GUIDANCE NOTES
GD028-2025

INTERNATIONAL SHIP CLASSIFICATION

GUIDELINES FOR INSPECTION OF SHIP NETWORK FIREWALLS

2025

Effective from December 1, 2025

CONTENTS

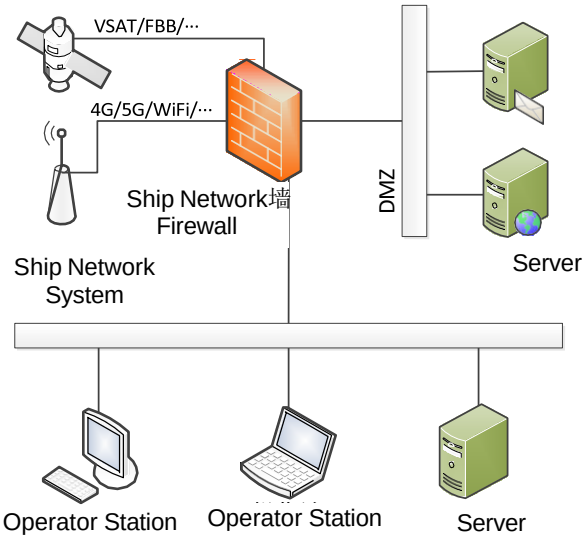
CHAPTER 1 GENERAL

Section 1 GENERAL PROVISIONS

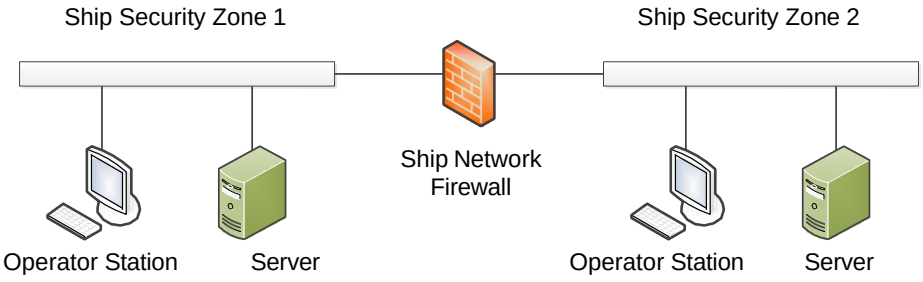
1.1.1 General Requirements

1.1.1.1 This Guideline stipulates the technical requirements and product inspection requirements for ship boundary firewalls and is applicable to the inspection of such firewalls.

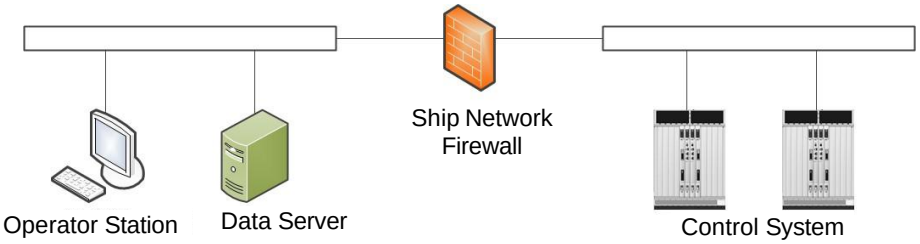
1.1.1.2 Ship network firewalls include ship boundary firewalls and firewalls deployed within shipboard computer-based systems (CBS), etc. Examples of their application scenarios are shown in Figure 1.1.1.2.



(1) Deployed at the boundary of the shipborne network system



(2) Deployed at the boundary of a shipboard security zone



(3) Deployed within a shipboard CBS

Figure 1.1.1.2 Application Scenarios of Ship Network Firewalls

1.1.2 Classification of Ship Network Firewalls

1.1.2.1 Ship network firewalls are classified into three levels according to Table 1.1.2.1:

Classification of Ship Network Firewalls **Table 1.1.2.1**

No.	Level	Technical requirements	Scope
1	Level 1	Meets the requirements of Sections 2.1, 2.2, 2.3, 2.4, and 2.7 of this Guideline.	SL0-class ships and CBS.
2	Level 2	Meets the requirements of Sections 2.1, 2.2, 2.3, 2.5, and 2.7 of this Guideline.	Ships and CBS of SL1-SL2.
3	Level 3	Meets the requirements of Sections 2.1, 2.2, 2.3, 2.6, and 2.7 of this Guideline.	Ships and CBS of SL3-SL4.

Note: The technical capabilities of higher-level firewalls cover the requirements of lower-level firewalls and are applicable to their respective scenarios.

1.1.3 Certification Requirements

1.1.3.1 Ship boundary firewalls shall hold a Type Approval Certificate; applications for ship network firewalls used in other scenarios may be submitted on a voluntary basis.

1.1.4 Data Provision and Confidentiality

1.1.4.1 ISC shall perform information disclosure of the data and information submitted by the applicant in accordance with Section 12, Chapter 2, Part 1 of the ISC Rules for Classification of Sea-going Steel Ships. Principles for intellectual property and confidentiality shall follow Article 3.1.10, Section 1, Chapter 2, Part 1 of the same rules.

1.1.5 Change management

1.1.5.1 For ship network firewalls approved/inspected by ISC, the applicant shall notify ISC when major changes occur to software or equipment components (including but not limited to major software version upgrades, changes in functions or performance, modifications to operational procedures, or changes in equipment components). ISC may require a re-evaluation to ensure compliance with relevant technical requirements.

1.1.6 Terms and Abbreviations

1.1.6.1 The terms and definitions in the Guidelines for Ship Cyber Security are applicable to this Guideline. Additional terms and definitions for this Guideline are as follows:

(1) Firewall: A security barrier established between network environments, consisting of a dedicated device or a combination of several components and technologies. All communication flows in both directions between network environments pass through this barrier, and only authorized communication flows defined according to local security policies are permitted to pass. Firewalls applied in ship networks are collectively referred to as ship network firewalls.

