Technical Specifications for Security Testing of Information and Communication Equipment for Critical Telecommunications Infrastructure

1. Legal foundation

These specifications are stipulated in accordance with Paragraph 8 of Article 42 of the Telecommunications Management Act (hereinafter referred to as the Act).

2. Scope of application

These specifications are in accordance with Paragraph 1 of Article 42 of the Act stating that the National Communications Commission (hereinafter referred to as the Commission) may designate the public switched telephone network (PSTN), in whole or in part, as the critical telecommunications infrastructure, and the installed facilities include firewalls, switches, and routers with the ethernet interface (hereinafter referred to as information and communication equipment).

3. Technical standards

These specifications are stipulated with reference to the Attached Table 10
Secure baseline of information and communication technology of the Regulations on Classification of Cyber Security Responsibility Levels, the US NIST SP 1800-14, and the Forum of Incident Response and Security Teams (FIRST) CVSS Based Patching Policy.

4. Terminology definitions

4.1 Firewall

Refers to a security gateway or gate (including a dedicated device or a device combining various components and technologies), where only the authorized traffic can flow past the device from one network environment to another network environment and vice versa.

4.2 Switch

Refers to a device provided with network device connection capabilities by an internal switch mechanism.

4.3 Router

Refers to a network device using path selection or routing based on the routing protocol mechanism and algorithm for establishing and controlling data flows between different networks; the network may be based on different network protocols.

4.4 Transport Layer Security (TLS)

Refers to the establishment of a security tunnel via the network between two applications, which is defined in RFC 5246, and can prevent wiretapping and tampering when conducting data exchange.

4.5 National Vulnerabilities Database (NVD)

Refers to the National Vulnerability Database provided by the National Institute of Standards and Technology (NIST). It is responsible for the release and update of information regarding common vulnerabilities and weaknesses.

4.6 Common Vulnerabilities and Exposures (CVE)

Refers to the vulnerability management proposal sponsored by the U.S. Department of Homeland Security, which assigns a unique and globally recognized code number to each of the vulnerabilities.

4.7 Common Vulnerability Scoring System (CVSS)

Refers to a set of determining criteria for a common vulnerability scoring system, and the evaluation scores include the severity of the affected damage due to the threat, the degree of availability in vulnerabilities of cyber security, and the degree of difficulty for the attacker's illegal utilization of the vulnerability. The score is from 0 to 10, where 0 indicates no risk and 10 indicates the highest risk.

4.8 Password

Refers to a set of character strings that enables the system to conduct identification of the user's identity, and then the system can take further control of the user's access authentication.

4.9 Security Event Log

Refers to the activity log defined by each of the rules for discovering and detecting the potential threats or attacks (e.g. user's login system).

4.10 Security Tunnel

Refers to the tunnel created between the End-to-End endpoints on the Internet, with privacy and completeness of the data. For example, at present, the common implementation of communication protocol includes the Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

4.11 Encryption

Refers to the plain text that is converted to achieve the objective of security through an algorithm.

4.12 Management Interface

Refers to the obtained interface for the control of the device system via local or remote network, for example:

(1) Execute product maintenance and access resources of the device in the controlling program, web management interface or command interface.

(2) Execute system settings such as Internet Protocol (IP) address in the control program, web management interface or command interface.

5. Testing items

5.1 The information and communication equipment set up in critical telecommunications infrastructure shall be in compliance with the national security of related agencies and the regulations in 5.3 and 5.4, unless otherwise specified in these specifications.

5.2 The functions of information and communication equipment that include the listed functions for other equipment in 5.4 must also be in compliance with the requirements for the included equipment.

5.3 Common testing items and qualification criteria

5.3.1 Access Control

5.3.1.1 Idle and timeout management of an account

The device under test should be equipped with an idle and timeout management mechanism for an account, which means that the account of the device under test should be locked or logged out when the device under test is idle for more than the preset time, and the account cannot continue to be operated after the name and password of the account are re-entered.

5.3.1.2 Management for failure of account login

The device under test should be equipped with a management mechanism for failure of account login; when the account authentication fails more than the preset number of times, the device under test should restrict the login of the account or restrict its permission of use within the preset time.

5.3.1.3 Management of account authority

The device under test should be equipped with the function of setting for more than two sets of account authorities and authorization of different account authorities.

