[a] ICS 35.040
[b] L80

中华人民共和国国家标准

GB/T 25068.2—20XX/ISO/IEC 27033-2:2015
代替 GB/T 25068.2—2012

信息技术 安全技术 网络安全 第2部分：网络安全设计和实现指南

Information technology—Security techniques —Network security—

Part 2: Guidelines for the design and implementation of network security

（ISO/IEC 27033-2:2015，IDT）

（送审稿）

（本稿完成时间：2019年11月5日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上

[3] XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 25068《信息技术 安全技术 网络安全》分为以下几部分：

——第 1 部分：综述和概念；

——第 2 部分：网络安全设计和实现指南；

——第 3 部分：参考网络场景—风险、设计技术和控制要素；

——第 4 部分：使用安全网关的网间通信安全保护；

——第 5 部分：使用虚拟专用网的跨网通信安全保护；

——第 6 部分：无线 IP 网络接入的安全保护。

本部分为 GB/T 25068 的第 2 部分。

注：GB/T 25068可能还会有其他部分。这些部分可能覆盖的主题包括局域网、城域网、宽带网、网页寄存、互联网电子邮件、接入第三方组织的路由。这些部分主要涉及威胁、设计技术和控制等问题。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 25068.2—2012《信息技术 安全技术 IT网络安全 第2部分：网络安全体系结构》，与后者相比，主要技术变化如下：

——本部分名称由《信息技术 安全技术 IT 网络安全 第 2 部分：网络安全体系结构》修改为《信息技术 安全技术 网络安全 第 2 部分：网络安全设计和实现指南》；

——对标准文本结构进行了调整，由原来的 10 章调整为现在的 8 章。对第 5-8 章的名称及内容进行了大幅度修改，增加了“网络安全设计准备”、“网络安全设计”、“网络安全实现”等章节，删除了“网络安全参考体系结构”、“安全维”、“安全层”、“安全面”、“安全威胁”、“对安全维应用于安全层所实现目标的描述”等章节；

——第 2 章中删除了对 GB/T 9387.2-1995 的引用，增加了对 GB/T 9387（所有部分）、GB/T 29246—2012、GB/T 22080—2016、GB/T 22081—2016、GB/T 31722—2015、GB/T 25068.1 的引用；

——第 4 章删除了“ASP”、“ATM”、“DHCP”、“DNS”、“DS-3”、“Ipsec”、“MD5”、“Megaco/H.248”、“MPLS”、“OAM&P”、“OSI”、“POP”、“PSTN”、“PVC”、“QoS”、“SHA-1”、“SIP”、“SNMP”、“SONET”、“SS7”、“SSL”、“VLAN”等缩略语，增加了“IPS”、“POC”、“RADIUS”、“SMS”、“TACACS”、“TFTP”等缩略语；

——附录 A、B、C 均为资料性附录。

本部分使用翻译法等同采用 ISO/IEC 27033-2:2012《信息技术 安全技术 IT 网络安全 第 2 部分：网络安全设计和实现指南》。

与本部分中规范性引用的国际文件有一致性对应关系对应关系的我国文件如下：

——GB/T 9387（所有部分） 信息技术 开放系统互连 基本参考模型[ISO/IEC 7498(所有部分)]

本部分做了下列编辑性修改：

——删除了“引言”；

本部分由全国信息安全标准化技术委员会（TC 260）提出并归口。

本部分起草单位：黑龙江省网络空间研究中心、中国电子技术标准化研究所、西安西电捷通无线网络通信股份有限公司、等。

本部分主要起草人：曲家兴、方舟、马遥、王大萌等。

本部分所代替的历史版本发布情况为：

——GB/T 25068.2—2012。

信息技术 安全技术 网络安全 第2部分：网络安全设计和实现指南

1 范围

本部分标准为组织给出了计划、设计、实施和记录网络安全的指南。

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（包括所有的修改版）适用于本文件。

GB/T 29246—2012 信息技术 安全技术 信息安全管理体系 概述和词汇(ISO/IEC 27000:2009)

GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求(ISO/IEC 27001:2005)

GB/T 22081—2016 信息技术 安全技术 信息安全管理体系 信息安全控制实践指南(ISO/IEC 27002:2005)

GB/T 31722—2015 信息技术 安全技术 信息安全风险管理(ISO/IEC 27005:2011)

GB/T 9387（所有部分） 信息技术 开放系统互连 基本参考模型(ISO/IEC 7498)

ISO/IEC 27033-1 信息技术 安全技术 网络安全 第1部分：综述和概念（Information technology —Security techniques —Network security—Part 1:Overview and Concepts）

3 术语和定义

GB/T 29246—2012、GB/T 22080—2016、GB/T 22081—2016、GB/T 31722—2015\GB/T 9387（所有部分）和ISO/IEC 27033.1中界定的以及下列术语和定义都适用于GB/T 25068的本部分。

4 缩略语

IPS	入侵防御系统（Intrusion Prevention System）
POC	概念证明（Proof of Concept）
RADIUS	远程认证拨号用户服务（Remote Authentication Dial-In User Service）
RAS	远程访问服务（Remote Access Service）
SMS	简单消息服务（Simple Message Service）
SMTP	简单邮件传输协议（Simple Mail Transfer Protocol）
TACACS	终端访问控制器访问控制系统（Terminal Access Controller Access-Control System）
TFTP	简单文件传输协议（Trivial File Transfer Protocol）
TLS	传输层安全协议（Transport Layer Security）

5 结构

本部分标准的结构包括：

•网络安全设计准备

—概述

—资产识别

—需求收集

—需求审查

—现有的设计和实施的审查

•网络安全设计

—概述

—设计原则

—设计核验

•网络安全实现

—概述

—网络组件的选择准则

—产品或供应商的选择准则

—网络管理

—日志、监视和事件响应

—文档

—测试计划和实施测试

—核验

6 网络安全设计准备

6.1 概述

网络安全的目标是促进能够提高组织业务流程的信息流，阻止降低组织业务流程的信息流。网络安全设计与实施的编制工作包括如下阶段：

- 资产识别
- 需求收集
- 需求审查
- 技术选择和技术约束的评估
- 现有设计和实施的评估

这些阶段形成了早期的文档，该文档包括：后续设计与实施阶段的所有输入。

6.2 资产识别

对任何网络来说，资产识别是确定信息安全风险的首要步骤。有些资产如果被不适当地泄露、修改或失效，将会影响组织的业务流程，这样的资产都需要保护。需要保护的资产包括物理资产（服务器，交换机，路由器等）和逻辑资产（配置设置，可执行代码，数据等）。作为持续性计划/灾难恢复风险分析的一部分，资产登记应提前执行。需要解决如下问题：

