ICS XXXXXX
CCS XXX

CIMA

云 南 省 电 力 行 业 协 会 团 体 标 准

T/XXXX XXX-XXXX

云南省电力行业综合数据网网络边界安全防护通用技术要求

Technical specification for network boundary security deployment of integrated data network in power industry

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

云南省电力行业协会　　发布

目　　次

前　　言

本文件按照《云南省电力行业协会团体标准管理办法（试行）》的要求，依据GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本标准由云南省电力行业协会提出。

本标准由云南省电力行业协会技术归口并解释。

本标准起草单位：

本标准主要起草人：

本标准为首次发布。

云南省电力行业综合数据网网络边界安全防护通用技术要求
（征求意见稿）

1 范围

本文件规定了云南省电力行业综合数据网网络边界安全防护部署技术原则，对综合数据网Ⅲ（生产管理系统）、Ⅳ（管理信息大区-信息内网）、Ⅴ（管理信息大区-信息外网）业务区域部署对应的安全防护设备提出了要求。

本文件适用于云南省电力行业综合数据网网络边界区域安全防护的新建、改造及优化工作。

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。

中华人民共和国网络安全法 第一章：总则 第三章：网络运行安全（2017-06-01 颁布）

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 36572-2018 电力监控系统网络安全防护导则

GB/T 36635-2018 信息安全技术 网络安全监测基本要求与实施指南

GB/T 20281-2020 信息安全技术 防火墙安全技术要求和测试评价方法

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 28454-2020 信息安全技术 安全技术入侵检测和防御系统的选择、部署和操作

3 术语、定义和缩略语

中华人民共和国网络安全法、GB/T 20271-2006、GB/T 36572-2018、GB/T 36635-2018 、GB/T 20281-2020、GB/T 22240-2020 、GB/T 28454-2020界定的以及下列术语和定义适用于本文件。

3.1

综合数据网 Integrated data network

用于承载管理信息类和企业办公类业务，实现厂站间、调度机构间、办公楼间、营业场所间数据通信的数据网络平台。

3.2

网络边界 Network security boundary

不同区域网络之间的边界线，网络边界区域负责转发来自其他网络的相关数据流量，可以实现用户访问权限控制、安全策略控制等功能。

3.3

网络安全防护 Network security protection

一种网络安全技术，致力于解决如何有效进行介入控制，以及如何保证数据传输的安全性的技术手段，主要包括物理安全分析技术，网络结构安全分析技术，系统安全分析技术，管理安全分析技术，及其它的安全服务和安全机制策略。

3.4

网络拓扑 Network topology

用传输介质互连各种设备的物理布局。指构成网络的成员间特定的物理的即真实的、或者逻辑的即虚拟的排列方式。如果两个网络的连接结构相同我们就说它们的网络拓扑相同，尽管它们各自内部的物理接线、节点间距离可能会有不同。

3.5

虚拟专用网络 Vitual private network（VPN)

在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN可通过服务器、硬件、软件等多种方式实现。

3.6

Ⅲ区（生产管理系统）

部署于综合数据网生产管理区，用于监测电力生产及供应过程的、基于计算机及网络技术的管理信息系统，以及作为基础支撑的通信及数据网络等。典型系统包括电力调度运行管理系统（OMS）、调度信息披露系统、雷电监测系统等。

3.7

Ⅳ区（管理信息大区-信息内网）

承载公司营销、资产、财务等管理与日常办公业务流程的信息系统，部署于信息内网区。典型的管理信息系统主要包括：营销管理系统、资产管理系统、人力资源管理系统、协同办公系统、决策支持系统等。

3.8

Ⅴ区（管理信息大区-信息外网）

用于向公司内部员工或社会公众提供互联网应用服务，不得涉及公司秘密与其他敏感信息。典型业务系统包括互联网网站系统、电子商务系统、网上营业厅、外网邮箱系统等。

3.9

旁路功能 Bypass

通过特定的触发状态（断电或死机）让两个网络不通过网络安全设备的系统，而直接物理上导通，所以有了Bypass后，当网络安全设备故障以后，还可以让连接在这台设备上的网络相互导通，当然这个时候这台网络设备也就不会再对网络中的封包做处理了。