5.3.1.4 Access management of remote login

For the device under test that is equipped with the access function of remote login, the data transmission shall be in compliance with the requirements in 5.3.3.1 Transmission encryption of remote access. The record log for the operations of login, access and management interface shall be in compliance with the requirements in 5.3.2.1 Records of security event log.

5.3.1.5 The input password is hidden with a special symbol

If the device under test is authorized with a password, the entered password should be hidden with a special symbol.

5.3.1.6 Security of password storage

If the device under test is authorized with a password, the entered password should be encrypted or stored once hash processed.

5.3.2 Audit and accountability

5.3.2.1 Records of security event log

The device under test should have a log for recording the operations of management interface for account login and logout, configuration settings, update of firmware, etc., as well as the establishment, suspension, failures of establishment, and failures of suspension for the connection of trusted tunnel, and the time stamp of event occurrence.

5.3.2.2 Protection of records for security event log

The records of the security event log must not be accessed, deleted or modified by an unauthorized account.

5.3.2.3 Time stamp and time synchronization

The internal clock of the device under test should be synchronized with the Coordinated Universal Time or Greenwich Mean Time at least once every 24 hours to ensure the correctness of the timestamp.

5.3.3 System and communication protection

5.3.3.1 Transmission encryption of remote access

For the device under test that is equipped with the access function of remote login, its data transmission shall adopt a security tunnel above TLS 1.2, and use the Advanced Encryption Standard 128-bit or an encrypted algorithm with the equivalent level of encryption strength or above.

5.3.4 System weaknesses and vulnerabilities

5.3.4.1 The discovered weaknesses and vulnerabilities

The operating system and network service of the device under test with a CVE that has a CVSS score of 7.0 or more is not available.

5.3.5 Continuity test

5.3.5.1 Abnormal power interruption

After the restart of the device under test due to an abnormal power interruption, the security policy, security event log, login authentication information, and configuration of remote management of the device under test should remain the same prior to the power interruption.

5.3.5.2 Configuration backup and restore

The device under test should be equipped with the function of configuration backup and restore.

5.4 Testing items for individual equipment and qualification criteria

5.4.1 Firewall

5.4.1.1 Rules for packet and filtering

The device under test should be able to block packets with specific filtering conditions. The filtering conditions must include the IP address of the source end and destination end of the packet, the port number, and the used communication protocol (such as TCP, UDP and ICMP).

5.4.1.2 Conversion of static network address

The device under test should be equipped with the function of mutual conversion of internal IP address and external IP address.

5.4.1.3 Conversion of dynamic network address

The device under test should be equipped with the function of mapping multiple internal IP addresses onto multiple external IP addresses in a dynamic and random way.

5.4.1.4 Abnormal flow test

During the eight-hour period of continuous reception of abnormal flow (the flow that violates the provisions of security policy), the device under test should properly filter packets based on the security policy and issue alert regarding the abnormal flow.

5.4.1.5 Function of flow restriction

The device under test should be equipped with a flow restriction function to restrict the transmission flow of receiving or transferring via the network interface.

5.4.1.6 Firewall protocol security test

The device under test should be in normal operation during the eight-hour period of continuous reception of variant packets with the following protocols:

(1) Internet Protocol Version 4 (IPv4) (RFC 791).

(2) Internet Protocol Version 6 (IPv6) (RFC 8200).

(3) Internet Control Message Protocol Version 4 (ICMPv4) (RFC 792).

(4) Internet Control Message Protocol Version 6 (ICMPv6) (RFC 4443).

5.4.2 Switch

5.4.2.1 The Address Resolution Protocol (ARP) security mechanism

The device under test should have the ARP security mechanism to defend against spoofing attacks.

5.4.2.2 The Virtual Local Area Network (VLAN) security mechanism

The device under test should have the Double Encapsulated 802.1Q VLAN security mechanism to defend against hopping attacks.

5.4.2.3 The Content Addressable Memory (CAM) table security mechanism

The device under test should have the Media Access Control (MAC) security mechanism to defend against traffic flow attacks.

5.4.2.4 Switch protocol security test

The device under test should be in normal operation during the eight-hour period of continuous reception of variant packets with the following protocols:

(1) ARP (RFC 826).

(2) Ethernet MAC Frame (IEEE 802.3).

(3) Ethernet Control Frame (IEEE 802.3).

(4) VLAN Tag (IEEE 802.1Q).

(5) Link Layer Discovery Protocol (LLDP) (IEEE 802.1AB).