——需要保护的不同类型的网络设备和设施分组有哪些？

——需要保护的不同类型的网络活动有哪些？

——需要保护哪些信息资产和信息处理能力？

——信息资产存储于信息系统架构的哪个位置？

可识别的资产包括安全支持管理、控制和用户流量所需的资产，以及网络基础设施、服务和应用程序正常生效的功能。这就包括主机、路由器、防火墙等设备，接口（内部和外部），信息存储/处理和使用的协议。基础设施资产的保护仅是网络安全设计目标的一部分。最终目标是保护商业资产，例如信息和业务流程。

6.3 需求收集

5.3.1 法律和监管需求

应该收集和审查法律监管对当地与网络功能的要求，以保证这些要求在网络设计中得到满足。需要特别注意跨管辖或监管边界的信息流。在这种情况下，需要记录边界两侧的要求。

5.3.2 业务需求

组织的业务流程和数据分类类型决定了其访问需求。网络应该配置成这样：对于适当授权的用户能够访问信息资产，并且阻止其他的访问。信息访问通常和一些服务相关，这些服务可以建立在开放端口（例如 TCP 端口 80 的 HTTP 服务）、特定主机（如 www.example.org，IP 地址为 10.11.12.13），特定主机组（例如 172.128.97.64/24 子网）或特定的网络接口设备（如 MAC 地址为 10:00:00:01:02:03 的接口）。该组织需要识别哪些是向他人提供的服务、哪些是由他人提供的服务以及哪些是内部服务。

5.3.3 性能要求

流量数据能够记录通信线路、服务器和安全网关/防火墙的配置，以便实现用户所期望的高水平服务—没有“过度配置”以及相关不必要的成本。收集的信息诸如现有通信连接的速度，任何位于第三方路由器的配置/容量，每个链接允许访问的用户数（并发访问和访问的用户数量），所需的最小、平均和最大用户连接时间，可访问的授权用户身份，网页点击次数，数据库访问的点击率，未来一年和三/五年的增长预期，以及是否需要窗口登录。可以使用电信表(排队)理论来确定所需端口、信道的数量，特别是拨号链路上的端口和信道。应对性能要求进行审查，排除疑问，性能标准要求应满足已经确认的技术架构和相关的技术安全架构。

6.4 需求审查

当前的性能和任何计划的技术网络架构的变化都需要进行审查，并和开发中的技术安全架构进行比较以发现不兼容之处。这些不兼容之处都需要重新审查并且进行适当的架构调整。

在审查过程中收集到的信息应至少包括以下内容：

—正在使用的网络连接类型的识别；

—安全风险的确定；

—制定技术安全体系架构和安全控制的需求列表；

—使用的网络协议；

—在网络各个层面使用的网络应用。

信息的收集应考虑网络性能。应获得相关网络体系结构的详细信息，并对此进行审查，以便为接下来的过程步骤提供必要的理解和衔接。尽早明确这些内容，确定相关的安全需求识别标准、识别控制区域、审查安全体系结构的技术选项并决定哪些应被采纳，可获得更高效更可行的安全解决方案。例如，由于位置的关系，建立所有网络连接只能集中通过一个管道，那么对于选定的地点来说，针对多种不同通道所设置的冗余连接的安全控制，就是无用无效的。其他控制也要设身处地考虑，才能找到保护网络

连接的最优方式。

在早期阶段，如果当前架构下尚未实现能被接受的安全解决方案，则应为网络和应用架构预留出时间，以便对这些架构进行审查和必要的修改。

6.5 现有设计和实施的审查

现有安全控制审查必须依据安全风险评估和管理审查的结果来进行。安全风险评价的结果可以指明被评估威胁相应的安全控制需求。应对当前网络安全架构进行差距分析，以确定现有的网络安全体系架构中还有哪些问题还未解决。

网络安全体系架构应该包含现有的网络控制以及任何遗漏和新的安全控制。

7 网络安全设计

7.1 概述

网络安全体系架构限制了不同信任域之间的数据流量。信任域之间最明显边界是一个组织内部网络和外部世界之间的接口。任何规模的组织，都会在可被识别和控制的内部信任域之间确立边界。网络安全体系架构包括：组织或行业内部网络与外界之间接口的描述，反映上述 6.4 节中提到的审查要求，并解决如何保护组织免受 GB/T 25068.1 中曾描述的常见威胁和弱点的攻击。

7.2 节提供了最佳实践设计指南，本系列标准第 4 部分及之后部分给出了针对当前和未来特定网络技术的网络安全体系架构指南，以及在特定场景下组织的设计指南。本系列标准第 3 部分给出了一个组织所需的特定网络场景的指南。

需求调研过程中形成的技术设定必须形成文档，例如：

—只允许有授权访问的 IP 通信（防火墙通常支持 IP 通信，如果允许并入其他协议，可能会造成管理困难）；

—如果需要引入非 IP 协议，则此类协议需视为安全体系架构之外或利用隧道技术的协议来进行接入。

网络安全体系架构通常包含服务，包括但不限于：

—身份验证和授权（密码、令牌、智能卡、证书、RAS /RADIUS/终端访问控制系统（TACACS+），等）；

—逻辑访问控制（单点登录、基于访问控制的角色、可信数据库、应用程序控制、防火墙、代理设备等）；

—安全审计和核查（审计日志、审计日志分析设备、入侵检测设施、写一次读多次（WORM）设备等）；

—存储清理/安全删除（可控“擦除”设施）；

—安全测试（脆弱性扫描、网络监听，渗透测试等）；

—安全的开发环境（独立开发和测试环境、免编译器等）；

—软件变更控制（配置管理软件、版本控制等）；

—安全软件部署（数字签名、SSL 协议、传输层安全（TLS）（RFC 5246）等）；

—安全维护和可用性（良好的备份/恢复设施、恢复、聚类、数据仓库、多样性通信等）；

—传输安全（传输加密的使用、扩频技术、无线局域网（WLAN）、虚拟专用网/外联网）。

7.2 设计原理

6.2.1 概述

设计失败是与网络安全体系架构相关的常见风险，是由不好的设计、对业务连续计划缺少适当的考

虑或设计无法对当前或未来威胁等级做出响应等引发。开发安全体系架构所必需的基本要素应覆盖所有已识别的安全控制和业务需求。通用的网络安全设计实践大多包括这些要素。本系列标准第 4 部分及之后的部分详细介绍了网络技术安全体系架构最佳实践的设计与实现。关于最佳实践实施的更多详细指导可参阅其他出版物。

