指导性文件
GUIDANCE NOTES
GDXX

中　国　船　级　社

船舶网络防火墙检验指南

（修订稿）

2025

生效日期：202X 年 X 月 X 日

北京

目　　录

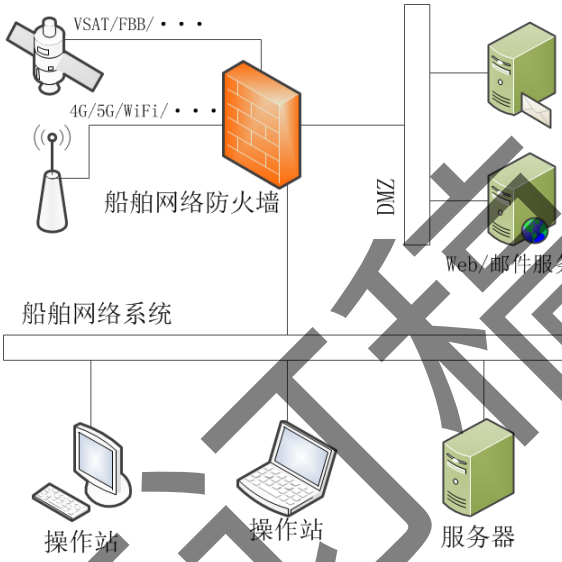
第 1 章 通则

第 1 节 一般规定

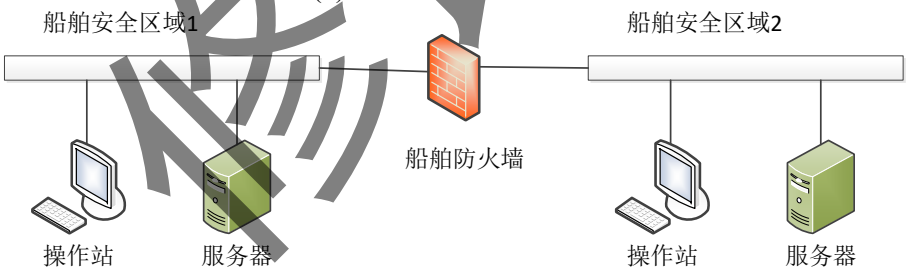
1.1.1 一般要求

1.1.1.1 本指南提出了船舶网络防火墙的通用性技术要求和产品检验要求，适用于申请中国船级社（China Classification Society, CCS）产品认可或检验的船舶网络防火墙设备。

1.1.1.2 船舶网络防火墙是指部署在船舶网络边界或船舶系统/区域间，阻隔不安全网络因素，保护船舶网络安全的一种设备，其应用场景示例如图 1.1.1.2 所示。



(1) 部署在船舶网络边界



(2) 部署在船舶安全区域边界

(3) 部署在船舶 CBS 内

图 1.1.1.2 船舶网络防火墙应用场景示例

1.1.2 船舶网络防火墙分级

1.1.2.1 船舶网络防火墙按照表 1.1.2.1 分为 3 个级别：

船舶网络防火墙分级 **表 1.1.2.1**

序号	级别	防御能力
1	I	对应《船舶网络安全指南》 SL0 要求或相应等级能力要求
2	II	对应《船舶网络安全指南》 SL1、SL2 要求或相应等级能力要求
3	III	对应《船舶网络安全指南》 SL3、SL4 要求或相应等级能力要求

1.1.3 持证要求

1.1.3.1 需在船舶网络边界和船舶安全区域边界使用的船舶网络防火墙，应向 CCS 提出书面申请，按照本指南要求在 CCS 或 CCS 认可/接受的试验机构进行测试验证，并按 CCS《钢质海船入级规范》第 1 篇第 3 章要求完成产品型式认可。在船舶 CBS 内的网络防火墙自愿申请，参考本指南实施。

1.1.4 数据提供与保密

1.1.4.1 CCS 对申请方提交的数据和信息按 CCS《钢质海船入级规范》第 1 篇第 2 章第 12 节的要求进行信息披露，知识产权及保密原则遵循 CCS《钢质海船入级规范》第 1 篇第 2 章第 1 节 3.1.10 的要求。

1.1.5 变更管理

1.1.5.1 对于通过 CCS 认可/检验的船舶网络防火墙，当其软件、设备部件等发生重要变更（包括但不限于软件版本重大升级，功能、性能的改变，操作流程的改变，设备部件的变更）时，申请方应通知 CCS，CCS 可要求重新评估，以确保其满足相关的技术要求。

1.1.6 规范性引用文件

1.1.6.1 相关文件中的条款通过本文件的引用将成为本文件的条款。凡是不注日期的引用文件，其最新版本适用于本文件。

引用文件列表　　表 1.1.6.1

序号	编号	文件名
1	R001-2025	《钢质海船入级规范》
2	GDXX-2025	《船舶网络安全指南》
3	GD008-2025	《船用软件安全及可靠性评估指南》
4	GD019-2024	《电气电子产品型式认可试验指南》
5	IACS UR E27	*Cyber resilience of on-board systems and equipment*
6	IEC 62443-1-1	*Industrial communication networks-network and system security-part 1-1: terminology, concepts and models*
7	IEC 62443-4-2	*Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components*
8	ISO/IEC 27033-4	*Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*
9	ISO/IEC 15408-2	*Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*
10	IEC 63154	*Maritime navigation and radiocommunication equipment and systems -Cybersecurity - General requirements, methods of testing and required test results*
11	IEC 61162-460	*Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security*
12	RFC 3511	*Benchmarking methodology for Firewall Performance*
13	RFC 2979	*Behavior of and Requirements for Internet Firewalls*