3.10

缩略语

下列缩略语适用于本文件。

IPS：入侵防御系统（Intrusion Prevention System）

IDS：入侵检测系统（Intrusion Detection System）

APN：接入点（Access Point Name）

WEB：全球广域网，也称万维网（World Wide Web）

WAF：WEB应用级防护系统（Web Application Firewal）

IP：互联网协议（Internet Protocol）

VPN：虚拟专用网络 （Vitual private network）

IDC：网络数据中心（Internet DataCenter）

DMZ：非军事化区（Demilitarized Zone）

4 总则

4.1

在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，应符合 2017 年 06 月 01 日颁布的中华人民共和国网络安全法的规定。

4.2

信息系统入网安全等级保护时，对网络安全建设的要求，应符合 GB/T 22239-2008 的规定。

4.3

综合数据网入网安全等级保护时，应符合 GB/T 22240-2020 的规定。

4.4

电力监控系统网络安全防护体系建设，应符合 GB/T 36572-2018 的规定。

4.5

电力行业综合数据网网络边界区域安全防护的新建、改造及优化工作应遵循逻辑隔离、最小化访问控制，报文过滤等基本安全原则。

5 技术要求

云南省电力行业综合数据网应采用单平面方式部署，应遵循“安全分区、网络专用、横向隔离、纵向认证”的安全防护原则，各应用系统必须在满足安全防护规定要求后方可接入。

各边界应部署安全防护设备，严禁计算机、服务器终端不经安全防护设备直接接入骨干综合数据网。

5.1 对外区域

5.1.1 第三方接入区域：第三方接入区中部署与电厂等第三方机构进行交换的前置机，根据业务需求，与电厂等第三方机构通过专线进行提供部分业务数据的交换。具体部署原则如下：

a) 网络防火墙：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，同时通过交换设备进行逻辑跳转，提供前置机到外联机构、信息外网其他区域到前置机的双重访问控制与防护；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS(入侵防御设备)：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，作为防火墙的合理补充；

2）作用用途：提供针对网络 1-7 层的安全攻击过滤与拦截功能。

5.1.2 第三方远端接入区域：第三方远端接入区中部署与远端业务（如：APN）进行交换的前置机，根据业务需求，运营商网络进行提供部分业务数据的交换。具体部署原则如下：

a) 网络防火墙：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，同时通过交换设备进行逻辑跳转，提供前置机到外联机构、信息外网其他区域到前置机的双重访问控制与防护；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS(入侵防御设备)：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，作为防火墙的合理补充；

2）作用用途：提供针对网络 1-7 层的安全攻击过滤与拦截功能。

5.2 内部区域

5.2.1 局域网区域（本部局域网、县公司局域网）：综合数据网内部局域网区域是面向内网的办公区域，包含内网办公终端，主要进行网络层与终端层的保护。具体部署原则如下：

a) 网络防火墙：

1）部署原则：应根据业务可用性要求部署 2 台设备，作为内部和外部网络的保护屏障；

2）作用用途：提供本区域的基本防护和网络访问控制功能。

b) IDS（入侵检测设备）：

1）部署原则：应根据业务可用性要求部署 1 台设备，作为 IPS 设备的合理补充；

2）作用用途：提供对网络攻击的检测与告警功能。

c) 终端防病毒：

1）部署原则：应根据业务可用性要求部署 1 套设备，具体应根据终端数量确定授权数；

2）作用用途：提供对终端的病毒检测与防范功能。

d) 桌面管理系统：

1）部署原则：应根据业务可用性要求部署 1 套设备，具体应根据终端数量确定授权数；

2）作用用途：提供对终端的安全管控功能。

e) 终端数据防泄密：

1）部署原则：应根据业务可用性要求部署 1 套设备，具体应根据终端数量确定授权数；

2）作用用途：提供对终端数据的防泄漏功能。

f) 网络准入系统：

1）部署原则：应根据业务可用性要求部署 1 套设备，具体应根据终端数量确定授权数；

2）作用用途：提供对可信终端的认证和网络准入控制功能。

5.2.2 变电站区域：综合数据网变电站区域同时存在信息内网和III区系统的业务，按照III、Ⅳ区边界的防护要求进行防护，强化该区域与内网之间的逻辑隔离与攻击防范。具体部署原则如下：