(2) Ship network system: A general term for CBS systems deployed on a ship, including IT system networks and OT system networks.

(3) Ship boundary firewall: Refers to a ship network firewall deployed at the boundary between a ship network system and an external network, or at the boundary of a ship security zone.

(4) Robustness: The property of a system or component to maintain correct operation of all its functions under environments such as invalid data input or high-intensity input.

(5) Robustness testing: Testing of the effective handling capability against system errors (including invalid, high-intensity, or undesired inputs, or malicious attacks).

1.1.6.2 The abbreviations in the Guidelines for Ship Cyber Security are applicable to this Guideline. Additional abbreviations for this Guideline are as follows:

(1) CA: Certificate Authority

(2) PKI: Public Key Infrastructure

(3) DoS: Denial of Service

(4) DDoS: Distributed Denial of Service

(5) MAC: Media Access Control

(6) DMZ: Demilitarized Zone

(7) NAT: Network Address Translation

(8) SNAT: Source Network Address Translation

(9) DNAT: Destination Network Address Translation

(10) OPC: Object Linking and Embedding for Process Control

(11) AES: Advanced Encryption Standard

(12) SYN: Synchronize Sequence Numbers

(13) SYSLOG: System Log or a protocol for log transmission (System Log)

1.1.7 Normative References

The clauses in the relevant documents become provisions of this document through reference. For undated references, the latest edition of the referenced document applies to this document.

1.1.7.1 ISC Rules for Classification of Sea-going Steel Ships and its amendments

1.1.7.2 ISC Guidelines for Ship Cyber Security

1.1.7.3 IACS UR E26 Cyber resilience of ships

1.1.7.4 IACS UR E27 Cyber resilience of on-board systems and equipment

1.1.7.5 IEC 62443 series: Security for industrial automation and control systems

1.1.7.6 IEC 61162-460: Maritime navigation and radio communication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security

1.1.7.7 RFC 3511: Benchmarking Methodology for Firewall Performance

1.1.7.8 RFC 2979: Requirements for Network Firewalls

CHAPTER 2 TECHNICAL REQUIREMENTS FOR SHIP NETWORK FIREWALLS

Section 1 GENERAL PROVISIONS

2.1.1 General Requirements

2.1.1.1 This chapter primarily describes the technical requirements for ship network firewalls, including interface requirements, security capability requirements, functional requirements, and performance requirements.

2.1.1.2 Data security for logs and other information shall meet the relevant requirements of Appendix 8 of the ISC Guidelines for Quality Assessment of Ship Data.

Section 2 INTERFACE REQUIREMENTS

2.2.1 Physical Interfaces

2.2.1.1 The types and quantities of physical interfaces of the ship network firewall shall meet the needs of device operation and maintenance. Physical interfaces such as Ethernet electrical ports and optical ports shall meet the corresponding interface definition standards. Specifications for proprietary physical interfaces shall be described.

2.2.1.2 All supported interface functions of each physical interface shall be described.

2.2.2 Data Interfaces

2.2.2.1 The ship network firewall shall clarify the standard interface protocols supported by its interfaces. If proprietary interface protocols are applicable, detailed documentation shall be provided.

2.2.2.2 The ship network firewall shall support the output of monitoring and alarm information through its interfaces.

Section 3 SECURITY CAPABILITY REQUIREMENTS

2.3.1 Identification and authentication

2.3.1.1 Human user identification and authentication

Security Level	Requirements
I	Shall be capable of identifying and authenticating all human users who access directly or through interfaces, and shall adopt multi-factor authentication for personnel accessing via untrusted networks.
II	Shall be capable of uniquely identifying and authenticating all human users.
III	Shall be capable of multi-factor identifying and authenticating all human users who access via interfaces.

2.3.1.2 Process and device identification and authentication

Security Level	Requirements
I	Shall be capable of identifying and authenticating all processes and devices that access directly or through interfaces.
II	
III	Shall be capable of uniquely identifying and authenticating all software processes and devices.

2.3.1.3 Account Management

Security Level	Requirements
I	Shall support authorized users in managing all accounts, including adding, activating, modifying, disabling, and deleting accounts.
II	
III	

2.3.1.4 Identification management

Security Level	Requirements
I	Shall support identification management via users, groups, roles, or system interfaces.
II	
III	

2.3.1.5 Authentication management

Security Level	Requirements
I	Shall have the following capabilities: ① Initialize the content of authenticators (passwords, tokens, etc.); ② Require the modification of default values for all authenticators upon installation; ③ Periodically modify/update all authenticators; ④ Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.
II	
III	Shall be capable of providing enhanced protection for authenticators through hardware mechanisms (e.g., TPM).

2.3.1.6 Wireless Access Management (applicable if a wireless module is present)

Security Level	Requirements
I	Shall be capable of identifying and authenticating all users (personnel, software processes, or devices) using wireless communication.
II	Shall be capable of uniquely identifying and authenticating all users (personnel, software processes, or devices) using wireless communication.
III	

2.3.1.7 Password strength

Security Level	Requirements
I	Shall be capable of enforcing configurable password strength based on minimum length and various character types.
II	Shall have the following capabilities: ① Shall prevent any given individual from reusing a configurable number of previous passwords; ② Shall be capable of limiting the minimum and maximum lifespan of personnel passwords;
III	

Security Level	Requirements
	③ Shall prompt the user to change the password within a configurable timeframe before expiration; ④ The CBS is to provide the capability to restrict the password minimum and maximum lifetime for all users.

