and IP address assignments. 9. Confirm that the AP is Operating on the Automatic Channel Selection using a Wi-Fi analyzer. 10. Introduce more interference on current operating channel. 11. Check AP switches to a less interference channel automatically or not. 12. Repeat the steps from 9 for all the supported bands.
Test Limits	NA
Expected Results	The FWA Device shall support automatic channel selection on all the available bands with less interference.

Test No.	**GR_TSTP_2.5.5.3**
Test Details	To verify that if enabled, the Automatic Channel Selection shall be performed every time the AP is turned on.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone). Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Check the List of available channels in all the supported bands. 4. Check ACS is enabled for supported bands. 5. Enable the Wi-Fi Access Point functionality. 6. Connect a Wi-Fi client device to the FWA Device. 7. Verify successful Wi-Fi association and IP address assignments. 8. Confirm that the AP is Operating on the Automatic Channel Selection using a Wi-Fi analyzer. 9. Power Off the FWA device. 10. Power On the FWA device. 11. Reconnect and check selected channels by ACS or not by Wi-Fi Analyzer.
Test Limits	NA
Expected Results	The FWA Device performs ACS every time AP is turned On, if ACS is enabled.

Test No.	**GR_TSTP_2.5.5.4**
Test Details	To verify that the AP of a FWA Device shall support Periodic Automatic Channel Selection.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone). Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Check the List of available channels in all the supported bands. 4. Check if Periodic ACS is enabled or not. If not, enable it. 5. Configure Periodic interval, if configurable using UI. 6. Enable the Wi-Fi Access Point functionality. 7. Connect a Wi-Fi client device to the FWA Device. 8. Verify successful Wi-Fi association and IP address assignments. 9. Confirm that the AP is Operating on the Automatically selected channel, using a Wi-Fi analyzer. 10. Verify that the AP is automatically switched to a channel after a periodic interval. Note: To validate AP switches to other channel, Introduce more interference in operating channel. Check AP switching or not after periodic time.
Test Limits	NA
Expected Results	The FWA device should support the periodic ACS.

Test No.	**GR_TSTP_2.5.5.5**
Test Details	To verify the default value for Periodic Automatic Channel Selection should be 24 hours.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone). Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Check if the Periodic ACS is enabled or not. If not, Enable. 4. Check the default Periodic interval value. 5. Confirm that the default periodic interval value is set to 24 hours.
Test Limits	NA
Expected Results	The default value for Periodic Automatic Channel Selection should be 24 hours for a FWA Device.

Test No.	**GR_TSTP_2.5.5.6**
Test Details	To verify that the Periodic Automatic Channel Selection shall be configurable by the procurer through customization.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone). Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Check if the Periodic ACS is enabled or not. If not, Enable. 4. Check the Periodic interval value configurable. 5. Modify the Periodic interval value and save the configs. 6. Confirm that Periodic interval value modifies using an interface.
Test Limits	NA
Expected Results	The Periodic Automatic Channel Selection shall be configurable by the procurer through customization of the FWA device.

Test No.	**GR_TSTP_2.5.5.7**
Test Details	To verify that the AP of a FWA Device shall permit the manual Bandwidth selection on all supported bands.
Test Instruments Required	FWA Device, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone). Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Check supported band list. 4. Select a band in the band list. 5. Check operational bandwidths on this band. 6. Manually selects a bandwidth out of supported bandwidth for this selected band. 7. Enable the Wi-Fi Access Point functionality. 8. Connect a Wi-Fi client device to the FWA Device. 9. Verify successful Wi-Fi association and IP address assignments. 10. Confirm that the AP is Operating on the manually selected bandwidth by using Wi-Fi Analyzer. 11. Repeat the steps from 4 for all the supported bands.
Test Limits	NA
Expected Results	The AP of a FWA Device shall permit the manual Bandwidth selection on all supported bands.

Test No.	**GR_TSTP_2.5.5.8**
Test Details	To verify that the AP of a FWA Device shall support Automatic Bandwidth Selection on all supported bands.
Test Instruments Required	FWA Device, Power supply unit, Interference Generator, Wi-Fi client device (PC/Laptop/Smartphone). Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Check the List of available bandwidths in all the supported bands. 4. Check ABS is enabled for all supported Bands, If not enabled. 5. Save and apply the configurations of AP. 6. Enable the Wi-Fi Access Point functionality. 7. Select a band out of supported bands. 8. Connect a Wi-Fi client device to the FWA Device to the selected band. 9. Verify successful Wi-Fi association and IP address assignments. 10. Confirm that the AP is Operating on the Automatic Bandwidth Selection using a Wi-Fi analyzer. 11. Repeat the steps from 7 for all the supported bands. Note: To Validate AP Switches automatically, Introduce more interference in operating bandwidth. Check AP switching or not.
Test Limits	NA
Expected Results	The AP of a FWA Device shall support Automatic Bandwidth Selection on all supported bands.

Test No.	**GR_TSTP_2.5.6.1**
Test Details	To verify that the AP of a FWA Device shall support at least 64 clients.
Test Instruments Required	FWA Device, Power supply unit, 64 or more Wi-Fi client device (PC/Laptop/Smartphone). Wi-Fi analyzer or client device network status tool, Configuration access (e.g. Web UI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Access to the configuration interface (e.g. Web UI) of the FWA Device. 3. Enable the Wi-Fi Access Point functionality. 4. Connect one by one Wi-Fi client device to the FWA Device. 5. Verify successful Wi-Fi association and IP address assignments for each client. 6. Check the connectivity of each client. 7. Generate traffic on each client and check FWA device is providing resources. 8. Verify the performance of AP with > =64 clients.
Test Limits	NA
Expected Results	The AP of a FWA Device shall support at least 64 clients.

Test No.	**GR_TSTP_2.5.8**
Test Details	To verify that AP of a FWA Device may support WPS with Push Button mode in order to facilitate the association between clients and the AP of the FWA Device. If present, WPS shall be disabled by default and enabled only with full awareness of risks and only when physical access is strictly controlled.
Test Instruments Required	1. WPS-capable Wi-Fi client device. 2. PC/Laptop for AP web management access. 3. Access Point.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA . 2. Ensure Wi-Fi AP is enabled on the FWA. 3. Verify WPS feature availability in the AP configuration. 4. Verify that WPS is disabled by default in factory or baseline configuration. 5. Attempt WPS association from a client while WPS is disabled and verify failure. 6. Enable WPS Push Button mode through the management interface or physical button. 7. Initiate the WPS Push Button on the Wi-Fi client within the allowed time window. 8. Verify successful client association to the FWA AP.
Test Limits	NA
Expected Results	WPS Push Button mode, if supported, shall successfully associate clients only when explicitly enabled.

Test No.	**GR_TSTP_2.5.9**
Test Details	To verify that AP of a FWA Device shall support IEEE 802.11k industry standard for radio resource measurement
Test Instruments Required	1. FWA and AP. 2. Wi-Fi client device supporting IEEE 802.11k 3. PC/Laptop for management access 4. Wi-Fi protocol analyzer (e.g., Wireshark in monitor mode).
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device and enable Wi-Fi AP. 2. Connect a Wi-Fi client that supports IEEE 802.11k. 3. Login to FWA management interface and verify 802.11k support/configuration. 4. Associate an 802.11k-capable client to the FWA AP. 5. Trigger radio resource measurement requests (neighbor report, beacon report, etc.). 6. Capture and analyze Wi-Fi frames to verify presence of 802.11k action frames. 7. Verify that AP responds correctly to client 802.11k requests.
Test Limits	NA
Expected Results	FWA AP shall advertise and support IEEE 802.11k capabilities.

Test No.	**GR_TSTP_2.5.10**
Test Details	To verify that AP of a FWA Device shall support Band Steering to steer clients from the more congested 2.4 GHz band to the less congested bands (5 GHz, and 6GHz if supported).
Test Instruments Required	1. FWA and AP. 2. Multiple Wi-Fi client devices (dual-band / tri-band capable). 3. PC/Laptop for FWA management access. 4. Wi-Fi analyzer/scanner tool.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON FWA and enable 2.4 GHz, 5 GHz (and 6 GHz if supported). 2. Enable Band Steering feature on FWA. 3. Enable Band Steering in FWA management interface. 4. Associate multiple clients on 2.4 GHz to create congestion. 5. Attempt to connect a dual-band/tri-band client to the SSID. 6. Monitor which band the client is assigned. 7. Increase traffic load on 2.4 GHz band. 8. Observe if AP steers capable clients to 5 GHz/6 GHz band.
Test Limits	NA
Expected Results	FWA AP shall support Band Steering feature, and Dual-band/tri-band clients shall be preferentially connected to 5 GHz/6 GHz under congestion.

Test No.	**GR_TSTP_2.5.11**
Test Details	To verify that Band Steering feature shall be manually configurable (ON/OFF selection).
Test Instruments Required	1. Access Point. 2. PC/Laptop with Ethernet/Wi-Fi connectivity 3. Web browser 4. Wi-Fi client device (dual-band/tri-band capable).
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the AP. 2. Ensure Wi-Fi radios (2.4/5/6 GHz if supported) are enabled. 3. Ensure Band Steering feature is available in the configuration menu. 4. Navigate to Wireless / Advanced Wi-Fi settings. 5. Locate Band Steering configuration options. 6. Set Band Steering to **ON** and save/apply configuration. 7. Verify configuration is accepted and stored. 8. Observe client association behavior. 9. Set Band Steering to **OFF** and save/apply configuration. 10. Reboot AP (if required) and verify setting persistence.
Test Limits	NA
Expected Results	Band Steering feature shall be manually configurable with clear ON/OFF selection.

Test No.	**GR_TSTP_2.5.12**
Test Details	To verify that AP of a FWA Device shall support RF Mesh functionality.
Test Instruments Required	1. FWA and AP. 2. Wi-Fi client device (laptop / smartphone). 3. FWA management GUI / CLI access. 4. Optional: iPerf3 or traffic generator for backhaul performance.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable RF Mesh functionality on the FWA Device (if present). 3. Verify mesh topology is formed in FWA management interface 4. Mesh node(s) connected via wireless backhaul. 5. Connect a Wi-Fi client to a mesh node. 6. Verify end-to-end connectivity. 7. Client to mesh node. 8. Mesh node to FWA AP (wireless backhaul). 9. FWA to Core Network / Internet. 10. Perform ping and throughput tests from client. 11. Verify traffic passes through mesh backhaul.
Test Limits	NA
Expected Results	The FWA Device AP shall successfully form an **RF Mesh network** with mesh-capable nodes.

Test No.	**GR_TSTP_2.5.13**
Test Details	To verify that Wi-Fi Diagnostic solution shall collect data also from the other APs connected in mesh, as well as from the clients connected to those Aps.
Test Instruments Required	1. FWA and AP. 2. RF Mesh support 3. Wi-Fi Diagnostic / Telemetry feature enabled 4. One or more mesh-capable AP. 5. FWA management GUI / CLI access.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Enable RF Mesh and verify all mesh APs are connected. 3. Enable Wi-Fi Diagnostic / Telemetry feature. 4. Connect at least one client to: • Main FWA AP • Each mesh AP 5. Generate traffic from each client (ping, web, iPerf). 6. Access Wi-Fi Diagnostic interface (local GUI or cloud portal). 7. Verify diagnostics data is collected and displayed for: • Main FWA AP • All mesh APs
Test Limits	NA
Expected Results	The Wi-Fi Diagnostic solution shall collect and display data from **all mesh-connected APs**.

Test No.	**GR_TSTP_2.5.14**
Test Details	To verify that AP of a FWA Device should support multimedia extensions in order to prioritize traffic in the Wireless Network according to Access Categories.
Test Instruments Required	1. Access Point. 2. PC/Laptop with Ethernet/Wi-Fi connectivity 3. Wi-Fi client devices (supporting QoS). 4. Web Browser.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the AP. 2. Connect PC to AP management interface (if present). 3. Ensure that QoS features are available and enabled. 4. Navigate to Wireless / Advanced / QoS or Multimedia settings. 5. Verify that the QoS feature option is present. 6. Enable QoS if not enabled by default. 7. Generate different types of traffic simultaneously are Voice (VoIP call), Video streaming, Best-effort data (file download/upload), Background traffic (large file transfer). 8. Monitor throughput, latency, and packet loss for each traffic type. 9. Observe traffic prioritization behavior.
Test Limits	NA
Expected Results	Traffic shall be prioritized according to Access Categories, and Enabling/disabling QoS shall function correctly and reflect traffic behavior.

Test No.	**GR_TSTP_2.5.15**
Test Details	To verify that If multimedia extensions is supported; the FWA Device shall provide the mechanism to enable/disable the feature and to configure the mappings (Access Categories vs DSCP).
Test Instruments Required	1. FWA. 2. PC/Laptop for FWA management access 3. Wi-Fi client devices 4. Traffic generator / QoS test tool (e.g., iPerf, VoIP test tool)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON FWA device and enable Wi-Fi AP. 2. Connect PC to FWA management interface. 3. Ensure multimedia extensions / WMM features are available. 4. Navigate to QoS / Multimedia / WMM settings. 5. Enable multimedia extensions feature. 6. Configure Access Category to DSCP mappings (e.g., Voice, Video, Best Effort, Background). 7. Save and apply settings. 8. Generate traffic with different DSCP values. 9. Capture packets on LAN/Wi-Fi side. 10. Verify the correct AC mapping for each DSCP value.
Test Limits	NA
Expected Results	FWA Device shall allow enabling and disabling of multimedia extensions,and Access Category to DSCP mappings shall be configurable.

Test No.	**GR_TSTP_2.5.16**
Test Details	To verify that It shall be possible for a procurer to customize the settings of a FWA Device as regards Wi-Fi region/country of operation, enabled bands and channels, power transmission limits, SSIDs, passphrases.
Test Instruments Required	1. FWA Device. 2. PC/Laptop with Ethernet/Wi-Fi connectivity. 3. Web browser for FWA management interface. 4. Administrator login credentials.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Connect PC to the FWA LAN port or Wi-Fi. 3. Login to the FWA Web UI using administrator credentials. 4. Navigate to Wireless / Regulatory / Advanced Wi-Fi settings. 5. Change the Wi-Fi region/country of operation (if configurable). 6. Enable/disable supported Wi-Fi bands (2.4 GHz / 5 GHz / 6 GHz if applicable). 7. Select and modify allowed Wi-Fi channels. 8. Configure transmit power limits. 9. Create/modify SSID names. 10. Configure Wi-Fi security mode and change passphrases. 11. Save and apply configuration. 12. Reboot FWA if required.
Test Limits	NA
Expected Results	Procurer shall be able to configure Wi-Fi country/region of operation and Enabled bands and channels shall be configurable within regulatory limits.

Test No.	**GR_TSTP_2.6.1.1**
Test Details	To verify the outdoor Unit (ODU) in an Outdoor FWA Solution, shall be able to map the traffic received on each PDN Connection / PDU Session, on different VLANs over the interface with the Indoor Unit (IDU), and vice versa.
Test Instruments Required	1. Outdoor Unit (ODU) and Indoor Unit (IDU) under test. 2. PC/Laptop for management access. 3. Managed Ethernet switch supporting VLANs. 4. VLAN traffic generator / test PC. 5. Packet capture tool (e.g., Wireshark).
Test Setup	TEST SETUP X
Test Procedure	1. Install and power ON ODU and IDU as per vendor guidelines. 2. Connect ODU–IDU interface through a managed switch (or directly if supported). 3. Configure multiple PDN connections / PDU sessions on the FWA system. 4. Map each PDN/PDU session to a unique VLAN ID on the ODU–IDU interface. 5. Generate uplink and downlink traffic on each PDN/PDU session. 6. Capture traffic on ODU–IDU Ethernet interface. 7. Verify the correct VLAN tags for each session. 8. Send VLAN-tagged traffic from the IDU side and verify correct mapping to PDN/PDU sessions on ODU. 9. Verify traffic isolation between VLANs.
Test Limits	NA
Expected Results	ODU shall correctly map each PDN/PDU session to its configured VLAN on the ODU–IDU interface, and VLAN tags shall be correctly applied and verified on captured traffic.

Test No.	**GR_TSTP_2.6.1.2**
Test Details	To verify the IDU shall be able to map the different traffic generated by the IDU itself or by hosts in LAN, and destined to the WAN, on different VLANs over the interface with the ODU, based on Service/VLAN mapping rules defined on the IDU.
Test Instruments Required	1. Indoor Unit (IDU) and Outdoor Unit (ODU) under test. 2. PC/Laptop for management access. 3. Managed Ethernet switch supporting VLANs. 4. Multiple LAN host devices (PCs). 5. VLAN traffic generator or test applications.
Test Setup	TEST SETUP X
Test Procedure	1. Install and power ON IDU and ODU as per vendor guidelines. 2. Connect IDU–ODU interface via managed switch or directly. 3. Connect multiple LAN hosts to IDU LAN ports. 4. Configure multiple Service/VLAN mapping rules on the IDU (e.g., per LAN port, per SSID, per traffic type). 5. Generate different types of traffic from LAN hosts and IDU (e.g., data, voice, management). 6. Capture traffic on the IDU–ODU interface. 7. Verify that each traffic type is tagged with the correct VLAN ID. 8. Verify that traffic is forwarded to ODU over the correct VLAN.
Test Limits	NA
Expected Results	IDU shall correctly map LAN and internally generated traffic to configured VLANs on the IDU–ODU interface.

Test No.	**GR_TSTP_2.6.1.3**
Test Details	To verify that ODU shall be configurable in order to operate on each VLAN, either in bridged mode or in routed mode.
Test Instruments Required	1. FWA. 2. Management access to ODU and IDU (Web GUI / CLI). 3. VLAN-capable Ethernet switch 4. Test PC / Laptop with VLAN tagging support.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the ODU, and IDU. 2. Verify normal end-to-end connectivity in default configuration. 3. Configure VLAN X on ODU in bridged mode. 4. Generate traffic from LAN side and verify. 5. VLAN X tagging on ODU interface using Wireshark. 6. Traffic is transparently bridged across ODU. 7. Verify IP address is assigned from upstream network (no NAT on ODU). 8. Change VLAN X configuration to routed mod**e** on ODU. 9. Configure IP interface on ODU for VLAN X. 10. Verify independent VLAN configuration.
Test Limits	NA
Expected Results	Traffic on each VLAN shall behave according to configured mode.

Test No.	**GR_TSTP_2.6.1.4**
Test Details	To verify that ODU shall allow to configure one PDN connection / PDU session to be locally terminated in the ODU itself, that is to operate in routed mode without being mapped on a VLAN with the IDU. Note: for example, this connection may be dedicated to ODU Remote Management.
Test Instruments Required	1. FWA. 2. Outdoor Unit (ODU) and Indoor Unit (IDU) under test. 3. PC/Laptop for management access. 4. Test SIM support multiple PDN/PDU sessions. 5. Network management system.
Test Setup	TEST SETUP X
Test Procedure	1. Install and power ON ODU and IDU as per vendor guidelines. 2. Configure multiple PDN connections / PDU sessions on ODU. 3. Configure one PDN/PDU session for local termination (routed mode) on ODU 4. Verify that this session is not mapped to any VLAN on the ODU–IDU interface. 5. Configure remote management for access to the locally terminated session. 6. Generate management of traffic to/from ODU over this session. 7. Capture traffic on the ODU–IDU interface. 8. Verify that no VLAN-tagged traffic for this PDN/PDU session appears on the IDU interface.
Test Limits	NA
Expected Results	ODU shall allow configuration of a PDN/PDU session in locally terminated (routed) mode.

Test No.	**GR_TSTP_2.6.2.1**
Test Details	To verify the Outdoor Unit (ODU) shall be able to operate in bridged mode, over one or more PDNs-PDUs/VLANs.
Test Instruments Required	1. FWA/ ODU. 2. Core Network / 5GC with support for multiple PDNs / PDU Sessions 3. Management access to ODU and IDU (Web GUI / CLI). 4. VLAN-capable Ethernet switch. 5. Test PC / Laptop with VLAN tagging capability.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the ODU, and IDU. 2. Verify default connectivity with single PDN / VLAN. 3. Configure multiple PDNs / PDU Sessions on Core Network (e.g., PDN1, PDN2). 4. Map each PDN / PDU Session to a unique VLAN: • PDN1 → VLAN X • PDN2 → VLAN Y 5. Configure ODU to operate in bridged mode for VLAN X and VLAN Y. 6. Generate traffic for each PDN / VLAN from LAN side. 7. Using Wireshark or switch mirroring, verify: • Correct VLAN tagging per PDN / PDU • Traffic is transparently bridged through ODU 8. Verify that ODU does NOT perform routing or NAT on these VLANs.
Test Limits	NA
Expected Results	The ODU shall operate in bridged mode over one or more PDNs / PDU Sessions / VLANs.

Test No.	**GR_TSTP_2.6.2.2**
Test Details	To verify that In bridged mode operation, the ODU shall use DHCP/DHCPv6 to assign to the IDU, on each VLAN, the network parameters received from the mobile network over a PDN/PDU a. IP Address b. DNS Servers IP Addresses (DHCP Option 6) Therefore, in bridge mode operation, the IP Address received on each PDN/PDU from the network, is not retained on the ODU itself, but is assigned to the IDU on the VLAN corresponding to that PDN/PDU.
Test Instruments Required	1. ODU and IDU. 2. 4G/5G Core Network (PDN/PDU capable) 3. VLAN-capable Ethernet switch 4. DHCP/DHCPv6 packet capture tool (e.g., Wireshark).
Test Setup	TEST SETUP X
Test Procedure	1. Configure ODU for **bridged mode operation**. 2. Configure one or more PDN/PDU sessions on the mobile network. 3. Map each PDN/PDU to a corresponding VLAN between ODU and IDU. 4. Power cycle or renew network connection on the IDU. 5. Capture DHCP/DHCPv6 packets on the IDU-ODU interface. 6. Verify that the IDU receives: • IP address via DHCP/DHCPv6 • DNS server IP address(es) via DHCP Option 6 7. Verify that the ODU does **not** retain the PDN/PDU IP address on its own interface. 8. Verify that the assigned IP on IDU matches the IP received from the mobile network.
Test Limits	NA
Expected Results	In bridged mode, the ODU shall use DHCP/DHCPv6 to assign mobile network IP parameters to the IDU on each VLAN.

