ilac-MRA

ACCREDITED
CERT#4344.01

TEST REPORT

Applicant:	DrayTek
Address:	No. 26, Fu Shing Road, Hukou County,Hsin-Chu Industrial Park, Hsinchu, Taiwan
EUT Name:	Dual-WAN Security Router
Model Name:	Vigor2927LVax-5G
Brand Name:	DrayTek
Test Standard:	EN 18031-1:2024
Sample Arrival Date:	Apr. 9, 2025
Test Date:	May 1, 2025 - Jun. 20, 2025
Date of Issue:	Jul. 10, 2025

ISSUED BY:

Shenzhen BALUN Technology Co., Ltd.

CERTIFICATION • CONSULTING • SOLUTION • SERVICES
BALUN

Tested by: Yang Shengzhao

Yang Shengzhao

Checked by: Sunny Zou

Sunny Zou

Approved by: Jason Yang (Supervisor)

Jason Yang

Revision History

Version	Issue Date	Revisions Content
Rev. 01	Jun. 27, 2025	Initial Issue
Rev. 02	Jul. 10, 2025	Updated Software Version

TABLE OF CONTENTS

1 GENERAL INFORMATION

1.1 Identification of the Testing Laboratory

Company Name	Shenzhen BALUN Technology Co., Ltd.
Address	Block B, 1/F, Baisha Science and Technology Park, Shahe Xi Road, Nanshan District, Shenzhen City, Guangdong Province, P. R. China
Phone Number	+86 755 6685 0100

1.2 Identification of the Responsible Testing Location

Test Location	Shenzhen BALUN Technology Co., Ltd.
Location	□Block B, 1/F, Baisha Science and Technology Park, Shahe Xi Road, Nanshan District, Shenzhen City, Guangdong Province, P. R. China
	☑1/F, Building B, Ganghongji High-tech Intelligent Industrial Park, No. 1008, Songbai Road, Yangguang Community, Xili Sub-district, Nanshan District, Shenzhen, Guangdong Province, P. R. China

2 PRODUCT INFORMATION

2.1 Applicant Information

Applicant	DrayTek
Address	No. 26, Fu Shing Road, Hukou County,Hsin-Chu Industrial Park, Hsinchu, Taiwan

2.2 Manufacturer Information

Manufacturer	DrayTek
Address	No. 26, Fu Shing Road, Hukou County,Hsin-Chu Industrial Park, Hsinchu, Taiwan

2.3 General Description for Equipment under Test (EUT)

EUT Name	Dual-WAN Security Router
Model Name Under Test	Vigor2927LVax-5G
Series Model Name	Vigor2927Lax-5G
Description of Model Name Differentiation	Hardware variations do not alter cybersecurity performance across models. Identical security protocols ensure consistent protection (this information provided by the applicant).
Hardware Version	V2865_V6F
Software Version	4.5.1
EUT SN/IMEI	EUT1 IMEI:865991060044439

2.4 Technical Information

Network and Wireless Connectivity	5G-NR: n1,3,7,8,20,28,38,40,77.78 WLAN: 2400MHz - 2483MHz, max. TX power: 19.86dBm 5150MHz - 5350MHz, max. TX power: 22.79dBm 5470MHz - 5725MHz, max. TX power: 29.78dBm
Applicable Scope	☑RED 3.3.d ☐RED 3.3.e ☐RED 3.3.f

3 SUMMARY OF TEST RESULTS

3.1 Test Standards

No.	Identity	Document Title
1	EN 18031-1:2024	Common security requirements for radio equipment - Part 1: Internet connected radio equipment