2.3.1.8 Public Key Infrastructure (PKI) Certificates

Security Level	Requirements
I	Not required.
II	When using PKI, the firewall shall be capable of operating the PKI according to best practices or obtaining public key certificates from an existing PKI.
III	

2.3.1.9 Strength of public key authentication

Security Level	Requirements
I	Not required.
II	When public key authentication is adopted, it shall be possible to: ① Verify certificates by checking the validity of the certificate signature; ② Verify certificates by building a certificate path to an accepted trusted CA, or in the case of self-signed certificates, by deploying sub-certificates to all hosts communicating with the subject that issued the certificate; ③ Verify certificates by checking the revocation status of a given certificate; ④ Establish control by the user (personnel, software process, or device) over the corresponding private key; ⑤ Map validated identities to users (personnel, software processes, or devices); ⑥ Use cryptographic mechanisms for public key authentication algorithms and keys in accordance with internationally recognized and proven security practices.
III	Shall be capable of protecting private keys through hardware mechanisms.

2.3.1.10 Authentication feedback

Security Level	Requirements
I	Shall be capable of obfuscating authentication feedback information during the authentication process.
II	
III	

2.3.1.11 Unsuccessful login attempts

Security Level	Requirements
I	Shall have the following capabilities: ① Enforce a limit on a configurable number of consecutive invalid access attempts for any user (personnel, software process, or device) within a configurable time period;
II	
III	

	② Deny access for a specified period, or until unlocked by an administrator once the limit has expired. Administrators may unlock accounts before the timeout period expires.

2.3.1.12 System use notification

Security Level	Requirements
I	Shall possess the capability to display system use notification messages before authentication, and the messages shall be configurable by authorized personnel.
II	
III	

2.3.1.13 Untrusted Network Access

Security Level	Requirements
I	Shall have the following capabilities: ① When accessing the network through the firewall, the firewall shall provide the capability to monitor and control all methods of access via untrusted networks; ② Shall provide the capability to deny access requests via untrusted networks unless explicitly authorized by a designated role on board.
II	
III	

2.3.2 Use control

2.3.2.1 Authorization enforcement

Security Level	Requirements
I	Shall be capable of providing authorization enforcement mechanisms for all identified and authenticated personnel based on assigned responsibilities and least privilege.
II	Shall provide authorization enforcement mechanisms for all users (personnel, software processes, and devices) based on assigned responsibilities and least privilege; shall be capable of authorizing users or roles, and defining and modifying mappings of all personnel or roles to permissions.
III	Shall support administrators in manually overriding current personnel authorizations during configurable times or events; dual permission confirmation shall be supported when an operation could seriously affect ship cyber security.

2.3.2.2 Wireless use control

Security Level	Requirements
I	Shall authorize, monitor, and restrict the use of wireless connections in accordance with generally accepted security industry practices.
II	
III	

2.3.2.3 Use control for portable and mobile devices

Security Level	Requirements
I	When the firewall supports the use of portable and mobile devices, the system shall include the following functions:
II	

Security Level	Requirements
	① Restrict the use of portable and mobile devices within the scope permitted by design; ② Restrict code and data transmission to/from portable and mobile devices.
III	Shall be capable of verifying whether a portable or mobile device attempting to connect to a zone meets the security requirements of that zone.

2.3.2.4 Mobile code

Security Level	Requirements
I	Shall have the following capabilities: ① Control the execution of mobile code; ② Control which users (personnel, software processes, or devices) are allowed to transfer code to or from the firewall; ③ Control code execution based on integrity verification of mobile code before execution.
II	
III	Shall verify the integrity of mobile code before allowing execution and control the execution of mobile code based on authentication check results.

2.3.2.5 Session lock

Security Level	Requirements
I	Shall possess session lock capability, which is activated automatically or manually after a configurable period of inactivity. Session access shall be re-established through re-authentication by the user or another authorized user.
II	
III	

2.3.2.6 Remote session termination

Security Level	Requirements
I	Shall be capable of automatically terminating remote sessions after a configurable period of inactivity, or manually by the user who initiated the session.
II	
III	

2.3.2.7 Concurrent session control

Security Level	Requirements
I	Not required.
II	Shall be capable of limiting the number of concurrent sessions per interface, with the limit being configurable.
III	

2.3.2.8 Auditable events

Security Level	Requirements
I	Security-related audit records shall be generated for at least the following events: access control, operating system events, backup and recovery events, configuration changes, and communication interruptions.
II	
III	

2.3.2.9 Audit storage capacity

Security Level	Requirements
I	Shall be capable of allocating audit record storage capacity according to recognized log management recommendations. Shall implement audit mechanisms to reduce the likelihood of exceeding the storage capacity.
II	
III	Shall be capable of issuing an alarm when the allocated audit record storage reaches a configurable percentage of the maximum capacity.

2.3.2.10 Response to audit processing failures

Security Level	Requirements
I	In the event of audit processing failure, the system shall support taking appropriate measures based on recognized industry practices and recommendations to respond to the failure.
II	
III	

2.3.2.11 Timestamps

Security Level	Requirements
I	Shall be capable of providing timestamps for generated audit records.
II	Shall be capable of synchronizing the UTC time of the server at a configurable frequency.
III	The time source is to be protected from unauthorized alteration and is to cause an auditable event upon alteration.

2.3.2.12 Use of physical diagnostic and test interfaces

Security Level	Requirements
I	Network devices are to prevent unauthorized use of the physical factory diagnostic and test interfaces.
II	
III	Network devices are to provide active monitoring of their diagnostic and test interfaces and generate an audit log when access to these interfaces is detected.

2.3.3 System Integrity

2.3.3.1 Communication integrity

Security Level	Requirements
I	Shall be capable of protecting the integrity of transmitted data.
II	

Security Level	Requirements
III	Shall possess the capability to verify the authenticity of information during communication.

2.3.3.2 Malicious code protection

Security Level	Requirements
I	Shall be capable of implementing appropriate protective measures to prevent, detect, and mitigate the impact of malicious code or unauthorized software, and shall have functions for updating protection mechanisms.
II	
III	

2.3.3.3 Security functionality verification

Security Level	Requirements
I	Shall support verification that security functions are operating as intended and report anomalies occurring during maintenance.
II	
III	During normal operation, automatic verification of security functions shall be supported.