1.1.7 术语及缩略语

1.1.7.1 除另有规定外，本文件有关缩略语如下：

(1) DoS：拒绝服务（Denial of Services）

(2) MAC：介质访问控制（Media Access Control）

(3) DMZ：隔离区（Demilitarized Zone）

(4) NAT：网络地址转换（Network Address Translation）

(5) SNAT：源网络地址转换（Source NAT）

(6) DNAT：目的网络地址转换（Destination NAT）

(7) OPC：过程控制的对象链接与嵌入式接口协议（Object Linking and Embedding for Process Control）

(8) AES：高级加密标准（Advanced Encryption Standard）

(9) SYN：同步序列编号（Synchronize Sequence Numbers）

(10) SYSLOG：系统日志或一种进行日志传输的协议（System Log）

第 2 章 船舶网络防火墙技术要求

第 1 节 一般规定

2.1.1 一般要求

2.1.1.1 本章主要描述船舶网络防火墙的技术要求，包括接口要求、安全能力要求、功能要求和性能要求。

2.1.1.2 日志等数据安全应满足船旗国相关法律法规要求以及 CCS《船舶网络安全指南》第 4.3.20 条和 CCS《船舶数据质量评估指南》附录 8 的相关要求。

2.1.1.3 日志等数据出境应满足船旗国、入境国和出境国相关法律法规要求。

第 2 节 接口要求

2.2.1 物理接口

2.2.1.1 船舶网络防火墙的物理接口类型和数量应满足设备运行和维护的需要。以太网电口、光口等物理接口应满足相应的接口定义标准，专用物理接口应描述其规格。

2.2.1.2 各接口应描述其支持的所有接口功能。

2.2.1.3 管理、诊断和测试接口，及 USB 等可移动设备接口应采用物理防护和技术防护，防止非授权接入，其中技术防护包括逻辑阻塞、加密认证等。

2.2.2 数据接口

2.2.2.1 船舶网络防火墙应明确其接口支持的标准接口协议，当适用专用接口协议时，应提供详细的文档说明。

2.2.2.2 船舶网络防火墙应支持通过接口输出监测与报警信息。

第 3 节 安全能力要求

2.3.1 标识和鉴别

2.3.1.1 人员身份标识和鉴别

安全等级	要求
I	应能鉴别和标识所有直接或通过接口访问的人员用户，并能对通过不可信网络访问的人员采用多因素身份认证。
II	应能唯一标识和鉴别所有人员用户。
III	应能多因子鉴别和标识所有通过接口访问人员用户。

2.3.1.2 进程和设备标识和鉴别

安全等级	要求
I	应能对所有可直接或通过接口访问的进程和设备进行标识和鉴别。
II	
III	应能唯一标识和鉴别所有软件进程和设备。

2.3.1.3 账号管理

安全等级	要求
I	应能支持授权用户管理所有账号，包括添加、激活、修改、禁用和删除账号。
II	
III	

2.3.1.4 标识管理

安全等级	要求
I	应能通过用户、组、角色或系统接口支持标识管理。
II	
III	

2.3.1.5 鉴别管理

安全等级	要求
I	应具有以下能力： ① 初始化鉴别符（密码、令牌等）内容； ② 安装时要求修改所有鉴别符的默认值； ③ 周期性修改/更新所有鉴别符； ④ 在存储和传输时，保护所有鉴别符不受未经授权的披露和修改。
II	
III	应能通过硬件机制（如 TPM）实现增强保护鉴别符。

2.3.1.6 无线访问管理（如有无线模块时适用）

安全等级	要求
I	应能标识和鉴别所有使用无线通信的用户（人员、软件过程或设备）。
II	应能唯一标识和鉴别全部使用无线通信的用户（人员、软件进程或设备）。
III	

2.3.1.7 口令强度

安全等级	要求
I	应能强制执行基于最小长度和各种字符类型的可配置密码强度。
II	应具有以下能力： ① 应防止任何给定人员重复使用可配置的生成口令； ② 应能限制人员口令的最短和最长使用期限； ③ 在口令过期前，应提示用户在可配置时间内更改口令。
III	应能限制所有用户口令的最短和最长使用期限。

2.3.1.8 公钥基础设施（PKI）证书

安全等级	要求
I	不做要求
II	使用 PKI 时，防火墙应能根据最佳实践运行 PKI，或从现有 PKI 中获取公钥证书。
III	

2.3.1.9 公钥认证强度

安全等级	要求
I	不做要求
II	当采用公钥认证时，应能： ① 通过检查证书签名的有效性验证证书； ② 通过构建到一个接受的可信 CA 的证书路径来验证证书，或者在自签名证书的情况下，通过将子证书部署到所有与颁发证书的主体通信的主机来验证证书； ③ 通过检查给定证书的撤销状态来验证证书； ④ 建立用户(人员、软件进程或设备)对相应私钥的控制； ⑤ 将已验证的身份映射到用户(人员、软件进程或设备)。