5.4.3 Router

5.4.3.1 Routing information protection mechanism

The device under test should have the routing information protection mechanism or Resource Public Key Infrastructure (RPKI) mechanism, and hence only the trusted sources of routing information will be received.

5.4.3.2 Router protocol security test

The device under test should be in normal operation during the eight-hour period of continuous reception of variant packets with the following protocols:

(1) Routing Information Protocol (RIP) (RFC 2453).

(2) Open Shortest Path First (OSPF) (RFC 2328).

(3) Border Gateway Protocol (BGP) (RFC 4271).

(4) IPv4 (RFC 791).

(5) IPv6 (RFC 8200).

6. Regulations for equipment certification

6.1 Application procedures

6.1.1 When applying for cyber security inspection (certification) of information and communication equipment, the critical telecommunications infrastructure operators, manufacturers, importers, distributors or agencies of information and communication equipment should fill in the Cyber Security Inspection Application Form for information and communication equipment of critical telecommunications infrastructure, and the following documents in the form of printed copies or electronic files shall be attached when applying to the Commission or the inspection agency for information and communication equipment of critical telecommunications infrastructure (hereinafter referred to as the inspection institution (agent)) commissioned by the Commission. Those who have passed the inspection will be issued an inspection certificate with the printed label of inspection qualification by the inspection institution (agent):

(1) The manual or instruction of the equipment in traditional Chinese or English (including the support period and expiration of software update, and plan for equipment replacement when the update is no longer available).

(2) The cyber security testing report for the information and communication equipment based on Point 5 (hereinafter referred to as the testing report).

(3) The original manufacturer's specifications for equipment performance, catalog, the rules for software and firmware version numbers in traditional Chinese or English, and the structure figure or block diagram for equipment function, security function and management function, as well as a summary table of security functions. The information of specifications for equipment performance shall include the following:

I. Firewall: Throughput, maximum number of connections per second, maximum number of simultaneous connections, performance stability and performance reliability.

II. Switch: Throughput/bandwidth, Spanning Tree protection, performance stability and performance reliability.

III. Router: Throughput/bandwidth, maximum number of routing settings, performance stability and performance reliability.

(4) The security statement for development and supply chain of software and firmware.

(5) The applicant should be a native natural person and attach the identity certificate. For corporates, unincorporated organizations or foreign manufacturers, they should attach the relevant organization certificate.

(6) Other relevant materials regarding inspection as required by the competent authority.

(7) The electronic files of (1) to (6) (not applicable to the electronic file applicants).

6.1.2 Other than the electronic files that will be retained by the inspection institution (agent), the remaining documents attached to the application for inspection shall be returned when the inspection certificate is issued.

6.1.3 The testing report should be issued by an inspection institution (hereinafter referred to as the inspection institution) that has been certified by the Taiwan Accreditation Foundation and approved by the Commission for implementation of the testing items specified in the technical specifications. If the inspection institution for providing the inspection service is not available, the applicant should contact the relevant institution for the provision of a testing report in the following order:

(1) A testing laboratory accredited by the members of the International Laboratory Accreditation Cooperation (ILAC) in other countries.

(2) Equipment manufacturer.

6.1.4 The following should be included in the testing report:

(1) Name and address of the applicant.

(2) Name and address of the inspection institution.

(3) The unique identification of the testing report and identification on each page.

(4) Name and address of the equipment manufacturer.

(5) Equipment’s name, brand, model number, software and firmware version, and 4×6 inch or above front color photos or pictures that are clear and identifiable, and the brand and model number must be clearly displayed and readable. The top view, bottom view, left view, right view, front view and back view of the sample shall also be included.

(6) Testing items and qualification criteria.

(7) Testing records and the determined results.

(8) Name, brand, model number, software and firmware version and the reference NVD version of the equipment for test.

(9) The testing date and completion date.

(10) Name, title and signature of the testing personnel and the person who signs the report.

6.1.5 The inspection institution (agent) shall notify the applicants to make complementary correction within one month if the attached documents or items are missing or incomplete; if the complementary correction is incomplete or fails to be completed by the deadline, the application shall be rejected.

6.1.6 The inspection institution (agent) carries out the inspection according to Point 5. After the inspection, the inspection institution (agent) may list the unqualified items for those unqualified testing items and notify the applicant to make an improvement within two months; for those who fail to make an improvement by the deadline or fail to pass the re-inspection after the improvement, the application shall be rejected.

6.1.7 If the applicant is different from the applicant of the testing report, the applicant should additionally attach a copy of the company or business registration certificate and the authorization letter for the use of the testing report.