2.3.3.4 Software and information integrity

Security Level	Requirements
I	Not required.
II	Shall be capable of performing authenticity verification on firmware, configurations, and other information, and recording and reporting the verification results.
III	During integrity verification, unauthorized changes shall be detected and alarms sent.

2.3.3.5 Input validation

Security Level	Requirements
I	Shall validate the syntax, length, and content of all input data used to control or directly affect firewall security protection configurations.
II	
III	

2.3.3.6 Deterministic output

Security Level	Requirements
I	If the firewall cannot maintain normal operation due to an attack, the system shall set the output to a predetermined state. Predetermined states may include: - Unpowered state - Last-known value - Fixed value
II	
III	

2.3.3.7 Session integrity

Security Level	Requirements
I	Shall be capable of protecting session integrity and rejecting the use of any invalid session IDs.
II	Mechanisms to protect the integrity of communication sessions shall be provided, including: ① Invalidation of session IDs upon user logout or other session termination (including browser sessions); ② Generation of a unique session ID for each session, recognizing only system-generated session IDs; ③ Capability to randomly generate unique session IDs using generally accepted methods.
III	

2.3.3.8 Protection of audit information

Security Level	Requirements
I	Shall be capable of protecting audit information and logs against unauthorized access, modification, and deletion.
II	
III	Shall provide the capability to store audit records on mandatory write-once hardware media.

2.3.3.9 Update Support

Security Level	Requirements
I	Updates and upgrades throughout the lifecycle shall be supported. Appropriate mechanisms shall be in place to ensure that the ship's fundamental functions are not affected during updates and upgrades.
II	Support for verifying the authenticity and integrity of any update before installation shall be provided.
III	

2.3.3.10 Physical Tampering Protection and Detection

Security Level	Requirements
I	Not required.
II	Shall be capable of detecting and preventing unauthorized physical access and tampering.
III	Automatic detection and monitoring of physical tampering shall be implemented, with records reported to authorized personnel.

2.3.3.11 Product Vendor Root of Trust

Security Level	Requirements
I	Not required.
II	Shall be capable of protecting the confidentiality, integrity, and authenticity of the product vendor's root of trust (keys and data used as roots of trust).
III	

2.3.3.12 Asset Owner Root of Trust

Security Level	Requirements
I	Not required.
II	Shall be capable of protecting the confidentiality, integrity, and authenticity of the asset owner's root of trust (keys and data used as roots of trust) without depending on components outside the firewall's security zone.
III	

2.3.3.13 Boot Process Integrity

Security Level	Requirements
I	Integrity verification of firmware, software, and configuration data required during the boot process shall be performed before the firewall starts.
II	Verification of the product vendor's root of trust shall be performed before the firewall starts.
III	

2.3.4 Data confidentiality

2.3.4.1 Data Confidentiality

Security Level	Requirements
I	Shall be capable of protecting the confidentiality of stored information and information in transit that supports explicit read authorization.
II	
III	

2.3.4.2 Information persistence

Security Level	Requirements
I	Not required.
II	The CBS is to provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.
III	The CBS is to provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.

2.3.4.3 Use of cryptography

Security Level	Requirements
I	If encryption is required, cryptographic security mechanisms shall be used in accordance with internationally recognized and proven security practices and recommendations.
II	
III	

2.3.5 Restricted data flow

2.3.5.1 Zone boundary protection

Security Level	Requirements
I	Shall be capable of monitoring and controlling communication at zone boundaries. All network traffic shall be denied by default at zone boundaries, except for traffic explicitly allowed.
II	
III	Automatic detection and monitoring of tampering shall be implemented, with records reported to authorized personnel.

2.3.5.2 User Communication Restriction

Security Level	Requirements
I	Shall be capable of identifying and blocking communications that violate security policies, such as social media content transmission or image transmission.
II	
III	

2.3.6 Timely Response to Events

2.3.6.1 Audit log accessibility

Security Level	Requirements
I	Read-only access to audit logs by authorized personnel and/or tools shall be supported.
II	
III	The CBS is to provide programmatic access to audit records using an application programming interface (API).

2.3.6.2 Continuous monitoring

Security Level	Requirements
I	Not required.
II	The CBS is to provide the capability to continuously monitor all security mechanism performance to detect, characterize and report security vulnerabilities in a timely manner according to commonly accepted security industry practices and recommendations.
III	

2.3.7 Resource availability

2.3.7.1 Denial of service protection

Security Level	Requirements
I	The CBS is to provide the capability to maintain important functions during a DoS event.
II	Shall be capable of mitigating the effects of information and/or message flooding types of DoS events.
III	

2.3.7.2 Resource management

Security Level	Requirements
I	Shall be capable of limiting the use of resources through security functions to prevent resource exhaustion.
II	
III	

2.3.7.3 System backup

Security Level	Requirements
I	Support for the identification and storage of critical files, as well as the backup of user-level and system-level information (including system status information), shall be provided, with the backup process not affecting normal operations.
II	The integrity of backup information shall be verified before recovery operations.
III	

2.3.7.4 Control system recovery and reconstruction

Security Level	Requirements
I	The CBS is to provide the capability to recover and reconstruct to a known secure state after a disruption or failure.
II	
III	

2.3.7.5 Power supply

Security Level	Requirements
I	The CBS is to provide the capability to switch to and from a power supply without affecting the existing security state or a preset degraded mode.
II	
III	

2.3.7.6 Network and security configuration settings

Security Level	Requirements
I	Shall be capable of system setup according to vendor-recommended network and security configurations, and shall provide an interface for setting up currently deployed network and security configurations.
II	
III	The CBS is to provide the capability to generate a security configuration report in CSV, JSON, XML and other formats.

2.3.7.7 Least functionality

Security Level	Requirements
I	Installation, availability, and access rights for the following items shall be restricted to the strict needs of the system's functions: - Operating system software components, processes, and services - Network services, ports, protocols, routes, host access, and any software
II	
III	

2.3.7.8 System Component Inventory

Security Level	Requirements
I	Not required.
II	Shall be capable of documenting a list of installed components and their associated attributes.
III	

2.3.8 Software and Hardware Requirements

2.3.8.1 The ship network firewall shall operate reliably under the environmental and working conditions required for computer systems in Chapter 2, Part 7 of the ISC Rules for Classification of Sea-going Steel Ships.