a) 网络防火墙：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，作为内部和外部网络的保护屏障；

2）作用用途：提供本区域的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，作为防火墙的合理补充；

2）作用用途：提供针对网络 1-7 层的安全攻击过滤与拦截功能。

5.2.3 改革后企业接入区域：改革后企业接入区域的安全防护终端部分的要求依据与局域网区域要求一致，边界网络控制与第三方接入要求一致。具体部署原则如下：

a) 网络防火墙：
   1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，作为内部和外部网络的保护屏障；
   2）作用用途：提供本区域的基本防护和网络访问控制功能。
b) IPS（入侵防御设备）：
   1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，作为防火墙的合理补充；
   2）作用用途：提供针对网络 1-7 层的安全攻击过滤与拦截功能。
c) 终端防病毒：
   1）部署原则：应根据业务可用性要求部署 1 套设备，具体应根据终端数量确定授权数；
   2）作用用途：提供对终端的病毒检测与防范功能。
d) 桌面管理系统：
   1）部署原则：应根据业务可用性要求部署 1 套设备，具体应根据终端数量确定授权数；
   2）作用用途：提供对终端的安全管控功能。
e) 终端数据防泄密：
   1）部署原则：应根据业务可用性要求部署 1 套设备，具体应根据终端数量确定授权数；
   2）作用用途：提供对终端数据的防泄漏功能。
f) 网络准入系统：
   1）部署原则：应根据业务可用性要求部署 1 套设备，具体应根据终端数量确定授权数；
   2）作用用途：提供对可信终端的认证和网络准入控制功能。

5.2.4 数据中心区域：综合数据网中数据中心区域提供内部办公的相关内网应用，是重要的服务器区域。该区域承载内网的相关 IT 支撑系统，应将相关的安全设备如域控、堡垒机、防病毒等与其他业务系统进行逻辑隔离。数据中心区域内部同时部署了Ⅲ区、Ⅳ区、Ⅴ区系统，Ⅲ、Ⅳ区之间的逻辑隔离应通过防火墙和 IPS 进行控制，形成Ⅲ、Ⅳ区的有效边界；Ⅳ、Ⅴ区之间的逻辑隔离也应通过防火墙和 IPS 进行控制，形成Ⅳ、Ⅴ区的有效边界。具体部署原则如下：

a) 网络防火墙：
   1）部署原则：应根据业务可用性要求部署 2 台设备，作为数据中心边界及Ⅲ、Ⅳ区边界；
   2）作用用途：提供针对边界的基本防护和网络访问控制功能。
b) IPS（入侵防御设备）：
   1）部署原则：应根据业务可用性要求部署 2 台设备，作为数据中心边界及Ⅲ、Ⅳ区边界；
   2）作用用途：提供针对网络 1-7 层的安全攻击过滤与拦截功能。
c) IDS（入侵检测设备）：
   1）部署原则：应根据业务可用性要求部署 1 台设备，作为 IPS 设备的合理补充；
   2）作用用途：提供对网络攻击的检测与告警功能。
d) WAF（网站应用级防护系统）：
   1）部署原则：应根据业务可用性要求部署 1 台设备，作为 Web 应用防护系统；
   2）作用用途：提供针对 web 应用层进行攻击的检测和阻断功能。
e) 网页防篡改系统：
   1）部署原则：应根据业务可用性要求部署 1 台设备，根据应用数量确定；
   2）作用用途：检测网站页面的篡改情况并进行实时恢复。
f) 数据库审计系统：