以下各节提供了在考虑网络安全体系结构时应遵循的设计最佳实践的一般指导。

6.2.2 纵深防御

组织不应仅从一个视角来看待网络安全，而应通过一种整体分层方法来进行综合考虑。安全必须全面覆盖所有网络层。采用分层方法的网络安全体系架构就称为纵深防御。安全组件是一个集策略、设计、管理和技术于一体的组合。每一个组织都需要确定需求，并设计一个基于这些需求的纵深防御。

许多移动设备有 USB 和网络连接，以及无线功能。这些设备可以 Ad-hoc 方式连接到内部网络或内部系统;如果这是在设备的无线连接打开和未加密的情况下完成的，这些设备可以作为内部网络上的恶意无线接入点，从而绕过周边控制。应采取严格措施，以限制不安全的移动设备连接到网络，并为检测恶意无线接入点而执行日常的无线信道扫描。

所有无线接入点应位于非军事区内。内部网络的无线接入点应该有严格的连接设置：最强的安全保护措施（在可能的情况下设置 WPA2），使用 MAC 地址过滤以限制有设备连接到已授权的设备。本标准的第 3 部分提供了更多关于移动通信技术和相关控制威胁的细节。

纵深防御原则体现了通过多个安全控制或安全技术的帮助以减少风险的用法，风险是来自于被破坏或被规避的防御组件。举例来说，当防火墙和同一环境中的服务器上已经有病毒保护时，可以在单个工作站上安装防病毒软件。来自多个供应商的不同的安全产品可能被部署用来防御网络中的不同的潜在载体，帮助防止任何一个防御出现短板，以防可能导致更大范围的失效，这种防御方法被称为“分层方法”。

图 1 显示了边界安全、基础设施安全、主机安全、应用程序安全和数据安全。所有的层都是为了保护数据。

图 1 纵深防御

基于分层方法的安全解决方案是灵活和可度量的，该解决方案适用于组织的安全需求。

6.2.3 网络分区

网络分区指将不同敏感度等级（不同风险容忍度和敏感度）的系统资源置于不同的安全分区。在系统内创建了一种方法，即在系统的特定区域内，只使用执行任务所必需的数据。（例如，只有在互联网

上提供服务的服务器才在公共 DNS 上注册）。
安全网关（专用防火墙设备、IPS 设备中的防火墙功能，以及网络路由器和交换机中的访问控制列表）就是用来保证所需的网络流量，限制不必要的网络流量。

有了适当的布局和配置，安全网关有助于创建安全架构，将网络基础设施划分为安全区域并控制它们之间的通信。如何布局和配置安全网关详见在本系列标准的第 4 部分。

划分原则体现出以下网络安全设计规则：

- 不同敏感度的网络应设在不同的安全区：
  - 为外网提供服务（例如互联网）的设备和计算机系统应位于不同的区域（非军事区 - DMZ）内网设备和计算机系统则无需进行分区；
  - 战略资产应设在专用安全区；
  - 低信任级别的设备和计算机系统，如远程访问服务器和无线网络接入点应设在专用安全区。
- 不同类型的网络应位于不同的安全区：
  - 用户工作站应同服务器位于不同的安全区；
  - 网络和安全管理系统应设在专用安全区；
  - 在开发阶段的系统应同产品系统位于不同的区域。

6.2.4 弹性设计

网络安全设计应包括几层的冗余，以防备单点故障并最大限度地提高网络基础设施的可用性。这包括使用冗余接口、备份模块、待机装备和拓扑冗余路径。此外，设计还使用了一组富功能设置，以使网络对攻击和网络故障具有更强的抵抗力。

6.2.5 场景

对网络环境的审查，通常围绕与已定义的网络威胁、设计考量和控制要素等特征相关的特定网络场景和相关的“技术”主题。对于审查技术安全架构/设计选项，选择和记录与首选技术安全架构/设计的相关安全控制来说，这些信息是非常有用的。

这一系列标准的第 3 部分引用了此类场景，对每个场景的安全威胁和安全设计技术与控制要素提供了详细的指导，以应对这些威胁。

6.2.6 模型和框架

安全系统工程组件包括安全模型或框架的选择、使用和制定。

安全模型通常关注通过访问控制实现的保密性或信息完整性，其中一些是正式定义的，另一些是非正式定义的。

典型的安全模型聚焦于进入过程的保密性或信息的完整性，其中一些被正式定义和其他被非正式的定义。

安全框架通常为组织提供一种如何形成安全系统大纲的方法，一个框架的例子是 ITU-T X.805。ITU-T X.800 这一系列的首要框架是 ITU-T X.805，其适用于终端到终端的网络安全机制。为此，X.805 定义了安全维度的概念，这些维度包括工具容器、技术、标准、法规、程序等。这些维度涵盖了安全的方方面面。X.805 定义了一个避免冗余安全的机制，通过识别某一层（特指在 X.805 中的层）的能力来保护另一个层，从而降低了安全解决方案的整体成本。X.805 是一个通用的安全框架且不提供任何特定信息系统或组件的规范。相反，它指定了安全规则和目标的安全功能，以促进终端到终端的网络安全。附件 C 中提供了 ITU-T X.805 如何在 GB/T 22080—2016 控制支持下进行应用。