2.3.8.2 Ship network firewalls should preferably be designed with natural cooling and a configuration without fans.

2.3.9 Security Requirements

2.3.9.1 The ship network firewall shall possess the declared functions and ensure its own product security, free from security risks such as malware and known vulnerabilities.

2.3.9.2 The "least privilege" principle shall be adopted, denying all traffic by default and allowing only traffic authorized by rules to pass.

2.3.9.3 The ship network firewall shall be capable of transmitting alarm information such as traffic, bandwidth, and abnormal statuses, and updating it promptly when the alarm status changes.

2.3.9.4 After restarting from a shutdown under abnormal conditions (e.g., power loss, forced shutdown), the ship network firewall shall meet the following requirements:

(1) Security policies shall be restored to their pre-shutdown state;

(2) Log information shall not be lost or overwritten;

(3) Accounts shall be re-authenticated.

2.3.9.5 In the event of an abnormal power outage of the ship network firewall, the internal and external interfaces shall be physically connected or disconnected based on the application scenario, with timely alarms. The reference action mechanisms for application scenarios are as follows:

(1) Firewalls for ship network boundary protection should preferably keep internal and external interfaces disconnected after device failure;

(2) Firewalls for inter-system/zone protection or between system layers should preferably have internal and external interfaces directly connected after device failure.

2.3.9.6 Failures of the ship network firewall's hardware or software shall not affect the essential services of the critical systems it protects.

2.3.9.7 The ship network firewall should support multiple working modes to ensure minimal impact on the protected systems during deployment, maintenance, and operation.

2.3.9.8 The underlying support system of the ship network firewall shall meet the following requirements:

(1) No unnecessary network services shall be provided;

(2) No medium-to-high risk vulnerabilities that could lead to loss of product permissions, denial of service, etc., shall be present.

2.3.9.9 Guidance documents for operations such as installation, upgrades, and O&M shall be formulated. For remote maintenance, the requirements of Article 4.3.16 of the ISC Guidelines for Ship Cyber Security shall also be met.

2.3.9.10 An incident response and recovery plan shall be formulated with reference to the requirements of Articles 4.3.21 and 4.3.22 of the ISC Guidelines for Ship Cyber Security.

Section 4 FUNCTIONAL REQUIREMENTS FOR LEVEL I SHIP NETWORK FIREWALLS

2.4.1 Networking and Deployment

2.4.1.1 The ship network firewall shall support routing forwarding and transparent transmission, and may also support proxy.

2.4.2 Network Layer Control

2.4.2.1 The ship network firewall shall support packet filtering, and the security policies shall meet the following requirements:

(1) The least privilege principle shall be used, i.e., deny unless explicitly allowed;

(2) Access control based on source and destination IP addresses shall be included;

(3) Access control based on MAC address shall be included;

(4) Access control based on source and destination ports shall be included;

(5) Access control based on protocol type shall be included;

(6) User-defined security policies shall be supported, which may be based on partial or full combinations of MAC address, IP address, port, etc.;

2.4.2.2 The ship network firewall shall support Network Address Translation (NAT) functionality, with the following technical requirements:

(1) Support for bidirectional NAT: SNAT and DNAT;

(2) SNAT shall enable "many-to-one" address translation, allowing the source IP addresses of internal network hosts to be translated when accessing external networks;

(3) DNAT shall enable "one-to-many" address translation, mapping internal network or DMZ IP addresses/ports to legitimate external network IP addresses/ports, allowing external network hosts to access internal network or DMZ servers by accessing the mapped addresses and ports.

2.4.2.3 The ship network firewall shall possess connection state detection capabilities and support access control based on stateful inspection technology.

2.4.2.4 The ship network firewall shall support dynamic port opening for protocols such as OPC DA, FTP, and H.323.

2.4.2.5 The ship network firewall shall support automatic or manual binding of IP/MAC addresses by an administrator, detect IP/MAC address spoofing, and block all access attempts through the firewall by hosts using spoofed IP/MAC addresses.

2.4.2.6 The product shall support traffic management functions, capable of adjusting client-occupied bandwidth based on policies, including but not limited to:

(1) Restricting traffic rates or totals based on source IP, destination IP, application type, and time period;

(2) Setting guaranteed bandwidth based on source IP, destination IP, application type, and time period;

(3) Automatically lifting traffic restrictions when the network is idle and automatically enabling restrictions when total bandwidth utilization exceeds a threshold.

2.4.3 Application Layer Control

2.4.3.1 Network access control based on user authentication shall be supported, including at least local user authentication.

2.4.3.2 The ship network firewall shall be able to identify and control common application layer protocols and proprietary protocols, with the following technical requirements:

(1) Support for common application layer protocols such as HTTP, FTP, and Telnet shall be

provided;

(2) Support for commonly used industrial control protocols in shipborne network systems, such as OPC, Modbus, and Profinet, shall be provided.

2.4.3.3 Deep content inspection for mainstream industrial protocols shall be supported, with the following technical requirements:

(1) Industrial control protocol format specification checks shall be performed, prohibiting communication that does not conform to protocol specifications;

(2) Parameters of industrial protocols such as operation type, operation object, and operation scope shall be controlled.

2.4.3.4 When the application scenario involves providing Web services externally through the firewall, access control for Web applications shall be supported based on the following, including but not limited to:

(1) Keywords in HTTP transmission content;

(2) HTTP request methods, including GET, POST, PUT, HEAD, etc.;

(3) HTTP request file types;

(4) Lengths of fields in the HTTP protocol header, including general header, request header, response header, etc.;

(5) HTTP uploaded file types;

(6) HTTP request frequency;

(7) HTTP response content, such as error messages/status codes returned by the server.