1）部署原则：应根据业务可用性要求部署 1 台设备，应将数据库与应用前后端分离，将数据库审计部署在前后端逻辑链路之间；

2）作用用途：应用系统中数据库相关数据操作的审计功能。

g) 数据库防火墙：

1）部署原则：应根据业务可用性要求部署 2 台设备，应将数据库与应用前后端分离，将数据库审计部署在前后端逻辑链路之间；

2）作用用途：对系统中数据库攻击操作进行识别和阻断。

h) 堡垒机：

1）部署原则：应根据业务可用性要求部署 2 台设备，保障网络和数据不受来自外部和内部用户的入侵破坏；

2）作用用途：对运维人员操作进行审计记录，并作为集中跳板机，控制访问业务系统后台的路径。

i) 主机安全防护软件：

1）部署原则：应根据业务可用性要求部署 1 台设备，具体根据服务器数量确定授权数；

2）作用用途：加强服务器主机的安全防护和检测能力。

5.2.5 综合数据网边界（省地互联边界）：综合数据网边界是信息内网连通综合数据网的出口，综合数据网连接众多，网络情况复杂，是重要的防护边界。因此，应特别加强该边界的安全防御和检测能力。具体部署原则如下：

a) 网络防火墙：

1）部署原则：应根据业务可用性要求部署 2 台设备，承载特别重要面向综数网业务的信息内网，可部署双重异构防火墙；

2）作用用途：提供面向综数网的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，作为防火墙的合理补充；

2）作用用途：提供针对网络 1-7 层的安全攻击过滤与拦截功能。

c) IDS（入侵检测设备）：

1）部署原则：应根据业务可用性要求部署 1 台设备，部署于广域网边界及城域网边界；

2）作用用途：提供对网络攻击的检测与告警功能。

d) 网络防泄密：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，采用旁路或串联方式，旁路方式下，仅提供告警功能，应仅部署 1 台；串联方式下可同时提供告警与阻断功能，但可能影响网络效率，串联方式下应部署 2 台；

2）作用用途：提供网络传输数据的检测分析功能，对敏感数据外发提供告警，并可进行阻断。

e) 防病毒网关：

1）部署原则：应根据业务可用性要求部署 2 台设备，保护网络内进出数据的安全；

2）作用用途：提供针对网络中僵木蠕毒的检测与阻断功能。

f) 流量分析：

1）部署原则：应根据业务可用性要求部署 1 台设备，对综合数据网进出流量进行分析；

2）作用用途：捕获网络中相关流量数据，根据自定义规则提供深度包解析和安全告警功能。

5.2.6 Ⅲ区Ⅳ区边界：Ⅲ、Ⅳ区是信息内网与生产管理区（调度侧）之间的边界，应强化该区域与内网之间的逻辑隔离与攻击防范。具体部署原则如下：

a) 网络防火墙：

1）部署原则：应根据业务可用性在Ⅲ、Ⅳ区分别要求部署 4 台设备，4 台设备“背靠背”进行部署，作为Ⅲ、Ⅳ区边界区域防护；

2）作用用途：提供针对边界的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）部署原则：应根据业务可用性要求部署 1 台或 2 台设备，作为防火墙的合理补充；

2）作用用途：提供针对网络 1-7 层的安全攻击过滤与拦截功能。

6 验证原则

为保证云南省电力行业综合数据网网络边界安全设备的正确部署，需要对各边界安全设备进行高可用性的验证，以保证每个安全边界可以满足综合数据网未来5年的业务发展需求。

6.1 对外区域

6.1.1 第三方接入区域：

a) 网络防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）验证原则：应根据业务需求，对 IPS 进行 bypass 功能性的测试；

2）作用用途：保证网络 1-7 层的业务正常交互。

6.1.2 第三方远端接入区域：

a) 网络防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）验证原则：应根据业务需求，对 IPS 进行 bypass 功能性的测试；

2）作用用途：保证网络 1-7 层的业务正常交互。

6.2 内部区域

6.2.1 局域网区域:

a) 网络防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IDS（入侵检测设备）：

1）验证原则：应根据业务需求，对 IDS 病毒库进行最新升级测试；

2）作用用途：提供对网络攻击的检测与告警功能。

c) 终端防病毒：

1）验证原则：应根据业务需求，验证终端授权数是否满足现有业务需求；

2）作用用途：提供对终端的病毒检测与防范功能。

d) 桌面管理系统：

1）验证原则：应根据业务可用性要求，验证终端授权数是否满足现有业务需求；

2）作用用途：提供对终端的安全管控功能。

e) 终端数据防泄密：

1）验证原则：应根据业务可用性要求，验证终端授权数是否满足现有业务需求；

2）作用用途：提供对终端数据的防泄漏功能。

f) 网络准入系统：

1）验证原则：应根据业务可用性要求，验证终端授权数是否满足现有业务需求；

2）作用用途：提供对可信终端的认证和网络准入控制功能。

6.2.2 变电站区域：

a) 网络防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）验证原则：应根据业务需求，对 IPS 进行 bypass 功能性的测试；