Test No.	**GR_TSTP_2.6.2.3**
Test Details	To verify that ODU shall define, for each VLAN, the following parameters: a. Subnet Mask b. Default Gateway c. and assign them to the IDU by means of DHCP/DHCPv6. Note 1: this is needed because the mobile network does not provide a UE (specifically, the ODU) with such parameters over a PDN/PDU, while they are needed to properly configure the IDU with DHCP/DHCPv6. Note 2: Subnet Mask is DHCP Option 1, Default Gateway is DHCP Option 3 (Router).
Test Instruments Required	1. ODU and IDU. 2. 4G/5G Core Network (PDN/PDU capable) 3. VLAN-capable Ethernet switch 4. DHCP/DHCPv6 packet capture tool (e.g., Wireshark).
Test Setup	TEST SETUP X
Test Procedure	1. Configure ODU for bridge mode operation. 2. Configure one or more PDN/PDU sessions on the mobile network. 3. Map each PDN/PDU to a corresponding VLAN. 4. Configure ODU to define: • Subnet Mask for each VLAN • Default Gateway for each VLAN 5. Renew DHCP/DHCPv6 lease on the IDU. 6. Capture DHCP/DHCPv6 packets on the IDU interface. 7. Verify that DHCP includes: • Option 1 (Subnet Mask) • Option 3 (Default Gateway / Router) 8. Verify that the IDU applies to the received Subnet Mask and Default Gateway.
Test Limits	NA
Expected Results	For each VLAN, the ODU shall define the Subnet Mask and Default Gateway.

Test No.	**GR_TSTP_2.6.2.4**
Test Details	To verify that ODU may define: a. For the Subnet Mask, a /30 (255.255.255.252) b. For the Default Gateway, the IP Address immediately after or before the one assigned to the IDU on each VLAN, following the rules of the Classless Inter-Domain Routing (CIDR).
Test Instruments Required	1. ODU and IDU. 2. 4G/5G Core Network (PDN/PDU capable) 3. VLAN-capable Ethernet switch 4. DHCP/DHCPv6 packet capture tool (e.g., Wireshark)
Test Setup	TEST SETUP X
Test Procedure	1. Configure ODU to use **/30 (255.255.255.252)** subnet mask for one or more VLANs. 2. Configure ODU to assign IP address to IDU via DHCP/DHCPv6. 3. Configure ODU to set Default Gateway as: • The IP immediately before, or • The IP immediately after the IDU IP address within the /30 subnet. 4. Renew DHCP/DHCPv6 lease on the IDU. 5. Capture DHCP packets on the IDU-ODU interface. 6. Verify: • Subnet Mask = 255.255.255.252 • Default Gateway matches valid adjacent host IP per CIDR rules 7. Verify IP connectivity between IDU and ODU.
Test Limits	NA
Expected Results	The ODU may define a /30 (255.255.255.252) subnet mask for each VLAN and shall define the Default Gateway as the IP address immediately before or after the IDU IP address.

Test No.	**GR_TSTP_2.6.3.1**
Test Details	To verify that If an APN is configured in bridged mode, the ODU shall guarantee that the IDU IP configuration will always be the same of the WAN (mobile) IP configuration.
Test Instruments Required	1. FWA. 2. Core Network / 5GC with APN configuration access. 3. Management access to ODU and IDU (Web GUI / CLI). 4. Test PC connected to IDU LAN.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the ODU, and IDU. 2. Configure the APN on the Core Network in **bridged mode**. 3. Establish PDU session for the bridged APN. 4. Verify WAN (mobile) IP address assigned to the ODU from Core Network. 5. From IDU management interface or test PC: • Check IP address assigned on IDU WAN/LAN interface (as applicable). 6. Compare: • ODU WAN (mobile) IP address • IDU IP address 7. Verify that both IP addresses are **identical**. 8. Verify subnet mask, gateway, and DNS (if applicable) are consistent.
Test Limits	NA
Expected Results	When APN is configured in bridged mode, the IDU IP address shall be identical to the WAN (mobile) IP address.

Test No.	**GR_TSTP_2.6.3.2**
Test Details	To verify that As soon as the WAN (mobile) IP connection state changes, the ODU shall trigger the IDU IP Address renewal by means of a reset of the physical interface with the IDU.
Test Instruments Required	1. FWA. 2. Core Network / 5GC with capability to trigger IP change. 3. Management access to ODU and IDU (Web GUI / CLI). 4. VLAN-capable Ethernet switch (for link monitoring).
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the ODU, and IDU. 2. Establish WAN (mobile) connection and verify: • Current WAN IP address on ODU • Current IP address on IDU 3. Start continuous ping from test PC to external host. 4. Trigger WAN IP change by one of the following: • PDU session release and re-establishment • APN reconnection • Core Network forced IP re-assignment • Toggle mobile data on ODU 5. Monitor ODU–IDU Ethernet link status. 6. Verify that ODU triggers: 7. Physical interface reset (link down/up) toward IDU 8. Verify IDU behavior: 9. DHCP renew or IP reconfiguration is triggered
Test Limits	NA
Expected Results	Upon WAN (mobile) IP connection state change, the ODU shall reset the physical interface toward the IDU.

Test No.	**GR_TSTP_2.6.4.1**
Test Details	To verify that Outdoor Unit (ODU) shall be able to operate in routed mode, over one or more PDNs-PDUs/VLANs.
Test Instruments Required	1. FWA. 2. Management access to ODU and IDU (Web GUI / CLI). 3. VLAN-capable Ethernet switch. 4. Test PC / Laptop connected behind IDU.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Base Station, RU, ODU, and IDU. 2. Verify default routed connectivity with single PDN / VLAN. 3. Configure multiple PDNs / PDU Sessions (e.g., PDN1, PDN2). 4. Map each PDN / PDU Session to a unique VLAN: • PDN1 → VLAN X • PDN2 → VLAN Y 5. Configure ODU to operate in **routed mode** for VLAN X and VLAN Y. 6. Verify ODU creates routed interfaces for each VLAN. 7. From test PC, generate traffic for each PDN / VLAN. 8. Using Wireshark and ODU diagnostics, verify: • ODU performs IP routing per VLAN • NAT is applied (if applicable) 9. Correct source IP per PDN / VLAN 10. Verify simultaneous operation of multiple VLANs in routed mode.
Test Limits	NA
Expected Results	The ODU shall operate in **routed mode** over one or more **PDNs / PDU Sessions / VLANs**.

Test No.	**GR_TSTP_2.6.4.2**
Test Details	To verify that In routed mode operation, the ODU shall retain for itself the IP Address received from the mobile network over a APN/DNN.
Test Instruments Required	1. FWA. 2. Management access to ODU and IDU (Web GUI / CLI). 3. Test PC connected behind IDU. 4. Traffic verification tools (iper3).
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the Base Station, RU, ODU, and IDU. 2. Configure APN / DNN in **routed mode**. 3. Establish PDU session and verify: • IP address assigned to ODU from mobile network 4. From ODU management interface, record: • ODU WAN (mobile) IP address 5. From IDU / LAN side, verify: • IDU LAN IP address (private IP) • Default gateway pointing to ODU 6. Compare IP addresses: • ODU WAN IP (public/private from mobile network) • IDU LAN IP (private, different subnet) 7. Generate traffic from LAN side and verify: 8. Source IP seen in Core Network is ODU WAN IP (NAT applied) 9. Verify that IDU does NOT receive the mobile WAN IP.
Test Limits	NA
Expected Results	In routed mode, the ODU shall retain the IP address received from the mobile network.

Test No.	**GR_TSTP_2.6.4.3**
Test Details	To verify that In routed mode operation, the ODU shall be able to configure the IP Address of the IDU, on each VLAN configured in routed mode, by means of DHCP, using a private IP address pool.
Test Instruments Required	1. FWA. 2. Management access to ODU and IDU (Web GUI / CLI). 3. VLAN-capable Ethernet switch 4. Test PC connected behind IDU
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the ODU, and IDU. 2. Configure multiple VLANs in **routed mode** on the ODU. 3. Enable DHCP server on ODU for each routed VLAN. 4. Reboot or renew DHCP on IDU. 5. From IDU management interface, verify: 6. IDU receives IP address via DHCP on each VLAN 7. Verify assigned IP addresses: 8. Belong to configured private IP pools 9. Are different per VLAN 10. Verify the default gateway on each VLAN point to the ODU interface.
Test Limits	NA
Expected Results	In routed mode, the ODU shall act as a DHCP server for each routed VLAN.

Test No.	**GR_TSTP_2.6.4.4**
Test Details	To verify that In routed mode operation, if DHCP is used, then ODU shall provide via DHCP also: a. The DNS Server IP Address(es), which can be either the ODU itself or the Servers received from network; b. The Default Gateway (Router), which is the IP Address of the ODU over the IDU-ODU connection.
Test Instruments Required	1. FWA. 2. Management access to ODU and IDU (Web GUI / CLI). 3. VLAN-capable Ethernet switch 4. Test PC connected behind IDU.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the ODU, and IDU. 2. Configure routed mode VLAN(s) on ODU. 3. Enable DHCP server on ODU for routed VLAN(s). 4. Configure DNS option on ODU: Option A: ODU as DNS proxy Option B: Pass-through DNS from mobile network 5. Renew DHCP lease on IDU / test PC. 6. On IDU / test PC, verify via IP configuration: Assigned IP address Default Gateway = ODU IP address DNS Server IP address(es) 7. Capture DHCP packets and verify: DHCP Option 3 (Router) = ODU IP DHCP Option 6 (DNS Servers) = ODU or network DNS 8. Perform DNS resolution tests. 9. lookup / dig to public domain 10. Verify connectivity to external networks.
Test Limits	NA
Expected Results	In routed mode, the ODU shall provide Default Gateway via DHCP, set to the ODU IP address.

Test No.	**GR_TSTP_2.6.4.5**
Test Details	In routed mode operation, the ODU shall be able to manage statically configured addresses for: a. The IP Address of the IDU over the IDU-ODU connection: this is a directly connected interface b. The LAN of the IDU: this will be a subnet routed through the IP Address of the IDU. Note: Static IP Addressing, for the IDU-ODU connection, can be used as an alternative to DHCP.
Test Instruments Required	1. FWA. 2. Management access to ODU and IDU (Web GUI / CLI). 3. VLAN-capable Ethernet switch. 4. Test PC connected behind IDU.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the ODU, and IDU. 2. Configure ODU for routed mode. 3. Configure static IP address on ODU for IDU–ODU interface. 4. Configure static subnet on IDU LAN routed through the IDU–ODU interface. 5. From test PC, verify: IDU LAN IP address belongs to configured static subnet Default gateway points to IDU interface IP 6. From ODU management interface, verify: ODU routing table for IDU LAN Directly connected IP for IDU–ODU interface 7. Generate traffic from IDU LAN subnet to external network and verify routing/NAT: Packets traverse ODU to mobile network 8. Correct source IP/NAT applied 9. Capture packet traces, routing tables, and configuration screenshots. 10. Reboot ODU/IDU and verify static IP configuration persists.
Test Limits	NA
Expected Results	The ODU shall correctly manage static IP addresses for: • The IDU–ODU directly connected interface • The IDU LAN subnet is routed via the IDU interface.

Test No.	**GR_TSTP_2.6.4.6**
Test Details	To verify that In routed mode operation, the ODU shall perform NAT of traffic coming from the IDU and destined to the Network.
Test Instruments Required	1. FWA. 2. Management access to ODU and IDU (Web GUI / CLI). 3. VLAN-capable Ethernet switch. 4. Test PC connected behind IDU.
Test Setup	TESTSETUP X
Test Procedure	1. Power ON ODU, and IDU. 2. Configure ODU in **routed mode** for IDU–ODU connection. 3. Verify ODU receives mobile WAN IP over APN / DNN. 4. From test PC behind IDU, generate traffic to external network: • Ping external IP • iPerf3 traffic test 5. Capture traffic at ODU and Core Network using Wireshark/tcpdump. 6. Verify NAT operation: • Source IP of traffic leaving ODU matches **ODU WAN IP** • Internal IDU LAN IP is translated 7. Verify return traffic is correctly mapped back to IDU client.
Test Limits	NA
Expected Results	In routed mode, the ODU shall perform NAT for all traffic coming from the IDU to the mobile network.

Test No.	**GR_TSTP_2.6.5.1**
Test Details	To verify that IDU shall be able to establish, through the ODU, one or more Tunnels or VPN connections, based on IPSec or PPTP or GRE, over one or more VLANs, towards Tunnel/VPN Terminators in the network.
Test Instruments Required	1. FWA. 2. Management access to ODU and IDU (Web GUI / CLI). 3. VLAN-capable Ethernet switch. 4. Test PC connected behind IDU.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the ODU, and IDU. 2. Configure ODU for routed mode and ensure VLAN(s) are active. 3. Configure IDU with VPN / Tunnel parameters: • Protocol: IPSec / PPTP / GRE • Remote terminator IP 4. Credentials / keys / encryption parameters 5. Initiate tunnel/VPN establishment from IDU. 6. Verify tunnel/VPN status on IDU: • Tunnel state = Established / Connected • Encryption/authentication successful 7. From test PC behind IDU, generate traffic through the tunnel: • Ping remote network IP • iPerf3 throughput test 8. Capture traffic at ODU and Core Network to verify tunneling: 9. Encapsulated traffic leaving ODU matches VPN protocol 10. No IP leakage outside tunnel 11. Repeat for multiple VLANs (if configured).
Test Limits	NA
Expected Results	The IDU shall establish one or more tunnels/VPNs through the ODU.

Test No.	**GR_TSTP_3.1.1**
Test Details	To verify that FWA device shall support standardized QCIs as specified in 3GPP TS 23.203.
Test Instruments Required	FWA CPE Power supply unit 5G NSA network connectivity (LTE EPC + NR access supporting QoS/QCI) LAN/Wi-Fi client device Voice/video service clients Network traffic analyzer / protocol analyzer Device management interface (Web UI/CLI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 5G NSA FWA Device and allow it to reach normal operational state. 2. Establish network attachment and service registration. 3. Configure multiple services including data, voice, video streaming, real-time gaming, and IMS signaling, each with distinct QoS/QCI profiles. 4. Initiate service sessions generating distinct traffic flows. 5. Capture traffic flows using a protocol/traffic analyzer (Wireshark). 6. Verify QCI/QoS parameter mapping for each service flow. 7. Validate compliance with standardized QCI characteristics as per 3GPP TS 23.203. 8. Confirm correct prioritization, handling, and traffic differentiation.
Test Limits	NA
Expected Results	The FWA Device shall correctly support and enforce standardized QCIs as defined in 3GPP TS 23.203, with proper QoS mapping and service differentiation.

Test No.	**GR_TSTP_3.1.2**
Test Details	To verify that FWA device should support operator-specific QCIs as specified in 3GPP TS 23.203.
Test Instruments Required	FWA CPE Power supply unit Network connectivity with operator QoS/QCI configuration support LAN/Wi-Fi client device Voice/video/data service clients Network traffic analyzer / protocol analyzer Device management interface (Web UI/CLI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 5G NSA FWA Device and allow it to reach normal operational state. 2. Establish IP-CAN session and network attachment. 3. Provision QoS control rules and QCI policies in PCRF. 4. Initiate multiple service data flows (SDFs) for different services. 5. Capture traffic flows using a protocol/traffic analyzer. 6. Verify one-to-one association between each SDF and its assigned QCI. 7. Validate QCI-based packet forwarding behavior and traffic treatment. 8. Confirm policy enforcement consistency across service flows.
Test Limits	NA
Expected Results	The FWA Device shall correctly enforce QCI-based packet forwarding behavior per QoS control rules in 3GPP TS 23.203, with proper SDF-to-QCI mapping and operator policy enforcement.

Test No.	**GR_TSTP_3.1.3**
Test Details	To verify that FWA device shall be compliant with 3GPP E-UTRAN and NR Access Stratum Release 16 baseline or later.
Test Instruments Required	FWA CPE, Power supply unit, 3GPP-compliant LTE/5G test network (gNB/eNB and core network), 3GPP conformance or protocol test tool (e.g. TTCN-3 based test system or protocol analyzer), LAN client (PC/Laptop), Test documentation for applicable 3GPP Release 16 specifications
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to reach idle state. 2. Connect the FWA Device to a 3GPP-compliant LTE and/or 5G test network provided by the conformance test system. 3. Select and execute the applicable Access Stratum conformance test suites: • LTE (E-UTRAN): TS 36.523-1 / 36.523-3, if LTE is supported. • NR: TS 38.523-1 / 38.523-3, if NR is supported. 4. Execute all mandatory Release 16 baseline test cases defined in the selected test suites. 5. Monitor UE behavior for correct Access Stratum procedures, including RRC connection establishment, security mode control, bearer establishment, capability exchange, mobility, and error handling. 6. Capture protocol traces and verdicts for each executed test case. 7. Review results and verify that all mandatory test cases complete with a PASS verdict.
Test Limits	NA
Expected Results	The FWA Device shall successfully pass all mandatory 3GPP E-UTRAN and/or NR Access Stratum Release 16 conformance test cases, demonstrating full compliance with the applicable Access Stratum specifications.

Test No.	**GR_TSTP_3.1.4**
Test Details	To verify that FWA device shall support periodical ANR measurements for reporting via the 4G network the Strongest NR Cells and related CGI (Cell Global Identity) when in ENDC operation.
Test Instruments Required	FWA CPE, Power supply unit, LTE eNB with EN-DC capability, NR gNB (secondary node), EPC/5GC supporting EN-DC, Multiple NR cells with known PCI and CGI, Protocol analyzer or 3GPP conformance test system, Test UE monitoring/logging tools
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to camp on the LTE eNB (Master Node). 2. Configure the network to enable EN-DC operation for the FWA Device. 3. Verify that the FWA Device is operating in LTE + NR dual connectivity mode. 4. Configure the LTE network to request periodical ANR measurement reporting for NR neighbor cells. 5. Ensure multiple NR cells are present and detectable by the FWA Device. 6. Monitor measurement and reporting messages sent by the FWA Device over the LTE network. 7. Verify that the FWA Device reports the strongest NR cells, including their CGI information, as part of ANR-related reporting. 8. Verify that reports are sent periodically as configured.
Test Limits	NA
Expected Results	The FWA Device shall correctly perform periodical ANR measurements and report, via the LTE network, the strongest NR neighbor cells along with their CGI information while operating in EN-DC mode, in accordance with 3GPP specifications.

Test No.	**GR_TSTP_3.1.5**
Test Details	To verify that FWA device should support periodical inter-RAT ANR measurements for reporting via the 4G network the Strongest NR Cells and related CGI (Cell Global Identity) when not in ENDC operation.
Test Instruments Required	FWA CPE device Power supply LTE eNodeB (commercial or test eNB) NR gNodeB (neighbor cell, not ENDC-enabled) Network simulator or live LTE+NR network Protocol analyzer (QXDM / Wireshark / TEMS / Amarisoft logs) LAN client (PC/Laptop)
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Verify the device camps on **LTE only** (no ENDC) 3. Confirm NR is not added as secondary cell 4. Configure LTE eNodeB with RRC measurement objects for **inter-RAT measurements** 5. Allow the FWA device to perform periodic NR scanning 6. Monitor LTE RRC signaling • Verify the device: o Detects strongest NR cells o Decodes NR CGI 7. Reports NR CGI via Measurement Report 8. Continue observation for multiple reporting cycles
Test Limits	NA
Expected Results	The FWA device remains camped on LTE while successfully performing inter-RAT NR measurements, detecting the strongest NR cells, correctly decoding and reporting their CGI to the LTE network via RRC signaling, without triggering ENDC or establishing an NR connection.

Test No.	**GR_TSTP_3.1.6**
Test Details	To verify that FWA device shall support periodical inter-RAT ANR measurements for reporting via the NR network the Strongest 4G Cells and related CGI (Cell Global Identity).
Test Instruments Required	NR simulator (supporting inter-RAT measurements) LTE eNB simulator (multiple LTE cells with known CGI) FWA CPE Device Power supply unit LAN Client
Test Setup	TEST SETUPX
Test Procedure	1. Power on the FWA device and allow it to Camp on NR, Establish RRC connection. 2. Configure NR simulator with **at least 4 LTE cells** (intra-frequency or inter-frequency as per requirement): a. Unique PCI b. Valid CGI (PLMN + TAC + Cell ID) c. Controlled and distinguishable signal strengths 3. Enable inter RAT Measurements in NR Simulator 4. Establish RRC Connection between FWA device and NR Simulator 5. Configure FWA Device to perform periodical Inter RAT Measurements (NR=> LTE). 6. Allow sufficient time for the FWA Device to a. Measure neighboring LTE cells b. Rank them based on signal strength 7. Verify FWA Device should report periodically configured in periodic timer. a. The **strongest LTE cells (up to 4)** b. Each cell CGI Information 8. Verify the Logs Measurement report should send periodically and CGI reporting information 9. Data sessions are active during measurement reporting.
Test Limits	NA
Expected Results	1. The FWA device successfully performs **periodical inter-RAT ANR measurements**. 2. The DUT reports **up to 4 strongest LTE neighbors' cells**. Reports its CGI Information

Test No.	**GR_TSTP_3.1.7**
Test Details	To verify that FWA device shall support periodical intra-RAT ANR measurements for reporting via the NR network the Strongest NR Cells and related CGI (Cell Global Identity).
Test Instruments Required	NR gNB Simulator supporting of supporting of multiple cells FWA CPE Power supply unit LAN Client 5G Core network
Test Setup	TEST SETUPX
Test Procedure	1. Power On FWA CPE Device 2. Configure **multiple NR cells** (minimum 2, preferably ≥4) a. Each NR cell shall have: i. Unique PCI ii. Valid CGI (PLMN + gNB ID + Cell ID) iii. Ensure all cells detected by FWA Device 3. Verify that FWA Device to camp on serving cell and establish connection 4. Verify that data sessions are successfully established and remain active. 5. Configure the NR gNB to a. Enable **intra-RAT ANR** b. Configure **periodical NR measurement reporting** 6. Trigger ANR measurement reporting from the NR network. 7. Allow sufficient time for the FWA Device to a. Measure neighboring LTE cells b. Rank them based on signal strength 8. Verify FWA Device should report periodically configured in periodic timer. a. The **strongest neighbor** b. Each cell CGI Information 9. Verify the Logs Measurement report should send periodically and CGI reporting information 10. Data sessions are active during measurement reporting.
Test Limits	NA
Expected Results	1. The FWA device successfully performs **periodical intra-RAT NR ANR measurements**. 2. The FWA Device reports the **strongest neighbouring NR cells** correctly 3. Each reported NR cell includes **valid and accurate CGI information**.