2.4.3.5 When the application scenario involves providing database-related services externally through the firewall, access control for databases shall be supported based on the following, including but not limited to:

(1) Applications and O&M tools accessing the database;

(2) Database username, database name, table name, and field name;

(3) SQL statement keywords and database response content keywords;

(4) Number of rows affected and number of rows returned.

2.4.3.6 When the application scenario involves providing file transfer or mail services externally through the firewall, control over protocols such as FTP, SMTP, POP3, and IMAP shall be supported based on the following, including but not limited to:

(1) Transferred file types;

(2) Transferred content, such as protocol commands or keywords.

2.4.4 Attack Protection

2.4.4.1 The ship network firewall shall be capable of resisting Denial of Service (DoS) attacks, including but not limited to:

(1) ICMP Flood attacks;

(2) UDP Flood attacks;

(3) SYN Flood attacks;

(4) Teardrop attacks;

(5) Land attacks;

(6) Oversized ICMP data attacks.

2.4.4.2 The ship network firewall shall be capable of detecting and recording scanning activities, including scans of protected networks.

2.4.5 Log Auditing

2.4.5.1 The ship network firewall shall be auditable, with the following requirements:

(1) Event types to be recorded:

① Attempts to log in to the management port of the ship network firewall and management authentication requests;

② All configuration operations on the ship network firewall system, including but not limited to IP address settings, route settings, addition/deletion/modification of management users, and security policy configurations;

③ Backup activities for log information;

④ Access requests matching security policies;

⑤ Detected attack behaviors.

(2) Log Content

① Protocol type, source address, destination address, source port, and destination port of the data packet;

② Time of access control occurrence;

③ Execution result of the access control policy that generated the log record;

④ Other information needing description for attack events;

⑤ Time of operation event occurrence;

⑥ The user who performed the operation and the result of the operation;

⑦ Log levels shall be set based on log content, including but not limited to debugging, information, warning, and error levels.

(3) Management

① Audit information such as records, logs, reports, settings, and tools shall be protected against unauthorized access and tampering;

② Tools for reviewing logs shall be provided, with the capability to retrieve audit events based on conditions such as time, date, subject identity, and object identity;

③ Management logs (showing management activities) and event logs (showing traffic activities) shall support writing to backup storage for periodic review;

④ Synchronizing logs, alarms, and other information to a log server via the SYSLOG protocol shall be supported;

⑤ Log storage shall support preservation in non-volatile storage media, with alarms issued when thresholds are reached.

Section 5 ADDITIONAL FUNCTIONAL REQUIREMENTS FOR LEVEL II SHIP NETWORK FIREWALLS

2.5.1 General Requirements

2.5.1.1 In addition to meeting the functional requirements for Level I ship network firewalls, Level II firewalls shall also meet the additional requirements in this section.

2.5.2 Networking and Deployment

2.5.2.1 Shipboard firewalls shall support redundant deployment (Active-Standby mode[①]), and redundancy failover shall not affect the operation of security functions.

2.5.3 Application Layer Control

2.5.3.1 The ship network firewall shall support custom protocols.

2.5.4 Configuration Management

2.5.4.1 Unified configuration management, monitoring, and O&M shall be supported.

Section 6 ADDITIONAL FUNCTIONAL REQUIREMENTS FOR LEVEL III SHIP NETWORK FIREWALLS

2.6.1 General Requirements

2.6.1.1 In addition to meeting the requirements for Level II firewalls, Level III firewalls shall also meet the additional requirements in this section.

2.6.2 Networking and Deployment

2.6.2.1 The ship network firewall shall support at least redundant deployment (Active-Active mode[②]) and meet the following:

(1) Redundancy failover shall not affect the operation of security functions;

(2) Real-time synchronization of firewall configurations (e.g., security policies, ACLs) and business session state information (e.g., network connection status) shall be maintained.

2.6.3 Boundary Protection

2.6.3.1 Firewalls used at ship network boundaries shall be configurable to ensure load balancing for network egress.

2.6.3.2 Firewalls used at ship network boundaries shall have certain traffic scrubbing capabilities to defend against DDoS attacks.

2.6.3.3 The confidentiality of information passing through any zone boundary shall be ensured.

Section 7 PERFORMANCE REQUIREMENTS

2.7.1 Performance Indicators

2.7.1.1 Performance parameters of the ship network firewall shall be specified, including at least throughput, latency and jitter, packet loss rate, maximum concurrent connections, and maximum connection rate.

2.7.1.2 Throughput performance indicators for ship boundary firewalls are as follows:

(1) Throughput

With a single permissive rule and zero packet loss, a pair of ports at their corresponding rates shall achieve the following bidirectional throughput targets:

① For 64-byte small packets, the throughput of a 100 Mbps firewall shall be no less than 30% of the line rate, and a 1 Gbps firewall shall be no less than 40% of the line rate;

② For 256-byte medium-long packets, a 100 Mbps firewall shall be no less than 70% of the line rate, and a 1 Gbps firewall shall be no less than 80% of the line rate;

[①] Active-Standby mode: One primary unit actively handles traffic while a secondary unit is on standby, automatically taking over in case of failure.
[②] Active-Active mode: Both primary units are active, sharing traffic load and providing mutual backup in case of failure.

③ For 512-byte long packets, a 100 Mbps firewall shall be no less than 90% of the line rate, and a 1 Gbps firewall shall be no less than 95% of the line rate.

(2) Latency

Under the condition of 90% throughput, the following shall be met:

① For 64-byte small, 256-byte medium-long, and 512-byte long packets, the average latency of a 100 Mbps firewall shall not exceed 1 ms;

② For 64-byte small, 256-byte medium-long, and 512-byte long packets, the average latency of a 1 Gbps firewall shall not exceed 200 μs.

(3) Maximum Concurrent Connections

① The maximum number of concurrent connections for a 100 Mbps industrial control firewall shall be no less than 60,000;

② The maximum number of concurrent connections for a 1 Gbps industrial control firewall shall be no less than 300,000.

