指导性文件
GUIDANCE NOTES
GD22-2023

中　国　船　级　社

船舶网络防火墙检验指南

2023

生效日期：2023 年 5 月 1 日

北京

目　　录

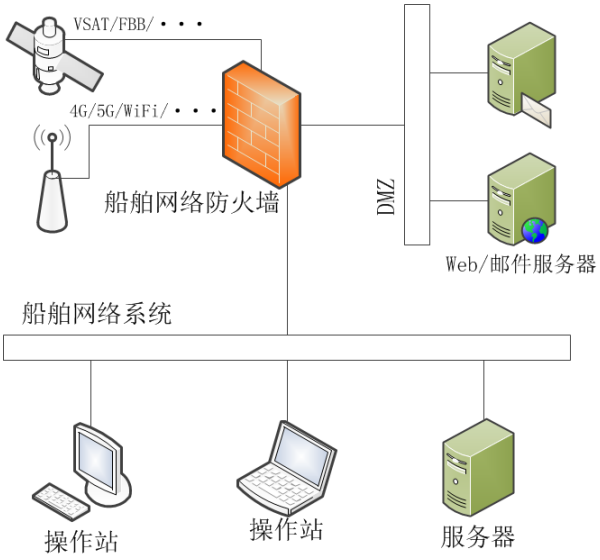
第 1 章 通则

第 1 节 一般规定

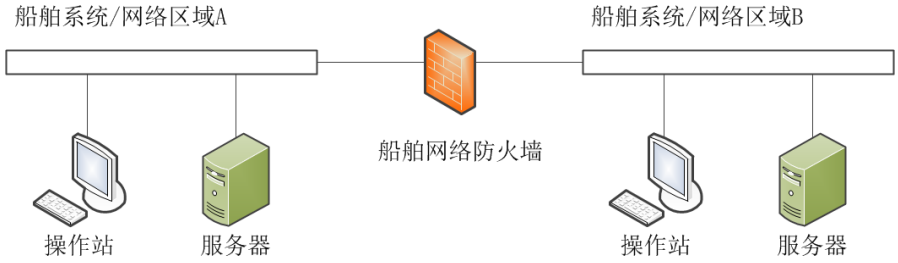
1.1.1 一般要求

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测试验证要求，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) 部署在船舶系统/区域之间

(3) 部署在监控系统网络与控制系统网络之间

图 1.1.1.2 船舶网络防火墙应用场景示例

1.1.2 持证要求

1.1.2.1 需在船舶上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 章要求完成型式认可。

1.1.3 数据提供与保密

1.1.3.1 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。

1.1.4 变更管理

1.1.4.1 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。

1.1.5 规范性引用文件

1.1.5.1 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 1.1.5.1

序号	编号	文件名
1		《钢质海船入级规范》
2	GD25-2019	《船舶网络系统要求及安全评估指南》
3	GD13-2017	《船用软件安全及可靠性评估指南》
4	GD22-2015	《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*

1.1.6 术语及缩略语

1.1.6.1 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) IP：网际协议（Internet Protocol）

(3) MAC：介质访问控制（Media Access Control）

(4) DMZ：非军事化区/隔离区（Demilitarized Zone）

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

(6) SNAT：源网络地址转换（Source NAT）

(7) DNAT：目的网络地址转换（Destination NAT）

(8) FTP：文本传输协议（File Transfer Protocol）

(9) 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）

(10) SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）
(11) IMAP：网络消息访问协议（Internet Message Access Protocol）
(12) AES：高级加密标准（Advanced Encryption Standard）
(13) SYN：同步序列编号（Synchronize Sequence Numbers）
(14) UDP：用户数据报协议（User Datagram Protocol）
(15) ICMP：网间控制报文协议（Internet Control Messages Protocol）
(16) 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、功能要求、性能要求，以及产品自身的安全要求。

2.1.1.2 船舶网络防火墙至少应满足以下若干需求：

(1) 网络隔离和分段（必选）；
(2) 隐藏内部网络结构（必选）；
(3) 访问控制（必选）；
(4) 数据加密传输（必选）；
(5) 抗 DoS 攻击（必选）；
(6) 流量限制和分析；
(7) 身份识别。