	⑥ 公钥鉴别算法和密钥应根据国际公认和已证实的安全实践使用加密机制。
III	应能通过硬件机制保护私钥。

2.3.1.10 身份鉴别反馈

安全等级	要求
I	应能在认证过程中对鉴别反馈信息模糊处理。
II	
III	

2.3.1.11 失败登陆尝试

安全等级	要求
I	应具有以下能力： ① 在可配置的时间段内，强制设置任意用户（人、软件进程或设备）连续无效访问尝试的可配置数量的限制； ② 在指定的时间段内拒绝访问，或直到当该限制已经到期后由管理员解锁为止。管理员可以在超时期限到期之前解锁帐户。
II	
III	

2.3.1.12 系统使用告知

安全等级	要求
I	应具有在身份验证前显示系统使用提示信息的能力。信息应能由授权人员设置。
II	
III	

2.3.1.13 不可信网络访问

安全等级	要求
I	应具有以下能力： ① 防火墙支持的设备访问网络时应提供监视和控制通过不可信网络访问的所有方法的能力。 ② 应提供拒绝通过不可信网络访问请求的能力，除非得到船上指定角色的明确授权。
II	
III	

2.3.2 使用控制

2.3.2.1 授权实施

安全等级	要求
I	应能根据分配的责任和最小权限为所有经过识别和鉴别的人员提供授权执行机制。
II	应根据分配的责任和最小权限为所有用户（人员、软件进程和设备）提供授权执行机制；应能授权用户或角色，定义和修改所有人员或角色到权限的映射。
III	应支持管理员在可配置时间或事件期间，手动覆盖当前人员的授权；当某个操作可能严重影响船舶网络安全时，应支持双重许可确认。

2.3.2.2 无线使用控制

安全等级	要求
I	应根据普遍接受的安全行业惯例，授权、监测和限制无线连接的使用
II	
III	

2.3.2.3 便携式和移动设备的使用控制

安全等级	要求

I	当防火墙支持使用便携式和移动设备时，系统应包括以下功能： a）将便携式和移动设备的使用限制在设计允许的范围内； b）限制与便携式和移动设备之间的代码和数据传输。
II	
III	应能验证试图连接到某个区域的便携式或移动设备是否符合该区域的安全要求。

2.3.2.4 移动代码

安全等级	要求
I	应具有以下能力： a）控制移动代码的执行； b）控制哪些用户（人员、软件进程或设备）被允许向防火墙或从防火墙传输代码； c）在代码执行之前基于对移动代码进行完整性校验控制代码执行。
II	
III	应在允许代码执行之前，验证移动代码的完整性，并基于鉴别检查结果控制移动代码的执行。

2.3.2.5 会话锁定

安全等级	要求
I	应具备会话锁定能力，在可配置的非活跃时间段后自动或手动启动。会话锁定将通过用户或其他授权用户重新进行身份验证建立访问。
II	
III	

2.3.2.6 远程会话终止

安全等级	要求
I	应能在可配置的非活动时间段后自动终止远程会话，或由启动会话的用户手动终止远程会话
II	
III	

2.3.2.7 并行会话控制

安全等级	要求
I	不做要求
II	应能在会话中限制每个接口的并发会话数量，该并发数可配置。
III	

2.3.2.8 可审计事件

安全等级	要求
I	应至少为以下事件生成与安全相关的审计记录：访问控制、操作系统事件、备份和恢复事件、配置更改、通信中断。
II	
III	

2.3.2.9 可审计日志存储容量

安全等级	要求
I	应能根据公认的日志管理建议分配审计记录存储容量。应实施审计机制，以降低超过该容量的可能性.
II	
III	当分配的审计记录存储达到最大审计记录存储容量的可配置百分比时，应能发出警报。

2.3.2.10 审计处理失败响应

安全等级	要求
I	应能在审计处理失败的情况下，根据公认的行业惯例和建议，支持采取适当措施以应对审计处理失败事件。
II	
III	

2.3.2.11 时间戳

安全等级	要求
I	应能提供用于生成审计记录的时间戳。
II	应能以一定的频率同步内部系统时钟，该频率可配置。
III	应保护时间源不受未经授权的更改，并应在更改时生成审计事件。

2.3.3 **系统完整性**

2.3.3.1 通信完整性

安全等级	要求
I	应能保护传输数据的完整性。
II	应具备在通信期间验证信息的能力。
III	

2.3.3.2 恶意代码防护

安全等级	要求
I	应能实施适当的保护措施，以防止、检测和减轻恶意代码或未授权软件造成的影响，并具有更新保护机制的功能。
II	
III	

2.3.3.3 安全功能验证

安全等级	要求
I	应支持验证安全功能按照预期运行，并报告在维护期间出现的异常。
II	
III	在正常运行过程中，应支持安全功能的自动验证。

2.3.3.4 软件和信息完整性

安全等级	要求
I	应能对固件、配置和其他信息进行完整性检查，并记录和报告检查结果。
II	应能对固件、配置和其他信息进行真实性校验，并对校验结果进行记录和报告。
III	执行完整性校验过程中，应能检测未经授权的更改行为，并对防火墙发送告警通知。