(4) Maximum Connection Rate

① The maximum connection rate for a 100 Mbps firewall shall be no less than 1,500 connections/second;

② The maximum connection rate for a 1 Gbps firewall shall be no less than 5,000 connections/second.

CHAPTER 3 INSPECTION REQUIREMENTS FOR SHIP NETWORK FIREWALLS

Section 1 DRAWINGS AND DOCUMENTATION

3.1.1 Documents

3.1.1.1 When applying for approval/inspection of a ship network firewall, the documents listed in Table 3.1.1.1 shall be submitted to ISC.

List of Documents **Table 3.1.1.1**

No.	Document Name	Details	Remarks
1	Technical Specifications	Clarify product models and specifications, functional and performance indicators, usage restrictions, protection ratings, power conditions, software-related information, etc.	Ⓐ
2	Technical Schematics	--	Ⓐ
3	Product Outline Drawings	External dimensions, protection ratings, interface types and quantities, indicator markings and colors, etc.	Ⓐ
4	Manuals (Chinese and English)	Product hardware and software versions, descriptions of relevant functions and performance, product specifications (such as interfaces and environmental conditions), as well as product operation, installation, maintenance, and use.	Ⓘ
5	Nameplates (Chinese and English)	--	Ⓘ
6	Security Capability Statement	Refer to the requirements of 3.1.3.2 of the Guidelines for Ship Cyber Security.	Ⓐ
7	Security Configuration Guide	This document shall specify the recommended configurations and default values for security functions. The objective is to ensure that the implementation of security functions complies with UR E26 and all specifications of the system integrator (e.g., user accounts, authorization, password policies, device security status, firewall rules, etc.).	Ⓘ
8	Software Quality Plan	Clarify that the quality management system is applicable to the design, construction, delivery, and maintenance of the specific system to be delivered. Clarify the method for unique identification of the system, its various software modules, and different versions of the same software module throughout the system and software lifecycle.	Ⓘ
9	Change Management Procedure	Clarify the control procedures for the initial installation and subsequent updates of system software modules and cyber security configurations.	Ⓘ
10	Security Development Lifecycle Documentation	Refer to the requirements in Section 4, Chapter 2 of the Guidelines for Ship Cyber Security.	Ⓐ

No.	Document Name	Details	Remarks
11	Maintenance and Verification Plan	Maintenance content, verification methods, records, etc.	Ⓘ
12	Incident Response and Recovery Plan	Formulate plans for response, backup, recovery, etc.	Ⓘ
13	Configuration Check Report	Refer to the requirements of 3.1.3.2 of the Guidelines for Ship Cyber Security.	Ⓘ
14	Test Procedure	Covers environmental tests and cyber security tests, including test objects, standards, methods, processes, etc.	Ⓐ

Note: The symbols used in the table and their meanings are as follows:

Ⓐ Submitted for ISC approval; Ⓘ Submitted for ISC reference.

3.1.1.2 Product approval for ship network firewalls shall be conducted in accordance with the relevant requirements for product inspection in Chapter 3, Part 1 of the ISC Rules for Classification of Sea-going Steel Ships, with the following requirements:

(1) Type tests shall be conducted in a ISC cyber security laboratory or a ISC-recognized laboratory according to the environmental test and cyber security type test outline approved by ISC;

(2) Type tests for all applicable requirements shall be completed in accordance with Sections 2 and 3 of this chapter;

(3) Vulnerability scanning shall be performed during on-site tests. The manufacturer shall complete code auditing and robustness testing and provide reports for on-site review;

(4) The ship network firewall shall meet the corresponding technical requirements according to its application level and scenario in accordance with 1.1.2.1.

Section 2 PREPARATION FOR TESTING AND VERIFICATION

3.2.1 General Requirements

3.2.1.1 The manufacturer shall formulate a test outline for the ship network firewall in accordance with Chapter 2. The test content shall cover interfaces, functions, performance, and product security testing of the firewall, and shall describe the correspondence between the test items identified in the test documentation and the technical requirements of the firewall.

3.2.1.2 The test data packet size and test duration shall be specified before testing.

3.2.1.3 The product application scenarios shall be specified before testing.

3.2.2 Testing and Verification Environment

3.2.2.1 The functional testing of the ship network firewall shall consider the following two test environments.

(1) In Test Environment 1, as shown in Figure 3.2.2.1(1), the ship network firewall (EUT) connects two network zones, with access traffic as follows:

① External network clients accessing internal network servers;

② Internal network clients accessing external network servers.

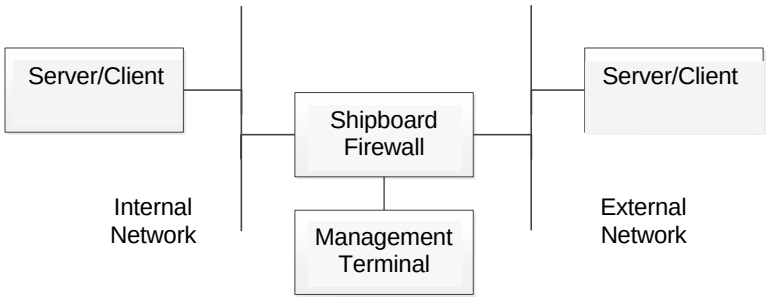


Figure 3.2.2.1(1) Test Environment 1

(2) In Test Environment 2, as shown in Figure 3.2.2.1(2), the ship network firewall (EUT) connects three network zones, with servers in the protected zone assigned to the DMZ. Access traffic is as follows:

① Internal network clients accessing external network servers;

② Internal network clients accessing DMZ servers;

③ External network clients accessing DMZ servers.