Test No.	**GR_TSTP_3.1.8**
Test Details	To verify that FWA device may be compliant to GSMA TS.24 for Antenna Performance acceptance values.
Test Instruments Required	1. FWA. 2. Calibrated anechoic chamber or OTA (Over-The-Air) test system. 3. RF test system / network emulator (4G/5G capable). 4. Spectrum analyzer / vector signal analyzer. 5. OTA antenna measurement system.
Test Setup	TEST SETUP X
Test Procedure	1. Install the FWA device in the OTA chamber per GSMA TS.24 setup guidelines. 2. Configure the RF test system according to GSMA TS.24 test cases. 3. Perform antenna performance measurements, including: • TRP measurements • TIS measurements 4. Radiation pattern scans (if required) 5. Record measured antenna performance values. 6. Compare measured values against GSMA TS.24 acceptance thresholds.
Test Limits	NA
Expected Results	The FWA device shall meet GSMA TS.24 antenna performance acceptance values.

Test No.	**GR_TSTP_3.1.9.1**
Test Details	To verify that The FWA device shall support EN-DC (Option 3x).
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone) Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the FWA device to support Dual Connectivity ensuring: a.LTE as Master node and 5G-NR as Secondary Node. b.Make sure LTE and 5G Gnb are connected to EPC network ensuring option 3x. 3.Attach the FWA device to the LTE network and verify successful registration 4. Establish an active data session (e.g.,EPS bearer) between the FWA and the network. 5.Initiate downlink and uplink data traffic from the FWA device. 6. Using network logs/test equipment, monitor the user plane traffic routing and verify that data is transmitted via NR.
Test Limits	N/A
Expected Results	The FWA device successfully establishes EN-DC connectivity with option 3x as LTE as the Master Node and NR as the Secondary Node and connected to EPC.

Test No.	**GR_TSTP_3.1.9.2**
Test Details	To verify that FWA device shall support DSS technology.
Test Instruments Required	FWA CPE Power supply unit LTE/NR network supporting **DSS** (commercial network or test gNB/eNB) LAN client (PC/Laptop) Network monitoring / diagnostic tools • RRC / NAS log capture (e.g., QXDM, Wireshark, UE logs) Throughput or connectivity test tool (e.g., ping, iPerf)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to attach to the DSS-enabled network. 2. Verify that the device camps on an LTE or NR cell operating with DSS. 3. Monitor RRC signaling to confirm DSS-related configuration (shared carrier usage). 4. Perform data traffic (e.g., ping or throughput test) via the LAN client. 5. Observe network behavior during LTE/NR coexistence on the shared spectrum. 6. Verify that the device maintains stable connectivity and service without errors.
Test Limits	NA
Expected Results	The FWA Device successfully operates in a DSS-enabled network, correctly supporting LTE and NR coexistence on the same frequency band while maintaining stable connectivity and data service.

Test No.	**GR_TSTP_3.1.9.3**
Test Details	To verify that FWA device shall support rateMatchingResrcSetSemi-Static Information element in the Capability Information message.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone) Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment). 3.Trigger the UE Capability Enquiry message from the network. 4. Capture the UE Capability Information message using the test sent by the FWA device. 5. Decode the UL-DCCH message by using any protocol analyzer. 6.Verify the rateMatchingResrcSetSemi-Static IE in Phy-ParametersCommon in the capability Information.
Test Limits	N/A
Expected Results	The FWA device successfully reports the rateMatchingResrcSetSemi-Static capability.

Test No.	**GR_TSTP_3.1.9.4**
Test Details	To verify that FWA device shall support rateMatchingResrcSetDynamic Information element in the Capability Information message.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment). 3.Trigger the UE Capability Enquiry message from the network. 4. Capture the UE Capability Information message using the test equipment sent by the FWA device. 5. Decode the UL-DCCH message by using any protocol analyzer. 6.Verify the rateMatchingResrcSetDynamic IE in Phy-ParametersCommon in the capability Information.
Test Limits	N/A
Expected Results	The FWA device successfully reports the rateMatchingResrcSetDynamic capability information.

Test No.	**GR_TSTP_3.1.9.5**
Test Details	To verify that FWA device shall support rateMatchingLTE-CRS Information element at least for one FDD mid-band (e.g. n1, n3) in the Capability Information message.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Establish the connection with the LTE test network (eNB or test equipment). 3.After the successful registration with LTE establish the connection with NR test network (gNB) 3.Trigger the UE Capability Enquiry message from the network. 4. Capture the UE Capability Information message using the test equipment sent by the FWA device. 5. Decode the UL-DCCH message by using any protocol analyzer. 6.Verify the rateMatchingLTE-CRS IE in RF-parameters in the capability Information.
Test Limits	N/A
Expected Results	The FWA device successfully reports the rateMatchingLTE-CRS capability information message.

Test No.	**GR_TSTP_3.1.9.6**
Test Details	To verify that FWA device should support AdditionalDMRS-DL-Alt Information element in the Capability Information message.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Establish the connection with the LTE test network (eNB or test equipment). 3.After the successful registration with LTE establish the connection with NR test network (gNB) 3.Trigger the UE Capability Enquiry message from the network. 4. Capture the UE Capability Information message using the test equipment sent by the FWA device. 5. Decode the UL-DCCH message by using any protocol analyzer. 6.Verify the additionalDMRS-DL-Alt IE in RF-parameters in the capability Information.
Test Limits	
Expected Results	The FWA device reports support for **additionalDMRS-DL-Alt** in the UE Capability Information message.

Test No.	**GR_TSTP_3.1.9.7**
Test Details	To verify that FWA device shall support NR SRS antenna switching 1T4R in 5G NR TDD high-bands (e.g. n77/n78).
Test Instruments Required	FWA CPE Power supply unit 5G NR base station emulator with support for sounding reference signal (SRS) measurements RF cabling or OTA environment for high NR bands (e.g., n77/n78) Test software capable of logging antenna configurations and SRS reports
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the 5G NR base station emulator configured for a high NR band (e.g., n77 or n78). 2. Configure the emulator to schedule SRS-based antenna switching measurements and to request 1T4R operation. 3. Initiate the connection and monitor the FWA device's antenna configuration via logs or measurement software. 4. COnfigure the gNB to signal FWA for SRS antenna switching. 4. Verify that the FWA device transmits sounding reference signals on one antenna and once received antenna switching it switches SRS transmit antenna. 5. Check that the base station emulator reports successful channel estimation and SRS reception.
Test Limits	NA
Expected Results	The FWA device supports 1T4R SRS antenna switching on high NR bands. Logs confirm one transmit and four receive antennas are used during SRS measurements and FWA switches SRS transmit antenna when signaled, enabling proper beam management.

Test No.	**GR_TSTP_3.1.9.8**
Test Details	To verify that FWA device shall support NR SRS antenna switching 1T2R in 5G NR TDD mid- and low-bands.
Test Instruments Required	FWA CPE Power supply unit 5G NR base station emulator with support for sounding reference signal (SRS) measurements RF cabling or OTA environment for NR low bands (e.g., n28) Test software capable of logging antenna configurations and SRS reports
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the 5G NR base station emulator configured for a low NR band. 2. Configure the emulator to schedule SRS-based antenna switching measurements and to request 1T2R operation. 3. Initiate the connection and monitor the FWA device's antenna configuration via logs or measurement software. 4. Configure the gNB to signal FWA for SRS antenna switching. 4. Verify that the FWA device transmits sounding reference signals on one antenna and once received antenna switching it switches SRS transmit antenna. 5. Check that the base station emulator reports successful channel estimation and SRS reception.
Test Limits	NA
Expected Results	The FWA device supports 1T2R SRS antenna switching on low NR bands. Logs confirm one transmit and four receive antennas are used during SRS measurements and FWA switches SRS transmit antenna when signaled, enabling proper beam management.

Test No.	**GR_TSTP_3.1.9.9**
Test Details	To verify that FWA device should support 2DL NR Inter-Band Carrier Aggregation.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/Smartphone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment) to support 2DL inter-band Carrier Aggregation ensuring: a.For example,DL CC1 is configured as the Primary Cell (PCell) in NR band n78 with 100 MHz channel bandwidth and DL CC2 is configured as the Secondary Cell (SCell) in NR band n28 with 20 MHz channel bandwidth. 3.Attach the FWA device to the NR network and verify successful registration. 4. Establish an active data session between the FWA and the network. 5.Initiate sustained downlink traffic from the network. 6.Using network logs/test equipment monitor the downlink transmission parameters and verify that the data is received simultaneously over both downlink component carriers confirming: a.Activation of CA b.Scheduling on both DL CCs
Test Limits	N/A
Expected Results	The FWA device successfully establishes **2DL NR inter-band carrier aggregation**.

Test No.	**GR_TSTP_3.1.9.10**
Test Details	The verify that FWA device shall support UL split bearer to transmit concurrently on LTE and NR.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Attach the FWA device to the LTE network and verify the successful registration and check the RRC-reconfiguration for the enabling NR gNB as secondary node and split bearer is configured. 3.Attach the FWA device to the NR network and verify successful registration for the ENDC connectivity. 4. Establish an active data session between the FWA and the network. 5.Initiate continuous uplink traffic from the FWA device. 6.Observe logs of PDCP/RLC if packets are transmitted over split bearers.
Test Limits	
Expected Results	Successful establishment of EN-DC with UL split bearer configured.

Test No.	**GR_TSTP_3.1.9.11**
Test Details	To verify that FWA device shall support MIMO 4x4 DL capability on NR mid-bands (e.g. NR bands n77/n78).
Test Instruments Required	FWA CPE Power supply unit 5G NR base station emulator supporting 4×4 MIMO downlink Multi-channel fading emulator or channel simulator (optional) Throughput measurement tool or test software
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR base station emulator configured on a mid-band carrier (e.g., n77 or n78) with 4×4 MIMO downlink capability. 2. Establish the connection and ensure that 4×4 MIMO mode is active. 3. Generate downlink traffic from the emulator using four spatial streams. 4. Monitor the FWA device's logs or use measurement software to verify that four parallel data streams are received. 5. Measure downlink throughput and confirm that it aligns with 4×4 MIMO performance expectations.
Test Limits	
Expected Results	The FWA device receives four spatial streams simultaneously on NR mid-band carriers. Throughput measurements reflect 4×4 MIMO capability.

Test No.	**GR_TSTP_3.1.9.12**
Test Details	To verify that FWA device shall support 4Rx diversity on NR bands.
Test Instruments Required	FWA CPE Power supply unit 5G NR base station emulator on a mid-band carrier RF channel emulator capable of emulating independent fading on multiple branches Measurement software to observe active receive branches
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the base station emulator on a mid-band carrier (e.g., n78). 2. Using the channel emulator, create independent fading conditions on up to four receive branches. 3. Initiate data transmission and monitor the FWA device's reported antenna status to confirm that four receive antennas are active. 4. Observe diversity performance by varying the fading profile on individual branches and ensuring the device maintains link quality through diversity combining.
Test Limits	NA
Expected Results	The FWA device engages four receive antennas on NR mid-band carriers and demonstrates diversity combining to maintain link quality under fading conditions.

Test No.	**GR_TSTP_3.1.9.13**
Test Details	To verify that FWA device should support 8Rx diversity on NR bands.
Test Instruments Required	FWA CPE with 8 receiver antennas Power supply unit 5G NR base station emulator on a mid-band carrier RF channel emulator capable of emulating independent fading on multiple branches Measurement software to observe active receive branches
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR base station emulator configured on a mid-band carrier. 2. Employ an RF channel emulator to create independent fading profiles on eight receive branches. 3. Establish a connection and monitor the device's antenna status to confirm eight active receive chains. 4. Vary the fading profiles on different branches and ensure that the device maintains performance using diversity combining.
Test Limits	NA
Expected Results	The FWA device supports eight active receive antennas on NR mid-band carriers and leverages diversity combining to sustain link quality.

Test No.	GR_TSTP_3.1.9.14
Test Details	To verify that FWA device may support more than 8Rx diversity on NR bands.
Test Instruments Required	FWA CPE with 16/32 receiver antennas Power supply unit 5G NR base station emulator on a mid-band carrier RF channel emulator capable of emulating independent fading on multiple branches Measurement software to observe active receive branches
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR base station emulator configured on a mid-band carrier. 2. Employ an RF channel emulator to create independent fading profiles on 16/32 receive branches. 3. Establish a connection and monitor the device's antenna status to confirm 16/32 active receive chains. 4. Vary the fading profiles on different branches and ensure that the device maintains performance using diversity combining.
Test Limits	NA
Expected Results	The FWA device supports 16/32 active receive antennas on NR mid-band carriers and leverages diversity combining to sustain link quality.

Test No.	**GR_TSTP_3.1.9.15**
Test Details	To verify that FWA device shall support 256QAM modulation for downlink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in downlink. 4. Initiate sustained downlink traffic to the FWA device. 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in downlink. 6. Verify that 256QAM is selected and used for downlink transmission.
Test Limits	NA
Expected Results	The FWA device supports 256QAM modulation for downlink

Test No.	**GR_TSTP_3.1.9.16**
Test Details	To verify that FWA device shall support 64QAM modulation for uplink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 64-QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 64-QAM modulation in uplink. 4. Initiate sustained uplink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 64QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	The FWA device supports 64QAM modulation for uplink.

Test No.	**GR_TSTP_3.1.9.17**
Test Details	To verify that FWA device should support 256QAM modulation for uplink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in uplink. 4. Initiate sustained uplink traffic to the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 256QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	The FWA device supports 256QAM modulation for uplink.

Test No.	**GR_TSTP_3.1.9.18**
Test Details	To verify that FWA device shall support power class 3 (23 dBm).
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-1 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 3. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-1. 8. Compare the measured output power against the limits defined for power class 3 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 3 in compliance with 3GPP standards.

Test No.	**GR_TSTP_3.1.9.19**
Test Details	To verify that FWA device should support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-1 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 2. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-1. 8. Compare the measured output power against the limits defined for power class 2 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 2 in compliance with 3GPP TS 38.101-1.

Test No.	**GR_TSTP_3.1.9.20**
Test Details	To verify that FWA device should support power class 1.5 (29 dBm) in compliance with 3GPP TS 38.101-1
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-1 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 1.5. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-1. 8. Compare the measured output power against the limits defined for power class 1.5 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 1.5 in compliance with 3GPP TS 38.101-1.

Test No.	**GR_TSTP_3.1.9.21**
Test Details	To verify that FWA device shall support 15 kHz Sub-Carrier Spacing in FR1 NR bands.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment) to operate on FR1 with 15Khz SCS. 3.Attach the FWA device to the NR network and verify successful registration. 4.Using network logs/test equipment capture and decode UE Capability Information. 5. Verify FWA device establish connection with 15kHz SCS. 6. Establish an active data session between the FWA and the network. 7.Initiate sustained downlink and uplink traffic to ensure stable operation
Test Limits	N/A
Expected Results	The FWA device successfully supports **15 kHz SCS** in FR1 NR bands.

Test No.	**GR_TSTP_3.1.9.22**
Test Details	To verify that FWA device shall support 30 kHz Sub-Carrier Spacing in FR1 NR bands.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/Smartphone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment) to operate on FR1 with 30Khz SCS. 3.Attach the FWA device to the NR network and verify successful registration. 4.Using network logs/test equipment capture and decode UE Capability Information. 5. Verify FWA device establish connection with 30kHz SCS. 6. Establish an active data session between the FWA and the network. 7.Initiate sustained downlink and uplink traffic to ensure stable operation
Test Limits	N/A
Expected Results	The FWA device successfully supports 30 **kHz SCS** in FR1 NR bands.

Test No.	**GR_TSTP_3.1.9.23**
Test Details	To verify that FWA device Should support all 3GPP Channel Bandwidths.
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply Lan Client (PC/Laptop) Logging tool
Test Setup	TEST SETUPX
Test Procedure	1. Power on the FWA Device 2. For each supported NR band and numerology a. Configure the Network Emulator with one 3GPP-defined channel bandwidth at a time, as specified in i. TS 30.101-1 (FR1) ii. TS 38.101-2 (FR2) 3. Activate the configured NR cell. Allow FWA Device to Search for available cells. 4. Verify from **system information logs** that: a. The configured **channel bandwidth** is accepted by the FWA device b. The configured bandwidth **does not exceed the device’s supported channel bandwidth** 5. Verify that the FWA device **selects and camps on the NR cell** with the **configured bandwidth**. 6. Establish a connection between FWA Device and emulator for configured bandwidth. 7. Verify from **signaling logs** that a. FWA Device should support the configured channel bandwidth 8. Establish data session verify the connectivity.
Test Limits	NA
Expected Results	1. The device accepts only **supported channel bandwidth configurations**.

Test No.	**GR_TSTP_3.1.10.1**
Test Details	To verify that FWA device shall support EN-DC (Option 3x)
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the FWA device to support Dual Connectivity ensuring: a. LTE as Master node and 5G-NR as Secondary Node. 3.Attach the FWA device to the LTE network and verify successful registration 4. Establish an active data session (e.g., EPS bearer) between the FWA and the network. 5.Configure EN-DC Option 3x activation from the network. 6.Initiate downlink and uplink data traffic from the FWA device. 7. Using network logs/test equipment, monitor the user plane traffic routing and verify that data is transmitted via NR.
Test Limits	N/A
Expected Results	The FWA device successfully establishes EN-DC connectivity with option 3x as LTE as the Master Node and NR as the Secondary Node.

Test No.	**GR_TSTP_3.1.10.2**
Test Details	To verify that FWA device shall support 2DL contiguous NR Carrier Aggregation.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment) to support 2DL contiguous Carrier Aggregation within the same NR band ensuring: a.Two downlink component carriers (DL CC1 and DL CC2) are configured with different bands. b.Corresponding downlink component carriers are configured as required for the DL CA operation 3.Attach the FWA device to the NR network and verify successful registration. 4.Configure and activate a secondary NR Cell (SCell) adjacent to the PCell. 4. Establish an active data session between the FWA and the network. 5.Initiate sustained downlink traffic from the network. 6.Using network logs/test equipment monitor and verify that the data is received simultaneously over both downlink component carriers confirming: a.Activation of CA b.Scheduling on both DL CCs
Test Limits	N/A
Expected Results	The FWA device successfully establishes **2DL contiguous NR carrier aggregation**.

Test No.	**GR_TSTP_3.1.10.3**
Test Details	To verify that FWA device should support 2UL contiguous NR Carrier Aggregation
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment) to support 2UL contiguous Carrier Aggregation within the same NR band ensuring: a.Two downlink component carriers (UL CC1 and UL CC2) are configured with different bands. b.Corresponding downlink component carriers are configured as required for the UL CA operation 3.Attach the FWA device to the NR network and verify successful registration. 4.Configure and activate a secondary NR Cell (SCell) adjacent to the PCell. 4. Establish an active data session between the FWA and the network. 5.Initiate sustained uplink traffic from the FWA device. 6.Using network logs/test equipment monitor the uplink transmission parameters and verify that the data is received simultaneously over both uplink component carriers confirming: a.Activation of CA b.Scheduling on both UL CCs
Test Limits	N/A
Expected Results	The FWA device successfully establishes **2UL contiguous NR carrier aggregation**.

Test No.	**GR_TSTP_3.1.10.4**
Test Details	To verify that FWA device shall support UL split bearer to transmit concurrently on LTE and NR..
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Attach the FWA device to the LTE network and verify the successful registration and check the RRC-reconfiguration for the Split IE. 3.Attach the FWA device to the NR network and verify successful registration for the ENDC connectivity. 4. Establish an active data session between the FWA and the network. 5.Initiate continuous uplink traffic from the FWA device. 6.Using network logs/test equipment capture and decode signaling to verify split bearer configuration and operation.
Test Limits	
Expected Results	Successful establishment of EN-DC with UL split bearer configured.

Test No.	**GR_TSTP_3.1.10.5**
Test Details	To verify that FWA device shall support MIMO 2 x 2 DL capabilities on NR FR2 bands (e.g., NR bands n257/n258).
Test Instruments Required	FWA CPE capable of mmWave operation Power supply unit 5G NR FR2 base station emulator (n257/n258) supporting 2×2 MIMO downlink mmWave antennas and cables or OTA test environment Throughput measurement tool or test software
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR FR2 base station emulator operating on n257 or n258 with 2×2 MIMO downlink enabled. 2. Establish a connection at mmWave frequencies using appropriate antenna positioning or waveguide cabling. 3. Generate downlink traffic using two spatial streams and monitor the FWA device’s reception. 4. Verify through logs or measurement software that two spatial streams are received simultaneously. 5. Measure downlink throughput to confirm that it corresponds to 2×2 MIMO capability.
Test Limits	NA
Expected Results	The FWA device receives two spatial streams on NR FR2 bands (n257/n258), demonstrating 2×2 MIMO downlink capability with expected throughput.

Test No.	**GR_TSTP_3.1.10.6**
Test Details	To verify that FWA device should support MIMO 4 x 4 DL capabilities on NR FR2 bands (e.g., NR bands n257/n258).
Test Instruments Required	FWA CPE capable of mmWave operation Power supply unit 5G NR FR2 base station emulator (n257/n258) supporting 4×4 MIMO downlink mmWave antennas and cables or OTA test environment Throughput measurement tool or test software
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR FR2 base station emulator operating on n257 or n258 with 4×4 MIMO downlink enabled. 2. Establish a connection at mmWave frequencies using appropriate antenna positioning or waveguide cabling. 3. Generate downlink traffic using two spatial streams and monitor the FWA device's reception. 4. Verify through logs or measurement software that 4 spatial streams are received simultaneously. 5. Measure downlink throughput to confirm that it corresponds to 4×4 MIMO capability.
Test Limits	NA
Expected Results	The FWA device receives two spatial streams on NR FR2 bands (n257/n258), demonstrating 4×4 MIMO downlink capability with expected throughput.

Test No.	**GR_TSTP_3.1.10.7**
Test Details	To verify that FWA device shall support 64QAM modulation for downlink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 64QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 64QAM modulation in downlink. 4. Initiate sustained downlink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in downlink. 6. Verify that 64QAM is selected and used for downlink transmission.
Test Limits	NA
Expected Results	FWA device supports 64QAM modulation for downlink.

