ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1726—2020

信息安全技术　负载均衡产品安全技术要求

Information security technology—Security technical requirements for load balancing products

2020-04-26 发布　　2020-08-01 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部网络安全保卫局、公安部计算机信息系统安全产品质量监督检验中心、深信服科技股份有限公司。

本标准主要起草人：郭运尧、严文卿、张艳、陆臻、沈亮、顾健、张轶。

信息安全技术　负载均衡产品安全技术要求

1　范围

本标准规定了负载均衡产品的安全功能要求、安全保障要求及安全等级要求。

本标准适用于负载均衡产品的设计、开发及测试。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.3—2015　信息技术　安全技术　信息技术安全评估准则　第3部分：安全保障组件

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 18336.3—2015 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

负载均衡　load balancing

通过特定的算法将同一任务分摊到多个操作单元上执行，使用健康检测机制保证调度合理性的技术。

3.2

自动化客户端　automated client

可以对属于另一个应用程序的公开对象进行操作的应用程序。

4　缩略语

下列缩略语适用于本文件。

DDoS：分布式拒绝服务攻击(Distributed Denial of Service)

HA：高可用性(High Availability)

HTTP：超文本传输协议(Hypertext Transfer Protocol)

HTTPS：基于安全套接层超文本传输协议(Hypertext Transfer Protocol over Secure Socket Layer)

ICMP：因特网控制报文协议(Internet Control Message Protocol)

SNMP：简单网络管理协议(Simple Network Management Protocol)

SSL：安全套接层(Secure Socket Layer)

TCP：传输控制协议(Transmission Control Protocol)

UDP：用户数据报协议(User Datagram Protocol)

URL：统一资源定位符(Uniform Resource Locator)

QoS：服务质量(Quality of Service)

ARP：地址解析协议(Address Resolution Protocol)

IT：信息技术(Information Technology)
SPX：序列分组交换协议(Sequenced Packet Exchange protocol)
RST：重置连接、复位连接(Reset the Connection)
IP：网络之间互连的协议(Internet Protocol)

5 负载均衡产品描述

负载均衡产品能够为用户的业务发布提供包括多数据中心负载均衡、多链路负载均衡、服务器负载均衡的解决方案。它利用多种检测手段实现对各个数据中心、链路以及服务器状态的实时监控，同时根据预设规则将用户的访问请求分配给相应的数据中心、链路以及服务器，进而实现数据流的合理分配，使所有的数据中心、链路和服务器都得到充分利用。配合服务器卸载、高速缓存、流量压缩、单边加速、连接复用和虚拟化等多项智能优化技术，可大幅提高业务系统的整体处理能力，提高其稳定性，切实改善用户的访问体验，有效降低 IT 投资成本。图 1 是负载均衡产品的一个典型运行环境。