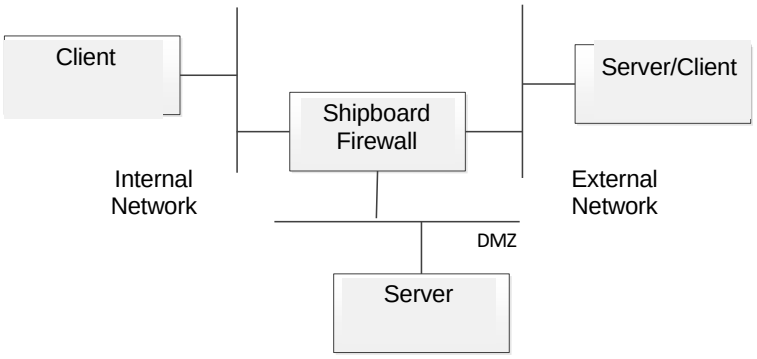


Figure 3.2.2.1(2) Test Environment 2

3.2.2.2 In the test environment, virtual clients/servers may be used to simulate data sources from multiple users or hosts, and the number of virtual clients/servers used in the test items shall be specified in the test report.

3.2.2.3 Dedicated performance testers may be used for the performance testing of the ship network firewall, with tester interfaces connected directly to the firewall's service interfaces.

3.2.2.4 To account for the impact of rule set size on the function and performance of the EUT, tests shall be conducted using rule sets of different sizes, and the rule under test shall be configured at the end of the rule set, not at the beginning.

3.2.2.5 Consider that when a request passes through a caching proxy, the proxy will attempt to serve the response from its cache. The ship network firewall shall be tested with any caching proxies disabled.

3.2.2.6 To account for the latency introduced by identity authentication, if a third-party device is used for authentication, the test environment shall include the authentication device.

Section 3 VERIFICATION REQUIREMENTS

3.3.1 Interface Testing

3.3.1.1 Observe whether the types and quantities of interfaces match the descriptions with reference to the product manual.

3.3.1.2 Test the communication connection status and functional integrity of corresponding

interfaces with reference to given data interface protocol standards/descriptions and interface functional specifications.

3.3.1.3 The physical interface protection status of the ship network firewall shall be tested in accordance with the test methods and requirements of Article 10.5.2.3 of IEC 61162-460.

3.3.1.4 Configure the ship network firewall's monitoring and alarm policies to generate alarm information. Capture the alarm information and verify its compliance and integrity.

3.3.2 Functional Verification

3.3.2.1 Functional verification shall be conducted in accordance with the relevant content of Chapter 2 of this Guideline. For the verification environment and technical requirements, refer to Table 3.3.2.1.

Verification Environment and Technical Requirements Table 3.3.2.1

No.	Verification Item	Verification Environment	Technical requirements
1	Networking and Deployment	Figure 3.2.2.1(1) Figure 3.2.2.1(2)	2.4.1、2.5.2、2.6.2
2	Network Layer Control	Figure 3.2.2.1(1) Figure 3.2.2.1(2)	2.4.2
3	Application Layer Control	Figure 3.2.2.1(1) Figure 3.2.2.1(2)	2.4.3
4	Attack Protection	Figure 3.2.2.1(1) Figure 3.2.2.1(2)	2.4.4
5	Log Auditing	Figure 3.2.2.1(1) Figure 3.2.2.1(2)	2.4.5
6	Configuration Management	Figure 3.2.2.1(1)	2.5.4
7	Boundary Protection	Figure 3.2.2.1(1) Figure 3.2.2.1(2)	2.6.3

3.3.3 Security Capability Verification

3.3.3.1 Security capability verification for the corresponding level shall be conducted in accordance with Table 1.1.2.1. For the verification environment and relevant requirements, refer to Table 3.2.3.1.

Security Capability Verification Environment and Technical Requirements Table 3.2.3.1

No.	Verification Item	Verification Environment	Technical requirements
1	Identification and Authentication	Figure 3.2.2.1(1)	2.3.1
2	Use control	Figure 3.2.2.1(1)	2.3.2
3	System Integrity	Figure 3.2.2.1(1)	2.3.3
4	Data confidentiality	Figure 3.2.2.1(1)	2.3.4
5	Restricted data flow	Figures 3.2.2.1(1) and (2)	2.3.5
6	Timely Response to Events	Figures 3.2.2.1(1) and (2)	2.3.6
7	Resource availability	Figures 3.2.2.1(1) and (2)	2.3.7
8	Software and Supporting Hardware	-	2.3.8

No.	Verification Item	Verification Environment	Technical requirements
9	Security Requirements	Figures 3.2.2.1(1) and (2)	2.3.9

3.3.4 Performance Testing

3.3.4.1 With reference to RFC 2544 or RFC 9411, a security testing device shall be used to send packets of different lengths to the EUT to test the throughput, latency and jitter, packet loss rate, and maximum concurrent connections of the ship network firewall, to verify whether the declared performance indicators are met. Ship boundary firewalls shall meet the indicator requirements of 2.7.1.2.

(1) Throughput

① The test shall include data packets with frame lengths of at least 64, 128, 256, 512, and 1518 bytes;

② Report output form: Results shall be presented in the form of tables or charts, identifying the theoretical and actual throughput under maximum load for different frame lengths.

(2) Latency and Jitter

① The test shall include data packets with frame lengths of at least 64, 128, 256, 512, and 1518 bytes;

② Report output form: Results shall be presented in the form of tables, identifying the minimum, average, and maximum latency under different frame lengths and loads.

(3) Packet Loss Rate

① The test shall include data packets with frame lengths of at least 64, 128, 256, 512, and 1518 bytes;

② Report output form: Results shall be presented in the form of tables, identifying the packet loss rate under different frame lengths and loads.

(4) Maximum Concurrent Connections / Maximum Connection Rate

① The test shall use a combination of business-related application traffic and shall record the application protocols and object sizes used in the test. The proportion of failed application events shall not exceed 0.001%;

② Report output form: Results shall be presented in the form of charts, where the horizontal axis shall indicate the test time, the vertical axis shall indicate the number of concurrent connections / new connection rate, and the maximum concurrent connections / maximum connection rate at steady state shall be marked.