2）作用用途：保证网络 1-7 层的业务正常交互。

6.2.3 改革后企业接入区域：

a) 网络防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）验证原则：应根据业务需求，对 IPS 进行 bypass 功能性测试

2）作用用途：保证网络 1-7 层的业务正常交互。

c) 终端防病毒：

1）验证原则：应根据业务需求，验证终端授权数是否满足现有业务需求；

2）作用用途：提供对终端的病毒检测与防范功能。

d) 桌面管理系统：

1）验证原则：应根据业务可用性要求，验证终端授权数是否满足现有业务需求；

2）作用用途：提供对终端的安全管控功能。

e) 终端数据防泄密：

1）验证原则：应根据业务可用性要求，验证终端授权数是否满足现有业务需求；

2）作用用途：提供对终端数据的防泄漏功能。

f) 网络准入系统：

1）验证原则：应根据业务可用性要求，验证终端授权数是否满足现有业务需求；

2）作用用途：提供对可信终端的认证和网络准入控制功能。

6.2.4 数据中心区域：

a) 网络防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行高可用性的测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）验证原则：应根据业务需求，对 IPS 进行 bypass 功能性的测试；

2）作用用途：保证网络 1-7 层的业务正常交互。

c) IDS（入侵检测设备）：

1）验证原则：应根据业务需求，对 IDS 病毒库进行最新升级测试；

2）作用用途：提供对网络攻击的检测与告警功能。

d) WAF（网站应用级防护系统）：

1）验证原则：应根据业务可用性要求，对网页应用防护进行压力测试；

2）作用用途：提供针对 web 应用层进行攻击的检测和阻断功能。

e) 网页防篡改系统：

1）验证原则：应根据业务可用性要求，根据应用对防篡改功能进行测试；

2）作用用途：检测网站页面的篡改情况并进行实时恢复。

f) 数据库审计系统：

1）验证原则：应根据业务可用性要求，将数据库与应用前后端分离，对数据库审计部署在前后端逻辑链路进行测试；

2）作用用途：应用系统中数据库相关数据操作的审计功能。

g) 数据库防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

h) 堡垒机：

1）验证原则：应根据业务可用性要求，通过堡垒机，以保障现有网络和数据不受来自外部和内部用户的入侵破坏；

2）作用用途：对运维人员操作进行审计记录，并作为集中跳板机，控制访问业务系统后台的路径。

i) 主机安全防护软件：

1）验证原则：应根据业务可用性要求，根据服务器数量，验证防护软件的授权数是否满足现有业务需求；

2）作用用途：加强服务器主机的安全防护和检测能力。

6.2.5 综合数据网边界（省地互联边界）：

a) 网络防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）验证原则：应根据业务需求，对 IPS 进行 bypass 功能性的测试；