3.2 Verdict

EN 18031-1:2024		
Clause	Test Items	Verdict
6.1.1	[ACM-1] Applicability of access control mechanisms	PASS
6.1.2	[ACM-2] Appropriate access control mechanisms	PASS
6.2.1	[AUM-1] Applicability of authentication mechanisms	PASS
6.2.2	[AUM-2] Appropriate authentication mechanisms	PASS
6.2.3	[AUM-3] Authenticator validation	PASS
6.2.4	[AUM-4] Changing authenticators	PASS
6.2.5	[AUM-5] Password strength	PASS
6.2.6	[AUM-6] Brute force protection	PASS
6.3.1	[SUM-1] Applicability of update mechanisms	PASS
6.3.2	[SUM-2] Secure updates	PASS
6.3.3	[SUM-3] Automated updates	PASS
6.4.1	[SSM-1] Applicability of secure storage mechanisms	PASS
6.4.2	[SSM-2] Appropriate integrity protection for secure storage mechanisms	PASS
6.4.3	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	PASS
6.5.1	[SCM-1] Applicability of secure communication mechanisms	PASS
6.5.2	[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	PASS
6.5.3	[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	PASS

EN 18031-1:2024		
Clause	Test Items	Verdict
6.5.4	[SCM-4] Appropriate replay protection for secure communication mechanisms	PASS
6.6.1	[RLM-1] Applicability and appropriateness of resilience mechanisms	PASS
6.7.1	[NMM-1] Applicability and appropriateness of network monitoring mechanisms	PASS
6.8.1	[TCM-1] Applicability of and appropriate traffic control mechanisms	PASS
6.9.1	[CCK-1] Appropriate CCKs	PASS
6.9.2	[CCK-2] CCK generation mechanisms	PASS
6.9.3	[CCK-3] Preventing static default values for preinstalled CCKs	N/A
6.10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	PASS
6.10.2	[GEC-2] Limit exposure of services via related network interfaces	PASS
6.10.3	[GEC-3] Configuration of optional services and the related exposed network interfaces	PASS
6.10.4	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces	PASS
6.10.5	[GEC-5] No unnecessary external interfaces	PASS
6.10.6	[GEC-6] Input validation	PASS
6.11.1	[CRY-1] Best practice cryptography	PASS

Possible test case verdicts:

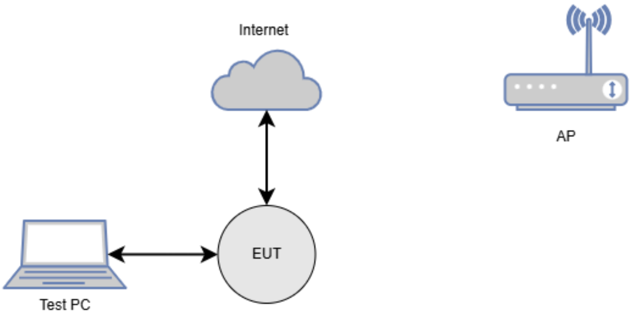
- test case does not apply to the test object	: N/A
- test case does not been tested	: --
- test object does meet the requirement	: PASS
- test object does not meet the requirement	: FAIL

4 GENERAL TEST CONFIGURATIONS

4.1 Test Environment

Temperature (℃)	15-35 ℃
Relative Humidity (%)	25 -70 %
Atmospheric Pressure (kPa)	86-106 kPa

4.1.1 Test Environment Setup



4.2 Hardware Resource

Equipment No.	Description	Model	Operating System
Equipment No.	Description	Model	Operating System
BZ-SIS-L008	Computer	ThinkBook 14 G5+IRH	Microsoft Windows 11
BZ-SIS-L041	Facedancer21	/	/

4.3 Test Tool

Equipment No.	Description	Version
BZ-SIS-L028	Wireshark	V4.4.1
BZ-SIS-L039	Nmap	V7.9.1
BZ-SIS-L036	cve-bin-tool	3.4rc0
BZ-SIS-L024	Burp Suite	V2024.4.5
BZ-SIS-L042	umap2	V2.0.1
BZ-SIS-L047	Binwalk	V2.4.3
BZ-SIS-L039	keytool	Jdk-8u131