Test No.	**GR_TSTP_3.1.10.8**
Test Details	To verify that FWA device should support 256QAM modulation for downlink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in downlink. 4. Initiate sustained downlink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in downlink. 6. Verify that 256QAM is selected and used for downlink transmission.
Test Limits	NA
Expected Results	FWA device supports 256QAM modulation for downlink.

Test No.	**GR_TSTP_3.1.10.9**
Test Details	To verify that FWA device shall support 64QAM modulation for uplink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 64QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 64QAM modulation in uplink. 4. Initiate sustained uplink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 64QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	FWA device supports 64QAM modulation for uplink.

Test No.	**GR_TSTP_3.1.10.10**
Test Details	To verify that FWA device should support 256QAM modulation for uplink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in uplink. 4. Initiate sustained uplink traffic to the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 256QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	FWA device supports 256QAM modulation for uplink.

Test No.	**GR_TSTP_3.1.10.11**
Test Details	To verify that FWA device shall support power class 3 (23 dBm).
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-2 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 3. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-2. 8. Compare the measured output power against the limits defined for power class 3 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 3 in compliance with 3GPP standards.

Test No.	**GR_TSTP_3.1.10.12**
Test Details	To verify that FWA device should support power class 2 (26 dBm).
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-2 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 2. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-2. 8. Compare the measured output power against the limits defined for power class 2 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 2 in compliance with 3GPP standards.

Test No.	**GR_TSTP_3.1.10.13**
Test Details	To verify that FWA device should support power class 1 (31 dBm).
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-2 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 1. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-2. 8. Compare the measured output power against the limits defined for power class 1 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 1 in compliance with 3GPP standards.

Test No.	**GR_TSTP_3.1.10.14**
Test Details	To verify that FWA device shall support 100 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply unit LAN Client (PC/Laptop) Logging Tool.
Test Setup	TEST SETUPX
Test Procedure	1. Power On the FWA CPE 2. Configure the **NR Network Emulator** with o FR2 NR TDD band (e.g., n257 or n258) o 100 MHz channel bandwidth o Supported numerology for FR2 (3GPP 101-1,101-2) 3. Activate the configured NR cell 4. Allow the FWA device to **search for and detect the NR cell**. 5. Verify the system information logs that o The configured **100 MHz channel bandwidth is accepted.** **6.** Verify that the FWA device **selects and camps on the NR cell** with the configured 100 MHz bandwidth. 7. Establish an **RRC connection** between the FWA device and the network emulator. 8. Verify the Signaling logs that o The configured **100 MHz channel bandwidth is accepted.** 9. Establish a data session very connectivity
Test Limits	NA
Expected Results	1. The FWA device successfully supports **100 MHz channel bandwidth** in **FR2 NR TDD bands (n257/n258)**.

Test No.	**GR_TSTP_3.1.10.15**
Test Details	To verify that FWA device should support 200 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply unit LAN Client (PC/Laptop) Logging Tool.
Test Setup	TEST SETUPX
Test Procedure	1. Power On the FWA CPE Device 2. Configure the **NR Network Emulator** with a. FR2 NR TDD band (e.g., n257 or n258) b. 200 MHz channel bandwidth c. Supported numerology for FR2 (3GPP 101-1,101-2) 3. Activate the configured NR cell 4. Allow the FWA device to **search for and detect the NR cell**. 5. Verify the system information logs that a. The configured 2**00 MHz channel bandwidth is accepted.** **6.** Verify that the FWA device **selects and camps on the NR cell** with the configured 200 MHz bandwidth. 7. Establish an **RRC connection** between the FWA device and the network emulator. 8. Verify the Signaling logs that a. The configured 2**00 MHz channel bandwidth is accepted.** 9. Establish a data session very connectivity
Test Limits	NA
Expected Results	1. The FWA device successfully supports 2**00 MHz channel bandwidth** in **FR2 NR TDD bands (n257/n258)**.

Test No.	**GR_TSTP_3.1.10.16**
Test Details	To verify that FWA device should support 400 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Device NR Emulator LAN Client (PC/Laptop) Power supply
Test Setup	TEST SETUPX
Test Procedure	1. Power On the FWA Device 2. Configure the **NR Network Emulator** with a. FR2 NR TDD band (e.g., n257 or n258) b. 400 MHz channel bandwidth c. Supported numerology for FR2 (3GPP 101-1,101-2) 3. Activate the configured NR cell 4. Allow the FWA device to **search for and detect the NR cell**. 5. Verify the system information logs that a. The configured **400 MHz channel bandwidth is accepted.** 6. Verify that the FWA device **selects and camps on the NR cell** with the configured 400 MHz bandwidth. 7. Establish an **RRC connection** between the FWA device and the network emulator. 8. Verify the Signaling logs that a. The configured 4**00 MHz channel bandwidth is accepted.** 9. Establish a data session very connectivity
Test Limits	NA
Expected Results	1. The FWA device successfully supports 4**00 MHz channel bandwidth** in **FR2 NR TDD bands (n257/n258).**

Test No.	**GR_TSTP_3.1.10.17**
Test Details	To verify that FWA device shall support Cell Carriers with ax50Mhz + bx100MHz channel bandwidth in FR2 NR TDD bands (i.e N258 , N257) , where a & b represents integer numbers
Test Instruments Required	FWA CPE Device NR Emulator LAN Client (PC/Laptop) Power supply
Test Setup	TEST SETUPX
Test Procedure	1. Power ON the FWA Device 2. Configure the Network Emulator with the following parameters: **a.** NR band: **n257 or n258** **b.** Duplex mode: **TDD** c. Channel bandwidth configuration: *i.* a × 50 MHz + b × 100 MHz, a=1, b=2 *50+200 = 250MHz* d. Sub-carrier spacing as applicable for FR2 (e.g., 60 kHz or 120 kHz) 3. Activate the configured FR2 NR cell(s). Search for NR Cells, select and camp on configured FR2 cell. 4. Verify that the FWA CPE successfully, Detects the FR2 cell and accepts the configured carrier bandwidth combination 5. Establish an **RRC connection** between the FWA CPE and the Network Emulator 6. Verify logs the total aggregated bandwidth matches 250MHz 7. Establish the data session and verify the connectivity.
Test Limits	NA
Expected Results	• The FWA device successfully o Camps on NR FR2 TDD cells in bands n257/n258 o Supports aggregated bandwidths of the form a × 50 MHz + b × 100 MHz • Establishes and maintains an RRC connection

Test No.	**GR_TSTP_3.1.10.18**
Test Details	To verify that FWA device shall support 60 KHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment) to support FR2 TDD bands with 60Khz SCS. 3.Attach the FWA device to the NR network and verify successful registration. 4. Using network logs/test equipment to capture and decode UE Capability Information. 5. Verify that the FWA device establish connection with 60kHz SCS. 6. Establish an active data session between the FWA and the network. 7.Initiate sustained downlink and uplink traffic to ensure stable operation
Test Limits	N/A
Expected Results	The FWA device successfully supports 60 **kHz SCS** in FR2 NR TDD bands.

Test No.	**GR_TSTP_3.1.10.19**
Test Details	To verify that FWA device shall support 120 KHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment) to support FR2 TDD bands with 120Khz SCS. 3.Attach the FWA device to the NR network and verify successful registration. 4. Using network logs/test equipment to capture and decode UE Capability Information. 5. Verify FWA device to establish connection with 120kHz SCS. 6. Establish an active data session between the FWA and the network. 7.Initiate sustained downlink and uplink traffic to ensure stable operation
Test Limits	N/A
Expected Results	The FWA device successfully supports 120 **kHz SCS** in FR2 NR TDD bands.

Test No.	**GR_TSTP_3.1.11.1**
Test Details	To verify that FWA device may be compliant to TS.24 for Antenna Performance acceptance values
Test Instruments Required	FWA CPE with mmWave capability Power supply unit 5G NR FR2 base station emulator (n257/n258) mmWave OTA measurement system capable of TRP/TIS measurements Measurement software and calibration equipment
Test Setup	TEST SETUP X
Test Procedure	1. Position the FWA device in a mmWave OTA chamber and connect it to a 5G NR FR2 base station emulator. 2. Establish a stable connection on the FR2 band (n257 or n258). 3. For TRP measurement: command the device to transmit a high-power uplink signal and measure the radiated power in all directions to compute Total Radiated Power. 4. For TIS measurement: transmit a downlink signal and evaluate the device's total isotropic sensitivity across all orientations. 5. Compare measured TRP and TIS values with the GSMA TS.24 acceptance requirements for FR2 bands. 6. Record findings and determine compliance.
Test Limits	TRP and TIS values shall meet or exceed GSMA TS.24 acceptance thresholds for FR2.
Expected Results	The FWA device's mmWave antenna performance meets GSMA TS.24 acceptance values for both TRP and TIS on NR FR2 bands.

Test No.	**GR_TSTP_3.2.1**
Test Details	To verify that FWA device shall support Option 2 SA deployment option
Test Instruments Required	1. FWA. 2. 5G Standalone Core Network (5GC) test environment 3. Base Station (gNB) capable of Option 2 SA configuration 4. Management access to FWA device (Web GUI / CLI). 5. Test PC or terminal connected to FWA LAN.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device and gNB. 2. Configure gNB and 5GC for Option 2 SA operation. 3. Register the FWA device to the 5G Core. 4. Verify registration parameters on FWA: • Access Type = 5G NR • Core Network = 5GC (not EPC) 5. PLMN ID and Slice configuration (if applicable) 6. From FWA LAN or Wi-Fi clients: • Verify IPv4 / IPv6 connectivity • Ping 5GC interfaces or test servers 7. Generate traffic (iPerf3) to validate end-to-end throughput. 8. Check logs on FWA and gNB for successful 5G registration.
Test Limits	NA
Expected Results	The FWA device successfully registers to the 5GC in **Option 2 SA mode**.

Test No.	**GR_TSTP_3.2.2**
Test Details	To verify that FWA device should support Option 4 NSA deployment option
Test Instruments Required	1. FWA. 2. 5G NR gNB capable of Option 4 NSA deployment 3. LTE EPC (Evolved Packet Core) configured for NSA operation 4. Management access to FWA device (Web GUI / CLI). 5. Test PC / terminal connected to FWA LAN or Wi-Fi.
Test Setup	TEST SETUP X
Test Procedure	1. Power On the FWA. 2. Configure LTE eNB and 5G gNB for **Option 4 NSA mode**. 3. Register the FWA device to the NSA network. 4. Verify registration parameters on FWA: • LTE anchor cell active for control plane • 5G NR used for user plane (data traffic) 5. PLMN ID and slice configuration (if applicable) 6. From FWA LAN or Wi-Fi clients: • Verify IPv4 / IPv6 connectivity 7. Ping external servers or EPC interfaces. 8. Generate traffic using iPerf3 to validate throughput. 9. Check logs on FWA, LTE eNB, and 5G gNB for successful NSA registration and user plane activation.
Test Limits	NA
Expected Results	The FWA device successfully registers in **Option 4 NSA mode**.

Test No.	**GR_TSTP_3.2.3**
Test Details	To verify that FWA device shall be compliant with 3GPP NR Access Stratum Release 16 baseline or later
Test Instruments Required	FWA Device Power Supply LAN Client Network Emulator Logging Tool
Test Setup	TEST SETUPX
Test Procedure	1. Power ON the FWA CPE 2. Configure the Network Emulator to broadcast an NR cell compliant with 3GPP Release-16 baseline. 3. Allow FWA Device to Search for available NR cells & select and camp on the configured NR cell. 4. Establish a connection between FWA Device and Network emulator. 5. Verify during UE capability exchange that **AccessStratumRelease IE should be release16.** Which release FWA Device is supporting 6. Establish data sessions and verify stability of RRC Connection.
Test Limits	NA
Expected Results	• The FWA device successfully o Camps on an NR cell operating with Release-16 baseline o Establishes and maintains an RRC connection • Correctly signals and operates NR AS Release-16 features

Test No.	**GR_TSTP_3.2.4**
Test Details	To verify that FWA device shall support standardized 5QIs as specified in 3GPP TS 23.501
Test Instruments Required	FWA CPE Power supply unit 5G network connectivity (5GC with QoS Flow control support) LAN/Wi-Fi client device Voice/video/data service clients Network traffic analyzer / protocol analyzer 5QI/QoS Flow configuration access in 5G core Device management interface (Web UI/CLI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and establish 5G network registration. 2. Establish a PDU session with default QoS Flow. 3. Configure standardized 5QIs and QoS profiles in the 5G core. 4. Initiate multiple service flows generating GBR and Non-GBR traffic. 5. Capture user plane traffic and QoS Flow identifiers (QFI). 6. Verify unique QFI assignment per QoS Flow within the PDU session. 7. Validate mapping of service flows to QoS Flows and 5QIs. 8. Confirm correct QoS Flow control and traffic treatment enforcement.
Test Limits	NA
Expected Results	The FWA Device shall correctly support 5G QoS Flow architecture with proper QFI assignment, 5QI mapping, and QoS Flow control in accordance with 3GPP TS 23.501.

Test No.	**GR_TSTP_3.2.5**
Test Details	To verify that FWA CPE shall comply with 5G NR security requirements as specified in 3GPP TS 33.501, including support for mandatory NR encryption, integrity protection, authentication algorithms, and SUCI-based registration as applicable to the UE category. Optional algorithms defined therein may be supported
Test Instruments Required	FWA CPE Power supply unit Network Protocol Analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device. 2. Register the FWA device with a network. 3. Establish NR radio connection between the FWA device and the gNB and capture the 3gpp signaling messages. 4. Register the FWA device with the 5G network and capture NGAP and NAS signaling exchanged using a network protocol analyzer (e.g., Wireshark or equivalent).
Test Limits	
Expected Results	1. Mobile Identity IE shall be set to SUCI concealed with ECIES Profile -A/ECIES Profile-B mechanism in Registration Request/Identity Request message from FWA. 2. Verify the presence of 5G-AKA/ EAP-AKA’ Authentication procedure. 3. In Security Mode Command integrity algorithm shall set to NULL/NIA1/NIA2/NIA3 and encryption algorithm shall set to NULL/NEA1/NEA2/NEA3.

Test No.	**GR_TSTP_3.2.6**
Test Details	To verify that FWA device shall support Initial 5GC Registration with SUCI, as per 3GPP TS 24.501. The FWA device may support 5G Slicing User Equipment Route Selection Policy (URSP) parameters.
Test Instruments Required	FWA CPE Power supply unit Network Protocol Analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device. 2. Register the FWA device with a network. 3. Establish NR radio connection between the FWA device and the gNB and capture the 3gpp signaling messages. 4. Register the FWA device with the 5G network and capture NGAP and NAS signaling exchanged using a network protocol analyzer (e.g., Wireshark or equivalent). 5. Make sure PDU session is established.
Test Limits	
Expected Results	1. Mobile Identity IE shall be set to SUCI concealed with ECIES Profile -A/ECIES Profile-B mechanism in Registration Request/Identity Request message from FWA. 2. After successful PDU Session Establishment procedure, Network must initiate Manage Ue policy Command for URSP rules. If FWA supports those then it must send Manage UE policy Complete or Reject.

Test No.	**GR_TSTP_3.2.7**
Test Details	To verify that FWA device may be compliant to GSMA TS.24 for Antenna Performance acceptance values
Test Instruments Required	FWA CPE Power supply unit NR base station emulator OTA measurement system capable of TRP/TIS measurements for NR bands Measurement software and calibration equipment
Test Setup	TEST SETUP X
Test Procedure	1. Place the FWA device in the OTA measurement chamber and connect it to an NR base station emulator on the relevant band (e.g., Band 3 or Band 5). 2. Establish NR connection with the device. 3. Perform TRP measurements by transmitting at maximum power and rotating the device through the required spatial grid. 4. Perform TIS measurements by sending a downlink signal and measuring the effective sensitivity across orientations. 5. Compare the measured TRP and TIS values to the acceptance thresholds defined in GSMA TS.24 for NR bands. 6. Document compliance.
Test Limits	TRP and TIS shall meet or exceed GSMA TS.24 acceptance values for NR FR1 bands.
Expected Results	The FWA device's NR antenna performance satisfies GSMA TS.24 acceptance values for TRP and TIS.

Test No.	**GR_TSTP_3.2.8**
Test Details	To verify that FWA device may support 5G Slicing Network Slice Selection Assistance Information (NSSAI) parameters, as per 3GPP TS 24.501
Test Instruments Required	FWA CPE Power supply unit Network Protocol Analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device. 2. Register the FWA device with a network. 3. Establish NR radio connection between the FWA device and the gNB and capture the 3gpp signaling messages. 4. Register the FWA device with the 5G network and capture NGAP and NAS signaling exchanged using a network protocol analyzer (e.g., Wireshark or equivalent). 5. Make sure PDU is established. 6. Verify the presence of the Requested NSSAI IE in the Registration Request and the Allowed NSSAI IE in the Registration Accept, in accordance with 3GPP TS 24.501. 7. NSSAI field must be present in the PDU session establishment request message.
Test Limits	
Expected Results	1. FWA device supports NSSAI information parameters as per 3gpp specification.

Test No.	**GR_TSTP_3.2.9**
Test Details	To verify that FWA device may support SST (Slice/Service Type) and SD (Slice Differentiator) parameters.
Test Instruments Required	FWA CPE Power supply unit Network Protocol Analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device. 2. Register the FWA device with a network. 3. Establish NR radio connection between the FWA device and the gNB and capture the 3gpp signaling messages. 4. Register the FWA device with the 5G network and capture NGAP and NAS signaling exchanged using a network protocol analyzer (e.g., Wireshark or equivalent). 5. Verify that the Requested NSSAI in the Registration Request includes SST and, if multiple SSTs are indicated, the associated SD values. For a single SST, the inclusion of the SD value is optional.
Test Limits	
Expected Results	1. FWA device supports SST values according to 3gpp specifications.

Test No.	**GR_TSTP_3.2.10**
Test Details	To verify that FWA device may support standardized SST values, as specified in 3GPP TS 23.501
Test Instruments Required	FWA CPE Power supply unit Network Protocol Analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device. 2. Register the FWA device with a network. 3. Establish NR radio connection between the FWA device and the gNB and capture the 3gpp signaling messages. 4. Register the FWA device with the 5G network and capture NGAP and NAS signaling exchanged using a network protocol analyzer (e.g., Wireshark or equivalent). 5. Verify that the Requested NSSAI in the Registration Request includes standardized SST.
Test Limits	
Expected Results	1. FWA device supports standardized SST values according to the 3gpp specification.

Test No.	**GR_TSTP_3.2.11**
Test Details	To verify that FWA device should support all 3GPP Channel Bandwidths.
Test Instruments Required	FWA Device Power supply LAN Client (PC/Laptop) Network emulator Logging Tool
Test Setup	TEST SETUPX
Test Procedure	1. Power on the FWA Device 2. For each supported NR band and numerology a. Configure the Network Emulator with one 3GPP-defined channel bandwidth at a time, as specified in i. TS 30.101-1 (FR1) ii. TS 38.101-2 (FR2) 3. Activate the configured NR cell. Allow FWA Device to Search for available cells. 4. Verify from **system information and logs** that: a. The configured channel bandwidth is **accepted by the FWA device** b. The configured bandwidth **does not exceed the device's supported channel bandwidth** 5. Verify that the FWA device **selects and camps on the NR cell** with the configured bandwidth. 6. Establish a connection between FWA Device and emulator for configured bandwidth. 7. Verify from **signaling logs** that a. FWA Device should support the configured channel bandwidth 8. Establish data session verify the connectivity.
Test Limits	NA
Expected Results	FWA Device should support all bandwidths and establish data sessions.

Test No.	**GR_TSTP_3.2.12.1**
Test Details	To verify that FWA device shall support SA option of connectivity to 5GC with Option-2 Architecture
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Access the FWA configuration interface. 3. Verify that SA mode is enabled, if not enabled configure FWA device to SA mode. 4. Confirm that the FWA CPE successfully: • Detects the SA gNB • Registers with the 5GC using Option-2 architecture 5. Verify FWA logs/status.
Test Limits	NA
Expected Results	FWA device supports SA option of connectivity to 5GC with Option-2 Architecture

Test No.	**GR_TSTP_3.2.12.2**
Test Details	To verify that FWA device shall support 2DL NR Carrier Aggregation
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Configure gNb with 2DL NR Carrier Aggregation. 3. Verify that: • One NR carrier is configured as PCell • One NR carrier is configured as SCell 4.Establish an **RRC connection** between the FWA device and 5g NR carrier. 5.Once RRC recconfiguration received from the network, check whether it is able to add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 6.Confirm that both DL component carriers are simultaneously active.
Test Limits	NA
Expected Results	FWA device supports 2DL NR Carrier Aggregation

Test No.	**GR_TSTP_3.2.12.3**
Test Details	To verify that FWA Device shall support all combinations of FDD and TDD duplexing (i.e., 2F, 2T, F+T and T+F) in 2DL NR Carrier Aggregation.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify successful registration of the FWA device to the NR network. 3. Configure and validate the following 2DL NR Carrier Aggregation scenarios, one at a time: a) 2F (FDD + FDD) • Configure two FDD NR carriers. • Verify PCell and SCell are both FDD. b) 2T (TDD + TDD) • Configure two TDD NR carriers. • Verify PCell and SCell are both TDD. c) F + T • Configure FDD carrier as PCell and TDD carrier as SCell. • Verify correct duplexing roles. d) T + F • Configure TDD carrier as PCell and FDD carrier as SCell. • Verify correct duplexing roles. 5. Once RRC reconfiguration is received from the network, check whether it is able to add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 6. For each scenario: • Confirm that both DL component carriers are active. • Verify duplexing mode of each carrier via FWA UI and/or gNB logs.
Test Limits	NA
Expected Results	FWA Device supports all combinations of FDD and TDD duplexing (i.e., 2F, 2T, F+T and T+F) in 2DL NR Carrier Aggregation.

Test No.	**GR_TSTP_3.2.12.4**
Test Details	To verify that the FWA device should support 3DL NR Carrier Aggregation.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify that the FWA device successfully registers to the NR network. 3. Configure gNb with 3DL NR Carrier Aggregation. 4. Monitor the FWA device logs. 5. Verify that: • One NR carrier is configured as PCell • Two NR carriers are configured as SCells 6. Once RRC reconfiguration is received from the network, check whether it can add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 7.Confirm that all three DL component carriers are simultaneously active.
Test Limits	NA
Expected Results	The FWA device supports 3DL NR Carrier Aggregation.