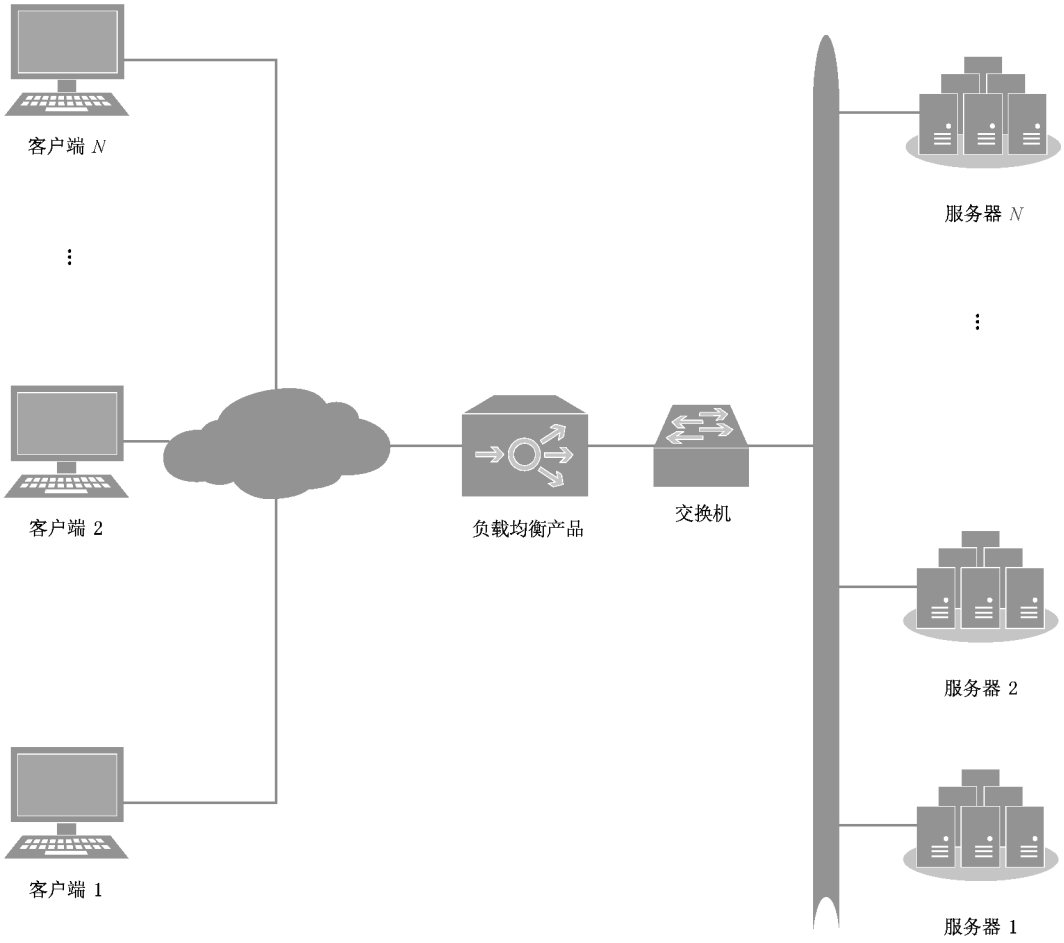

图 1 负载均衡产品典型运行环境

6 总体说明

6.1 安全技术要求分类

负载均衡产品安全技术要求分为安全功能要求和安全保障要求两大类。其中，安全功能要求是对

负载均衡产品应具备的安全功能提出具体要求，包括负载均衡、组件和链路监测、访问控制及路由和攻击防护等；安全保障要求针对负载均衡产品的开发和使用文档提出具体的要求，例如开发、指导性文档、生命周期支持和测试等。