ANNEX A TEST RESULT

EN 18031-1:2024			
Clause	Mechanism	Requirement	Verdict
6.1	[ACM] Access control mechanism		
6.1.1	[ACM-1] Applicability of access control mechanisms	The equipment shall use access control mechanisms to manage entities' access to security assets and network assets.	PASS
	Asset-GatewayPwd, Asset-Publickey of https certificate, Asset-PrivacyKey of https certificate, Asset-ECDSAPublickey, Asset-VPNcertificate, Asset-RouterSettings, Asset-Network Settings, Asset-CellularData , Asset-SMS, Asset-VOIP, Asset-VPN, Asset-Bandwidth Management, Asset-TR069, Asset-Bonjour, Asset-RADIUS, Asset-Hotspot Web Portal, Asset-MyVigor Services, Asset-Diagnostics, Asset-TACACS+, Asset-Firewall, Asset-User Management: The access control mechanism based on RBAC ensures that only authorized entities can access the corresponding permission assets.		
6.1.2	[ACM-2] Appropriate access control mechanisms	Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and network assets.	PASS
	Access control mechanism based on RBAC and only authenticated users can access assets corresponding to their authorized permissions.		
6.2	[AUM] Authentication mechanism		
6.2.1	[AUM-1] Applicability of authentication mechanisms		
6.2.1.1	[AUM-1-1] Requirement network interface	Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via network interfaces that allow to: read confidential network function configuration or confidential security parameters or modify sensitive network function configuration or sensitive security parameters or use network functions or security functions.	PASS
	Asset-GatewayPwd, Asset-Publickey of https certificate, Asset-PrivacyKey of https certificate, Asset-HTTP digest, Asset-ECDSAPublickey, Asset-VPNcertificate, Asset-RouterSettings, Asset-Network Settings, Asset-CellularData , Asset-SMS, Asset-VOIP, Asset-VPN, Asset-Bandwidth Management, Asset-TR069, Asset-Bonjour, Asset-RADIUS, Asset-Hotspot Web Portal, Asset-MyVigor Services, Asset-Diagnostics, Asset-TACACS+, Asset-Firewall, Asset-User Management: Only SSH authenticated entities can access assets corresponding to their authorized permissions.		

EN 18031-1:2024			
6.2.1.2	[AUM-1-2] Requirement user interface	Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to: read confidential network function configuration or confidential security parameters or modify sensitive network function configuration or sensitive security parameters or use network functions or security functions.	PASS
	Asset-GatewayPwd, Asset-Publickey of https certificate, Asset-PrivacyKey of https certificate, Asset-HTTP digest, Asset-ECDSAPublickey, Asset-VPNcertificate, Asset-RouterSettings, Asset-Network Settings, Asset-CellularData , Asset-SMS, Asset-VOIP, Asset-VPN, Asset-Bandwidth Management, Asset-TR069, Asset-Bonjour, Asset-RADIUS, Asset-Hotspot Web Portal, Asset-MyVigor Services, Asset-Diagnostics, Asset-TACACS+, Asset-Firewall, Asset-User Management: Only GateWay authenticated users can access assets corresponding to their authorized permissions.		
6.2.2	[AUM-2] Appropriate authentication mechanisms	Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity’s claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication).	PASS
	1.Gateway authentication: The gateway authentication mechanism used password for identity authentication, which is a knowledge-based authentication factor. Users need to enter the correct password to pass the authentication. 2.SSH authentication: The SSH authentication mechanism used password for identity authentication, which is a knowledge-based authentication factor. Users need to enter the correct username and password to pass the authentication.		
6.2.3	[AUM-3] Authenticator validation	Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use.	PASS

EN 18031-1:2024			
	1.Gateway authentication: The gateway authentication mechanism verifies the account and password provided by the user to ensure that only authorized users can access the gateway functions in the current operating environment. 2.SSH authentication: The SSH authentication mechanism verifies the account and password provided by the user to ensure that only authorized users can access assets the in the current operating environment.		
6.2.4	[AUM-4] Changing authenticators	Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change.	PASS
	1.Gateway authentication: The password for the authenticator can be changed in the settings page and prior to modification, the old authenticator must be verified. Once modified, the new authenticator enables access to the assets, while the old authenticator is permanently invalidated for assets access. 2.SSH authentication: Changes in the gateway settings because it used same password with gateway.		
6.2.5	[AUM-5] Password strength		
6.2.5.1	[AUM-5-1] Requirement for factory default passwords	If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall: -- be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or -- be defined by an authorized entity within a network where access is limited to authorised entities; or -- be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.	PASS
	1.Gateway authentication: The EUT used factory default password but the user must be changed when users use the device for the first time. 2.SSH authentication: The EUT used factory default password but the user must be changed when users use the device for the first time.		

