**XXX单位**

**网络安全管理规范**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479441402)

[2 适用范围 1](#_Toc479441403)

[3 网络结构安全 1](#_Toc479441404)

[3.1 结构设计 1](#_Toc479441405)

[3.2 边界隔离 1](#_Toc479441406)

[4 网络管理安全 2](#_Toc479441407)

[4.1 配置管理 2](#_Toc479441408)

[4.2 审计管理 3](#_Toc479441409)

[4.3 监控管理 3](#_Toc479441410)

[5 网络设备安全 4](#_Toc479441411)

[5.1 安全管理 4](#_Toc479441412)

[5.2 补丁管理 4](#_Toc479441413)

[5.3 安全防护 5](#_Toc479441414)

[5.4 废弃和重用 5](#_Toc479441415)

[6 附则 5](#_Toc479441416)

# 目的

网络安全保护的目的是为保障XXX单位网络系统的安全稳定运行，抵御内部和外部各种形式的网络攻击或威胁。

本文档规定了XXX单位网络安全要求和网络设备管理规范。

# 适用范围

本文档适用于XXX单位信息系统网络建设和网络设备使用。

# 网络结构安全

## 结构设计

在网络设计中须采用冗余设计，应考虑硬件故障、软件故障、链路故障等，保证业务平稳有效的运行。网络整体的拓扑结构需进行严格的规划、设计和管理。

1）核心网络设备具有热备设备，满足业务高峰期需要。

2）绘制与当前运行情况相符的网络拓扑结构图。

## 边界隔离

* **内部逻辑区域之间的隔离**

内部网络不同业务网络之间必须实施安全措施，对网络区域进行保护，利用防火墙设备或者VLAN技术措施等将不同业务网络进行逻辑隔离，区域间互联的基本要求是“最小化原则”，即在满足业务和维护的需求的前提下，最大限度的减少的互联地址和端口数量。

* **与第三方网络之间的隔离**

1）网络之间互连点采取集中原则，并考虑安全冗余。

2）单位内部计算机禁止直接连接到第三方网络，连接必须取得相关部门审批同意后方可实施。

3）网络互连点及安全设备必须纳入到网管体系的监控。

4）与第三方网络的连接中，在互连点上的路由器上应该进行IP地址转换，保护单位内部服务器真实的IP地址。

5）互连点上必须实施安全措施，如安装防火墙、实施入侵检测等，在防火墙上实施策略控制，严格限制访问的地址和端口。

* **与互联网之间的隔离**

1）禁止内网网络与互联网之间直接连接，在网络边界上部署防火墙，并配置访问控制策略。

2）互联网业务系统出口统一集中在单位总出口，单位以下各部门禁止开放互联网业务出口。

# 网络管理安全

网络安全管理的目标是保证网络信息安全，确保网络基础设施的可用性，加强跨越信息系统边界的网络安全管理。

应全面、系统地考虑整个网络的安全控制措施，并紧密协调，一致实施。明确规定有关网络的规划、实施、运作、更改和监控的安全技术要求，对网络安全状况进行持续监控，保存有关错误、故障和应急措施的记录。

## 配置管理

1）单位信息安全管理部门对各骨干网的统一配置管理工作，未经上级信息安全管理部门或相关主管领导同意，不得随意更改骨干网的网络配置。

2）根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

3）对业务网络进行QOS策略配置，保证在业务高峰期重要业务网络不受影响。

4）所有的网络配置工作都要有文档记录，网络设备的配置文件需要定期备份。

5）网络需保持持续不断的运行，维护工作尽量选择在非正常工作时间内进行。

## 审计管理

1）在网络中部署堡垒机或者网络管理软件，对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录。

2）重要的网络设备要有日志，系统管理员需要每天检查防火墙和IDS设备日志，在必要时对路由器及交换机的日志进行检查（如防火墙日志发现异常时），检查违规行为。

3）网络管理员至少要每一个月对涉及网络配置的增、删、修改等操作的配置更改记录进行审计。

4）至少要每一个月对系统用户和管理员的访问权限进行审查。

5）重要资源的访问控制策略至少要每六个月审计一次。

6）如果在上述审计和检查工作中发现有安全事故,应遵照安全事故处理流程进行处理。

## 监控管理

1）网络管理员负责网络设备的日常检查，监测网络设备性能参数和网络运行状况。对关键设备要做到每日检查，发现问题应迅速解决，全部管理工作应保留记录。

2）应对网络设备进行监控，监控内容包括CPU使用率、硬盘使用率、内存、接口流量、系统事件、安全事件等信息。

3）在网络边界处部署入侵监测设备，监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等。

4）在监控过程中，如发现网络异常、严重影响业务的问题，要启动应急处理机制，并向上一级报告。

5）通过网络管理软件对内部网络中未通过准许私自联到外部网络的行为进行检测，并及时阻断，追查源头并向相关部门进行报告。

6）网络管理部门要对所有在线网络设备运行情况记录登记，并定期向上级上报网络运行状况报告。

# 网络设备安全

## 安全管理

1）终端接入系统时必须通过用户名、口令进行身份验证后方能接入。

2）网络设备的登录口令应符合复杂性要求、长度要求、有效期要求。

3）根据不同的使用人员分配不同的账号或账号组，修改系统默认的账号及口令，删除或锁定与设备运行和维护无关的账号。

4）应对登录网络设备的用户进行角色划分，至少包含管理员角色、安全员角色和审计员角色，根据用户的角色分配权限，实现用户的权限分离，仅授予用户所需的最小权限。

5）网络设备应启用用户登录失败锁定功能，并限制失败登录次数和频率。

6）网络设备应对连接超时进行限制，当用户登录设备后，一段时间未进行操作后，就将自动中断此用户的连接。

7）网络设备远程管理过程中，应采用安全可靠的加密协议对通信过程中的整个报文或会话过程进行加密。

## 补丁管理

1）应采用专业的漏洞扫描、评估技术对网络设备进行定期安全评估，并根据结果对系统进行修复。

2）在网络设备的补丁进行更新前，应对补丁与现有业务系统的兼容性进行测试，确认后与系统提供厂商配合进行相应的修复。

3）应对网络设备的漏洞发展情况进行跟踪，形成详细的安全更新状态报表。安装补丁软件包则以必要为原则，非必需的就不装。

## 安全防护

1）网络设备应启用自身安全防护功能，防护对网络设备的攻击行为，保障自身设备的安全、稳定运行。

2）重要网络设备可采用IP/MAC绑定防止地址欺骗。

3）应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制。

4）使用SNMP网络协议时，应修改默认的SNMP团体字。

5）禁止使用Telnet等存在安全隐患的协议。

## 废弃和重用

1）网络设备废弃时，应对废弃信息进行管理，主要包括数据备份、剩余信息清除和软硬件处理，并保存过程记录文档。

2）网络设备重用应确保硬件上的数据被彻底删除。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。