6.2 安全等级划分

负载均衡产品的安全等级按照其安全功能要求和安全保障要求的强度不同划分为基本级和增强级，其中安全保障要求参考了 GB/T 18336.3—2015。

7 安全功能要求

7.1 负载均衡

7.1.1 链路负载均衡

链路负载均衡分为出、入站负载均衡：

a) 出站链路负载均衡：应能将内网用户发起的访问，根据策略分发到对应出口线路，供用户访问互联网；

b) 入站链路负载均衡：应能将外网用户发起的访问，根据策略设定的机制分发到对应线路，供用户接入内部服务器。

7.1.2 服务器负载均衡

服务器负载均衡包括应用负载均衡和数据库负载均衡：

a) 应用服务器负载均衡，应能将用户发起的访问，根据策略分发到后台应用服务器；

b) 数据库服务器负载均衡，应通过分表、读写分离等技术手段对数据服务器实现负载均衡。

7.1.3 全局负载均衡

应将广域网（包括互联网）用户发起的访问，根据策略设定的机制分发到不同地域的服务器。

7.2 负载均衡调度算法支持

基本级负载均衡产品应支持 3 种及以上算法，增强级负载均衡产品应支持 5 种及以上算法：

a) 轮循（Round Robin）；

b) 加权轮循（Weighted Round Robin）；

c) 随机（Random）；

d) 最少连接数（Least Connection）；

e) 加权最少连接（Weighted Least Connection）；

f) 基于代理的自适应负载均衡（Agent Based Adaptive Balancing）；

g) 固定权重（Fixed Weighted）；

h) 加权响应（Weighted Response）；

i) 源 IP 哈希（Source IP Hash）；

j) 其他。

7.3 组件和链路监测

7.3.1 链路状态检查

应可以检查链路的健康状况（带宽，延时和丢包等），并将入站方向流量引至正常链路。

7.3.2 服务器状态检查

应支持以下各层的服务器状态检查：

a) 网络层(ICMP)检查后台服务器的服务器服务状态，并移除故障服务器；

b) 传输层(TCP、UDP、SPX)检查后台服务器的服务器服务状态，并移除故障服务器；

c) 应用层(应用程序服务及 Agent 等)检查后台服务器的服务状态，并移除故障服务器。

7.3.3 服务器被动状态检查

应可通过监控 HTTP 协议和 TCP 协议中异常特征数据包(如 TCP 协议中的 RST 包，HTTP 协议中的 404)的比例，判断服务器的健康状态。

7.3.4 应用性能监测

应详细监控中间件、数据库的关键应用性能指标，并予以呈现。

7.4 优化加速

7.4.1 单边加速

应通过自动、实时、持续或动态地侦测网络路径中的延迟、丢包、重传的情况，改变传输机制和改善传输拥塞机制，避免数据报文过度重发，减少应用响应时间并提升传输效率。

7.4.2 TCP 连接复用

应将众多客户端访问请求捆绑处理，通过复用服务器端 TCP 连接，将客户端请求依次转发到服务器，从而减轻服务器压力。

7.4.3 SSL 加速

应截断 SSL 连接请求，可在将用户请求转发给后台前将 HTTPS 变为 HTTP，减轻服务器压力。

7.4.4 RAM 高速缓存

应实现基于内存的反向代理 Cache 功能，在内存中缓存网站等相关资源的页面内容，采用内存缓存和包存储结构等方式，通过动态调整缓存空间提高响应速度。

7.4.5 HTTP 压缩

应通过标准的 HTTP 压缩规范自动识别客户端对 gzip 或 deflate 压缩算法支持情况，并能够实现对数据动态压缩。

7.4.6 服务器上线及退出优化

服务器上线及退出优化包括上线及退出两类场景：

a) 在服务器上线时，负载均衡器应逐步增加发往该服务器的请求，直至达到最大值，避免大量请求导致新上线的服务器服务异常；

b) 在服务器退出时，负载均衡器应不再将用户请求发往该服务器，并维持该服务器上的原有连接，直至该服务器上没有用户后，再移除该服务器。

7.4.7 出入站链路繁忙保护

在某条链路的流量达到预设阈值时，负载均衡应将后续流量引至流量较小的链路，待原链路流量恢

复正常后，再依据原有调度策略进行链路选择。

7.4.8 QoS

应可为指定的网络通信提供更好的服务，以解决网络延迟和阻塞等问题。

7.4.9 IP-Anycast

应支持多台负载均衡器以相同的服务 IP 发布相同的业务，通过与动态路由协议的联动来为用户选择最优路径，实现就近访问和站点冗余。

7.4.10 服务器浪涌保护

应将超过服务器处理能力的数据做队列处理，缓慢发送给服务器，避免浪涌导致服务器异常。

7.4.11 不对称负载均衡

应支持服务器回包时数据不经过负载均衡器，通过第三方产品直接发送至客户端，以此来提高产品的吞吐性能。

7.4.12 图片优化转码

负载均衡器可将服务器上的图片做优化转码处理，减少图片的文件大小，同时保证图片质量，提高传输速度。

7.5 会话保持

应将同一用户一次完整交互过程中的连接请求转发至相同的后台服务器或相同的链路。

7.6 设备访问控制

应对服务器设备接入或接入请求进行访问控制。

7.7 高可用性

7.7.1 集群部署

应支持集群部署，有效保证自身高可用的同时提高资源利用率。

7.7.2 功能恢复

应确保断电恢复后，相关的均衡策略、系统日志和系统配置恢复到断电前状态。

7.7.3 双机热备

应支持通过双机热备的方式实现负载均衡产品自身的高可用性。

7.7.4 故障告警

应支持通过 SNMP-Traps、邮件等方式实现告警，报警内容至少包括服务器和链路的故障信息。

7.8 自身安全

7.8.1 鉴别失败处理

检测并记录任何鉴别验证相关的剩余鉴别尝试的操作及次数(用户名及鉴别信息)：

a) 当鉴别尝试次数还有 2 次时，产品应采取提示用户确认该鉴别操作（提示应遵循最小反馈原则）；
b) 当鉴别数据验证或用户失败次数达到上限时（不超过 10 次），产品应采取有效措施防止用户进一步尝试操作。

7.8.2 单一鉴别、管理机制的使用

同一管理员账号同一时间不得同时进行产品管理操作，不同用户同一时间不得同时修改产品的同一属性。

7.8.3 日志

记录以下日志信息：
a) 应记录用户通过 HTTP 协议访问服务器时的基本信息（如 URL 等）；
b) 应通过 Syslog 协议将日志传输至远程日志服务器；
c) 应内置日志管理系统，可跟踪管理员的操作信息，提高产品安全性。

7.8.4 安全功能数据的管理

具备以下管理功能：
a) 应仅限管理员能够对鉴别信息、失败次数进行重置操作；
b) 应仅限管理员能够对要求存储的安全数据进行修改操作；
c) 应以安全方式存储敏感信息数据（用户鉴别信息、用户身份信息等）。