EN 18031-1:2024			
6.2.5.2	[AUM-5-2] Requirement for non-factory default passwords	If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall: -- be unique per equipment; and -- follow best practice concerning strength; or -- be enforced to be changed by the user before or on first use.	N/A
	The device has no non-factory default password.		
6.2.6	[AUM-6] Brute force protection	Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks.	PASS
	1.Gateway authentication: Based on [IC. AUM - 6. TimeDelay],The device will be locked for five minutes after entering the wrong account and password five times and user can custom Penalty period. 2.SSH authentication: Based on [IC. AUM - 6. TimeDelay],The device will be locked for five minutes after entering the wrong account and password six times and user can custom Penalty period.		
6.3	[SUM] Secure update mechanism		
6.3.1	[SUM-1] Applicability of update mechanisms	The equipment shall provide at least one update mechanism for updating software, including firmware,affecting security assets and/or network assets.	PASS
	Software: SUM-1:The device has an update mechanism to update, the update mechanism is OTA. SUM-2:EUT can be updated via TR069.		
6.3.2	[SUM-2] Secure updates	Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.	PASS
	EUT`s SUM base on [IC.SUM-2.AuthIntVal.Generic] and the firmware is transmitted over HTTPS, encrypted with TLS, and a signature verification is conducted after the transmission is completed to ensure the authenticity and confidentiality of the entire process and the signature algorithm is ECDSA with sha256 nid secp256k1.		

EN 18031-1:2024			
6.3.3	[SUM-3] Automated updates	Each update mechanism that is required per SUM-1 shall be capable of updating the software: —without human intervention at the equipment; or —via scheduling the installation of an update under human approval; or —via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment.	PASS
	The EUT will automatically check for updates and install them if a new update package is available.		
6.4	[SSM] Secure storage mechanism		
6.4.1	[SSM-1] Applicability of secure storage mechanisms	The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, except for persistently stored security assets or network assets where: -- the physical or logical measures in the target environment ensures the security asset or network asset stored on the equipment accessibility is limited to authorized entities.	PASS
	Asset-Publickey of https certificate, Asset-HTTPS digest, Asset-ECDSAPublickey, Asset-CellularData: EUT implements the secure storage mechanism and secure storage mechanism based on RBAC. Asset-GatewayPwd, Asset-PrivacyKey of https certificate, Asset-HTTPS digest, Asset-VPNcertificate, Asset-RouterSettings, Asset-Network Settings: EUT implements the secure storage mechanism and secure storage based on RBAC with encryption.		
6.4.2	[SSM-2] Appropriate integrity protection for secure storage mechanisms	Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and network assets it stores persistently.	PASS

EN 18031-1:2024			
	Asset-Publickey of https certificate, Asset-HTTPS digest, Asset-ECDSAPublickey, Asset-CellularData: The access control mechanism can reject unauthorized modifications. Asset-GatewayPwd, Asset-PrivacyKey of https certificate, Asset-HTTPS digest, Asset-VPNcertificate, Asset-RouterSettings, Asset-Network Settings: The access control mechanism can reject unauthorized modifications.		
6.4.3	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently.	PASS
	Asset-Publickey of https certificate, Asset-HTTPS digest, Asset-ECDSAPublickey, Asset-CellularData: The access control mechanism can deny unauthorized reading. Asset-GatewayPwd, Asset-PrivacyKey of https certificate, Asset-HTTPS digest, Asset-VPNcertificate, Asset-RouterSettings, Asset-Network Settings: Encryption is carried out using the AES algorithm to ensure confidentiality.		
6.5	[SCM] Secure communication mechanism		
6.5.1	[SCM-1] Applicability of secure communication mechanisms	The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces.	PASS
	Intf-Wi-Fi, Intf-5GNR, Intf-WAN, Intf-LAN: Asset-Publickey of https certificate, Asset-HTTPS digest, Asset-ECDSAPublickey, Asset-CellularData , Asset-GatewayPwd, Asset-PrivacyKey of https certificate, Asset-HTTPS digest, Asset-VPNcertificate, Asset-RouterSettings, Asset-Network Settings: Ensures secure communication through TLS1.2 or 1.3.		
6.5.2	[SCM-2] Appropriate integrity and authenticity protection for secure communication Mechanisms	Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the integrity and authenticity of the security assets and network assets communicated.	PASS