Test No.	**GR_TSTP_3.2.12.5**
Test Details	To verify that FWA device may support 4DL NR Carrier Aggregation or higher order.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify successful registration of the FWA device to the NR network. 3. Configure gNb with 4DL NR Carrier Aggregation. 4. Monitor the FWA device logs. 5. Verify that: • One NR carrier is configured as PCell • Three NR carriers are configured as SCells 6. Once RRC reconfiguration is received from the network, check whether it can add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 7. Confirm that all four DL component carriers are simultaneously active.
Test Limits	NA
Expected Results	FWA device supports 4DL NR Carrier Aggregation or higher order.

Test No.	**GR_TSTP_3.2.12.6**
Test Details	To verify that FWA device should support 2UL NR Carrier Aggregation
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify that the FWA device successfully registers to the NR network. 3. Configure gNb with 2UL NR Carrier Aggregation. 4. Monitor the FWA device logs. 5. Verify that: • One UL carrier is configured as PCell • One UL carrier is configured as SCell 6. Once RRC reconfiguration is received from the network, check whether it can add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 7. Confirm that both UL component carriers are simultaneously active.
Test Limits	NA
Expected Results	FWA device supports 2UL NR Carrier Aggregation

Test No.	**GR_TSTP_3.2.12.7**
Test Details	To verify that FWA device shall support 15 kHz Sub-Carrier Spacing in FR1 NR bands
Test Instruments Required	FWA CPE Power Supply LAN Client Network Emulator Logging tool
Test Setup	TEST SETUPX
Test Procedure	• Power On the FWA Device • Configure the **NR Network Emulator** with o FR1 NR TDD band (e.g., n78 or n79) o With supported channel bandwidth (3GPP 101-1) o SCS 15kHZ for FR1 • Activate the configured NR cell • Allow the FWA device to **search for and detect the NR cell**. • Verify the system information logs that o The configured Subcarrier spacing for supported channel bandwidth is supported by FWA Device • Verify that the FWA device **selects and camps on the NR cell** with the configured bandwidth with 15kHZ SCS. • Establish an **RRC connection** between the FWA device and the network emulator. • Verify the Signaling logs that o The configured Subcarrier spacing 15kHZ for supported channel bandwidth is supported by FWA Device • Establish a data session very connectivity
1. Test Limits	NA
Expected Results	• The FWA device **shall support NR FR1 operation with 15 kHz SCS** • The device **shall not reject** the cell due to unsupported numerology.

Test No.	**GR_TSTP_3.2.12.8**
Test Details	To verify that FWA device shall support 30 kHz Sub-Carrier Spacing in FR1 NR bands.
Test Instruments Required	FWA CPE Power Supply LAN Client Network Emulator Logging tool
Test Setup	TEST SETUP X
Test Procedure	• Power On the FWA Device • Configure the **NR Network Emulator** with o FR1 NR TDD band (e.g., n78 or n79) o With supported channel bandwidth (3GPP 101-1) o SCS 30kHZ for FR1 • Activate the configured NR cell • Allow the FWA device to **search for and detect the NR cell**. • Verify the system information logs that o The configured Subcarrier spacing (30kHZ) for supported channel bandwidth is supported by FWA Device • Verify that the FWA device **selects and camps on the NR cell** with the configured bandwidth with 15kHZ SCS. • Establish an **RRC connection** between the FWA device and the network emulator. • Verify the Signaling logs that o The configured Subcarrier spacing 30kHZ for supported channel bandwidth is supported by FWA Device • Establish a data session very connectivity
Test Limits	NA
Expected Results	1. The FWA device **shall support NR FR1 operation with 30 kHz SCS** 2. The device **shall not reject** the cell due to unsupported numerology.

Test No.	**GR_TSTP_3.2.12.9**
Test Details	To verify that FWA device shall support MIMO 4x4 DL capability on NR high-bands (e.g. NR bands n260/n261).
Test Instruments Required	FWA CPE Power Supply LAN Client Network Emulator Logging tool
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR base station emulator operating on a high-band carrier (e.g., n260/n261) with 4×4 MIMO downlink enabled. 2. Establish the connection and ensure that the 4×4 MIMO mode is active. 3. Generate downlink traffic across four spatial streams. 4. Monitor the FWA device to verify that four streams are received simultaneously. 5. Measure downlink throughput and confirm it is consistent with 4×4 MIMO capability.
Test Limits	NA
Expected Results	The FWA device successfully receives four spatial streams on NR high-band carriers and demonstrates throughput commensurate with 4×4 MIMO capability.

Test No.	**GR_TSTP_3.2.12.10**
Test Details	To verify that FWA device shall support MIMO 2x2 UL capability on NR high-bands (e.g. n260/n261).
Test Instruments Required	FWA CPE Power Supply LAN Client Network Emulator Logging tool
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR base station emulator on a high-band carrier. 2. Configure the emulator to request 2×2 uplink MIMO (two parallel PUSCH streams). 3. Establish the connection and instruct the device to transmit uplink data. 4. Use measurement software or base station logs to verify that two uplink streams are transmitted simultaneously. 5. Measure uplink throughput to ensure it corresponds to 2×2 MIMO.
Test Limits	NA
Expected Results	The FWA device transmits two simultaneous uplink streams on NR high-band carriers, demonstrating 2×2 UL MIMO capability.

Test No.	**GR_TSTP_3.2.12.11**
Test Details	To verify that FWA device shall support 4Rx diversity on NR mid-bands (e.g. n77/n78).
Test Instruments Required	FWA CPE Power Supply LAN Client Network Emulator Logging tool
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the base station emulator on a mid-band carrier. 2. Use the channel emulator to produce independent fading conditions on up to four receive branches. 3. Establish a connection and monitor the FWA device's reported receive chain activity. 4. Verify that four receive antennas are active and that diversity combining maintains link quality under varying fading conditions.
Test Limits	NA
Expected Results	The FWA device engages four receive antennas on NR mid-band carriers and leverages diversity combining to sustain link performance.

Test No.	**GR_TSTP_3.2.12.12**
Test Details	To verify that FWA device should support 8Rx diversity on NR high-bands (e.g. n260/n261).
Test Instruments Required	FWA CPE Power Supply LAN Client Network Emulator Logging tool
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the base station emulator on a high-band carrier. 2. Use an RF channel emulator to create independent fading on eight receive branches. 3. Establish a call and observe the FWA device's antenna status to confirm eight active receive chains. 4. Vary the fading profiles to verify diversity combining and link robustness.
Test Limits	NA
Expected Results	The FWA device uses eight active receive antennas on NR high-band carriers and maintains performance through diversity combining.

Test No.	**GR_TSTP_3.2.12.13**
Test Details	To verify that FWA device may support more than 8Rx diversity on NR mid-bands
Test Instruments Required	FWA CPEPower Supply LAN Client Network Emulator Logging tool
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the base station emulator on a mid-band carrier. 2. Use an RF channel emulator to create independent fading on eight receive branches. 3. Establish a call and observe the FWA device’s antenna status to confirm eight active receive chains. 4. Vary the fading profiles to verify diversity combining and link robustness.
Test Limits	NA
Expected Results	The FWA device uses eight active receive antennas on NR mid-band carriers and maintains performance through diversity combining.

Test No.	**GR_TSTP_3.2.12.14**
Test Details	To verify that FWA device shall support 256QAM modulation for downlink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in downlink. 4. Initiate sustained downlink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in downlink. 6. Verify that 256QAM is selected and used for downlink transmission.
Test Limits	NA
Expected Results	FWA device supports 256QAM modulation for downlink.

Test No.	**GR_TSTP_3.2.12.15**
Test Details	To verify that FWA device may support 1024QAM modulation for downlink on NR TDD FR1 high-bands (e.g. n77/n78).
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to: a. Operate in NR TDD FR1 high band (e.g., n77/n78) b. Enable 1024QAM modulation for downlink c. Configure suitable radio conditions for high order modulation. 3. Access the configurations of the FWA device and configure it to: a. Support 1024QAM modulation for downlink b. Operate on the selected NR TDD FR1 band. 4. Initiate sustained downlink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in downlink. 6. Verify that 1024QAM is selected and used for downlink transmission.
Test Limits	NA
Expected Results	FWA device may/may not 1-24QAM modulation for downlink on NR TDD FR1 high-bands (e.g., n77/78)

Test No.	**GR_TSTP_3.2.12.16**
Test Details	To verify that FWA device shall support 64QAM modulation for uplink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 64QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 64QAM modulation in uplink. 4. Initiate sustained uplink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 64QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	FWA device supports 64QAM modulation for uplink.

Test No.	**GR_TSTP_3.2.12.17**
Test Details	To verify that FWA device should support 256QAM modulation for uplink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in uplink. 4. Initiate sustained uplink traffic to the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 256QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	FWA device supports 256QAM modulation for uplink.

Test No.	**GR_TSTP_3.2.12.18**
Test Details	To verify that FWA device shall support power class 3 (23 dBm).
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-1 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 3. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-1. 8. Compare the measured output power against the limits defined for power class 3 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 3 in compliance with 3GPP standards.

Test No.	**GR_TSTP_3.2.12.19**
Test Details	To verify that FWA device should support power class 2 (26 dBm) in compliance with 3GPP TS 38.101-1
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-1 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 2. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-1. 8. Compare the measured output power against the limits defined for power class 2 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 2 in compliance with 3GPP TS 38.101-1.

Test No.	**GR_TSTP_3.2.12.20**
Test Details	To verify that FWA device should support power class 1.5 (29 dBm) or class 1 (31 dBm) in compliance with 3GPP TS 38.101-1.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-1 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 1.5 or class 1. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-1. 8. Compare the measured output power against the limits defined for power class 1.5 or class 1 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 1.5 or class 1 in compliance with 3GPP TS 38.101-1.

Test No.	**GR_TSTP_3.2.13.1**
Test Details	To verify that FWA device shall support SA option of connectivity to 5GC with Option-2 Architecture
Test Instruments Required	FWA CPE, Power supply unit, 5G SA network (Option-2), • NR gNB connected to 5GC LAN client (PC/Laptop), Network monitoring / protocol analysis tools, • RRC / NAS signaling logs (e.g., UE logs, Wireshark, QXDM) Data connectivity test tool (e.g., ping, iPerf
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device. 2. Allow the device to search for and camp on the NR cell. 3. Verify that the device performs NR RRC connection establishment directly with the gNB. 4. Verify 5GC registration via NAS signaling (no LTE involvement). 5. Confirm successful PDU session establishment. 6. Perform data traffic from the LAN client. 7. Monitor signaling to ensure Option-2 architecture is used throughout the session.
Test Limits	NA
Expected Results	The FWA Device successfully connects to the 5G Core using NR Standalone (Option-2), completes registration and PDU session establishment, and provides stable data service without LTE involvement.

Test No.	**GR_TSTP_3.2.13.2**
Test Details	To verify that FWA device shall support 2DL intra-band contiguous NR Carrier Aggregation
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify that the FWA device successfully registers to the NR network. 3. Configure gNb with 2DL intra-band contiguous NR Carrier Aggregation. 4. Once RRC reconfiguration is received from the network, check whether it can add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network Monitor the FWA device logs. 5. Verify that: • Both DL component carriers belong to the same NR band • The carriers are contiguous in frequency • One carrier is configured as PCell and the other as SCell 6. Confirm that both DL component carriers are simultaneously active.
Test Limits	NA
Expected Results	FWA device supports 2DL intra-band contiguous NR Carrier Aggregation

Test No.	**GR_TSTP_3.2.13.3**
Test Details	To verify that FWA device should support 4DL intra-band contiguous NR Carrier Aggregation
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify that the FWA device successfully registers to the NR network. 3. Configure gNb with 4DL intra-band contiguous NR Carrier Aggregation. 4. Once RRC reconfiguration is received from the network, check whether it can add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 5. Monitor the FWA device logs. 6. Verify that: • All four DL component carriers belong to the same NR band • The carriers are contiguous in frequency • One carrier is configured as PCell • Three carriers are configured as SCells 7. Confirm that all four DL component carriers are simultaneously active.
Test Limits	NA
Expected Results	FWA device supports 4DL intra-band contiguous NR Carrier Aggregation

Test No.	**GR_TSTP_3.2.13.4**
Test Details	To verify that FWA device may support 8DL intra-band contiguous NR Carrier Aggregation
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify that the FWA device successfully registers to the NR network. 3. Configure gNb with 8DL intra-band contiguous NR Carrier Aggregation. 4. Once RRC reconfiguration is received from the network, check whether it can add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 5. Monitor the FWA device logs. 6. Verify that: • All eight DL component carriers belong to the same NR band • The carriers are contiguous in frequency • One carrier is configured as PCell • Seven carriers are configured as SCells 7. Confirm that all eight DL component carriers are simultaneously active.
Test Limits	NA
Expected Results	FWA device supports 8DL intra-band contiguous NR Carrier Aggregation

Test No.	**GR_TSTP_3.2.13.5**
Test Details	To verify that FWA device should support 2UL intra-band contiguous NR Carrier Aggregation
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify that the FWA device successfully registers to the NR network. 3. Configure gNb with 2UL intra-band contiguous NR Carrier Aggregation 4. Once RRC reconfiguration is received from the network, check whether it can add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 5. Monitor the FWA device logs. 6. Verify that: • Both UL component carriers belong to the same NR band • The carriers are contiguous in frequency • One carrier is configured as PCell • Another carrier is configured as SCells 7. Confirm that both UL component carriers are simultaneously active.
Test Limits	NA
Expected Results	FWA device supports 2UL intra-band contiguous NR Carrier Aggregation

Test No.	**GR_TSTP_3.2.13.6**
Test Details	To verify that FWA device may support 4UL intra-band contiguous NR Carrier Aggregation
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Verify that the FWA device successfully registers to the NR network. 3. Configure gNb with 4UL intra-band contiguous NR Carrier Aggregation. 4. Once RRC reconfiguration is received from the network, check whether it can add NR as secondary cell w.r.t sCell configurations in CellGroupConfig message sent by the network. 5. Monitor the FWA device logs. 6. Verify that: 7. All four UL component carriers belong to the same NR band 8. The carriers are contiguous in frequency 9. One carrier is configured as PCell 10. Three carriers are configured as SCells 11. Confirm that all four UL component carriers are simultaneously active.
Test Limits	NA
Expected Results	FWA device supports 4UL intra-band contiguous NR Carrier Aggregation

Test No.	**GR_TSTP_3.2.13.7**
Test Details	To verify that FWA device shall support 100 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply unit LAN Client (PC/Laptop) Logging Tool.
Test Setup	TEST SETUPX
Test Procedure	1. Power On the FWA Device 2. Configure the **NR Network Emulator** with a. FR2 NR TDD band (e.g., n257 or n258) b. 100 MHz channel bandwidth c. Supported numerology for FR2 (3GPP 101-1,101-2) 3. Activate the configured NR cell 4. Allow the FWA device to **search for and detect the NR cell**. 5. Verify the system information logs that a. The configured 1**00 MHz channel bandwidth is accepted.** **6.** Verify that the FWA device **selects and camps on the NR cell** with the configured 100 MHz bandwidth. 7. Establish an **RRC connection** between the FWA device and the network emulator. 8. Verify the Signaling logs that a. The configured 1**00 MHz channel bandwidth is accepted.** 9. Establish a data session very connectivity
Test Limits	1. NA
Expected Results	• The FWA device successfully supports **100 MHz channel bandwidth** in **FR2 NR TDD bands**.

Test No.	**GR_TSTP_3.2.13.8**
Test Details	To verify that FWA device should support 200 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply unit LAN Client (PC/Laptop) Logging Tool.
Test Setup	TEST SETUPX
Test Procedure	1. Power On the FWA Device 2. Configure the **NR Network Emulator** with a. FR2 NR TDD band (e.g., n257 or n258) b. 200 MHz channel bandwidth c. Supported numerology for FR2 (3GPP 101-1,101-2) 3. Activate the configured NR cell 4. Allow the FWA device to **search for and detect the NR cell**. 5. Verify the system information logs that a. The configured 2**00 MHz channel bandwidth is accepted.** **6.** Verify that the FWA device **selects and camps on the NR cell** with the configured 200 MHz bandwidth. 7. Establish an **RRC connection** between the FWA device and the network emulator. 8. Verify the Signaling logs that a. The configured 2**00 MHz channel bandwidth is accepted.** 9. Establish a data session very connectivity
Test Limits	NA
Expected Results	1. The FWA device successfully supports 2**00 MHz channel bandwidth** in **FR2 NR TDD bands**.

Test No.	**GR_TSTP_3.2.13.9**
Test Details	To verify that FWA device may support 400 MHz channel bandwidth in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply unit LAN Client (PC/Laptop) Logging Tool.
Test Setup	TEST SETUPX
Test Procedure	1. Power On the FWA Device 2. Configure the **NR Network Emulator** with a. FR2 NR TDD band (e.g., n257 or n258) b. 400 MHz channel bandwidth c. Supported numerology for FR2 (3GPP 101-1,101-2) 3. Activate the configured NR cell 4. Allow the FWA device to **search for and detect the NR cell**. 5. Verify the system information logs that a. The configured 4**00 MHz channel bandwidth is accepted.** **6.** Verify that the FWA device **selects and camps on the NR cell** with the configured 400 MHz bandwidth. 7. Establish an **RRC connection** between the FWA device and the network emulator. 8. Verify the Signaling logs that a. The configured 4**00 MHz channel bandwidth is accepted.** 9. Establish a data session very connectivity
Test Limits	NA
Expected Results	• The FWA device successfully supports 4**00 MHz channel bandwidth** in **FR2 NR TDD bands**.

Test No.	**GR_TSTP_3.2.13.10**
Test Details	To verify that FWA device shall support Cell Carriers with [a x 50Mhz + b x100MHz] channel bandwidth in FR2 NR TDD bands (i.e. n258, n257), where a & b represents integer numbers.
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply unit LAN Client (PC/Laptop) Logging Tool.
Test Setup	TEST SETUPX
Test Procedure	1. Power ON the FWA Device 2. Configure the Network Emulator with the following parameters: **a.** NR band: **n257 or n258** **b.** Duplex mode: **TDD** c. Channel bandwidth configuration: *i.* a × 50 MHz + b × 100 MHz, where *a* ≥ *0* and *b* ≥ *0* *ii. Values a=1, b=2; 50+200 = 250MHz total bandwidth.* d. Sub-carrier spacing as applicable for FR2 (e.g., 60 kHz or 120 kHz) 3. Activate the configured FR2 NR cell(s). Search for NR Cells, select and camp on configured FR2 cells. 4. Verify that the FWA CPE successfully, Detects the FR2 cell and accepts the configured carrier bandwidth combination 5. Establish an **RRC connection** between the FWA CPE and the Network Emulator 6. Verify logs for the total aggregated bandwidth matches 250MHz. 7. Establish the data session and verify the connectivity.
Test Limits	NA
Expected Results	• The FWA device successfully o Camps on NR FR2 TDD cells in bands n257/n258 o Supports aggregated bandwidths of the form a × 50 MHz + b × 100 MHz • Establishes and maintains an RRC connection

Test No.	**GR_TSTP_3.2.13.11**
Test Details	To verify that FWA device shall support 60 kHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply unit LAN Client (PC/Laptop) Logging Tool.
Test Setup	TEST SETUPX
Test Procedure	1. Power On the FWA Device 2. Configure the **NR Network Emulator** with a. FR2 NR TDD band (e.g., n257 or n258) b. With supported channel bandwidth (3GPP 101-1,101-2) c. SCS 60kHZ for FR2 3. Activate the configured NR cell 4. Allow the FWA device to **search for and detect the NR cell**. 5. Verify the system information logs that **a.** The configured Subcarrier spacing for supported channel bandwidth is supported by FWA Device **6.** Verify that the FWA device **selects and camps on the NR cell** with the configured bandwidth with 60kHZ SCS. 7. Establish an **RRC connection** between the FWA device and the network emulator. 8. Verify the Signaling logs that **a.** The configured Subcarrier spacing 60kHZ for supported channel bandwidth is supported by FWA Device 9. Establish a data session very connectivity
Test Limits	NA
Expected Results	1. Verify SCS is 60KHz supported Connection is established

Test No.	**GR_TSTP_3.2.13.12**
Test Details	To verify that FWA device shall support 120 kHz Sub-Carrier Spacing in FR2 NR TDD bands (e.g., n257/n258).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply unit LAN Client (PC/Laptop) Logging Tool.
Test Setup	TEST SETUPX
Test Procedure	1. Power On the FWA Device 2. Configure the **NR Network Emulator** with a. FR2 NR TDD band (e.g., n257 or n258) b. With supported channel bandwidth (3GPP 101-1,101-2) c. SCS 120kHZ for FR2 3. Activate the configured NR cell 4. Allow the FWA device to **search for and detect the NR cell**. 5. Verify the system information logs that **a.** The configured Subcarrier spacing 120kHZ for supported channel bandwidth is supported by FWA Device **6.** Verify that the FWA device **selects and camps on the NR cell** with the configured bandwidth with 120kHZ SCS. 7. Establish an **RRC connection** between the FWA device and the network emulator. 8. Verify the Signaling logs that **a.** The configured Subcarrier spacing 120kHZ for supported channel bandwidth is supported by FWA Device 9. Establish a data session very connectivity
Test Limits	NA
Expected Results	1. Verify SCS is 120KHz supported Connection is established

Test No.	**GR_TSTP_3.2.13.13**
Test Details	To verify that FWA device shall support MIMO 2x2 DL capability on NR FR2 bands (e.g., NR bands n257/n258)
Test Instruments Required	FWA CPE capable of mmWave operation Power supply unit 5G NR FR2 base station emulator (n257/n258) configured for 2×2 MIMO downlink mmWave antennas and cables or OTA chamber Throughput measurement tool
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR FR2 base station emulator on n257 or n258 with 2×2 MIMO downlink configuration. 2. Establish the mmWave connection using proper antenna alignment or waveguide connection. 3. Generate downlink traffic across two spatial streams. 4. Monitor the FWA device to confirm two streams are received simultaneously. 5. Measure downlink throughput to verify performance consistent with 2×2 MIMO.
Test Limits	NA
Expected Results	

Test No.	**GR_TSTP_3.2.13.14**
Test Details	To verify that FWA device should support MIMO 4x4 DL capability on NR FR2 bands (e.g., NR bands n257/n258).
Test Instruments Required	FWA CPE with multiple mmWave antenna arrays Power supply unit 5G NR FR2 base station emulator configured for 4×4 MIMO downlink mmWave OTA chamber or waveguide setup Throughput measurement tool and monitoring software
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a 5G NR FR2 base station emulator on n257/n258 with 4×4 MIMO downlink configuration. 2. Establish a mmWave connection ensuring proper antenna alignment. 3. Generate downlink traffic using four spatial streams. 4. Monitor the FWA device's receive status to confirm four simultaneous streams are present. 5. Measure downlink throughput and confirm it aligns with 4×4 MIMO capabilities.
Test Limits	NA
Expected Results	The FWA device receives four spatial streams on NR FR2 bands and achieves throughput indicative of 4×4 MIMO operation.