7.9 性能要求

7.9.1 网络层性能要求

7.9.1.1 新建连接

验证产品标称网络层新建连接性能值（包大小覆盖 128 B 和 16 KB），测试时长 300 s。

7.9.1.2 并发

验证产品标称网络层并发性能值（包大小覆盖 128 B 和 16 KB），测试时长 300 s。

7.9.1.3 吞吐量

验证产品在不丢包的情况下的标称网络层吞吐量性能值（包大小覆盖 128 B 和 16 KB），测试时长 300 s。

7.9.2 应用层性能要求

7.9.2.1 新建请求

验证产品标称应用层新建请求性能值（包大小覆盖 128 B 和 16 KB），测试时长 300 s。

7.9.2.2 吞吐量

验证在不丢包的情况下的产品标称应用层吞吐量性能值（包大小覆盖 128 B 和 16 KB），测试时长 300 s。

7.9.3 SSL 性能要求

7.9.3.1 SSL 传输新建 TPS(Transaction per Second)

验证产品标称 TPS 性能值(包大小覆盖 128 B 和 16 KB),测试时长 300 s。

7.9.3.2 加密吞吐量

验证产品在不丢包的情况下的标称加密吞吐量性能值(包大小覆盖 128 B 和 16 KB),测试时长 300 s。

7.9.4 攻击防护

7.9.4.1 网络层 DDoS 攻击防护

应能有效识别并防护网络层的 DDoS 攻击,测试时长 300 s。

7.9.4.2 应用层 DDoS 攻击防护

应有效识别并防护应用层的 DDoS 攻击,测试时长 300 s。

7.9.4.3 自动化客户端程序识别(有则适用)

应有效识别并阻止恶意的由自动化客户端发起的访问。

7.10 虚拟化环境中纯软件形态部署(有则适用)

应可提供纯软件形态的产品,方便用户将其部署于虚拟化环境中,对虚拟机实现负载均衡。

7.11 云管理平台对接(有则适用)

应支持与主流云管理平台(Openstack、VMware 等)对接,方便用户统一管理。

8 安全保障要求

8.1 开发

8.1.1 安全架构

开发者应提供产品安全功能的安全架构描述,安全架构描述应满足以下要求:

a) 与产品设计文档中对安全功能实施抽象描述的级别一致;
b) 描述与安全功能要求一致的产品安全功能的安全域;
c) 描述产品安全功能初始化过程为何是安全的;
d) 证实产品安全功能能够防止被破坏;
e) 证实产品安全功能能够防止安全特性被旁路。

8.1.2 功能规范

开发者应提供完备的功能规范说明。功能规范说明应满足以下要求:

a) 完全描述产品的安全功能;
b) 描述所有安全功能接口的目的与使用方法;

c) 标识和描述每个安全功能接口相关的所有参数；
d) 描述安全功能接口相关的安全功能实施行为；
e) 描述由安全功能实施行为处理而引起的直接错误消息；
f) 证实安全功能要求到安全功能接口的追溯；
g) 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h) 描述可能由安全功能接口的调用而引起的所有直接错误消息。

8.1.3 实现表示

开发者应提供全部安全功能的实现表示。实现表示应满足以下要求：
a) 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b) 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c) 以开发人员使用的形式提供。

8.1.4 产品设计

开发者应提供产品设计文档。产品设计文档应满足以下要求：
a) 根据子系统描述产品结构；
b) 标识和描述产品安全功能所有子系统；
c) 描述产品安全功能所有子系统间的相互作用；
d) 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e) 根据模块描述安全功能；
f) 提供安全功能子系统到模块间的映射关系；
g) 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
h) 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
i) 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

8.2 指导性文档

8.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：
a) 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b) 描述如何以安全的方式使用产品提供的可用接口；
c) 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d) 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e) 标识产品运行的所有可能状态(包括操作导致的失败或者操作性错误)，以及它们与维持安全运行之间的因果关系和联系；
f) 充分实现安全目的所必须执行的安全策略。

8.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：

a) 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
b) 描述安全安装产品及其运行环境必需的所有步骤。

8.3 生命周期支持

8.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：
a) 为产品的不同版本提供唯一的标识。
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项。
c) 提供配置管理文档，描述用于唯一标识配置项的方法。
d) 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变。
e) 配置管理文档包括一个配置管理计划，描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致。
f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

8.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：
a) 产品、安全保障要求的评估证据和产品的组成部分；
b) 实现表示、安全缺陷报告及其解决状态。