EN 18031-1:2024			
	TLS 1.2 or 1.3 is used to ensure the integrity and authenticity of data transmission.		
6.5.3	[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed.	PASS
	TLS 1.2 or 1.3 is used to ensure the confidentiality of data transmission.		
6.5.4	[SCM-4] Appropriate replay protection for secure communication mechanisms	Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the network assets communicated against replay attacks.	PASS
	Intf-Wi-Fi, Intf-5GNR, Intf-WAN, Intf-LAN TLS is used as a secure communication mechanism to ensure protection against replay attacks.		
6.6	[RLM] Resilience mechanism		
6.6.1	[RLM-1] Applicability and appropriateness of resilience mechanisms	The equipment shall use resilience mechanisms to mitigate the effects of Denial of Service (DoS) Attacks on the network interfaces and return to a defined state after the attack	PASS
	The RLM mechanism can defend against common DOS attacks such as SYN flood attacks, UDP flood attacks,ICMP flood , TCP port scans, and UDP port scans.		
6.7	[NMM] Network monitoring mechanism		
6.7.1	[NMM-1] Applicability and appropriateness of network monitoring mechanisms	If the equipment is a network equipment, the equipment shall provide network monitoring mechanism(s) to detect for indicators of DoS attacks in the network traffic between networks which it processes.	PASS
	The NMM of EUT [IC.NMM-1.Generic] can not only reflect the overall load and health status of the network by collecting basic indicators such as interface traffic (TX/RX) and device operating time, but also conduct security filtering by collecting packets of source/destination IP to prevent network layer attacks.		
6.8	[TCM] Traffic control mechanism		

EN 18031-1:2024			
6.8.1	[TCM-1] Applicability of and appropriate traffic control mechanisms	If the equipment is a network equipment, the equipment shall provide network traffic control mechanism(s).	PASS
	EUT adopts the TCM mechanism. By setting firewall rules, it controls the transmission of traffic data to handle abnormal patterns, malicious traffic, or data packets with specific source/destination addresses. These rules can specify the discarding, blocking or other operations on the identified data packets.		
6.9	[CCK] Confidential cryptographic keys		
6.9.1	[CCK-1] Appropriate CCKs	Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits.	PASS
	CCK-1 used RSA2048 provides support for a minimum security strength of 112 bits. CCK-2 used AES-128 or 256 support for a minimum security strength of 112 bits. CCK-3 used AES-128 or 256 provides support for a minimum security strength of 112 bits.		
6.9.2	[CCK-2] CCK generation mechanisms	The generation of confidential cryptographic keys shall adhere to best practice cryptography.	PASS
	The AESKeyExpansion technology is used to generate the round keys required for multiple rounds of encryption from the original key in accordance with NIST.FIPS.197.		
6.9.3	[CCK-3] Preventing static default values for preinstalled CCKs	Preinstalled confidential cryptographic keys shall be practically unique per equipment.	N/A
	CCK-RSAPrivacyKey of https certificate-RSA 2048: The certificate is the same certificate compiled and generated by the manufacturer when it leaves the factory. This is an expected function. AES Original key: This CCK is generated by the manufacturer at the factory to extend and derive the key for encrypting assets. This is the expected function of the EUT, so this CCK is not unique.		
6.10	[GEC] General equipment capabilities		
6.10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and network assets	PASS
	The device has no publicly known vulnerabilities.		