2.3.3.5 输入有效性验证

安全等级	要求
I	应验证所有用于控制或直接影响防火墙安全防护配置的输入数据的语法、长度和内容。
II	
III	

2.3.3.6 确定性输出

安全等级	要求
I	如果由于攻击导致防火墙无法维持正常运行，系统应将输出设置为预定状态。预定状态可以是： -无动力状态 -最后已知值 -固定值
II	
III	

2.3.3.7 会话完整性

安全等级	要求
I	应能保护会话的完整性，拒绝任何无效会话 ID 的使用。
II	应提供保护通信会话完整性的机制，包括：

III	a）在用户注销或因其他会话终止时(包括浏览器会话)，应使会话 ID 失效; b）应为每个会话生成唯一的会话 ID，并仅识别系统生成的会话 ID; c）应能利用普遍接受的方式随机性生成唯一会话 ID。

2.3.3.8 审计信息保护

安全等级	要求
I	应能保护审计信息、审计日志，防止未授权情况下的访问、修改和删除。
II	
III	应提供在强制一次性写入硬件介质中存储审计记录的能力。

2.3.3.9 更新支持

安全等级	要求
I	应支持在生命周期内的更新和升级。应具备适当的机制支持更新和升级过程中不会影响船舶的基本功能。
II	应支持安装之前验证任何更新的真实性和完整性。
III	

2.3.3.10 物理防篡改和检测

安全等级	要求
I	不做要求。
II	应能检测和防止未经授权的物理访问和篡改。
III	对物理篡改实施自动检测和监控，记录并报告给授权人员。

2.3.3.11 产品供应商的信任根

安全等级	要求
I	不作要求
II	应能保护产品供应商信任根（密钥和被用作信任根的数据）的机密性、完整性和真实性。
III	

2.3.3.12 资产所有者的信任根

安全等级	要求
I	不作要求
II	应能保护资产所有者信任根（密钥和被用作信任根的数据）的机密性、完整性和真实性，且不依赖于防火墙安全区域之外的组件。
III	

2.3.3.13 启动过程完整性

安全等级	要求
I	应在防火墙启动之前，对启动过程中所需的固件、软件和配置数据进行完整性校验。
II	应在防火墙启动前，对其产品供应商的信任根进行校验。
III	

2.3.4 数据保密性

2.3.4.1 信息保密性

安全等级	要求
I	应能保护支持显式读取授权的存储信息和传输中信息的机密性。
II	
III	

2.3.4.2 信息持久性

安全等级	要求

I	不做要求。
II	组件退役或服务释放时应能清除所有相关读授权的信息。
III	应能防止通过易失性共享内存资源进行未授权和非计划的信息传输。

2.3.4.3 使用加密

安全等级	要求
I	不做要求。
II	应能检测和防止未经授权的物理访问和篡改。
III	对物理篡改实施自动检测和监控，记录并报告给授权人员。

2.3.5 受限数据流

2.3.5.1 区域边界保护

安全等级	要求
I	应能在区域边界监视和控制通信。
II	应默认拒绝所有网络流量通过区域边界，例外允许通过的流量除外。
III	对物理篡改实施自动检测和监控，记录并报告给授权人员。

2.3.5.2 用户通信限制

安全等级	要求
I	应能识别和阻止违反安全策略的通信，如社交媒体内容、图像传输等。
II	
III	

2.3.6 事件的及时响应

2.3.6.1 （1）审计日志可访问性

安全等级	要求
I	应支持授权人员和/或工具以只读方式访问审计日志。
II	
III	应能使用应用程序编程接口（API）提供对审计记录的程序化访问。

2.3.6.2 持续监控

安全等级	要求
I	不做要求。
II	应使用普遍接受的安全行业实践和建议，持续监控所有安全机制的性能，以及时发现、表征和报告安全漏洞。
III	

2.3.7 资源可用性

2.3.7.1 抗拒绝服务攻击

安全等级	要求
I	应能在 DoS 事件期间维持重要功能。
II	应能减轻信息和/或消息泛滥类型的 DoS 事件影响。
III	

2.3.7.2 资源管理

安全等级	要求
I	应能通过安全功能限制资源的使用，防止资源耗尽。
II	
III	

2.3.7.3 系统备份

安全等级	要求
I	应支持重要文件的标识和存放，以及用户级和系统级信息（包括系统状态信息）的备份，备份过程不影响正常运行
II	应在恢复操作之前，验证备份信息的完整性。
III	

2.3.7.4 控制系统恢复和重建

安全等级	要求
I	应能在中断或故障后恢复并重建到已知的安全状态。
II	
III	

2.3.7.5 应急电源

I	控制系统应能在不影响现有安全状态或确定的降级模式的情况下切换至应急电源。
II	
III	

2.3.7.6 网络和安全配置设置

安全等级	要求
I	应能根据供应商推荐的网络和安全配置进行系统设置，并为当前部署的网络和安全配置设置提供接口。
II	
III	应能生成安全配置报告，可采用 CSV、JSON、XML 等格式。

2.3.7.7 最小功能

安全等级	要求
I	以下各项目的安装、可用性和访问权限应仅限于系统功能的严格需求： -操作系统软件组件、流程和服务 -网络服务、端口、协议、路由、主机访问以及任何软件
II	
III	