8.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

8.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

8.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行必要控制，并提供生命周期定义文档，描述用于开发和维护产品的模型。

8.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档，无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

8.4 测试

8.4.1 覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：
a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；

b） 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

8.4.2 深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a） 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；

b） 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

8.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a） 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；

b） 预期的测试结果，表明测试成功后的预期输出；

c） 实际测试结果和预期的测试结果一致。

8.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

8.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗具有增强型基本攻击潜力的攻击者的攻击。

9 不同安全等级的要求

9.1 安全功能要求

不同安全等级的负载均衡产品的安全功能要求如表1所示。

表1 不同安全等级的负载均衡产品的安全功能要求

安全功能要求		安全等级	
		基本级	增强级
负载均衡	链路负载均衡	7.1.1	7.1.1
	服务器负载均衡	7.1.2 a)	7.1.2
	全局负载均衡	7.1.3	7.1.3
负载均衡调度算法支持		7.2(3种及以上)	7.2(5种及以上)
组件和链路监测	链路状态检查	7.3.1	7.3.1
	服务器状态检查	7.3.2	7.3.2
	服务器被动状态检查	—	7.3.3
	应用性能监测	—	7.3.4

表 1（续）

安全功能要求			安全等级	
			基本级	增强级
优化加速	单边加速		—	7.4.1
	TCP 连接复用		7.4.2	7.4.2
	SSL 加速		7.4.3	7.4.3
	RAM 高速缓存		7.4.4	7.4.4
	HTTP 压缩		7.4.5	7.4.5
	服务器上线及退出优化		—	7.4.6
	出入站链路繁忙保护		—	7.4.7
	QoS		7.4.8	7.4.8
	IP-Anycast		7.4.9	7.4.9
	服务器浪涌保护		—	7.4.10
	不对称负载均衡		—	7.4.11
	图片优化转码		—	7.4.12
会话保持			7.5	7.5
设备访问控制			7.6	7.6
高可用性	集群部署		—	7.7.1
	功能恢复		7.7.2	7.7.2
	双机热备		—	7.7.3
	故障告警		7.7.4	7.7.4
自身安全	鉴别失败处理		7.8.1	7.8.1
	单一鉴别、管理机制的使用		7.8.2	7.8.2
	日志		7.8.3	7.8.3
	安全功能数据的管理		7.8.4	7.8.4
性能要求	网络层性能要求	新建连接	7.9.1.1	7.9.1.1
		并发	7.9.1.2	7.9.1.2
		吞吐量	7.9.1.3	7.9.1.3
	应用层性能要求	新建请求	7.9.2.1	7.9.2.1
		吞吐量	7.9.2.2	7.9.2.2
	SSL 性能要求	SSL 传输新建 TPS	7.9.3.1	7.9.3.1
		加密吞吐量	7.9.3.2	7.9.3.2
	攻击防护	网络层 DDoS 攻击防护	7.9.4.1	7.9.4.1
		应用层 DDoS 攻击防护	7.9.4.2	7.9.4.2
		自动化客户端程序识别	—	7.9.4.3(有则适用)
虚拟化环境中纯软件形态部署			—	7.10(有则适用)
云管理平台对接			—	7.11(有则适用)

9.2 安全保障要求

不同安全等级的负载均衡产品的安全保障要求如表 2 所示。

表 2 不同安全等级的负载均衡产品的安全保障要求

安全保障要求		安全等级	
		基本级	增强级
开发	安全架构	8.1.1	8.1.1
	功能规范	8.1.2 a)～f)	8.1.2
	实现表示	—	8.1.3
	产品设计	8.1.4 a)～d)	8.1.4
指导性文档	操作用户指南	8.2.1	8.2.1
	准备程序	8.2.2	8.2.2
生命周期支持	配置管理能力	8.3.1 a)～c)	8.3.1
	配置管理范围	8.3.2 a)	8.3.2
	交付程序	8.3.3	8.3.3
	开发安全	—	8.3.4
	生命周期定义	—	8.3.5
	工具和技术	—	8.3.6
测试	覆盖	8.4.1 a)	8.4.1
	深度	—	8.4.2
	功能测试	8.4.3	8.4.3
	独立测试	8.4.4	8.4.4
脆弱性评定		8.5	8.5

中华人民共和国公共安全
行业标准
信息安全技术　负载均衡产品安全技术要求
GA/T 1726—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2020年10月第一版
*
书号:155066·2-35514

GA/T 1726-2020