7.3 设计核验

已完成的网络安全设计的核验工作应由适当级别的管理人员验收。

8 网络安全实现

8.1 概述

网络安全应基于第 7 章网络安全设计的描述来实现。

网络安全的实现主要包括：

- 分区和分块；
- 网络组件选择标准；
- 产品或供应商选择标准；
- 网络管理；
- 记录、监视和事件响应；
- 文档；
- 测试计划与测试实施；
- 核验。

8.2 网络组件选择标准

对于任何安全网络设计而言，都会用到通用组件的组合。这些组件的组合将创建一个技术层面上的网络安全设计。第 8 章和 GB/T 25068.3 之后的部分将讨论下列组件的细节。这些组件形成一定组合，以满足在 6.4 节中所反映的需求。

这些组件可能包括：

- 分区和分块；
- 安全管理系统（如监视和配置管理）；
- 基本安全技术，如身份管理、密码等；
- 网络准入控制设备；
- 威胁削减技术；
- 边界设备；
- 网络过滤器，如防火墙和远程访问设备的内容监测；
- 入侵检测系统/入侵防御系统；
- 端点保护；
- 路由器和交换机；
- 外网连接。

8.3 产品或供应商的选择标准

产品选择不应该孤立的进行，应建立一个与网络安全体系架构设计相关联的迭代过程。

举例来说，产品选择应基于以下内容：

- 产品的技术适用性和优点；
- 性能；
- 协议支持；
- 弹性；
- 兼容性；

- 可扩展性；
- 网络管理设施；
- 审计能力；
- 一致性；
- 技术文档；
- 维护性；
- 远程诊断设备；
- 逻辑安全；
- 遵循类似 GB/T 18336（信息技术安全性评估准则）标准中定义的评估方法来保证安全功能的实现；
- 供应商的特点（能力、跟踪记录、对质量的承诺、市场地位、规模、对产品定位\组织\财务稳定性\参考和培训设施的综合能力）；
- 按交货时间表交货；
- 成本。

8.4 网络管理

网络管理是指网络系统操作、管理、维护和供给网络系统所属的活动、方法、程序和工具。

• 保持网络和网络提供的服务正常平稳运行的操作，包括监测网络，以便于在用户受到影响之前及时发现问题。

• 跟踪并合理分配网络资源的管理。包括所有处于网络控制下的“管家”服务。

• 与执行维修和升级有关的维护。例如，当设备必须更换时、当路由器需要操作系统镜像的补丁程序时、当为网络添加一个新的交换机时。维护纠正和预防措施，以使得网络运行的更好，例如调整设备配置参数。

有意或故意地错误配置相关的网络组件，会产生重大风险，不仅关系到其可用性，也常常关系到完整性和保密性。

因此解决这些风险的控制是必要的。这种控制可以分为组织控制和技术控制。

组织控制包括适当任命管理人员、双人操作原则、适当的职责分离，以及为避免出现默认或弱密码所采取的程序和策略。操作控制包括配置和版本控制，以解决或跟踪潜在的错误配置或设备配置变更。

技术控制包括使用管理接口和工具提供适当的身份验证、授权和数据保密。技术管理需要大量的与网络相关的组件。安全网关可以在本地或远程进行管理，但远程管理应该使用工具来完成，此类工具应保证具有强身份验证或双身份验证，或至少能够在技术上避免默认或弱密码，并且能够尽可能提供完整性和保密性的功能。例如使用加密 VPN 通道时，适当地配置加密等级或 SSH 终端仿真。服务器也可以在本地或远程管理。服务器对敏感信息进行远程管理时，使用工具应保证具有强身份验证或双身份验证，或至少能够在技术上避免默认或弱密码，并且能够尽可能提供完整性和保密性的功能。

基础设施组件，如交换机和路由器，可以从控制台端口进行本地管理，也可从中央管理工作站，通过在线的远程计算机或分布式管理系统上运行的远程终端仿真程序进行远程管理。然而，这些协议是不安全的,除非他们可以配置一个对连接进行完全加密的方法。完全加密并含有一个安全文件传输工具的 SSH 就是安全的远程连接一个典型例子。此外，访问基础设施组件应由身份验证服务器控制。

外包给服务提供商的网络通常有自己的管理系统。他们应该从一个使用安全远程管理方法的中央管理站进行管理，远程管理的方法应该包括使用公钥密码加密和认证。可以使用的安全方法例如 Telnet、通过 VPN 隧道的 FTP 或由一个认证服务器控制的 SSH。

许多组织使用简单网络管理协议(SNMP)管理陷阱来直接监视网络。SNMP 版本 1 和版本 2 有重大风险以致网络存在漏洞或不安全。因此，如果一个组织决定使用 SNMP，应该使用版本 3 以实现完整的安

全控制。

8.5 日志、监视和事件响应

就如同用安全相关设备保护起来的 DMZ 一样，位于 DMZ 的审计服务器也是通过配置所有安全网关系统来实现面向内网和外网的安全。审计服务器不是内部网络域的一部分，应该只能被分配授权管理安全网关/防火墙系统的安全人员直接访问。另外，需要允许写入访问操作，以使得审计日志通过基础设施组件、服务器和防火墙内的安全协议上传(例如安全复制协议(SCP))。所有防火墙和指向审计服务器的审计日志都应经由安全检查人员利用专用于审计日志文件审查的审计分析软件进行事后检验。

安全信息管理包括信息的收集和标准化，以便于决策。收集的信息可能包括系统记录、SNMP 信息、IDS/IPS 警报和流信息。

在可能的情况下，应根据已检测到的异常活动优先级信息来配置审计服务器和/或 IDS/IPS 系统，通过电子邮件、短信等方式，向指定的安全管理人员发出警报。任何一项异常活动被视为一次未遂攻击，被任命的安全管理人员应该按照警报优先级来对实施事件响应程序。

8.6 文档

网络安全架构文档是关键技术安全文档之一，如前所述，应符合相关的安全风险评估和风险管理审查结果，且满足组织/行业网络和信息安全策略和相关的其他安全策略的有关要求。与其他文档一样，网络安全架构文档也应实施变更控制管理。附件 B.1 中给出了一个示例模板。它应该参考相关技术架构文档和其他技术安全文档。主要相关的文档包括：