Test No.	**GR_TSTP_3.2.13.15**
Test Details	To verify that The FWA device shall support 64QAM modulation for downlink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 64QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 64QAM modulation in downlink. 4. Initiate sustained downlink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in downlink. 6. Verify that 64QAM is selected and used for downlink transmission.
Test Limits	NA
Expected Results	FWA supports 64QAM modulation for downlink.

Test No.	**GR_TSTP_3.2.13.16**
Test Details	To verify that FWA device should support 256QAM modulation for downlink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in downlink. 4. Initiate sustained downlink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in downlink. 6. Verify that 256QAM is selected and used for downlink transmission.
Test Limits	NA
Expected Results	FWA device supports 256QAM modulation for downlink.

Test No.	**GR_TSTP_3.2.13.17**
Test Details	To verify that FWA device shall support 64QAM modulation for uplink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 64QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 64QAM modulation in uplink. 4. Initiate sustained uplink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 64QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	FWA device supports 64QAM modulation for uplink.

Test No.	**GR_TSTP_3.2.13.18**
Test Details	To verify that FWA device should support 256QAM modulation for uplink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in uplink. 4. Initiate sustained uplink traffic to the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 256QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	FWA device supports 256QAM modulation for uplink.

Test No.	**GR_TSTP_3.2.13.19**
Test Details	To verify that FWA device shall support power class 3.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-2 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 3. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-2. 8. Compare the measured output power against the limits defined for power class 3 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 3 in compliance with 3GPP standards.

Test No.	**GR_TSTP_3.2.13.20**
Test Details	To verify that FWA device should support power class 2 or class 1 in compliance with 3GPP TS 38.101-2.
Test Instruments Required	FWA CPE, Power supply unit, Wi-Fi client device (PC/Laptop/Smartphone), Wi-Fi analyzer or client device network status tool, Configuration access (e.g., Web UI), RF measurement equipment or 5G NR test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device 2. Connect the FWA to the 5G NR base station (gNB) or certified RF conformance test equipment. 3. Configure the test environment according to 3GPP TS 38.101-2 requirements including, a. Operating frequency band b. Channel bandwidth c. Test channels and reference measurement conditions d. Output power measurement setup 4. Verify UE capability signaling, ensuring FWA device indicates support for power class 2 or class 1. 5. Establish an NR connection and place the FWA device in an active transmission state. 6. Configure the FWA device for maximum uplink transmit power as specified for the selected power class. 7. Measure the maximum output power of the FWA using calibrated RF measurement equipment in accordance with TS 38.101-2. 8. Compare the measured output power against the limits defined for power class 2 or class 1 and verify compliance with the specified power class requirements.
Test Limits	NA
Expected Results	The FWA device should support power class 2 or class 1 in compliance with 3GPP TS 38.101-2.

Test No.	**GR_TSTP_3.3.1.1**
Test Details	To verify that FWA device should support 256QAM modulation for downlink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the NR test network (gNB or test equipment) to schedule downlink transmissions using 256 QAM. 3.Attach the FWA device to the NR network and verify successful registration. 4. Establish an active downlink data session between the FWA and the network. 5.Using logs/test equipment monitor downlink modulation and coding scheme 5.Verify that 256QAM is selected and used for downlink transmission.
Test Limits	N/A
Expected Results	The FWA device successfully supports **256QAM downlink modulation**.

Test No.	**GR_TSTP_3.3.1.2**
Test Details	To verify that FWA CPE shall comply with EPS (LTE/EPC) security requirements as specified in 3GPP TS 33.401, including support for mandatory EPS encryption, integrity protection, and authentication algorithms applicable to the UE category. Optional EPS algorithms defined therein may be supported.
Test Instruments Required	FWA CPE Power supply unit Network Protocol Analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA device. 2. Register the FWA device with a network. 3. Capture and observe packets using a network protocol analyzer
Test Limits	
Expected Results	1. Verify the presence of EPS-AKA' Authentication procedure. 2. In Security Mode Command integrity algorithm shall set to NULL/EIA1/EIA2/EIA3 and encryption algorithm shall set to NULL/EEA1/EEA2/EEA3

Test No.	**GR_TSTP_3.3.1.3**
Test Details	To verify that RRC, User Plane, and NAS security procedures shall be implemented in accordance with 3GPP TS 36.323 and TS 24.301
Test Instruments Required	FWA CPE Device NR Emulator LAN Client (PC/Laptop) Core Network Logging tool
Test Setup	TEST SETUPX
Test Procedure	1. Power ON the FWA CPE. 2. Allow the FWA device to: a. Initiate **NAS Attach / Registration procedure** **3.** Verify that **NAS security mode control** is initiated by the network: a. NAS ciphering and integrity protection are activated 4. Establish an **RRC connection** between the FWA device and the network. 5. Verify that **RRC Security Mode Command / Complete** procedures occur: a. Integrity and ciphering are enabled for RRC Signaling 6. Establish data session 7. Verify that **PDCP security** is applied: a. User Plane data is ciphered
Test Limits	NA
Expected Results	• Verify FWA Device should successfully o Completes NAS security mode control o Activates RRC ciphering and integrity protection o Applies PDCP ciphering for User Plane data

Test No.	**GR_TSTP_3.3.1.4**
Test Details	To verify that In order to support the transmission techniques reported above, the FWA device shall support ue-CategoryDL 11 and ue-CategoryUL 5 or higher and all fallback configurations foreseen by the standard.
Test Instruments Required	FWA CPE Power supply unit LTE base station emulator capable of supporting UE Categories up to at least Cat 11 SIM card or eSIM for the FWA device Throughput measurement tool (iperf or equivalent)
Test Setup	TEST SETUP X
Test Procedure	1. Disable 5G connectivity on the FWA device or operate in an area without 5G coverage to force fallback to LTE. 2. Connect the FWA device to an LTE base station emulator configured to support the desired category (Cat 11 or higher) on a suitable band. 3. After registration, retrieve the device's reported LTE UE category via AT commands or emulator logs. 4. Initiate downlink and uplink data sessions using a throughput measurement tool. 5. Measure downlink throughput to verify support for Category 11 speeds or higher and uplink throughput for Category 5 or better. 6. Validate if the device supports 64QAM and 256 QAM modulation order and carrier aggrigation of min. 2 CC. 7. If the device supports a higher category (e.g., Cat 11), record the improved uplink performance.
Test Limits	NA
Expected Results	When operating on LTE, the FWA device reports at least UE Category 11 for downlink and Category 5 for uplink. Throughput measurements are consistent with these categories or higher.

Test No.	**GR_TSTP_3.3.1.5**
Test Details	To verify that FWA device should support ue-CategoryDL 12 and ue-CategoryUL 13 (Uplink CA support) or higher and all fallback configurations foreseen by the standard.
Test Instruments Required	FWA CPE Power supply unit LTE base station emulator supporting 256-QAM, DL 4x4 MIMO and UL 2×2 MIMO (Cat 12/13) Throughput measurement tool Configuration access
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to an LTE base station emulator configured for a mid-band carrier (e.g., Band 3) supporting UE Category 12 downlink and Category 13 uplink. 2. Ensure that 256-QAM is enabled on the downlink along with 4x4 MIMO and 2×2 MIMO is enabled on the uplink. 3. After the device registers, retrieve the reported UE category and confirm support for Cat 12/13 or higher. 4. Generate downlink traffic and verify that the modulation order reaches 256-QAM (via device or emulator logs) and 4 DL data streams are working. 5. Generate uplink traffic and confirm that two uplink streams are transmitted simultaneously, indicating 2×2 MIMO. 6. Configure uplink CA with min. 2 CC and measure the UL throughput and ensure FWA is able to transmit on 2 bands. 7. Measure downlink and uplink throughput to ensure performance consistent with Cat 12/13 capabilities.
Test Limits	NA
Expected Results	The FWA device supports UE Category 12 downlink, 4x4 MIMO with 256-QAM and Category 13 uplink with 2×2 MIMO & UL CA. Throughput measurements reflect these capabilities.

Test No.	**GR_TSTP_3.3.1.6**
Test Details	To verify that FWA device shall support at least 3DL LTE Carrier Aggregation capability
Test Instruments Required	1. FWA. 2. Spectrum analyzer (optional, for RF verification). 3. Device management access (Web GUI / CLI). 4. Test PC connected to FWA LAN or Wi-Fi.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Configure LTE eNB to enable 3DL Carrier Aggregation. 3. Register the FWA device to the LTE network. 4. Verify on FWA or eNB side that: 5. Three DL component carriers are active 6. CA status shows 3DL CA enabled. 7. Generate continuous downlink traffic using iPerf3 or equivalent. 8. Monitor throughput and radio parameters.
Test Limits	NA
Expected Results	The FWA device shall successfully establish LTE connectivity with at least 3DL Carrier Aggregation enabled.

Test No.	**GR_TSTP_3.3.1.7**
Test Details	To verify that FWA device should support 2UL LTE Carrier Aggregation capability
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone) Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the LTE test network (eNB or test equipment) to support 2UL Carrier Aggregation ensuring: a.Two uplink component carriers (UL CC1 and UL CC2) are configured. b.Corresponding downlink component carriers are configured as required for the UL CA operation 3.Attach the FWA device to the LTE network and verify successful registration 4. Establish an active data session (e.g.,EPS bearer) between the FWA and the network. 5.Initiate sustained uplink data traffic from the FWA device. 6.Using network logs/test equipment monitor the uplink transmission parameters and verify that the uplink data is transmitted simultaneously on two uplink component carriers confirming: a.Activation of UL CA b.Scheduling on both UL CCs
Test Limits	NA
Expected Results	The FWA device shall support 2UL LTE Carrier Aggregation capability.

Test No.	**GR_TSTP_3.3.1.8**
Test Details	To verify that FWA device shall support MIMO 4x4 capability at least on one LTE mid-band (e.g., LTE B3 for Europe/Asia or B2 for US)
Test Instruments Required	FWA CPE Power supply unit LTE base station emulator configured for a mid-band (e.g., Band 3) with 4×4 MIMO downlink support Throughput measurement tool or MIMO stream analyzer
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to an LTE base station emulator on the selected mid-band (such as Band 3) with 4×4 MIMO configuration. 2. Ensure that the device registers and that 4×4 MIMO mode is active. 3. Generate downlink traffic using four spatial streams. 4. Monitor the device’s status or use measurement software to confirm that four MIMO streams are received. 5. Measure throughput and verify that it reflects 4×4 MIMO performance.
Test Limits	NA
Expected Results	The FWA device supports 4×4 MIMO on at least one LTE mid-band. It successfully receives four spatial streams and achieves throughput consistent with 4×4 MIMO.

Test No.	**GR_TSTP_3.3.1.9**
Test Details	To verify that FWA device shall support 256QAM modulation for downlink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in downlink. 4. Initiate sustained downlink traffic from the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in downlink. 6. Verify that 256QAM is selected and used for downlink transmission.
Test Limits	NA
Expected Results	FWA device shall support 256QAM modulation for downlink

Test No.	**GR_TSTP_3.3.1.10**
Test Details	To verify that FWA device shall support 64QAM modulation for uplink.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 64QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 64QAM modulation in uplink. 4. Initiate sustained uplink traffic from the FWA device 5. Using the network logs/test equipment to monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 64QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	FWA device shall support 64QAM modulation for uplink.

Test No.	**GR_TSTP_3.3.1.11**
Test Details	To verify that FWA device should support 256QAM modulation for uplink
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device Configuration access (e.g., Web UI) gNB or 5G test equipment
Test Setup	TEST SETUP X
Test Procedure	1. Power on the FWA 2. Access the configurations of the gNB or test equipment and configure it to enable 256QAM modulation. 3. Access the configurations of the FWA device and configure it to allow 256QAM modulation in uplink. 4. Initiate sustained uplink traffic to the FWA device 5. Using the network logs/test equipment monitor the modulation and coding scheme (MCS) in uplink. 6. Verify that 256QAM is selected and used for uplink transmission.
Test Limits	NA
Expected Results	FWA device shall support 256QAM modulation for uplink.

Test No.	**GR_TSTP_3.3.1.12**
Test Details	To verify that FWA device shall support standardized QCIs as specified in 3GPP TS 23.203
Test Instruments Required	4G LTE FWA Device. Power supply unit. LTE network connectivity (EPC supporting QoS/QCI). LAN/Wi-Fi client device. Voice/video/data service clients Network traffic analyzer / protocol analyzer Device management interface (Web UI/CLI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the 4G FWA Device and allow it to reach normal operational state. 2. Establish network attachment and service registration. 3. Configure multiple services (e.g. data, voice, video) with QoS profiles. 4. Initiate service sessions generating distinct traffic flows. 5. Capture traffic flows using a protocol/traffic analyzer (Wireshark). 6. Verify QCI/QoS parameter mapping for each service flow. 7. Validate compliance with standardized QCI characteristics as per 3GPP TS 23.203. 8. Confirm correct prioritization, handling, and traffic differentiation.
Test Limits	NA
Expected Results	The 4G LTE FWA Device shall correctly support and enforce standardized QCIs as defined in 3GPP TS 23.203, with proper QoS mapping and service differentiation.

Test No.	**GR_TSTP_3.3.1.13**
Test Details	To verify that FWA device should support operator specific QCIs as specified in 3GPP TS 23.203.
Test Instruments Required	1. FWA. 2. 5G Core with QoS/QCI configuration capability. 3. 5G gNB supporting QoS bearer configuration 4. PCRF/PCF (Policy and Charging Rules Function / Policy Control Function). 5. Traffic generator capable of marking flows per QCI/QoS. 6. Packet capture tool (e.g., Wireshark).
Test Setup	TEST SETUP X
Test Procedure	1. Configure operator-specific QCI profiles in EPC/5GC per TS 23.203. 2. Configure PCRF/PCF to assign different QCIs to different traffic flows. 3. Register the FWA device to the network. 4. Establish multiple bearers with different QCIs. 5. Generate traffic flows corresponding to different service types (e.g., voice, video, best effort, signaling). 6. Capture traffic and bearer information on network side and/or FWA. 7. Verify that: • Correct QCI is assigned per flow • Bearer characteristics match operator policy 8. Monitor QoS behavior (latency, packet loss, priority handling).
Test Limits	NA
Expected Results	The FWA device shall support operator-specific QCIs as defined in 3GPP TS 23.203.

Test No.	**GR_TSTP_3.3.1.14**
Test Details	To verify that FWA device shall support periodical intra-frequency ANR measurements for reporting to the network in the Strongest Cells and related CGI (Cell Global Identity).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply Lan client (PC/Laptop) Logging Tool
Test Setup	TEST SETUPX
Test Procedure	1. Power ON the FWA device and allow it to camp on the serving NR cell. 2. Configure the Network Emulator to trigger **periodical intra-frequency (Serving cell and neighbor cell on same carrier) measurement reporting** for ANR purposes 3. Allow the FWA device to perform **intra-frequency measurements** on the configured neighbor cells 4. Verify that the FWA device detects the **strongest intra-frequency neighbor cells**. 5. trigger CGI acquisition for the detected neighbor cells 6. Verify that the FWA device reports the following information to the network: a. Measured strongest neighbor cell(s) b. Corresponding **CGI Information (Cell Global Identity)** 7. **Verify Measurement Reports are sent periodically for every periodicity configured.**
Test Limits	NA
Expected Results	1. FWA Device Successfully identify strongest cell and Report CGI Info to the network. 2. The measurement report is sent periodically.

Test No.	**GR_TSTP_3.3.1.15**
Test Details	To verify that FWA device shall support periodical inter-frequency ANR measurements for reporting to the network the Strongest Cells and related CGI (Cell Global Identity).
Test Instruments Required	FWA CPE Device NR Network Emulator Power supply Lan client (PC/Laptop) Logging Tool
Test Setup	TEST SETUPX
Test Procedure	1. Power ON the FWA device. 2. Configure the Network Emulator with • One **Serving NR Cell** on **Frequency F1** • At least **two Inter-Frequency Neighbor NR Cells** on **Frequency F2** • Configure **measurement gaps** for inter-frequency measurements. • Configure Neighbor cell frequencies for Frequency F2. 3. Allow the FWA device to perform **inter-frequency measurements** using the configured measurement gaps. 4. Verify that the FWA device tunes to the target inter-frequency cell during measurement gaps, and Identifies 5. Verify that the FWA device detects and ranks **inter-frequency neighbor cells** based on measured RSRP 6. Verify that the FWA device tunes to the target inter-frequency cell during measurement gaps and reads CGI Information 7. FWA Device starts sending reports periodically containing CGI Information (CGI Cell Identity, Measured cell power).
Test Limits	NA
Expected Results	1. FWA Device Successfully identify strongest cell and Report CGI Info to the network. 2. The measurement report is sent periodically.

Test No.	**GR_TSTP_3.4.1**
Test Details	To verify the Operating frequency and Channel bandwidth shall be as per the applicable National Frequency Allocation Plan.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the FWA device to operate in an NFAP-compliant operating frequency and channel bandwidth. 3.Attach the FWA device to the NR network and verify successful registration. 4. Using network logs/test equipment to measure the operating frequency and occupied channel bandwidth 5. Verify that the measured values match the NFAP specifications.
Test Limits	N/A
Expected Results	The FWA device successfully operates at the correct frequency as per NFAP and channel bandwidth comples with the applicable NFAP requirements.

Test No.	**GR_TSTP_3.4.2**
Test Details	To verify that equipment shall be capable of operating in at least one of the frequency bands as per the applicable National Frequency Allocation Plan.
Test Instruments Required	FWA CPE Power supply unit Wi-Fi client device (PC/Laptop/SmartPhone)Wi-Fi analyze or client device network status tool eNB or test equipment Configurations access (e.g., Web UI)
Test Setup	TEST SETUP X
Test Procedure	1.Power on the FWA device 2.Configure the FWA device (RF device) to operate in an NFAP-compliant frequency band. 3.Attach the FWA device to the NR network and verify successful registration. 4. Using network logs/test equipment to capture and decode UE Capability Information. 5. Verify that the equipment successfully operates in the configured band. 6. Establish an active data session between the FWA and the network. 7.Initiate sustained downlink and uplink traffic to ensure stable operation.
Test Limits	N/A
Expected Results	The FWA device successfully operates in at least one frequency band defined by the applicable **NFAP**.

Test No.	**GR_TSTP_3.5.1.1**
Test Details	Maximum Output Power
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device’s RF output to a spectrum analyzer via a calibrated attenuator. 2. Set up a connection to a base station emulator on the band under test. 3. Configure the FWA device to transmit at its maximum rated power (e.g., by sending a continuous uplink signal). 4. Measure the conducted output power on the spectrum analyzer/power meter and apply correction factors for the coupler and attenuator. 5. Repeat the measurement for each supported band and technology (LTE, NR FR1, NR FR2). 6. Compare the measured maximum output power to the limits specified in the relevant standards.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The measured maximum output power for each band does not exceed the specified limit and is within the allowed tolerance of the declared value.

Test No.	**GR_TSTP_3.5.1.2**
Test Details	Power Control
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the base station emulator and configure a test call on the desired band. 2. For open loop power control, change the path loss or RSRP of the FWA and observe if the FWA's transmit power is changing based on the received RSRP. 3. For close loop power control issue power control commands from gNB emulator to the FWA device to step the transmit power up and down across its dynamic range. 3. At each commanded power level, measure the actual transmitted power using the spectrum analyzer. 4. Record the difference between commanded and measured power for each step and verify that the step size and absolute accuracy meet the specifications. 5. Repeat for multiple bands and configurations.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The FWA device adjusts it's transmit power according to network commands, with errors within the specified tolerances across the entire dynamic range.

Test No.	**GR_TSTP_3.5.1.3**
Test Details	Minimum Output Power
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Establish a connection between the FWA device and the base station emulator. 2. Command the FWA device to transmit at its minimum power setting. 3. Measure the conducted output power using the spectrum analyzer. 4. Ensure that the measured power is above the noise floor and within the specified minimum power range. 5. Repeat the test on all supported bands.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The FWA device can reduce its transmit power to the specified minimum level without dropping below functional limits.

Test No.	**GR_TSTP_3.5.1.4**
Test Details	Transmit OFF Power
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Ensure the FWA device is powered on and connected to the control interface. 2. Disable the device’s transmitter (e.g., by setting it to idle mode or using base station DRX commands). 3. Connect the RF output to a spectrum analyzer via a coupler and attenuator. 4. Sweep the analyzer across the relevant frequency range to measure residual RF emissions. 5. Record the power of any emissions and compare to spurious emission limits for transmit-OFF conditions.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	When the transmitter is disabled, the FWA device emits only negligible RF power, well below spurious emission limits.

Test No.	**GR_TSTP_3.5.1.5**
Test Details	Frequency Error
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a vector signal analyzer via a directional coupler and attenuator. 2. Establish a connection on the desired band using the base station emulator. 3. Command the FWA device to transmit a continuous wave or modulated signal at a known frequency. 4. Measure the actual carrier frequency using the vector signal analyzer. 5. Calculate the frequency error as the difference between the nominal and measured frequency. 6. Repeat for various bands and operating conditions.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The measured frequency error is within the allowed tolerance for all tested bands and configurations.

Test No.	**GR_TSTP_3.5.1.6**
Test Details	Error Vector Magnitude (EVM)
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device’s RF output to the vector signal analyzer through a coupler and attenuator. 2. Establish a connection to the base station emulator and configure the FWA device to transmit predefined modulation schemes (e.g., QPSK, 16QAM, 64QAM, 256QAM). 3. At each modulation, measure the EVM using the vector signal analyzer. 4. Compare the measured EVM values against the limits specified for each modulation order in the standards. 5. Repeat for different frequencies and bandwidths.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	EVM measurements for all modulation schemes are within specified limits across all bands and bandwidths.