2.3.7.8 系统组件清单

安全等级	要求
I	不做要求。
II	应能够记录已安装组件及其关联属性的列表。
III	

2.3.8 软件和支撑硬件

2.3.8.1 船舶网络防火墙的研制应符合制造商的质量体系。

2.3.8.2 船舶网络防火墙应能在 CCS《钢质海船入级规范》第 4 篇第 1 章第 2 节所述环境、电压和频率波动等工作条件下正常工作。当防火墙作为船载系统的部件/组件时，还应满足 CCS《钢质海船入级规范》相应的要求（如有时）。

2.3.8.3 船舶网络防火墙的硬件设计、制造与安装应符合 CCS《钢质海船入级规范》第 4 篇第 1 章第 3 节的适用要求。

2.3.8.4 当船舶网络防火墙的硬件~~载体~~有规定的技术要求时，除满足本文件要求外，还应满足支撑硬件有关规定的技术要求。

2.3.8.5 船舶网络防火墙宜采用自然散热，无风扇方式设计。

2.3.8.6 应参考 CCS《智能设备检验指南》表 7.3 确定防火墙运行环境类型（一般为 A1

至 C2），应能够适应船舶运行环境（高温、潮湿、振动等），能在中国船级社《钢质海船入级规范》第 7 篇第 2 章第 1 节的要求环境条件和工作条件下可靠地工作。

2.3.9 **安全要求**

2.3.9.1 船舶网络防火墙应具备所声明的功能，并确保产品自身安全性，不应存在恶意代码、已知漏洞等安全风险。

2.3.9.2 应采用“最小特权”原则，默认拒绝所有入站流量，只允许规则授权的流量通过。

2.3.9.3 应能在启动前验证启动过程所需的固件、软件和可配置数据的完整性。

2.3.9.4 船舶网络防火墙人机交互界面应能告知以下信息：

(1) 只有授权用户才能访问系统；

(2) 提示可能会监控并跟踪未授权使用行为；

(3) 使用该系统表示同意监控和记录。

2.3.9.5 船舶网络防火墙应能传输流量、带宽、异常状态等报警信息，并在报警状态改变时及时更新。

2.3.9.6 船舶网络防火墙在异常条件（比如掉电、强行关机）关机再重新启动后，应满足如下要求：

(1) 安全策略恢复到关机前的状态；

(2) 日志信息不会丢失或覆盖；

(3) 帐户应重新鉴别。

2.3.9.7 当船舶网络防火墙异常断电时，应根据应用场景使船舶网络防火墙内部接口与外部接口直接物理连通或断开，并及时告警，应用场景动作机制参考如下：

(1) 用于船舶网络边界防护的防火墙宜在设备失效后使内外部接口保持断开；

(2) 用于船舶系统/区域间防护或系统层级间的防火墙宜在设备失效后使内外部接口直接连通。

2.3.9.8 船舶网络防火墙的硬件或软件等故障应不影响受保护的重要系统的重要服务。

2.3.9.9 船舶网络防火墙宜支持多种工作模式，保证船舶网络防火墙在部署、维护和工作过程中对被防护系统的最小影响。

2.3.9.10 船舶网络防火墙的底层支撑系统应满足以下要求：

(1) 不提供多余的网络服务；

(2) 不含任何导致产品权限丢失、拒绝服务等中高风险的漏洞。

2.3.9.11 应制定安装、升级及运维等操作的指导性文件，远程维护时还应满足 CCS《船舶网络安全指南》第 4.3.16 条的要求。

2.3.9.12 应参照 CCS《船舶网络安全指南》第 4.3.21 和 4.3.22 条要求制定事件响应及恢复计划。

第 4 节 I 级船舶网络防火墙功能要求

2.4.1 组网与部署

2.4.1.1 船舶网络防火墙应支持路由转发和透明传输，也可支持代理。

2.4.2 网络层控制

2.4.2.1 船舶网络防火墙应支持包过滤，安全策略应满足以下要求：

(1) 应使用最小权限原则，即除非明确允许，否则就禁止；

(2) 应包含基于源 IP 地址、目的 IP 地址的访问控制；

(3) 应包含基于 MAC 地址的访问控制；

(4) 应包含基于源端口、目的端口的访问控制；

(5) 应包含基于协议类型的访问控制；

(6) 应支持用户自定义的安全策略，安全策略可以是 MAC 地址、IP 地址、端口的部分或全部组合；

2.4.2.2 船舶网络防火墙应支持网络地址转换（NAT）功能，具体技术要求如下：

(1) 支持双向 NAT：SNAT 和 DNAT；

(2) SNAT 可实现“多对一”地址转换，使得内部网络主机访问外部网络时，其源 IP 地址被转换；

(3) DNAT 可实现“一对多”地址转换，将内部网络或 DMZ 的 IP 地址/端口映射为外部网络合法 IP 地址/端口，使外部网络主机通过访问映射地址和端口实现对内部网络或 DMZ 服务器的访问。

2.4.2.3 船舶网络防火墙应具备连接状态检测功能，支持基于状态检测技术的访问控制。

2.4.2.4 船舶网络防火墙应具备动态开放端口功能，如 OPC、FTP 协议。

2.4.2.5 船舶网络防火墙应支持自动或管理员手动绑定 IP/MAC 地址，应能够检测 IP/MAC 地址盗用，拦截盗用 IP/MAC 地址的主机经过船舶网络防火墙的各种访问。