2.1.1.3 日志等数据安全应满足 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。

2.1.1.4 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/或技术防护，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 功能要求

2.3.1 组网与部署

2.3.1.1 船舶网络防火墙应支持透明传输、路由转发和代理。

2.3.1.2 宜支持冗余部署模式。

2.3.2 网络层控制

2.3.2.1 船舶网络防火墙应支持包过滤，具体技术要求至少应满足如下：

(1) 安全策略应使用最小权限原则，即除非明确允许，否则就禁止；

(2) 安全策略应包含基于源 IP 地址、目的 IP 地址的访问控制；

(3) 安全策略应包含基于源端口、目的端口的访问控制；

(4) 安全策略应包含基于协议类型的访问控制；

(5) 安全策略可包含基于 MAC 地址的访问控制；

(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。

2.3.2.2 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) 宜支持双向 NAT：SNAT 和 DNAT；

(2) SNAT 至少可实现“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 至少可实现“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。

2.3.2.3 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。

2.3.2.4 船舶网络防火墙宜具备动态开放端口功能，至少支持 OPC、FTP 协议。

2.3.2.5 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。

2.3.2.6 船舶网络防火墙应支持流量会话管理，能够设置单 IP 的最大会话数，防止非合规/过多连接影响网络性能。

(1) 会话管理，船舶网络防火墙应支持手动或在会话处于非活跃一定时间后自动锁定或终止会话；

(2) 流量监测，部署在不同区域间的船舶网络防火墙应具备流量统计功能：

① 能够通过 IP 地址、网络服务、时间和协议类型等参数或它们的组合对流量进行正确的统计；

② 能够实时或者以报表形式输出流量统计结果；

③ 能够对流量超过预警值的行为进行告警。

(3) 带宽监测，部署在不同区域间的船舶网络防火墙宜对客户端占用带宽进行监测，并在达到设定预警值时告警。

2.3.3 应用层控制

2.3.3.1 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。

2.3.3.2 船舶网络防火墙应能识别并控制通用应用层协议及船舶系统专用协议，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；

(3) 应支持自定义协议，适用所在船舶网络系统的专用协议。

2.3.3.3 宜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。

2.3.3.4 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。

2.3.3.5 应支持基于以下内容对 FTP、Telnet、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。