- 所有受控的网络组件(如安全网关、防火墙、路由器等)信息安全需求记录。这些需求也包括功能安全需求如防火墙规则库的需求。——模板示例见附件 B.2；
- 审计日志分析软件需求文档；
- 产品分析报告。

8.7 测试计划与测试实施

安全测试策略文档是描述用测试来验证网络技术安全体系架构的方法。它应该专注于如何测试关键技术安全控制，以确保定义的需求得到满足，所设计的策略得以实施。为了验证这些观点，要执行系统测试和基于检查表的检查。

测试策略文档应该包括：

- 识别和身份验证机制；
- 弹性设计；
- 授权机制；
- 实施策略的控制；
- 验证加固后的操作系统；
- 验证审计日志解决方案。

测试策略还应该包括单元测试和可用性测试，以确保设计的适用性。

进行系统测试之前，应制定测试计划。测试计划应包括测试数据和测试场景以留作证据。测试计划还应该包括一个适当的测试清单。应该精心准备测试数据以检验技术安全控制的功能。

8.8 核验

已完成的网络安全实现的核验工作应由适当级别的管理人员验收。

附 录 A

（资料性附录）
检 查 表 描 述

GB/T 22080—2016、GB/T 22081—2016 中的网络安全相关控制内容与 GB/T 25068 章节交叉引用对比。

GB/T 22080—2016、GB/T 22081—2016 章节	内容描述	GB/T 25068 对应章节
0.6.1 网络控制	网络需要充分的管理和控制，以免受到威胁，并保持使用网络的系统、应用程序和传输信息的安全。	详见下列的 GB/T 22080—2016、GB/T 22081—2016 内 10.6.1 IG a）到 e）章节
10.6.1 IG a)	网络操作与计算机操作权限适当分开。	8.3 网络管理
10.6.1 IG d)	采用适当的日志记录和监视，以便能够记录与安全有关的操作。	8.4 日志记录和监视
10.6.1 IG e)	管理活动应密切协调，以便优化对组织的服务能力，并确保全程对信息处理基础设施保持控制。	8.3 网络管理
10.6.2 网络服务安全	所有网络服务的安全特性、服务水平和管理需求都要被识别并包含在任何网络服务协议中合同内，无论这些服务是内部提供的还是外包的是否为内供或外购。	6.3 需求收集 6.4 审查需求
10.8.1 信息交互策略和程序	需制定正式的交互策略、程序和控制，以保护使用所有类型的通信设施进行的信息交互。	8.6 文档
11.4.1 使用网络服务的政策	只能向用户提供访问被明确授权使用的特定服务。	8.3 网络管理
11.4.2 从外部连接的用户身份验证	使用适当的身份验证方法来控制远程用户的访问。	8.3 网络管理

附 录 B

（资料性附录）

实 例 文 档 模 板

B.1 网络安全架构文档模板的示例

B.1.1 介绍

包括以下部分:

•目的/目标/范围，
•技术和其他方面的假设，
•文档状态，
•文档结构。

B.1.2 业务相关的需求

包括以下部分:

•介绍，
•上下文，
•网络和其他IT服务。

B.1.3 技术架构

包括以下部分:

•介绍，
•技术概述，
——概要，
——主要领域1，
——主要领域2，
——主要领域3等等，
——服务器，
——工作站，
——日志记录，
——管理，
——身份验证和访问控制，
——服务覆盖和弹性。
•系统物理位置，
•系统组件，
•相互连接，
•组件1，
——概述，
——配置，

——日志记录，
——管理，
•组件2，
——概述，
——配置，
——日志记录，
——管理，
•组件3，
——概述，
——配置，
——日志记录，
——管理，
•组件“X”等。
•服务器管理，
——简介，
——监视服务，
——扩展系统管理(XSA)，
——企业安全管理器(ESM)，
——其他经理，
•防火墙，
——简介，
——概述，
——防火墙配置备份，
——设计标准和配置，
——规则库，
•防火墙管理，
——配置，
——防火墙警报，
——远程访问控制，
•日志记录，
•备份系统，
——简介，
——防火墙，
——服务器，
——应用程序，
•网络通信，
——局域网络，例如虚拟局域网（VLAN），无线局域网（WLAN），
——路由器，
——交换机，，
——IP寻址，
•管理责任，
——服务器，
——防火墙，

——基础设施，
——应用程序管理。

B.1.4 网络服务

包括以下部分:
•简介，
•位置X的服务，，
•位置Y的服务，
应该按位置列出所有网络服务，包括：
•千位流（KiloStream）服务，
•超高速数据流（MegaStream）服务，
•帧中继服务，
•异步传输模式（ATM），
•IP清除/多协议标签交换（MPLS），
•宽带服务，
•无线局域网（wifi）/全球互通微波访问（WiMax），
•局域网连接服务，
•全球移动通信系统（GSM)，
•初级速率的综合数字业务网ISDN(通过兆流服务实现64 Kbps传输的30信道)，
•ISDN基本速率接口(BRI)，(2条64Kbps通道)，
•模拟直接交换线路(DELs)，
•内网/外网服务，
•互联网服务提供商，
覆盖所有线路和服务。
如列表内容过于广泛，应在文件正文之后，以附录形式引用。

B.1.5 硬件/物理布局

包括以下部分:
•简介，
•位置。
应按照平面图和格段布局上所有硬件的位置进行罗列，包括：服务器、路由器、交换机、防火墙和其他通讯设备。所有的硬件应该贴上标签，至少应有标签贴放的规划或参照表。
表B.1显示了一个硬件列表示例。每个类型的硬件应该有一个表,示例表中包括服务器组件。

表 B.1 — 例如硬件列表

服务器组件	硬件	软件	内容
服务器名称和生产商	零件编号	软件和版本	要求的具体意见。例如，垂直摆放，或集群。

B.1.6软件

包括以下部分:

•简介，
•软件列表，
——位置X的软件，
——位置Y的软件，
——等等。
所有软件的列表,包括版本号，还应包括如：
•Windows软件，
•防火墙，
•远程访问服务RAS/远程身份认证拨号服务RADIUS，
•路由器软件，
•交换机软件，
•代理服务器，
•审核管理，
•邮件服务器，
• SMTP邮件中继，
• 内容管理，
• java / ActiveX筛选，
• 网络服务器，
• FTP服务器，
• 域控制器，
• 备份软件，
• 其他软件。
该清单应列入附录，并在文件正文中提及时引用该清单。