2.4.3 应用层控制

2.4.3.1 应支持基于用户认证的网络访问控制功能，至少包括本地用户认证。

2.4.3.2 船舶网络防火墙应能识别并控制通用应用层协议及专用协议，具体技术要求如下：

(1) 应支持 HTTP、FTP、Telnet 等常见通用应用层协议；

(2) 应支持船舶网络系统涉及的常用工业控制协议，例如 OPC、Modbus、Profinet 等。

2.4.3.3 当使用场景包含通过防火墙对外提供 Web 服务时，应支持基于以下内容对 Web 应用的访问进行控制，包括但不限于：

(1) HTTP 传输内容的关键字；

(2) HTTP 请求方式，包括 GET、POST、PUT、HEAD 等；

(3) HTTP 请求文件类型；

(4) HTTP 协议头中各字段长度，包括 general header、request header、response header 等；

(5) HTTP 上传文件类型；
(6) HTTP 请求频率；
(7) HTTP 返回的响应内容，如服务器返回的出错信息等。

2.4.3.4 当使用场景包含通过防火墙对外提供数据库相关服务时，应支持基于以下内容对数据库的访问进行控制，包括但不限于：
(1) 访问数据库的应用程序、运维工具；
(2) 数据库用户名、数据库名、数据表名和数据字段名；
(3) SQL 语句关键字、数据库返回内容关键字；
(4) 影响行数、返回行数。

2.4.3.5 当使用场景包含通过防火墙对外提供文件传输或邮件服务时，应支持基于以下内容对 FTP、SMTP、POP3 和 IMAP 等应用进行控制，包括但不限于：
(1) 传输文件类型；
(2) 传输内容，如协议命令或关键字。

2.4.4 攻击防护

2.4.4.1 船舶网络防火墙应具有抗拒绝服务攻击（抗 DoS）的能力，至少抵抗以下攻击（包括，但不限于）：
(1) ICMP Flood 攻击；
(2) UDP Flood 攻击；
(3) SYN Flood 攻击；
(4) TearDrop 攻击；
(5) Land 攻击；
(6) 超大 ICMP 数据攻击。

2.4.4.2 船舶网络防火墙应能够检测和记录扫描行为，包括对受保护网络的扫描。

2.4.5 日志审计

2.4.5.1 船舶网络防火墙应可审计，要求如下：
(1) 记录事件类型
① 试图登录船舶网络防火墙管理端口和管理身份鉴别请求；
② 对船舶网络防火墙系统所有配置操作，包括但不限于 IP 地址设置，路由设置，管理用户的增加、删除、修改，安全策略的配置等；
③ 日志信息的备份等；
④ 安全策略匹配的访问请求；
⑤ 检测到的攻击行为；
(2) 日志内容
① 数据包的协议类型、源地址、目标地址、源端口和目标端口；
② 访问控制发生的时间；
③ 产生日志记录的访问控制策略执行结果；
④ 攻击事件其他需要描述的信息；
⑤ 操作事件发生的时间；
⑥ 执行操作的用户、执行操作的结果；
⑦ 应根据日志内容设置日志级别，包括但不限于调试、信息、警告、错误等多个级别