2.3.4 攻击防护

2.3.4.1 当应用于船舶边界网络防护时，船舶网络防火墙应具备恶意代码防护能力，包括但不限于：

(1) 能拦截典型的木马攻击行为；

(2) 检测并拦截被 http 网页和电子邮件等携带的恶意代码。

2.3.4.2 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。

2.3.4.3 当通过门户网站/web 应用程序与外部网络建立连接时，船舶网络防火墙应具备 web、数据库、应用、自动化工具等攻击防护能力。

2.3.4.4 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。

2.3.5 配置管理

2.3.5.1 应支持对安全配置、日志等信息进行备份，且备份过程不应影响设备或系统的正常运行。

2.3.5.2 船舶网络防火墙应具备配置管理功能，要求如下：

(1) 应支持添加、激活、修改、禁用和删除帐户；

(2) 应支持用户权限分配和管理；

(3) 创建帐户应遵循最小特权授予原则，应支持基于角色的帐户管理；

(4) 多次认证失败后应支持设置锁定，尝试次数、锁定时长可设置，且该机制应能在应急等特定场景下禁用，如不锁定可信设备或帐户为实现基本功能建立的会话；

(5) 口令认证时，应能通过设置最小长度和多种字符类型，配置口令强度；

(6) 应在所有授权帐户、主机和用户请求执行任何操作之前，对每个授权帐户、主机和用户进行唯一的身份标识与鉴别，且验证过程中应能隐藏身份验证信息；

(7) 应对授权管理员和通过不可信网络访问的用户采用多因素身份鉴别；

(8) 应能清除退役设备或软件的相关信息；

(9) 应支持本地管理；

(10) 宜支持通过安全管理平台方式对船舶网络防火墙进行集中管理；

(11) 宜支持通过网络进行远程管理，并能限定进行远程管理的网络接口及其功能；

(12) 远程管理过程中，所有通信数据应非明文传输；

(13) 更改配置前应能保存原有配置，并提供恢复至原有配置的方法；

(14) 应能恢复至出厂设置；

(15) 应支持在中断或故障后恢复至已知安全配置状态；

(16) 应能限制设备资源的使用，防止资源耗尽。

2.3.6 审计

2.3.6.1 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、删除、查找等；

④ 从内部网络、外部网络发起的试图穿越或到达船舶网络防火墙的违反安全策略的访问请求；

⑤ 被访问控制策略允许、禁止的访问请求；

⑥ 检测到的攻击行为；

⑦ 其他应该记录的事件信息；

(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，包括年、月、日、时、分、秒；

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 船舶网络防火墙操作事件发生的时间，包括年、月、日、时、分、秒；

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 格式存储或兼容格式进行存储；

⑤ 宜支持第三方日志管理系统对船舶网络防火墙日志信息进行集中收集、存储；

⑥ 至少保存 6 个月的日志记录，以备查。

第 4 节 性能要求

2.4.1 性能指标

2.4.1.1 应说明船舶网络防火墙的性能参数，至少包括吞吐量、延迟、最大并发数以及最大连接数。

第 5 节 安全要求

2.5.1 软件和支撑硬件

2.5.1.1 船舶网络防火墙的研制应符合制造商的质量体系。

2.5.1.2 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）。

2.5.1.3 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。

2.5.1.4 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。

2.5.1.5 船舶网络防火墙宜采用自然散热，无风扇方式设计。

2.5.1.6 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），按照表 2.5.1.6 确定试验项目，并按 CCS《电气电子产品型式认可试验指南》要求进行环境试验，若对试验项目使用经验或有效的公认标准，经 CCS 总部同意，可以接受作为代替和等效方法。

环境试验项目 **表 2.5.1.6**

试验项目	环境类型①				
	A	B		C	
	A1	B1	B2	C1	C2
外观检查	X②	X	X	X	X
绝缘电阻测量	X	X	X	X	X
能源波动试验	X	X	X	X	X
能源故障试验	X	X	X	X	X
振动试验	X(Fc.1)③	X(Fc.1)	X(Fc.1)	X(Fc.1)	X(Fc.1)
高温试验	--②	X(B.1)	X(B.1)	X(B.2)	X(B.2)
低温试验	--	X(A.1)	X(A.1)	X(A.1)	X(A.1)
交变湿热试验	--	X(Db.1)	X(Db.1)	X(Db.1)	X(Db.1)
恒定湿热试验	X(Cab.1)	--	--	--	--

耐电压试验	X	X	X	X	X
外壳防护实验	X(IP20)	X(IP20)	X(IP20)	X(IP20)	X(IP22)
滞燃试验	适用于有塑料部件的设备				
电磁兼容试验	X(EMC2④)				
注：①环境试验类型由 CCS《智能设备检验指南》表 7.3 定义。 ②表中：“X”表示应做项目；“--”表示不适用，下同。 ③括号内表示对应试验项目的试验要求，Fc.1、A.1、B.1、Cab.1、Db.1 为 IEC60062 对应试验项目的分类编号。 ④开敞甲板和驾驶室用 EMC1，一般配电区域内应用 EMC2。					