Test No.	**GR_TSTP_3.5.1.7**
Test Details	Time Alignment Error
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the base station emulator and configure multi-antenna or multi-carrier transmission. 2. Use the vector signal analyzer or oscilloscope to capture the baseband signals from different antenna paths or component carriers. 3. Measure the relative time alignment between the signals. 4. Verify that the time alignment error does not exceed the specified limit for the technology. 5. Repeat measurements for various configurations and bands.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The time alignment error between antenna paths and carriers is within the permissible limit across all tested configurations.

Test No.	GR_TSTP_3.5.1.8
Test Details	Occupied Bandwidth
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the spectrum analyzer via a coupler and attenuator. 2. Establish a call on the desired band and configure the FWA device to transmit using each supported channel bandwidth (e.g., 5 MHz, 10 MHz, 20 MHz, 100 MHz). 3. For each bandwidth, measure the 99% occupied bandwidth on the spectrum analyzer. 4. Compare the measured occupied bandwidth to the nominal channel bandwidth and ensure it does not exceed the specified tolerance. 5. Repeat for other bands and technologies.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	For each channel bandwidth, the occupied bandwidth is within the allowed tolerance across all bands.

Test No.	**GR_TSTP_3.5.1.9**
Test Details	Adjacent Channel Leakage Ratio
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the spectrum analyzer via a coupler and attenuator. 2. Establish an uplink transmission on the desired band and configure the device at nominal power. 3. Measure the power in the assigned channel and in the adjacent channels using the spectrum analyzer. 4. Calculate the adjacent channel leakage ratio as the difference between in-band and adjacent-band powers, or configure the spectrum analyzer in ACLR mode. 5. Repeat for different bands and channel bandwidths.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	Measured ACLR values meet or exceed the minimum specified ratios for all tested bands and bandwidths.

Test No.	**GR_TSTP_3.5.1.10**
Test Details	Carrier Leakage & In-band emissions
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the vector signal analyzer. 2. Transmit a modulated signal at nominal power. 3. Measure carrier leakage (i.e., undesired carrier component) relative to the modulated signal and evaluate in-band emissions using the spectrum analyzer. 4. Ensure that the carrier leakage ratio and in-band emission spectrum comply with specified limits. 5. Repeat for each band.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	Carrier leakage and in-band emissions measured on all bands comply with the specified limits.

Test No.	**GR_TSTP_3.5.1.11**
Test Details	Spurious Emissions
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Establish a connection on the desired band and configure the FWA device for normal transmission at nominal power. 2. Connect the RF output to the spectrum analyzer using a coupler/attenuator or perform a radiated measurement if required. 3. Sweep the spectrum analyzer across the required frequency range (e.g., 30 MHz–12 GHz). 4. Identify and record the power of any spurious emissions outside the assigned channel. 5. Compare measured spurious emission levels against regulatory limits.
Test Limits	Spurious emissions shall be below the limits defined by TEC.
Expected Results	All spurious emissions fall below the specified limits across the swept frequency range.

Test No.	**GR_TSTP_3.5.1.12**
Test Details	Transmitter Intermodulation
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer and calibrated attenuator Signal generator to generate interfering signal Base station emulator RF cables or radiated test environment
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the base station emulator and establish a connection. 2. Inject CWs or OFDM interfering signal along with the desired signal to the spectrum analyzer. 3. Measure the output spectrum using a vector signal analyzer. 4. Identify the received signal spectrum using the signal analyzer. 5. Compare the intermodulation levels with specified limits.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	Transmitter intermodulation products are below the specified limits for all tested configurations.

Test No.	**GR_TSTP_3.5.1.13**
Test Details	Spectrum Emission Mask
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer capable of SEM measurement Base station emulator Directional coupler and attenuator
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to the spectrum analyzer via a coupler and attenuator and establish a connection on the desired band. 2. Transmit a signal at nominal power and set the spectrum analyzer to SEM measurement mode. 3. Measure the transmitted spectrum and compare it to the emission mask defined by the regulatory standard for that band. 4. Identify any deviations beyond the mask limits. 5. Repeat for each supported band and bandwidth.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	For every tested band and bandwidth, the spectrum stays within the emission mask, indicating compliance.

Test No.	**GR_TSTP_3.5.2.1**
Test Details	Reference Sensitivity
Test Instruments Required	FWA CPE Power supply unit Base station emulator RF attenuator or channel emulator Throughput/BLER measurement tool
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA device to a base station emulator and establish a call at a nominal receive power level. 2. Gradually reduce the power level of the desired signal using an attenuator or channel emulator while monitoring throughput or block error rate (BLER). 3. Determine the minimum power at which the device still meets performance criteria (e.g., BLER < 5% for LTE). 4. Repeat for each supported band and bandwidth.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The FWA device maintains required performance at or below the reference sensitivity threshold across all bands.

Test No.	**GR_TSTP_3.5.2.2**
Test Details	Adjacent Channel Selectivity
Test Instruments Required	FWA CPE Power supply unit Base station emulator to provide the desired signal Signal generator to create an interfering signal in an adjacent channel RF combiner and attenuators Measurement software for performance monitoring
Test Setup	TEST SETUP X
Test Procedure	1. Establish a call between the FWA device and the base station emulator at a nominal desired signal power. 2. Inject an interfering signal on the adjacent channel using a signal generator. Adjust its power according to the test specification. 3. Monitor the FWA device’s throughput or BLER while increasing the interfering signal’s power until performance degrades beyond the acceptable limit. 4. Calculate the adjacent channel selectivity as the difference between desired and interfering signal powers at the performance threshold. 5. Repeat for upper and lower adjacent channels and for various bands.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The FWA device maintains performance in the presence of adjacent channel interference up to the specified selectivity limit.

Test No.	**GR_TSTP_3.5.2.3**
Test Details	Blocking
Test Instruments Required	FWA CPE Power supply unit Base station emulator to generate the desired signal Signal generator(s) to produce high-power blocking signals at specified frequency offsets RF combiner and attenuators Measurement software
Test Setup	TEST SETUP X
Test Procedure	1. Establish a connection between the FWA device and the base station emulator at nominal signal power. 2. Introduce one or more high-power blocking signals at specified frequency offsets (e.g., ±1 MHz, ±5 MHz, ±10 MHz) using signal generators. 3. Gradually increase the power of the blocking signals while monitoring the FWA device's throughput or BLER. 4. Determine the blocking signal level at which device performance falls outside acceptable limits. 5. Repeat for each offset and for different bands.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The FWA receiver meets blocking performance requirements on all tested bands and frequency offsets.

Test No.	**GR_TSTP_3.5.2.4**
Test Details	Spurious Response
Test Instruments Required	FWA CPE Power supply unit Base station emulator Signal generator to provide unwanted frequencies that may cause spurious responses RF combiner and attenuators Measurement software
Test Setup	TEST SETUP X
Test Procedure	1. Establish a call between the FWA device and the base station emulator with the desired signal at nominal power. 2. Inject spurious tones or signals at frequencies known to cause mixer products or spurious responses into the receiver chain. 3. Monitor device performance (throughput or BLER) and identify any degradation or erroneous behaviour. 4. Increase the level of the spurious signals until performance degrades; record the threshold level. 5. Repeat across different frequencies and bands.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The FWA receiver exhibits immunity to spurious responses within the specified thresholds for all bands.

Test No.	**GR_TSTP_3.5.2.5**
Test Details	Intermodulation
Test Instruments Required	FWA CPE Power supply unit Base station emulator to generate the desired signal Two signal generators to produce two interfering tones RF combiner and attenuators Measurement software
Test Setup	TEST SETUP X
Test Procedure	1. Establish a connection between the FWA device and the base station emulator at nominal signal power. 2. Use two signal generators to inject two interfering signals at specified frequency offsets relative to the desired signal. 3. Adjust the power levels of the interfering signals according to the test specification. 4. Monitor the receiver performance (throughput or BLER) and determine if intermodulation products degrade performance. 5. Increase interfering signal power until performance falls outside acceptable limits. 6. Repeat for different offset frequencies and bands.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	The FWA receiver maintains performance in the presence of intermodulation interference up to the specified limit.

Test No.	**GR_TSTP_3.5.2.6**
Test Details	Spurious Emission
Test Instruments Required	FWA CPE Power supply unit Spectrum analyzer with broadband coverage Antenna or conducted measurement setup Base station emulator (optional)
Test Setup	TEST SETUP X
Test Procedure	1. Ensure the FWA device is in receive mode with no uplink transmission active. 2. Connect the device’s antenna port to a spectrum analyzer via a suitable coupler or, for radiated tests, place the device in an anechoic chamber. 3. Sweep the spectrum analyzer across the required frequency range to search for spurious emissions from the receiver. 4. Identify any emissions and measure their power. 5. Compare the measured spurious emissions to the limits specified by TEC.
Test Limits	Test guide and limits as per applicable 3GPP TS clause mentioned in GR as per applicable 4G/5G support.
Expected Results	All spurious emissions observed when the FWA receiver is idle are below regulatory limits.

Test No.	**GR_TSTP_4.1.2**
Test Details	To verify that failure of any component/ sub-system in the system may not result in failure of the complete system.
Test Instruments Required	1. PC/Laptop with FWA management interface access 2. Fault injection capability (e.g., disable modules via software, disconnect interfaces) 3. Power supply with current monitoring.
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA to normal power and network. 2. Verify that FWA is operating normally before fault injection. 3. Disable or simulate failure of a non-critical sub-system (e.g., LAN port, Wi-Fi AP antenna, USB, GPS if applicable). 4. Verify FWA core functions (power, cellular connectivity, basic routing) to continue to operate. 5. Restore the failed sub-system and verify recovery.
Test Limits	NA
Expected Results	FWA shall continue to provide core services despite failure of a single non-critical component, and system shall recover normal operation after restoration.

Test No.	**GR_TSTP_4.1.3**
Test Details	To verify that Provision shall be made for continuous testing of the system to allow both system qualities to check and fault indication as a fault arises.
Test Instruments Required	1. PC/Laptop for management access. 2. Network connectivity (LAN/Wi-Fi). 3. OMC. 4. Fault simulation capability (e.g., link disconnect, interface disable).
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA to power and network. 2. Connect PC/Laptop to the FWA management interface. 3. Ensure that OMC/NMS (if used) is connected and operational. 4. Access system health and status via PC/Laptop management interface. 5. Simulate a fault condition (e.g., disconnect WAN, disable interface, remove antenna). 6. Verify that the FWA detects the fault automatically. 7. Verify that fault alarms/indications are generated locally and/or at OMC. 8. Verify that system quality/status indicators are updated in real time.
Test Limits	NA
Expected Results	FWA shall support continuous system testing and real-time quality monitoring.

Test No.	**GR_TSTP_4.1.4**
Test Details	To verify that In case a fault is detected requiring reloading of the program, this shall be carried out automatically. In case of manual re-loading, it shall be possible to stop and start at any particular point in the program
Test Instruments Required	1. FWA. 2. PC/Laptop for management access. 3. FWA firmware/software image. 4. Power control (to simulate faults/restart). 5. Fault injection or reboot trigger method.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device and ensure normal operation. 2. Connect PC to FWA management interface. 3. Simulate a software fault or abnormal condition (e.g., watchdog trigger). 4. Observe whether the system automatically reloads/restarts the program. 5. Verify system returns to normal operational state after automatic reload. 6. Initiate a manual program to reload via management/maintenance interface. 7. During manual reload (if supported), attempt-controlled stop/start at defined checkpoints. 8. Verify system resumes operation correctly from selected point.
Test Limits	NA
Expected Results	FWA device shall automatically reload/restart the program upon critical fault detection, and System shall recover to normal operational state without manual intervention.

Test No.	**GR_TSTP_4.1.7**
Test Details	To verify that FWA Device shall comply with the eco-design and energy efficiency regulations of the market where it is meant to be used.
Test Instruments Required	1. Power analyzer / power meter (true RMS) 2. PC/Laptop for management access 3. Plug Adapter.
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA to a calibrated power analyzer. 2. Configure the FWA in normal operating mode. 3. Ensure stable power supply and normal network connectivity. 4. Measure FWA power consumption in idle, normal, and peak operation modes. 5. Verify low-power or sleep mode functionality (if supported). 6. Review vendor eco-design and energy efficiency compliance certificates (if any).
Test Limits	NA
Expected Results	FWA shall comply with applicable eco-design and energy efficiency regulations, and FWA shall comply with applicable eco-design and energy efficiency regulations.

Test No.	**GR_TSTP_4.1.8**
Test Details	To verify that FWA Device shall comply to the restrictions of use of hazardous materials and waste management regulations of the market where it is meant to be used
Test Instruments Required	1. Full Material Disclosure. 2. Supplier compliance declarations 3. Applicable national waste management documents.
Test Setup	TEST SETUP X
Test Procedure	1. Obtain compliance certificates for the FWA device. 2. Review Material Declaration for restricted substances. 3. Verify product labeling and disposal of information if required.
Test Limits	NA
Expected Results	FWA Device shall be compliant with RoHS/REACH and applicable hazardous material restrictions.

Test No.	**GR_TSTP_4.2.1**
Test Details	To verify that The System shall support following methods: a. RPC methods b. Data model structure c. Security d. Performance monitoring e. Data model parameters
Test Instruments Required	1. FWA. 2. PC/Laptop for management access 3. Management protocol client/tools 4. Performance monitoring tools.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Enable management interfaces supported by the FWA. 3. Verify supported RPC methods (e.g., Get/Set/Subscribe/Action calls). 4. Validate data model structure against vendor/standard documentation. 5. Verify authentication, authorization, and secure transport (e.g., HTTPS, TLS)
Test Limits	NA
Expected Results	FWA system shall support required RPC methods for management operations, and Standardized and/or vendor-defined data model structure shall be supported and accessible.

Test No.	**GR_TSTP_4.3.1**
Test Details	To verify that in case of loss of power, when the power is restored the FWA Device shall return automatically to the operational state, with all services (e.g., data, voice) restored according to the configuration of the device prior the power interruption.
Test Instruments Required	FWA CPE Regulated power supply unit Controlled power interruption device (e.g. power switch / programmable power source) Network connectivity (4G/5G as applicable) LAN/Wi-Fi client device for data validation Voice terminal / VoIP client (as applicable) Device management interface (e.g. Web UI / CLI)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to reach steady operational state. 2. Verify active network attachment and service registration. 3. Validate data service connectivity and voice service availability. 4. Induce controlled power interruption by disconnecting power supply. 5. Maintain power-off state for a defined interval (≥ 30 seconds). 6. Restore power supply to the FWA Device. 7. Allow device boot, initialization, and service re-registration. 8. Verify automatic restoration of services and configuration state by performing IP reachability (ping) validation for data services and validating voice service re-registration and successful outgoing and incoming call setup.
Test Limits	NA
Expected Results	The FWA Device shall automatically recover to a stable operational state after power restoration, with all configured services restored using the pre-interruption configuration.

Test No.	**GR_TSTP_4.3.2**
Test Details	To verify that in case of loss of radio signal(s), when the radio signal is restored the FWA Device shall return automatically to the operational state, with all services (e.g., data, voice) restored according to the configuration of the device prior the radio signal interruption.
Test Instruments Required	FWA CPE, Power Supply Unit, Live or simulated LTE/5G network, RF shielding box / RF attenuator or antenna disconnect mechanism, LAN client (PC/Laptop), Traffic generation or connectivity verification tool (e.g. ping, iPerf), Voice service setup
Test Setup	TEST SETUP X
Test Procedure	1.Power ON the FWA Device and allow it to reach normal operational state. 2.Verify that data (and voice, if supported) services are active. 3.Initiate loss of radio signal by applying RF shielding, attenuation, or disconnecting the antenna. 4. Maintain radio signal loss for a defined period. 5. Restore the radio signal. 6.Verify that the FWA Device automatically re-attaches to the network. 7.Verify that all previously active services (data and voice) are restored without manual intervention.
Test Limits	NA
Expected Results	The FWA Device shall automatically recover from radio signal loss and return to full operational state, with all services restored according to the configuration prior to the interruption, without requiring manual reboot or reconfiguration.

Test No.	**GR_TSTP_4.3.5**
Test Details	To verify that If voice service is supported, the FWA Device shall maintain uninterrupted voice (SIP protocol) registration for at least 72 consecutive hours, during which the Device is idle for Voice
Test Instruments Required	FWA CPE, Power supply unit, Stable LTE/5G network connection, IMS / SIP server (or operator voice network), LAN client (PC/Laptop), SIP registration monitoring or logging tool, Time measurement and logging tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to reach normal operational state. 2. Ensure that voice service is configured, and SIP/IMS registration is successfully established. 3. Do not initiate or receive any voice calls during the test period. 4. Monitor SIP registration status continuously while the device remains idle for voice service. 5. Maintain the test for 72 consecutive hours under normal operating conditions. 6. Log any SIP de-registration, re-registration, or registration failure events attributable to the FWA Device. 7. Verify that SIP registration remains continuously active throughout the observation period.
Test Limits	NA
Expected Results	The FWA Device shall maintain uninterrupted SIP registration for at least **72 consecutive hours** while idle for voice service, without device-initiated de-registration or registration failures.

Test No.	**GR_TSTP_4.3.6**
Test Details	To verify that in normal operating conditions, the FWA Device shall offer a service availability for voice service of at least 99.5%.
Test Instruments Required	FWA CPE, Power supply unit, Stable LTE/5G network connection, LAN client (PC/Laptop), Voice service setup (VoLTE/VoNR or VoIP client), Call monitoring or logging tool, Time measurement and logging tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to reach normal operational state. 2. Ensure that voice service is configured and registered (e.g. IMS registration successful). 3. Establish voice call capability through the FWA Device. 4. Monitor voice service availability continuously over a predefined observation period under normal operating conditions. 5. Record any voice service interruptions attributable to the FWA Device. 6. Exclude interruptions caused by external network issues from the measurement. 7. Calculate voice service availability based on total available time versus total test duration. 8. Verify that the measured voice service availability meets the required threshold.
Test Limits	NA
Expected Results	The FWA Device shall maintain voice service availability equal to or greater than **99.5%** under normal operating conditions, excluding network-related outages, and operate stably without device-related voice service interruptions beyond the allowed limit.

Test No.	**GR_TSTP_4.3.7**
Test Details	To verify that If voice service is supported, the FWA Device shall be able to support long-lasting voice calls (1.5 hours at least).
Test Instruments Required	FWA CPE, Power supply unit, Stable LTE/5G network connection, IMS / SIP server or operator voice network, Voice call endpoints (e.g. SIP clients, VoLTE/VoNR terminals), Call duration monitoring or logging tool, Time measurement and logging tool
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to reach normal operational state. 2. Ensure that voice service is configured and registered successfully. 3. Establish a voice call through the FWA Device with a remote endpoint. 4. Maintain the voice call continuously for a minimum duration of **1.5 hours**. 5. Monitor call status, media continuity, and signaling throughout the call. 6. Log any call drops, signaling failures, or media interruptions attributable to the FWA Device. 7. Verify that the call remains established for the entire test duration.
Test Limits	NA
Expected Results	The FWA Device shall successfully maintain a continuous voice call for at least **1.5 hours** without call drop, media interruption, or signaling failure attributable to the device.

Test No.	**GR_TSTP_4.4.1**
Test Details	To verify that FWA Device shall offer a Web UI to the end user for customizing the configuration of the FWA Device
Test Instruments Required	FWA CPE Power supply unit LAN/Wi-Fi client device (PC/Laptop/Tablet) Web browser Network connectivity Device access credentials (Admin/User)
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to reach a stable operational state. 2. Connect a client device to the FWA Device via LAN or Wi-Fi interface. 3. Access the Web UI using the management IP address/URL and verify secure session establishment (HTTP/HTTPS). 4. Navigate to network configuration sections (WAN/LAN/Wi-Fi/Services). 5. Modify core parameters (e.g. SSID, Wi-Fi security mode, LAN IP range, DHCP scope, firewall/NAT settings). 6. Modify service parameters (e.g. voice enable/disable, VLAN mapping, PDN/PDU association if applicable). 7. Save and apply the configuration changes via the Web UI. 8. Verify applied configurations through status pages and functional validation (connectivity/service behavior). 9. Can verify rejection of invalid configuration and retention of last valid operational configuration when invalid configurations are applied.
Test Limits	NA
Expected Results	The FWA Device shall provide a functional Web UI enabling end users to configure and manage device settings, with successful application and persistence of configuration changes.

Test No.	**GR_TSTP_4.4.2**
Test Details	To verify that Web UI should permit the configuration of all the service features relevant for the end user.
Test Instruments Required	FWA CPE Power supply unit LAN/Wi-Fi client device Web browser Network connectivity Device access credentials
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to reach full operational state. 2. Establish management access to the Web UI using valid credentials. 3. Enumerate all service domains exposed in the Web UI, including (Data/Voice/Wireless/Network/Security/ QoS/VLAN services (if supported)) 4. Verify that each service domain exposes configurable parameters relevant to the end user. 5. Configure data services (e.g. routing mode, DHCP behavior, NAT/firewall rules). 6. Configure voice services (e.g. enable/disable service, interface binding, service profiles). 7. Configure service separation features (e.g. VLAN tagging, service mapping, QoS/QCI/5QI if applicable). 8. Apply and commit all service-level configurations. 9. Validate service behavior via operational checks and status monitoring.
Test Limits	NA
Expected Results	The Web UI shall provide access to all end-user service configuration features, with successful application and persistence of service configurations.

Test No.	**GR_TSTP_4.4.3**
Test Details	To verify that Web UI shall be customizable based on procurer requirements.
Test Instruments Required	FWA CPE Power supply unit LAN/Wi-Fi client device Web browser Network connectivity Procurer UI Specification Document (Brand guidelines and feature list) and configuration access (profiles/templates/policies) Device access credentials.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA Device and allow it to reach stable operational state. 2. Connect a client device and access the Web UI using valid credentials. 3. Log in with valid credentials and verify that the dashboard layout aligns with the procurer's requested user interface design. 4. Navigate through the menus to confirm that all required configuration sections (WAN/LAN/Wi-Fi/Services) are visible and that restricted features are correctly masked/hidden per procurer requirements. 5. Perform and validate configuration changes using customized UI.
Test Limits	NA
Expected Results	The Web UI shall support procurer-specific customization with correct application of UI structure, feature exposure, and functional operation.