(3) 管理

① 记录、日志、报告、设置和工具等审计信息应受到保护，防止未经授权的访问和篡改；

② 应提供能查阅日志的工具，具备对审计事件以时间、日期、主体标识、客体标识等条件检索的能力；

③ 管理日志（显示管理活动）和事件日志（显示流量活动）应支持写入备用存储以备定期审查；

④ 日志应采用 SYSLOG 协议存储或兼容格式进行存储；

⑤ 至少保存一个检验周期的日志记录，以备查。

第 5 节 II 级船舶网络防火墙附加功能要求

2.5.1 组网与部署

2.5.1.1 船用防火墙应支持冗余部署模式（主备模式），应支持堆叠、M-LAG 跨设备链路聚合等冗余技术。

2.5.1.2 船用防火墙应具有硬件冗余，如双电源、双核心、双板卡等。

2.5.2 应用层控制

2.5.2.1 船舶网络防火墙应能支持自定义协议。

2.5.3 配置管理

2.5.3.1 应支持统一配置管理。

第 6 节 III 级船舶网络防火墙附加功能要求

2.6.1 组网与部署

2.6.1.1 船用防火墙应支持冗余部署模式（双活模式），应能满足：

(1) 业务切换应不影响安全功能的运行。

(2) 应能保持防火墙配置（如安全策略、访问控制列表等）与业务会话状态信息（如网络连接状态等）实时同步。

2.6.2 边界防护

2.6.2.1 用于船舶网络边界的防火墙应能进行相应的配置保障网络出口的负载均衡功能。

2.6.2.2 用于船舶网络边界的防火墙应能具有一定的流量清洗功能抵御 DDOS 攻击。

2.6.2.3 应能保护通过任何区域边界的信息的保密性。

第 7 节 性能要求

2.7.1 性能指标

2.7.1.1 应说明船舶网络防火墙的性能参数，至少包括吞吐量、时延与抖动、丢包率、

最大并发数等。

第 3 章 船舶网络防火墙检验要求

第 1 节 图纸资料

3.1.1 文件资料

3.1.1.1 申请船舶网络防火墙认可/检验时，应根据表 3.1.1.1 向 CCS 提交所列资料。

提交资料 **表 3.1.1.1**

序号	文件名称	说明	备注
1	技术规格书	阐明产品型号规格、功能和性能指标、使用限定、防护等级、电源条件、软件相关信息等	Ⓐ
2	技术原理图	--	Ⓐ
3	产品外形图	外形尺寸、防护等级、接口类型与数量、指示灯标识及其颜色等	Ⓐ
4	说明书（中英文）	产品硬件和软件版本、相关功能及性能描述， 产品规格说明，如接口、环境条件等，以及产品操作、安装、维护和使用	Ⓘ
5	铭牌（中英文）	--	Ⓘ
6	安全能力说明	--	Ⓐ
7	安全配置指南	该文件应说明安全功能的建议配置及默认值，目标是确保安全功能的实施符合 UR E26 和系统集成商的所有规范（如用户帐户、授权、密码策略、 设备的安全状态、防火墙规则等）	Ⓘ
8	软件质量计划	阐明质量管理体系适用于将要交付的具体系统的设计、施工、交付和维护。 阐明在系统和软件整个生命周期内对系统及其不同软件模块和同一软件模块的不同版本进行唯一标识的方法。	Ⓘ
	变更管理程序	阐明系统软件模块、网络安全配置的初始安装和后续更新的控制程序。	Ⓘ
9	安全开发生命周期文件	对安全开发生命周期的要求说明供应商的流程和控制措施。应说明软件更新与补丁情况	Ⓐ
11	维护和验证计划	维护内容、验证方式、记录等	Ⓘ
12	事件响应及恢复计划	制定响应、备份、恢复等计划方案	Ⓘ
13	配置核查报告		Ⓘ
14	型式试验大纲	测试对象、标准、方法、流程等	Ⓐ

注：表中采用的符号及其含义如下:
Ⓐ提交 CCS 批准　　Ⓘ提交 CCS 备查

3.1.1.2 船舶网络防火墙的产品认可应按照 CCS《钢质海船入级规范》第 1 篇第 3 章产品检验的相关要求执行，并有如下要求：

(1) 按 CCS 批准的网络安全型式试验大纲，在 CCS 网络安全实验室或经 CCS 认可的实验室进行型式试验；

(2) 应按照本章第 2 节和第 3 节的要求完成所有适用要求的型式试验；

(3) 应进行漏洞扫描、代码审计、健壮性测试和渗透测试对设备进行安全性测试并提供报告。

3.1.1.3 船舶网络防火墙应根据申请等级和适用场景满足对应的技术要求：

(1) Ⅰ级船舶网络防火墙应满足第 2 章 2.1、2.2、2.3 对应等级、2.4 以及 2.7 节的要求；

(2) Ⅱ级船舶网络防火墙除满足（1）中所有要求外，还应满足 2.5 节要求；

(3) Ⅲ级船舶网络防火墙除满足（1）（2）要求外，还应满足 2.6 节要求；

(4) 应根据适用场景和服务满足第 2.4.3、2.4.4 和 2.6.2 节对应要求。

第 2 节 测试验证准备

3.2.1 一般要求

3.2.1.1 制造商应根据第 2 章要求编制船舶网络防火墙测试大纲，测试内容涵盖船舶网络防火墙的接口、功能、性能以及产品安全性测试，并描述测试文档中标识的测试项与船舶网络防火墙技术要求的对应性。