2.5.2 安全支撑

2.5.2.1 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。

2.5.2.2 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。

2.5.2.3 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。

2.5.2.4 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。

2.5.2.5 当船舶网络防火墙组件或系统需采用加密时，应根据国际公认或经过证明的方式和建议实施加密机制，加密算法的密码强度应满足以下要求：

(1) 不应采用已破解的算法；

(2) 非对称加密算法密钥长度至少为 2048bits，密码强度不低于 RSA；

(3) 对称加密算法密钥长度至少为 256bits，密码强度不低于 AES。

2.5.2.6 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。

2.5.2.7 船舶网络防火墙在非正常条件（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。

2.5.2.8 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。

2.5.2.9 船舶网络防火墙的硬件或软件等故障不应影响受保护的重要系统的重要服务。

2.5.2.10 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。

2.5.2.11 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。

2.5.2.12 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。

2.5.2.13 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 3 章 船舶网络防火墙检验要求

第 1 节 资料审查

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	需提交的文件	说明	供应商
1	软件质量计划	质量计划（质量管理体系支撑材料、软件开发生命周期的质量计划）	Ⓐ
2	生命周期支持文档	应建立用于开发和维护防火墙的生命周期支持程序	Ⓐ
3	脆弱性分析文档	说明在预期使用环境中是否存在明显可利用的脆弱性，如有，需明确说明该脆弱性对于认证产品不构成威胁或是不能利用的	Ⓘ
4	说明书	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	Ⓐ
5	配置文件	产品各功能的推荐配置	Ⓘ
6	用户手册	产品操作、安装、维护和使用手册	Ⓘ
7	维护计划	维护内容、方式、记录等	Ⓐ
8	事件响应及恢复计划	制定响应、备份、恢复等计划方案	Ⓐ
9	型式试验报告（环境试验）	完成震动、高低温等试验	Ⓐ
10	型式试验大纲（性能和功能试验）	测试内容、流程等	Ⓐ
11	型式试验报告（性能和功能试验）	—	Ⓦ

注：表中采用的符号及其含义如下:
Ⓐ提交 CCS 批准　　Ⓘ提交 CCS 备查　　Ⓦ需 CCS 验船师见证

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，并参照《船舶网络安全指南》第 3 章 3.2.2 进行安全漏洞扫描或渗透测试、负载测试、压力测试和性能测

试等测试。

3.1.1.3 申请单件单批检验需按照 CCS《钢质海船入级规范》第 1 篇第 3 章第 2 节的要求进行，并至少完成以下试验：

(1) 接口测试，相关要求参见本指南第 2 章第 2 节；
(2) 包过滤，相关要求参见 2.3.2.1；
(3) 网络访问控制功能，相关要求参见 2.3.3.1；
(4) 配置管理功能，相关要求参见 2.3.5.2；
(5) “最小特权”，相关要求参见 2.5.5.2。

3.1.1.4 CCS 验船师见证船舶网络防火墙产品功能和性能测试前，供应商应至少提供涉及以下内容的文件资料备查：

(1) 测试流程说明；
(2) 被测功能描述；
(3) 被测软件列表及版本号；
(4) 软件维护和使用手册；
(5) 支撑硬件设备的接口列表及描述；
(6) 数据传输标准列表；
(7) 基于故障模式的风险分析报告。