B.1.7 性能

应包括预期的性能细节，其中含“子系统”的细节，例如：
• 桌面，
• 服务器，
• 局域网，
• 广域网，
• 网关，
• 外部服务。

B.1.8 已知问题

已知问题的细节，含不合规相关领域的已知问题，其细节应列入技术、物理及环境等标题下，须含以下各节：
• 概述，
• 不合规的相关领域。

B.1.9 参考资料

参考资料应包括所有相关文件，包括：
• 安全风险评估和管理审查结果，
• 网络安全政策，

•信息安全政策，
•其他相关安全政策，
• 技术架构文档，
• 每个防火墙系统（含防火墙规则库）的服务访问（安全）需求文件，
• （审核）日志分析软件需求文档，
• 产品分析报告，
• 通用测试策略和计划，
• 信息安全事件管理计划，
•安全操作程序SecOPs，
• 第三方安全连接条件，
• 为第三方用户提供用户指南。

B.1.10 附录

包括如下的细节：
• 硬件配置，
• 服务器/控制台配置，
• 防火墙配置，
• 路由器配置，
• 软件配置，
•数据库配置，
•IP地址规划，
•SNMP配置，
•系统陷阱，
•应用陷阱，
•标准。

B.1.11 注释词表

B.2 功能安全需求文档的示例模板

注释：每一个防火墙系统应该对应生成一个文档。

B.2.1 介绍

包括部分如：
•背景/范围/目标，
•防火墙系统名称，
•防火墙位置，
•防火墙角色，
•负责防火墙操作的人员/群组名称，
•对文件内容的修订记录，
•参考文献。

B.2.2 防火墙配置

包含部分有：

•简介，

•基于防火墙系统的链路标识，

•防火墙架构概要，

•防火墙系统详细信息：

- 硬件，
- 软件，
- 防火墙体系结构，
- 防火墙服务，
- 防火墙管理，
- 内部路由器，
- 外部路由器，
- DMZ集线器，
- 反恶意代码服务器，
- SMTP邮件服务，
- 网络页面，
- SMTP邮件服务器，
- （审计）记录服务器，
- 不间断电源UPS，
- 其他组成部分，
- 其他控制要求，

•与其他系统链接，或其他系统之间链接的描述，

•所涉及的信息类型及其敏感性，

•用户类型和编号等。

B.2.3 安全风险

包含部分有：

• 简介，

•潜在的不利业务影响（有时被称为资产评估），

•威胁评估，

•脆弱性评估，

•风险评估，

应考虑防火墙使用的环境。

B.2.4安全管理

含有职责内容的各节，如：

•安全员/组，

•网络人员，

•防火墙支持人员，

•网络管理，

•其他IT管理，

•用户。

B.2.5安全行政管理

包含如下部分：
•安全操作程序（SecOPs），
•安全合规审查，
•可用性，
•维护，
•配置控制，
•容量管理，
•问题管理，
•服务水平管理，
•本文件的有效期。

B.2.6 身份验证和访问控制

包括部分：
•简介，
•逻辑访问控制，如防火墙管理员、内部和远程用户，
•外部访问控制，如网络防火墙规则库，安全平台和应用程序代理服务器，
•网络等级保护。

B.2.7（审核）日志记录

包括日志等部分：
•被记录的信息，
•进行的分析，以及所使用的工具，
•安全。

B.2.8 信息安全事件管理

包括日志相关的部分：
•简介，
•事件报告，
•事件处理，
•等等。

B.2.9 物理安全

包括关于访问控制权限的章节：
•防火墙系统，
•综合布线。

B.2.10 人员安全

包括适用于防火墙相关人员的章节，如：
•招聘筛选/检查，
•安全意识和培训。

B.2.11 附录

包括服务和协议细节：

- 向内和向外的访问，
- 远程管理，
- 防火墙管理，
- DMZ服务器管理，
- 任何其他相关的服务和协议细节。

B.2.12注释词表

附 录 C

（资料性附录）

表 A.1　ITU-T X.805 框架和 GB/T 22080—2016 控制映射

ITU-T X.805 框架也可用来对 GB/T 22080—2016 标准中的技术要素进行增强力度。特别是，如图 C.1 所示，ITU-T X.805 可以增强 GB/T 22080—2016 中安全政策、资产管理、访问控制、信息安全事件管理等四个方面的控制力度。适用于控制要素的 ITU-T X.805 框架层、面和维度都如图所示。例如，资产管理的控制要素中，X.805 层里管理基础设施、管理服务、控制基础设施和控制服务是最常用的增强手段，而访问控制、可用性维度则是最受关注的控制要素。