6.1.8 For the critical telecommunications infrastructure operators who apply for inspection of information and communication equipment, the inspection results are applicable to all information and communication equipment with the same brand, model, and software and firmware version. For the manufacturer, importer, distributor or agency of information and communication equipment who applies for inspection, the inspection results shall be applicable to the information and communication equipment with the same brand, model, and software and firmware version. Except otherwise specified in the specifications, the same software and firmware version is based on the major/main release of the information and communication equipment.

6.1.9 The information and communication equipment with different brands and model numbers shall apply for inspection respectively. For information and communication equipment that pass the inspection, it shall reapply for inspection if its brand or model is changed; for change of software and firmware version, its version and performance difference shall be stated in written documents and reported to the original inspection institution for reference within 14 days; if necessary, the inspection institution may request re-inspection or an inspection on the modified part.

6.2 Management of inspection certificate

6.2.1 The label of inspection qualification exclusively belongs to the party who obtained the inspection certificate. The party who has obtained the inspection certificate may allow others to use the certification label for critical information and communication equipment with the same brand, model and firmware version upon the submission of the following documents to the inspection institution for review:

(1) A copy of the inspection certificate.

(2) A copy of the user’s company or business registration certificate.

6.2.2 If one of the following circumstances is applicable to the manufacturer, importer, distributor or agency of the information and communication equipment who has obtained an inspection certificate of information and communication equipment, the inspection institution (agent) that issues the inspection certificate should note the wording “security vulnerabilities to be patched” on the inspection certificate of equipment. For those who have obtained the inspection certificate, the inspection institution (agent) will delete the “security vulnerabilities to be patched” note on the inspection certificate if they attach a testing report issued by the inspection institution showing that the related CVE have been patched.

(1) The operating system or network service of the information and communication equipment has been disclosed with a CVE that has a CVSS score of 7.0 or above, but failed to attach a testing report, showing that the CVE has been patched, issued by the inspection institution within 14 days from the date of disclosure.

(2) The operating system or network service of the information and communication equipment has been disclosed with a CVE that has a CVSS score of 4.0–6.9, but failed to attach a testing report, showing that the CVE has been patched, issued by the inspection institution within 45 days from the date of disclosure.

(3) The operating system or network service of the information and communication equipment has been disclosed with a CVE that has a CVSS score of 0.1–3.9, but failed to attach a testing report, showing that the CVE has been patched, issued by the inspection institution within six months from the date of disclosure.

6.2.3 For any of the following circumstances, the inspection certificate may be abolished or revoked:

(1) Providing false information when applying for an inspection.

(2) Violation of regulations in 6.1.9.

(3) Failure to fulfill the regulations in 5.1 and 5.2 upon random inspection.

(4) Due to dispute of power of attorney and patent rights, the case has lost the lawsuit and is finalized by the court, or violation of other regulations resulting in sale being prohibited.

(5) It may cause danger to national security that is announced or notified by relevant agencies.

6.2.4 If the inspection certificate is lost or damaged, the applicant shall attach an application form for reissuance and apply to the original inspection institution (agent) for certificate reissuance or replacement.

6.2.5 For the modification of items listed on the inspection certificate, the applicant shall apply to the original inspection institution (agent) for certificate reissuance if any of the following circumstances is applicable:

(1) Change or addition of a manufacturer.

(2) Name or address of the applicant is changed.

(3) If the company of the applicant is merged or divided, the remaining or newly established company after merger or division can continue to use the original inspection certificate upon the approval of the competent authority.

6.2.6 According to the provisions of the preceding paragraph, the application for reissuance shall attach the following documents:

(1) According to 6.2.5(1): application form for reissuance, related proof documents for commission of equipment production, and a declaration for the equipment complying with the technical specifications.

(2) According to 6.2.5(2): application form for reissuance, a copy of identification document (two identification documents are required) for natural persons, and relevant organization certificate for corporates and unincorporated organizations.

(3) According to 6.2.5(3): application form for reissuance, company or business registration certificate, and an approval document from the competent authority.

6.3 Supplementary provisions

6.3.1 The relevant documents and forms, operating procedures, and the format of the inspection certificate specified in the specifications shall be stipulated and announced by the Commission.

6.3.2 Those who apply for inspection and reissuance of the inspection certificate shall pay the inspection fee or license fee to the inspection institution (agent) according to the fee standard stipulated by the Commission.