第 2 节 测试准备

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。

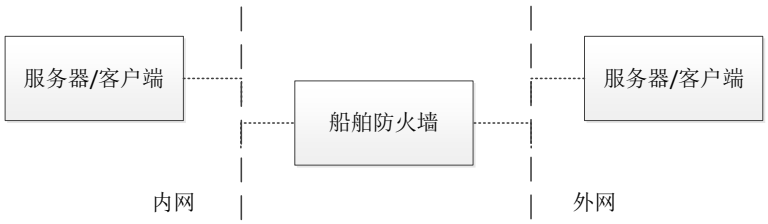


图 3.2.2.1（1）测试环境 1

(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。

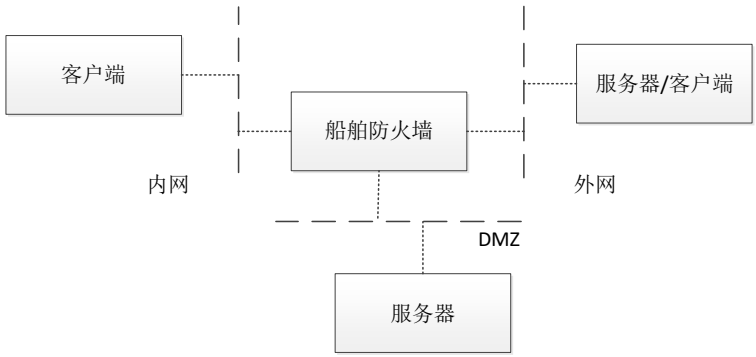


图 3.2.2.1（2）测试环境 2

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。

3.2.2.7 考虑到性能测试中可通过修改 TCP 堆栈参数影响设备性能测试结果，应在测试报告中说明 TCP 堆栈参数。

第 3 节 测试要求

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 功能测试

3.3.2.1 验证是否按预设功能模式实现透明传输、路由转发以及代理功能。

3.3.2.2 根据声明支持的冗余部署方式，配置防火墙，验证是否按预期在一台设备故障时，能继续保持原有网络的通信和安全策略。

3.3.2.3 检查防火墙缺省安全策略是否禁止，在测试环境中设置防火墙基于 IP、MAC、端口、协议的访问控制策略并测试。

3.3.2.4 NAT 功能测试应对比 NAT 使能和禁止状态，并在报告中描述。

3.3.2.5 启用基于状态检测的访问控制规则后，测试防火墙是否能过滤通过数据包回放等方式实现的连接或请求。

3.3.2.6 测试在安全策略允许时，通过 FTP 或 OPC 等动态端口实现的服务是否正常。

3.3.2.7 测试 IP/MAC 地址绑定后是否能按预期执行安全访问控制策略，防止 IP 盗用和 MAC 欺骗的会话连接。

3.3.2.8 测试船舶网络防火墙是否能实现会话超时管理和流量会话管理。

3.3.2.9 检查船舶网络防火墙是否能对受保护网络的流量和带宽进行监测和报警。

3.3.2.10 分别配置基于本地用户认证和基于第三方用户认证的访问控制策略，验证安全策略是否按预期实现。

3.3.2.11 测试船舶网络防火墙是否支持 HTTP、FTP、Telnet 等常用协议，以及声明的工

控协议的访问控制，并支持自定义船舶专用协议的访问控制。

3.3.2.12 在测试环境中分别运行 Web、数据库、FTP、Telnet、SMTP、POP3 和 IMAP 等应用，根据 2.3.3.3-2.3.3.5 的要求验证应用内容的访问控制功能。

3.3.2.13 应用在船舶网络边界的船舶网络防火墙应测试是否能检测并拦截 http 和邮件中的木马等恶意代码。

3.3.2.14 抗拒绝服务攻击的测试中应包括 ICMP Flood、UDP Flood、SYN Flood、Teardrop、Land、Ping of Death 等攻击，且攻击包通过的比例不大于 5%、正常连接建立成功率不低于 90%。

3.3.2.15 当受保护网络需要通过门户网站/web 应用程序域外部互联网相连时，应根据预期需求测试防火墙的 web、数据库以及自动化工具等攻击防护能力。

3.3.2.16 测试船舶网络防火墙是否能阻断网络扫描数据包。

3.3.2.17 应根据本文件 2.3.5 和 2.3.6 的配置管理和安全审计要求逐项测试或检查船舶网络防火墙的帐户、权限管理、日志等。

3.3.3 性能测试

3.3.3.1 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、延迟、最大并发数以及最大连接数，验证是否满足声明的性能指标。

3.3.3.2 性能测试参照 RFC 3511 的相关要求实施。

3.3.3.3 性能测试报告中应记录具体测试方案和测试结果。

3.3.4 安全性测试

3.3.4.1 检查防火墙制造商的质量体系是否满足要求。

3.3.4.2 检查散热方式是否与声明的散热方式一致。

3.3.4.3 检查是否已具备所有声明的功能，并进行漏洞扫描，确认是否含有已知风险和漏洞，核查是否提供了多余的网络服务。

3.3.4.4 验证是否默认拒绝所有流量通过，并检查用户权限配置是否符合“最小特权”原则。

3.3.4.5 验证人机交互界面是否显示 2.5.2.4 要求的信息

3.3.4.6 通过检查数据加密算法说明文档验证加密强度。

3.3.4.7 验证船舶网络防火墙失电重启后的访问控制策略、安全策略以及日志信息是否恢复到失电前状态。

3.3.4.8 测试网络流量、状态异常时是否能按预期报警，并能在恢复正常后自动或手动消除报警。

3.3.4.9 分别设置船舶网络防火墙失效后，验证是否按预期实现旁通或隔离。

3.3.4.10 验证船舶网络防火墙支持的多种工作模式是否符合所声明的功能预期。

3.3.4.11 检查产品相关文档，依照文档执行相关操作，见证产品安装，并验证产品升级、运维操作及日志的合规性。