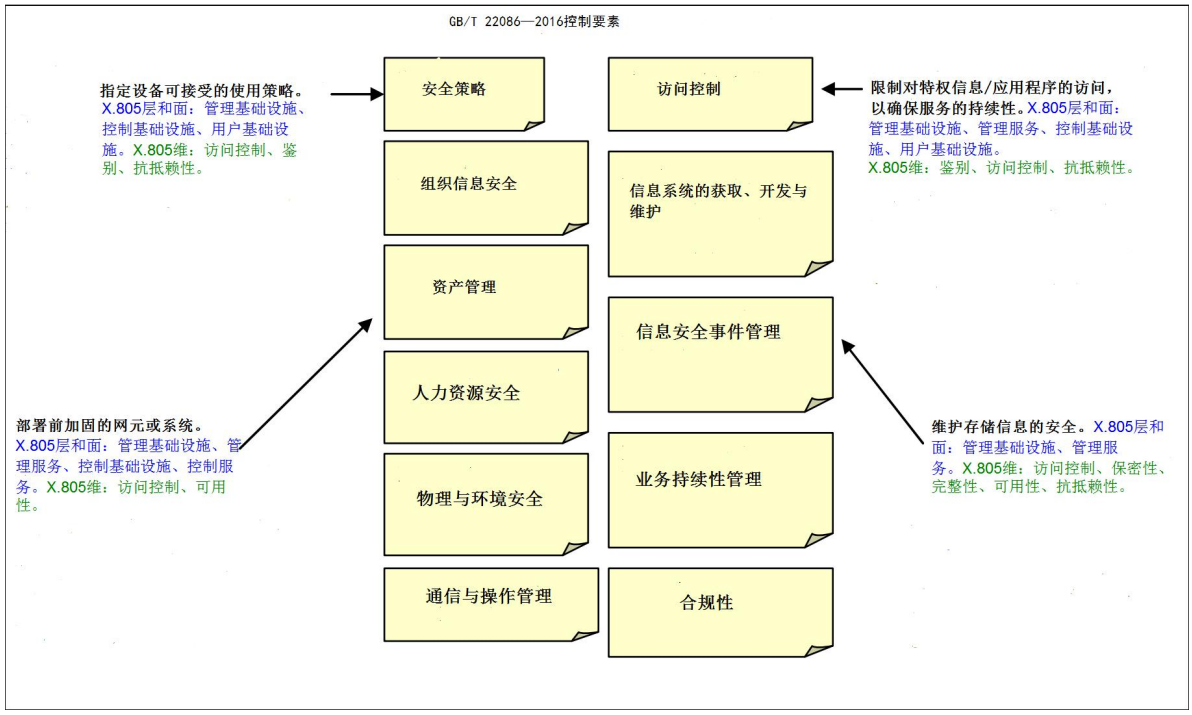

图 C.1 ITU-T X.805 框架增强了 GB/T 22080—2016 控制的力度

例如，增强可用于系统地评定和设计企业数据中心的安全性，该中心存储员工信息，特别是存储着仅限于授权用户可访问的个人信息。这些员工信息对企业雇用的几个支持部门开放访问，其中之一是服务台，此外，数据中心及内部各系统则由公司的 IT 部门维护。如图 C.2 所示，服务台访问员工信息以便去处理投诉，支持新的 IT 服务订单，或者解决员工在 IT 服务方面遇到的问题(例如远程访问)等等。此外，文件系统维护，系统更新，补丁管理等行为是维修活动的一部分，故而 IT 部门也会访问员工信息。

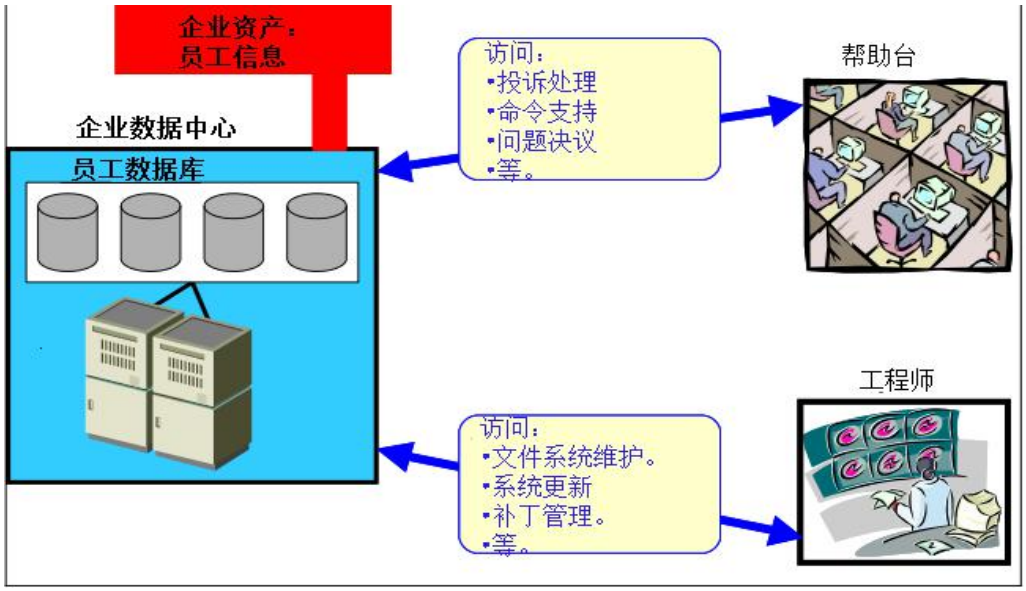

图 C.2 企业资产的访问情况

ITU-T X.805 威胁/脆弱性分析表明，企业 IT 部门的成员可以查看和修改员工信息，从而导致基础设施层的泄露和损坏（见图 C.3）。此外，作为执行问题解决方案的一部分，员工信息在数据中心和帮助服务台之间传送，从而使它在服务层容易被泄露、损坏或拦截。因此，必须识别和选择控制，以保护员工信息不受其基础设施和服务层管理层面上的威胁和弱点的影响。需注意，本文并未对 ITU-T X.805 进行逐步分析。这个分析结果仅仅是简单的假设。