2）作用用途：保证网络 1-7 层的业务正常交互。

c) IDS（入侵检测设备）：

1）验证原则：应根据业务需求，对 IDS 病毒库进行最新升级测试；

2）作用用途：提供对网络攻击的检测与告警功能。

d) 网络防泄密：

1）验证原则：应根据业务可用性要求，验证相关安全设备的告警及阻断功能；

2）作用用途：提供网络传输数据的检测分析功能，对敏感数据外发提供告警，并可进行阻断。

e) 防病毒网关：

1）验证原则：应根据业务可用性要求，验证相关安全设备的病毒库更新功能；

2）作用用途：提供针对网络中僵木蠕毒的检测与阻断功能。

f) 流量分析：

1）验证原则：应根据业务可用性要求，验证综合数据网网络设备流量镜像功能；

2）作用用途：捕获网络中相关流量数据，根据自定义规则提供深度包解析和安全告警功能。

6.2.6 Ⅲ区Ⅳ区边界

a) 网络防火墙：

1）验证原则：应根据业务需求，对防火墙进行高可用性、白名单及地址转换等功能进行测试；

2）作用用途：提供面向外联机构的基本防护和网络访问控制功能。

b) IPS（入侵防御设备）：

1）验证原则：应根据业务需求，对 IPS 进行 bypass 功能性的测试；

2）作用用途：保证网络 1-7 层的业务正常交互。

附 录 A
（资料性）
网络安全防护整体框架构成

A.1 网络安全防护整体框架构成

根据电力监控系统网络安全防护导则（GB/T 36572-2018）相关规定，电力行业在不同安全等级的网络之间应进行安全防护，从而确保电力行业网络信息系统的安全性，数据完整性及可靠性，通过划分不同的安全区域来保证综合数据网网络安全可靠运行。

在电力行业综合数据网中根据业务类型进行详细划分，应划分出：内网办公区、Ⅲ区、Ⅳ区边界区、内网数据中心区、内网DMZ区、内网核心交换区、内外网边界区、外网办公区、外网外联区、外网核心交换区、外网DMZ区、互联网边界区，并在各个区域边界根据防护要求部署符相应的网络安全防护设备。