EN 18031-1:2024			
6.10.2	[GEC-2] Limit exposure of services via related network interfaces	In factory default state the equipment shall only expose -- network interfaces; and -- services via network interfaces affecting security assets or network assets which are necessary for equipment setup or for basic operation of the equipment.	PASS
	Intf-Wi-Fi, Intf-5GNR, Intf-WAN, Intf-LAN: The EUT is a network device, and these interfaces are necessary for the basic network functions and operations of the EUT: Wi-Fi and 5GNR provide wireless connectivity, the WAN interface provides Internet gateway functionality, and the LAN interface provides local network connectivity, which are all necessary components of the EUT's core functionality.		
6.10.3	[GEC-3] Configuration of optional services and the related exposed network interfaces	Optional network interfaces or optional services exposed via network interfaces affecting security assets or network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service.	PASS
	Authorized users are permitted to enable/disable the following interfaces: Intf-Wi-Fi, Intf-5GNR, Intf-WAN, Intf-LAN		
6.10.4	[GEC-4] Documentation of exposed network interfaces and exposed services via network Interfaces	The equipment’s user documentation shall contain a description of -- all exposed network interfaces; and -- all services exposed via network interfaces, which are delivered as part of the factory default state.	PASS
	Intf-Wi-Fi, Intf-5GNR, Intf-WAN, Intf-LAN: All exposed network interfaces are described in the user documentation QUICK_START_GUIDE.		
6.10.5	[GEC-5] No unnecessary external interfaces	The equipment shall only expose physical external interfaces if they are necessary for its intended functionality.	PASS
	intf-USB, intf-DC, intf-Cellular communication: Physical external interfaces on the device must exist for the intended functionality.		
6.10.6	[GEC-6] Input validation	The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network assets.	PASS

EN 18031-1:2024			
	The EUT defends against common input attacks through syntactic and semantic input checking. The WebUI's data transmission leverages Wi-Fi,LAN as its transport layer, with all user inputs undergoing rigorous syntactic validation at the interface level. Input fields enforce strict character type restrictions and length constraints, while network configuration parameters implement comprehensive IPv4 format verification to prevent structural anomalies. For USB interface security, the test lab conducted protocol-aware fuzzing tests on the USB ports using umap2. The results demonstrated the interface's robust input sanitization capabilitie.		
6.11	[CRY] Cryptography		
6.11.1	[CRY-1] Best practice cryptography	The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets.	PASS
	CRY-1-Asset-PrivacyKey of https certificate: The use of AES 256-bit encryption algorithm is in line with current cryptographic best practices. CRY-2-Asset-VPNcertificate: The use of AES 256-bit encryption algorithm is in line with current cryptographic best practices. CRY-3-Asset-RouterSettings: The use of AES 128-bit encryption algorithm is in line with current cryptographic best practices. CRY-4-Asset-Network Settings: The use of AES 128-bit encryption algorithm is in line with current cryptographic best practices.		

ANNEX B EUT EXTERNAL PHOTOS

Please refer the document “BL-SZ2540410-AW.PDF”.

ANNEX C EUT INTERNAL PHOTOS

Please refer the document “BL-SZ2540410-AI.PDF”.

Statement

1. The laboratory guarantees the scientificity, accuracy and impartiality of the test, and is responsible for all the information in the report, except the information provided by the customer. The customer is responsible for the impact of the information provided on the validity of the results.
2. The report without China inspection body and laboratory Mandatory Approval (CMA) mark has no effect of proving to the society.
3. For the report with CNAS mark or A2LA mark, the items marked with "☆" are not within the accredited scope.
4. This report is invalid if it is altered, without the signature of the testing and approval personnel, or without the “inspection and testing dedicated stamp” or test report stamp.
5. The test data and results are only valid for the tested samples provided by the customer.
6. This report shall not be partially reproduced without the written permission of the laboratory.
7. Any objection shall be raised to the laboratory within 30 days after receiving the report.

-- End of Report --