3.2.1.2 测试前应明确测试数据包大小和测试持续时间。

3.2.1.3 测试前应明确产品的应用场景。

3.2.2 测试验证环境

3.2.2.1 船舶网络防火墙的功能测试应考虑如下两种测试环境。

(1) 图 3.2.2.1（1）所示测试环境 1 中，船舶网络防火墙（被测设备）连接两个网络区域，访问流量如下：

① 外网客户端访问内网服务器；

② 内网客户端访问外网服务器。

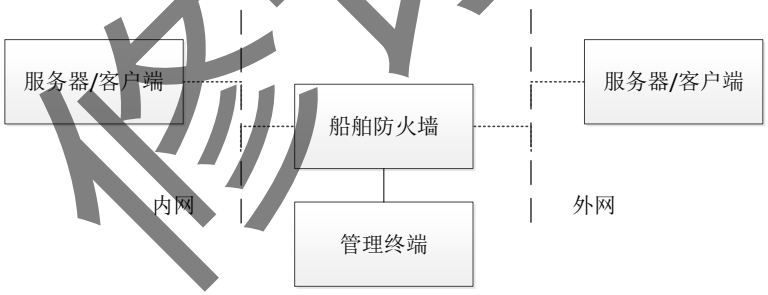


图 3.2.2.1（1）测试环境 1

(2) 图 3.1.2.1（2）所示测试环境 2 中，船舶网络防火墙（被测设备）连接三个网络区域被保护区域的服务器划分至 DMZ 区域，访问流量如下：

① 内网客户端访问外网服务器；

② 内网客户端访问 DMZ 服务器；

③ 外网客户端访问 DMZ 服务器。

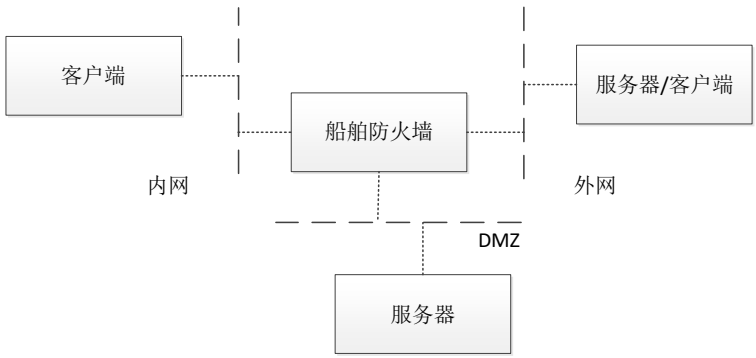


图 3.2.2.1（2）测试环境 2

3.2.2.2 测试环境中可采用虚拟客户端/服务器模拟多个用户或主机的数据源，并在测试报告中说明测试项目中虚拟客户端/服务器的数量。

3.2.2.3 船舶网络防火墙的性能测试可采用专用性能测试仪，测试仪接口直接连接防火墙业务接口。

3.2.2.4 考虑规则集大小对被测设备功能和性能的影响，测试中应采用不同规模的规则集完成测试，且被测规则应配置在规则集末尾而不是开头。

3.2.2.5 考虑当请求通过缓存代理时，缓存代理会尝试从其缓存提供响应服务。船舶网络防火墙应在禁用任何缓存代理的情况下执行测试。

3.2.2.6 考虑身份认证产生的延迟时间，当采用第三方设备进行身份认证时，测试环境中应包括身份认证设备。

第 3 节 测试验证要求

3.3.1 接口测试

3.3.1.1 参照产品说明文档，观察接口类型和数量是否与描述相符合。

3.3.1.2 参照给定的数据接口协议标准/描述文档、接口功能说明，测试对应接口的通信连接情况以及功能完整性。

3.3.1.3 船舶网络防火墙的物理接口防护状态应依据 IEC 63154 第 13.3 条的测试方法和要求进行测试。

3.3.1.4 配置船舶网络防火墙监测与报警策略并产生报警信息，捕获报警信息，验证报警信息的合规性和完整性。

3.3.2 功能验证

3.3.2.1 应根据 3.1.1.3 进行功能验证，验证环境及技术要求参考表 3.2.3.1 所示。

验证环境及技术要求 **表 3.2.3.1**

序号	验证项目	验证环境	技术要求
1	组网与部署	图 3.2.2.1（1） 图 3.2.2.1（2）	2.4.1、2.5.1、2.6.1
2	网络层控制	图 3.2.2.1（1） 图 3.2.2.1（2）	2.4.2

3	应用层控制	图 3.2.2.1（1） 图 3.2.2.1（2）	2.4.3、2.5.2
4	攻击防护	图 3.2.2.1（1） 图 3.2.2.1（2）	2.4.4
5	日志审计	图 3.2.2.1（1） 图 3.2.2.1（2）	2.4.5
6	配置管理	图 3.2.2.1（1）	2.5.3
7	边界防护	图 3.2.2.1（1） 图 3.2.2.1（2）	2.6.2

3.3.3 安全能力验证

3.3.3.1 应按照表 1.1.1.5 进行对应等级的安全能力验证。验证环境及相关要求参考表 3.2.4.1 所示。

安全能力验证环境及技术要求　　表 3.2.4.1

序号	验证项目	验证环境	技术要求
1	标识与鉴别	图 3.2.2.1（1）	2.3.1
2	使用控制	图 3.2.2.1（1）	2.3.2
3	系统完整性	图 3.2.2.1（1）	2.3.3
4	数据保密性	图 3.2.2.1（1）	2.3.4
5	受限数据流	图 3.2.2.1（1）（2）	2.3.5
6	事件的及时响应	图 3.2.2.1（1）（2）	2.3.6
7	资源可用性	图 3.2.2.1（1）（2）	2.3.7
8	软件和支撑硬件	-	2.3.8
9	安全要求	图 3.2.2.1（1）（2）	2.3.9

3.3.4 性能测试

3.3.4.1 应参考 RFC2544 或 RFC9411 使用安全测试设备对被测设备进行不同长度数据包发包，测试船舶网络防火墙的吞吐量、时延抖动、丢包率、最大并发数，验证是否满足声明的性能指标。

（1） 吞吐量

① 测试应至少包括 64、128、256、512、1518 字节的帧长度数据包，也可采用帧大小混合测试，结合现场环境和业务需求设置混合帧比例。

② 报告输出形式：结果应使用表格的形式表示，标识出不同帧长最大负载下的理论吞吐量和实际吞吐量。

（2） 时延与抖动

① 测试应至少包括 64、128、256、512、1518 字节的帧长度数据包，也可采用帧大小混合测试，结合现场环境和业务需求设置混合帧比例。

② 报告输出形式：结果应使用表格的形式表示，标识出不同帧长不同负载下的最小时延、平均时延和最大时延。

（3） 丢包率

① 测试应至少包括 64、128、256、512、1518 字节的帧长度数据包，也可采用帧大小混合测试，结合现场环境和业务需求设置混合帧比例。

② 报告输出形式：结果应使用表格的形式表示，标识出不同帧长不同负载下的丢包率。

（4） 最大并发数

① 测试应使用业务相关的应用流量组合，并记录测试使用的应用协议及对象大

小，失败的应用事件应不高于 0.001%；

② 报告输出形式：结果应使用图表的形式表示，其中横轴应标出测试时间，纵轴应标注并发数，标注出平稳状态最大并发数。