综合数据网的安全管理应遵循统一管理、分级负责的原则，应按照信息安全等级保护二级系统要求定级、备案及测评。

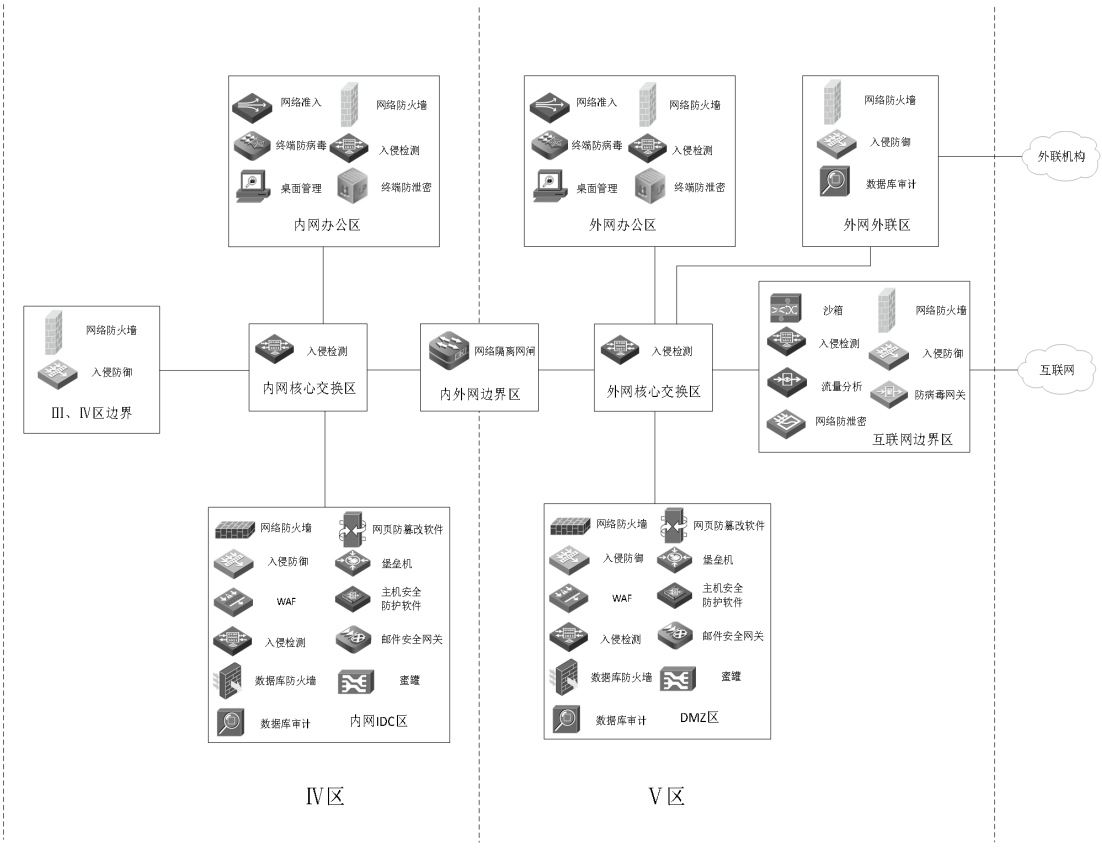


图 A.1 网络安全防护整体框架示意图

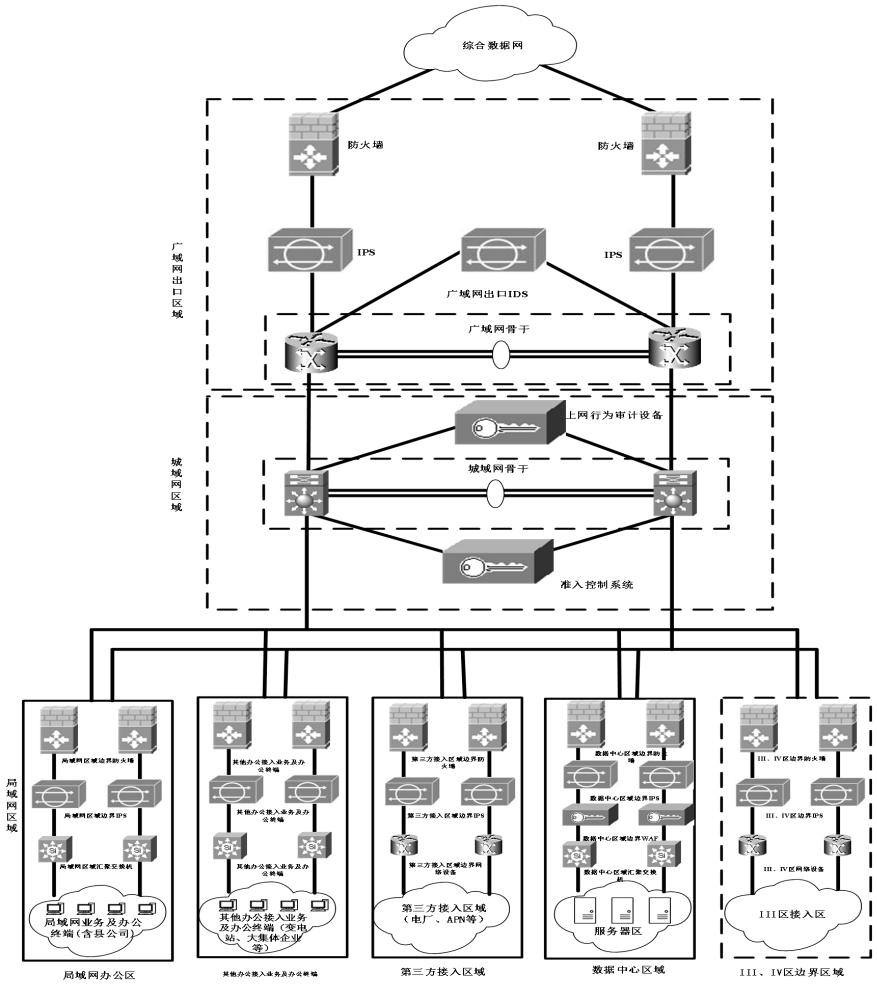
附 录 B
（资料性）
网络拓扑构成

B.1 网络拓扑构成

电力行业综合数据网根据组网原则，应分为广域网、城域网、局域网；根据业务划分，应分为Ⅲ（生产管理系统）、Ⅳ（管理信息大区-信息内网）、Ⅴ（管理信息大区-信息外网）区业务。

电力行业综合数据网依据组网和业务划分原则，划分为各个安全区域，为保证整个综合数据网网络安全、稳定运行，在各个区域边界应部署相应的安全防护设备，如：防火墙、IPS 等，每个区域再根据业务类型部署符合该区域防护要求的配套安全设备。

各个边界区域，根据业务需求，在网络安全防护设备上应设置访问控制策略，对源地址、目的地址进行单向或双向的策略控制，策略按照最小化原则进行黑、白名单限制，只允许符合白名单的策略进行互访。



图B.1 网络拓扑示意图