Test No.	**GR_TSTP_4.7.1**
Test Details	To verify the Availability The facility shall be available for the introduction of centralized Operation and Maintenance Control (OMC). b. The maintenance spares
Test Instruments Required	1. OMC workstation with access credentials. 2. Network connectivity. 3. PC/Laptop for local FWA access.
Test Setup	TEST SETUP X
Test Procedure	1. Integrate the FWA with the centralized OMC/NMS. 2. Ensure FWA is visible and manageable from OMC. 3. Verify FWA registration and visibility on centralized OMC. 4. Verify remote monitoring and management functions from OMC.
Test Limits	NA
Expected Results	FWA shall be manageable through centralized OMC, supporting high system availability, and Required maintenance spares shall be available to support timely repair and replacement.

Test No.	**GR_TSTP_4.7.2**
Test Details	To verify the Diagnostic Capability a. The diagnostic capability of the system shall be such as to minimize the human efforts required. The diagnostic programs which are normally resident in the on-line program shall be indicated. Details of the off-line diagnostic programs shall be given. The procedure for invoking such programs shall be described. The procedure for consulting fault dictionary for diagnostic programs shall be made available. b. The system shall provide facility for automatic restart under severe fault conditions. Where automatic restart fails to restore system sanity, facility shall be provided for manual restart of the system.
Test Instruments Required	1. FWA. 2. PC/Laptop for management and diagnostics access. 3. Vendor diagnostic and maintenance documentation. 4. Fault injection or fault simulation tools/method.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device and ensure normal operation. 2. Connect PC to FWA management/maintenance interface. 3. Verify documented procedures to invoke diagnostics. 4. Run built-in diagnostics and observe results. 5. Trigger or simulate common fault conditions. 6. Verify system fault detection and fault code generation. 7. Access fault dictionary and verify fault description and guidance.
Test Limits	NA
Expected Results	FWA system shall provide built-in diagnostic programs.

Test No.	GR_TSTP_4.8.1.1
Test Details	To verify that operation of the equipment shall be in the frequency band allotted.
Test Instruments Required	1. FWA. 2. Spectrum analyzer / RF scanner. 3. RF attenuators and RF cables (if cabled testing). 4. Test SIM / Network access. 5. PC/Laptop for FWA management access.
Test Setup	TEST SETUP X
Test Procedure	1. Connect FWA to test antenna or RF cable with suitable attenuation. 2. Power ON the FWA and ensure network registration. 3. Configure FWA to operate in allotted band(s) only (if configurable). 4. Monitor transmitted and received RF signals using a spectrum analyzer. 5. Record observed center frequencies and bandwidth.
Test Limits	NA
Expected Results	FWA equipment shall operate strictly within the allotted frequency of band(s).

Test No.	**GR_TSTP_4.8.1.2**
Test Details	To verify the Support of Multiple Equipment Vendors as per tender requirement
Test Instruments Required	1. SIMs/profiles from different operators or vendor networks 2. Multi-vendor base station or network simulator 3. PC/Laptop with FWA management interface access
Test Setup	TEST SETUP X
Test Procedure	1. Configure FWA with required SIMs/profiles. 2. Enable management access for monitoring and configuration. 3. Connect and register the FWA with Vendor **A** network equipment. 4. Verify data connectivity and basic services. 5. Connect and register the FWA with Vendor **B** network equipment. 6. Verify data connectivity and basic services. 7. Validate compliance with tender-specified interfaces and features.
Test Limits	NA
Expected Results	FWA shall demonstrate successful operation with multiple equipment vendors as per the tender requirements.

Test No.	**GR_TSTP_4.8.1.3**
Test Details	To verify that system shall support the possibility of using equipment and sub-systems of different vendors as per defined industry standards, wherever relevant.
Test Instruments Required	1. SIMs from different operators. 2. Network elements from different vendors (e.g., core network / base station simulator) 3. PC/Laptop with FWA management access.
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA to a multi-vendor test network environment. 2. Insert SIMs or configure profiles associated with different vendor networks. 3. Register the FWA on network equipment from Vendor A. 4. Verify data connectivity and basic services. 5. Register the FWA on network equipment from Vendor B. 6. Verify data connectivity and basic services. 7. Verify that FWA operates using standard interfaces and protocols (3GPP, IP, Ethernet, etc.).
Test Limits	NA
Expected Results	FWA shall interoperate successfully with equipment from different vendors using industry-standard interfaces.

Test No.	**GR_TSTP_4.8.2.1**
Test Details	To verify that system hardware shall be modular in design and shall permit growth in steps. The arrangement shall be such that failure/ deterioration of service shall not occur when implementing the growth.
Test Instruments Required	1. FWA. 2. PC/Laptop for management and monitoring 3. Test SIM / network connectivity 4. Performance test tool (iperf3).
Test Setup	TEST SETUP X
Test Procedure	1. Verify modular hardware architecture from vendor documentation. 2. Operate FWA in base configuration and establish live data traffic. 3. Measure baseline performance and service continuity. 4. Add supported expansion module or enable growth step (if applicable). 5. Monitor service during expansion activity. 6. Verify system recognition of new module/capacity.
Test Limits	NA
Expected Results	FWA hardware shall be modular and support stepwise growth/expansion.

Test No.	**GR_TSTP_4.8.2.2**
Test Details	To verify that Design precautions shall be taken to minimize the possibility of equipment damage arising from the insertion of an electronic package into the wrong connector or the removal of any package from any connector.
Test Instruments Required	1. Basic hand tools for service access (if applicable). 2. Visual inspection tools (flashlight, magnifier). 3. FWA hardware design and service documentation.
Test Setup	TEST SETUP X
Test Procedure	1. Power OFF the FWA and disconnect all power sources. 2. Open serviceable areas to access electronic packages or modules (if applicable). 3. Verify labeling and orientation markings on connectors and modules. 4. Attempt controlled incorrect insertion without force. 5. Verify connectors do not mate incorrectly. 6. Verify that removal of any module does not cause damage to connectors or adjacent components.
Test Limits	NA
Expected Results	FWA shall include effective mechanical and design precautions to prevent damage from wrong insertion or removal.

Test No.	**GR_TSTP_4.8.2.3**
Test Details	To verify that system hardware shall not pose any problem, due to changes in date and time caused by events such as changeover of leap year etc., in the normal functioning of the system.
Test Instruments Required	1. PC/Laptop with FWA management interface access 2. Time/date manipulation capability. 3. Stopwatch or system log access
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA to power and network. 2. Ensure FWA is operational and registered to the network. 3. Enable management access to view system time and logs. 4. Set FWA system date/time to just before a leap year event (e.g., Feb 28/29, 23:59:50). 5. Verify system date/time updates correctly. 6. Verify logs and scheduled functions to operate normally.
Test Limits	NA
Expected Results	FWA shall correctly handle leap year and date/time rollovers without functional impact.

Test No.	**GR_TSTP_4.8.3.1**
Test Details	To verify that Provision shall be made to prevent the loss/alteration of memory contents due to power failures, improper operating procedures and the procedure for restoring the system to its normal state, etc.
Test Instruments Required	1. Controlled DC power supply with power interruption capability 2. FWA management interface access 3. PC/Laptop for FWA configuration and monitoring 4. Power switch / relay for sudden power cut simulation
Test Setup	TEST SETUP X
Test Procedure	1. Connect the FWA to normal power supply and network. 2. Verify that FWA is operational and registered to the network. 3. Enable remote/local management for access to the FWA. 4. Perform an abrupt power interruption to the FWA. 5. Restore power and allow the FWA to boot normally. 6. Verify that all previously saved configurations are retained. 7. Perform an improper shutdown (power OFF without graceful logout). 8. Repeat power ON and verify memory integrity.
Test Limits	NA
Expected Results	FWA shall retain all saved configuration and memory content after power failures and improper shutdowns.

Test No.	**GR_TSTP_4.8.4.1**
Test Details	To verify the communication facilities provided for exchange of information between the elements of FWA device and the maintenance and operating personnel shall include facilities for a system test, control and alarm indication at OMC.
Test Instruments Required	1. OMC workstation with access credentials. 2. Network connectivity between FWA and OMC. 3. PC/Laptop for local FWA management access. 4. Alarm simulation or fault injection capability.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA and verify normal operation. 2. Log in to the OMC and verify FWA visibility. 3. Verify that FWA status is visible on the OMC dashboard. 4. Perform a remote system test command from the OMC to the FWA. 5. Verify remote control functions (e.g., reboot, configuration read/write). 6. Simulate a fault condition on the FWA (e.g., disconnect WAN, power cycle radio module). 7. Verify alarm generation and display at the OMC.
Test Limits	NA
Expected Results	FWA shall support full communication with OMC for system test, control, and alarm indication.

Test No.	**GR_TSTP_4.8.4.2**
Test Details	To verify that Input / output terminals shall be capable of transmitting/ receiving characters of a subset of the ITU-T T.50 alphabet. The printing/display device shall print/display different graphic symbols for the digit zero and the capital letter O. The input/output terminal shall have the English Keyboard.
Test Instruments Required	1. FWA. 2. PC/Laptop with English (US/UK) keyboard layout. 3. Web browser / CLI terminal application (e.g., SSH, serial console if available). 4. Test character string file including ITU-T T.50 subset characters.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA device. 2. Connect PC to FWA management interface (Web UI or CLI). 3. Access FWA management interface (Web UI or CLI). 4. Input test strings containing ITU-T T.50 subset characters. 5. Enter strings containing digit “0” and capital letter “O”. 6. Transmit and display entered characters through FWA interface. 7. Verify displayed/printed output on management interface or logs.
Test Limits	NA
Expected Results	FWA I/O interfaces shall correctly transmit and display supported ITU-T T.50 characters.

Test No.	**GR_TSTP_4.8.4.3**
Test Details	To verify that Adequate number of man-machine interfaces shall be available.
Test Instruments Required	1. PC/Laptop, tablet, or smartphone for web UI/app access. 2. Ethernet cable. 3. FWA user manual and interface specification.
Test Setup	TEST SETUP X
Test Procedure	1. Power ON the FWA and connect it to the network. 2. Connect a PC or mobile device to the FWA via Ethernet and/or Wi-Fi. 3. Access to the FWA management interface (web UI, app, or CLI if available). 4. Verify availability of physical interfaces (LED indicators, buttons, ports). 5. Verify availability of logical interfaces (web GUI, mobile app, CLI, TR-069/remote management). 6. Verify access to configuration, monitoring, and diagnostics. 7. Verify the ability to perform basic operations (status view, reboot, configuration, logs).
Test Limits	NA
Expected Results	FWA shall provide an adequate number of man–machine interfaces for effective user and operator interaction.

Test No.	**GR_TSTP_4.8.4.4**
Test Details	To verify that If provision is made for monitoring from a remote terminal, it shall be ensured that the data links conform to the ITU-T Recommendation Q.513. Care shall be taken that the reliability of the data links towards remote terminal does not, in any way, affect the reliability of the device. Special provision shall also be made for storage of failure event even when the system is unable to transmit an output message
Test Instruments Required	1. FWA. 2. Remote monitoring/OMC system or NMS (if applicable). 3. PC/Laptop for FWA management access.
Test Setup	TEST SETUP X
Test Procedure	1. Configure FWA for remote monitoring/management to OMC/NMS. 2. Ensure logging and event storage features are enabled. 3. Verify configuration of remote monitoring interface and protocol. 4. Confirm data link characteristics as per ITU-T Q.513 (as applicable to IP-based systems). 5. Monitor normal transmission of status and alarms to remote terminal. 6. Simulate remote link failure (disconnect WAN or block management traffic).
Test Limits	NA
Expected Results	FWA remote monitoring link shall operate reliably without affecting device operation.

Test No.	**GR_TSTP_4.8.4.5**
Test Details	To verify the suitable alarm and display system at OMC shall be provided for a continuous indication of the system' s status.
Test Instruments Required	1. OMC workstation with access credentials 2. Test SIMs / test UEs / FWAs. 3. System log access
Test Setup	TEST SETUP X
Test Procedure	1. Power ON all network elements and ensure normal operation. 2. Log in to the OMC and verify dashboard accessibility. 3. Verify alarm generation and visual indication on the OMC. 4. Verify visual alarm and proper alarm severity classification.
Test Limits	NA
Expected Results	OMC shall continuously display accurate real-time system status for all network elements.

Test No.	**GR_TSTP_4.8.5.1**
Test Details	To verify that It shall be indicated whether printed board connectors are of edge-type or plug-and-socket type. They shall not be easily damaged during replacements and removals. The contact particulars as well as life test performance on contact resistance for each type of connector shall be supplied.
Test Instruments Required	1. Visual inspection tools (flashlight, magnifier) 2. FWA hardware design documentation and BOM 3. Basic hand tools for service access
Test Setup	TEST SETUP X
Test Procedure	1. Power OFF the FWA and disconnect from all power sources. 2. Open serviceable compartments (if applicable). 3. Visually inspect PCB connectors and identify type (edge connector or plug-and-socket). 4. Perform controlled insertion and removal cycles (limited number). 5. Review connector datasheets for contact specifications and life-cycle ratings.
Test Limits	NA
Expected Results	All PCB connectors shall be clearly identified and shall withstand replacement/removal without damage.

Test No.	**GR_TSTP_4.8.5.2**
Test Details	To verify that All components and material used in the equipment shall be non-inflammable or in absence of it, self-extinguishable. They shall be fully tropicalized.
Test Instruments Required	1. Visual inspection tools (flashlight, magnifier). 2. Multimeter (for basic safety checks). 3. Environmental chamber (for humidity/temperature, if applicable).
Test Setup	TEST SETUP X
Test Procedure	1. Ensure equipment is powered ON for inspection. 2. Perform visual inspection for the presence of flame-retardant markings on components. 3. Subject to equipment for high-humidity and elevated-temperature conditions as per tropicalization requirements. After exposure, inspect for corrosion, moisture ingress, or material degradation.
Test Limits	NA
Expected Results	All materials shall be non-inflammable or self-extinguishing and compliant with flame-retardant standards.

Test No.	**GR_TSTP_4.8.5.3**
Test Details	To verify that method used for connection of permanent wiring outside the printed cards shall be indicated.
Test Instruments Required	1. Visual inspection tools (flashlight, magnifier). 2. FWA installation and service manuals. 3. Labeling and marking checklist.
Test Setup	TEST SETUP X
Test Procedure	1. Install the FWA in normal operating configuration. 2. Ensure access to all permanent wiring connection points (power input, grounding, external antenna, Ethernet, etc.). 3. Verify labeling for power, grounding, and signal interfaces. 4. Review installation manual for permanent wiring instructions. 5. Cross-check physical markings with documentation.
Test Limits	NA
Expected Results	FWA shall clearly indicate the method for connecting all permanent external wiring.

Test No.	**GR_TSTP_4.8.5.4**
Test Details	To verify that buses, if any, shall be suitably protected against electrical and magnetic interference from neighbouring systems (like electromechanical systems, fluorescent tubes, motors, etc.).
Test Instruments Required	1. EMI/EMC test equipment (EMI receiver, spectrum analyzer, near-field probes). 2. Environmental EMI source simulators (motors, fluorescent lamps, switching power supplies). 3. Shielded and unshielded cables (for disturbance simulation). 4. PC/Laptop for monitoring FWA operations and logs.
Test Setup	TEST SETUP X
Test Procedure	1. Place the FWA in a controlled EMI/EMC test environment or lab. 2. Power ON the FWA and establish normal network connectivity. 3. Operate the FWA under normal conditions. 4. Activate nearby EMI sources (motors, fluorescent lamps, switching supplies). 5. Monitor FWA for performance degradation, errors, or resets. 6. Repeat for different EMI source positions and distances.
Test Limits	NA
Expected Results	FWA internal buses shall remain immune to electrical and magnetic interference from neighboring systems.

Test No.	**GR_TSTP_4.8.5.5**
Test Details	To verify that different plug-in cards shall have suitable mechanical safeguards to prevent damage due to accidental interchange of cards.
Test Instruments Required	1. Basic hand tools for opening serviceable compartments (if applicable) 2. Visual inspection tools (flashlight, magnifier) 3. FWA hardware service manual.
Test Setup	TEST SETUP X
Test Procedure	1. Power OFF the FWA and disconnect from all power sources. 2. Open serviceable areas that allow access to plug-in modules (if applicable). 3. Verify that modules cannot be inserted into incorrect slots. 4. Attempt controlled incorrect orientation or slot insertion (without applying force). 5. Verify labeling and orientation markings. 6. Reinstall modules correctly and verify normal operation.
Test Limits	NA
Expected Results	FWA plug-in modules shall have suitable mechanical safeguards to prevent accidental interchange or incorrect insertion.

Test No.	**GR_TSTP_4.8.5.6**
Test Details	To verify that requirement at the external interface against induced voltages and currents due to lightning, high power system, etc. shall be indicated.
Test Instruments Required	1. Visual inspection tools (flashlight, magnifier). 2. FWA hardware installation manual and safety documentation. 3. PC/Laptop for management access (optional).
Test Setup	TEST SETUP X
Test Procedure	1. Install the FWA in normal operating configuration. 2. Ensure access to all external interfaces (power, Ethernet, RF, grounding, etc.). 3. Inspect all external interfaces for lightning/surge protection indications. 4. Review FWA installation manual for external interface protection requirements. 5. Verify that protection devices (e.g., surge protectors, isolation) are documented and indicated.
Test Limits	NA
Expected Results	FWA external interfaces shall be clearly labeled and documented for protection against induced voltages and currents.

Test No.	**GR_TSTP_4.8.5.7**
Test Details	To verify that system shall provide for human isolation and protection from accidental high voltage power contact.
Test Instruments Required	1. Insulation resistance tester 2. Digital multimeter (DMM) 3. High-voltage probe (if applicable) 4. Personal Protective Equipment (PPE) – insulated gloves, safety shoes 5. Warning labels and lockout/tagout ki
Test Setup	TEST SETUP X
Test Procedure	1. Connect power source as per system installation guidelines. 2. Ensure system is powered ON and operating under normal conditions. 3. Ensure all protective covers, shields, and enclosures are properly installed.
Test Limits	NA
Expected Results	Insulation, grounding, and protective barriers shall meet specified safety limits and prevent accidental human contact.

Test No.	**GR_TSTP_4.9.1**
Test Details	To verify that software shall be written in a High-Level Language. The software shall be modular and structured.
Test Instruments Required	1. FWA software source code access (as permitted) or software architecture documentation 2. Source code access. 3. Version control system access (if applicable).
Test Setup	TEST SETUP X
Test Procedure	1. Obtain software to build and release information for the FWA firmware. 2. Review FWA software architecture documents to confirm the use of high-level languages (e.g., C, C++, Java, Python, etc.). 3. Verify structured programming practices that are followed (clear interfaces, layered design). 4. Confirm that no critical functionality is implemented solely in unstructured or low-level assembly (except where justified).
Test Limits	NA
Expected Results	FWA software shall be confirmed to be developed in high-level languages with a clearly modular and structured architecture.

Test No.	**GR_TSTP_4.9.2**
Test Details	To verify that The software shall include the following characteristics: a.The design of the software shall be such that the system is easy to handle both during installation and normal operations as well as during extensions. b.The functional modularity of the software shall permit introduction of changes wherever necessary with least impact on other modules. c.It shall be open-ended to allow addition of new features. d.Adequate flexibility shall be available to easily adopt changes in service features & facilities and technological evolution in hardware. e. The design shall be such that propagation of software faults is contained. f. Test programs shall include fault tracing for detection and localization of system faults.
Test Instruments Required	1. FWA firmware/software package 2. PC/Laptop with FWA management and diagnostic tools 3. Test and diagnostic utilities/log access.
Test Setup	TEST SETUP X
Test Procedure	1. Load the FWA software version under test. 2. Ensure FWA is operational for functional verification. 3. Review software architecture for functional modularity. 4. Introduce a controlled configuration or feature change and verify minimal impact on other modules. 5. Verify support for adding/enabling new features via software upgrade or configuration. 6. Verify flexibility to support service feature changes and hardware evolution (via firmware update or modular drivers).
Test Limits	NA
Expected Results	FWA software shall demonstrate ease of use, modularity, extensibility, and flexibility as per requirements.

Test No.	**GR_TSTP_4.9.3.1**
Test Details	To verify that all software updates, for a period as specified, shall be supplied on a continuing basis. These updates shall include new features and services, and other maintenance updates. The design shall be such that propagation of software faults is contained. f. Test programs shall include fault tracing for detection and localization of system faults.
Test Instruments Required	1. Access to vendor software update server or update packages 2. Access to vendor software update server or update packages 3. Network connectivity for update download.
Test Setup	TEST SETUP X
Test Procedure	1. Configure the FWA with management access and network connectivity. 2. Ensure current software version is installed and operational. 3. Verify availability of multiple software versions and release history. 4. Perform a software update/upgrade on the FWA. 5. Verify new features, fixes, or maintenance updates are applied successfully. 6. Verify that existing configurations are retained after update. 7. Simulate or observe a software fault and verify fault containment.
Test Limits	NA
Expected Results	FWA shall successfully receive and apply for continuing software updates including new features and maintenance releases.

Test No.	**GR_TSTP_4.9.3.2**
Test Details	To verify that all Integration of software updates without posing any problem to the existing functionality shall be possible.
Test Instruments Required	1. Access to vendor software update packages. 2. PC/Laptop with FWA management interface access. 3. Network connectivity for update process.
Test Setup	TEST SETUP X
Test Procedure	1. Configure the FWA with a stable baseline software version. 2. Ensure access to update mechanism. 3. Perform software update/upgrade on the FWA. 4. Verify software version is updated successfully. 5. Execute full regression tests on existing features and services. 6. Verify user configuration and settings are retained.
Test Limits	NA
Expected Results	FWA shall integrate software updates successfully without impacting existing functionality.

J. Summary of test results

GR/IR No.____________________________

TSTP No.______________________________

Equipment name & Model No.____________

Clause No.	***Compliance*** *(Complied /Not Complied / Submitted/Not Submitted / Not Applicable)*	*Remarks / Test Report Annexure No.*

[Add as per requirement]

Date:

Place: *Signature & Name of TEC testing Officer /*
** Signature of Applicant / Authorized Signatory*

** Section J as given above is also to be submitted by the Applicant/ Authorised signatory as part of in-house test results along with Form-A. The Authorised signatory shall be the same as the one for Form 'A'.*