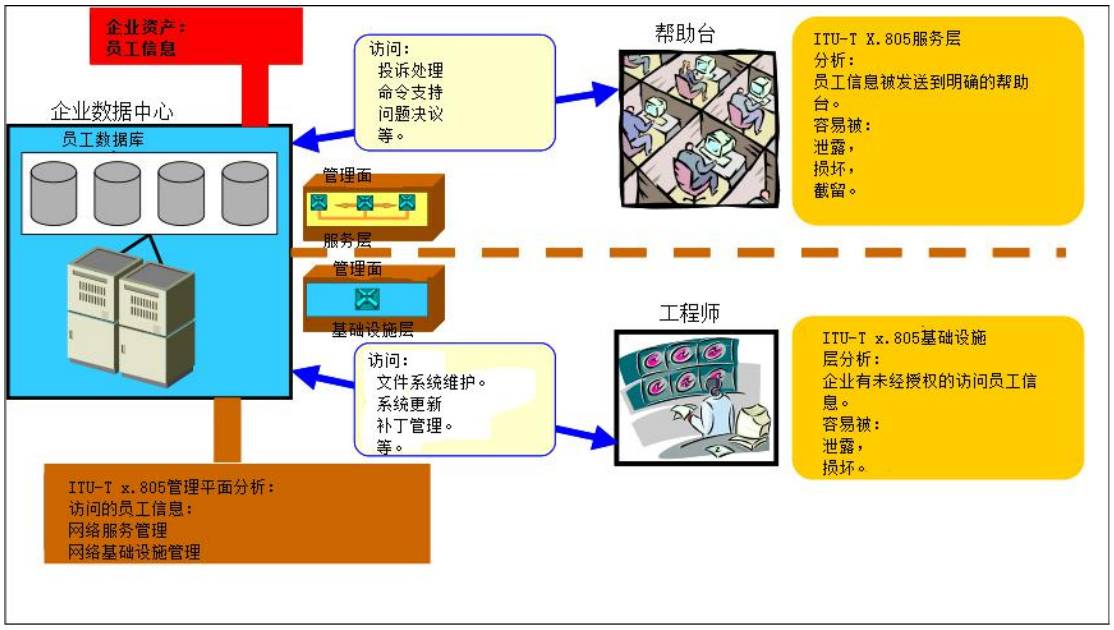

图 C.3 ITU-T X.805 对企业资产的威胁和脆弱性的分析结果

经过 ITU-T X.805 分析（图 C.4）出的弱点与威胁，表明在服务和基础设施层，需要对员工信息进行管理，所以选用了 GB/T 22080—2016 Control A.10.9.2。GB/T 22080—2016 Control A.10.9.2 规定，涉及在线交易的信息应受到保护，以防止不完整的传输、错误路由、未经授权的消息更改\泄露\消息复制或重播。

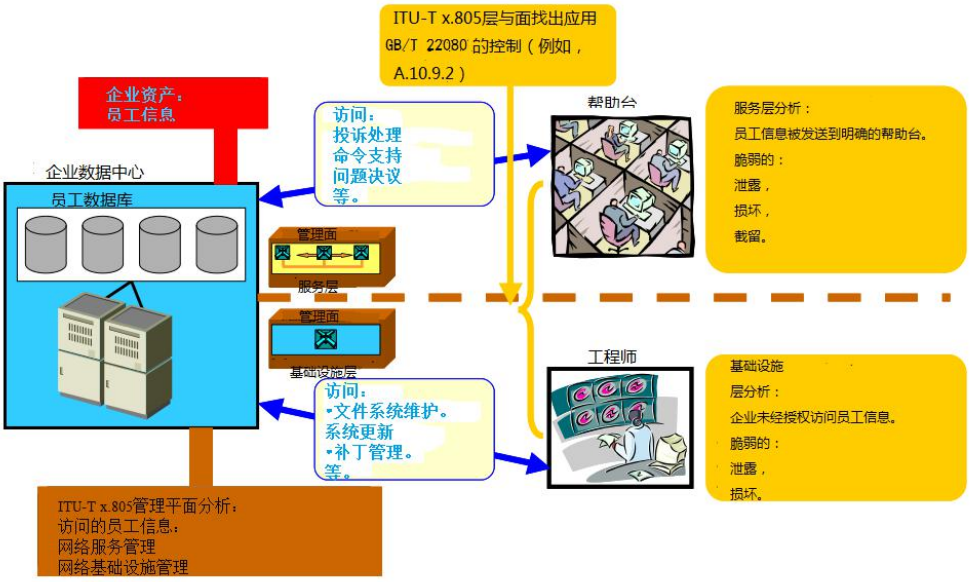

图 C.4-- GB/T 22080—2016 控制

对处于服务和基础设施层的员工信息资产，ITU-T X.805 维度提供了用 A.10.9.2（在线交易）控制的实施和操作细节。在服务层，通信安全维度提供了防止错误路由 VPN 的用法。数据完整性维度提供 IPSecAH 防止完全传输使用，未经授权的信息变更、复制以及防止消息重放。数据保密性维度提供 IPSec ESP 以防止不完整的传输、错误路由、未经授权的消息更改\泄露\消息复制或重播。数据保密性维度规定使用 IPSec ESP 来防止未经授权的泄露。在基础设施层，数据完整性维度提供了文件校验，以防止未经授权的变更，数据保密性维度提供了文件加密，以防止未经授权的泄露。访问控制维度提供对文件系统的访问控制列表(ACL)的使用，以防止未经授权的复制。图 C.5 描绘了 ITU-T X.805 是如何用 A.10.9.2 控制来实施和操作对员工信息资产的保护。

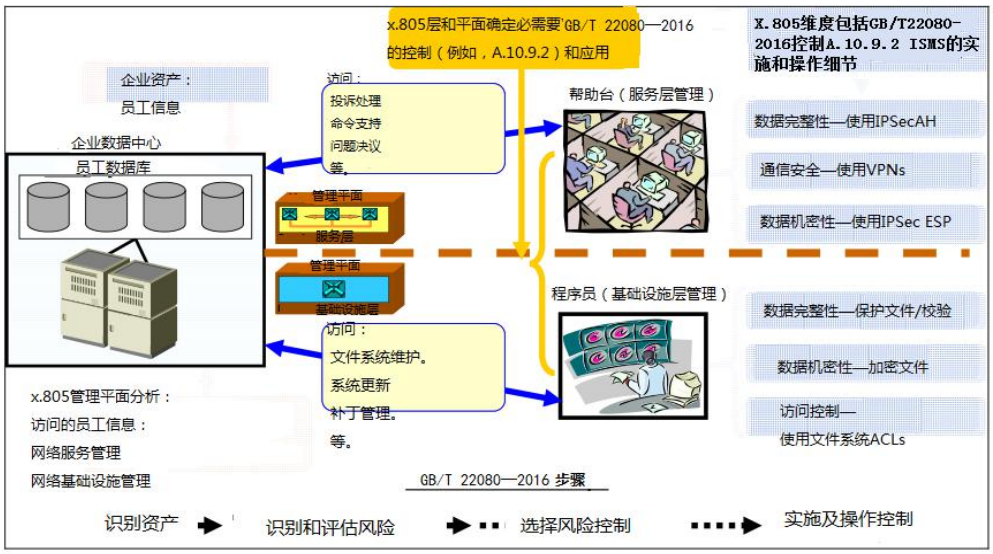

图 5--ITU-T X.805 在 GB/T 22080—2016 中的实现

参考文献

[1] ITU-T X.805, Security architecture for systems providing end-to-end communications
[2] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, IETF, August 2008