YD

中华人民共和国通信行业标准

YD 5177—2009

互联网网络安全设计暂行规定

Provisional Specification of Design for
Internet Network Security

2009-02-26 发布　　2009-05-01 实施

中华人民共和国工业和信息化部　发布

统一书号：155635·185

定价：8.00 元

中华人民共和国通信行业标准

互联网网络安全设计暂行规定

Provisional Specification of Design for Internet Network Security

YD 5177—2009

主管部门：工业和信息化部通信发展司
批准部门：中华人民共和国工业和信息化部
施行日期：2009 年 5 月 1 日

北 京 邮 电 大 学 出 版 社
2009 北京

中华人民共和国通信行业标准

互联网网络安全设计暂行规定

YD 5177—2009

*

北京邮电大学出版社出版发行

北京忠信诚胶印厂印刷

*

850 mm×1 168 mm　1/32　印张 1.125　字数 23 千字

2009 年 5 月第 1 版　2009 年 5 月第 1 次印刷

印数:1—5 000 册

统一书号:155635・185　定价:8.00 元

关于发布《通信工程建设环境保护技术暂行规定》等 17 项通信建设规定的通知

工信部通〔2009〕76 号

各省、自治区、直辖市通信管理局，中国电信集团公司、中国移动通信集团公司、中国联合网络通信有限公司，各相关单位：

现将《通信工程建设环境保护技术暂行规定》等 17 项通信建设规定发布，自 2009 年 5 月 1 日起施行，各标准名称、编号如下：

一、《通信工程建设环境保护技术暂行规定》，编号为 YD5039—2009，原《通信工程建设环境保护技术规定》（编号：YD5039—1997）同时废止；

二、《电信客服呼叫中心工程设计规范》，编号为 YD/T 5163—2009；

三、《电信客服呼叫中心工程验收规范》，编号为 YD/T 5164—2009；

四、《本地网光缆波分复用系统工程设计规范》，编号为 YD/T 5166—2009；

五、《本地网光缆波分复用系统工程验收规范》，编号为 YD/T 5176—2009；

六、《通信用柴油发电机组消噪音工程设计暂行规定》，编号为 YD5167—2009；

七、《移动 WAP 网关工程设计规范》，编号为 YD/T 5168—2009；

八、《移动 WAP 网关工程验收规范》，编号为 YD/T 5169—2009；

九、《个性化回铃音平台工程设计暂行规定》，编号为 YD/T 5170—2009；

十、《个性化回铃音平台工程验收暂行规定》，编号为 YD/T 5171—2009；

十一、《通信局(站)防雷与接地工程验收规范》，编号为 YD/T 5175—2009；

十二、《互联网网络安全设计暂行规定》，编号为 YD5177—2009；

十三、《通信管道人孔和手孔图集》，编号为 YD5178—2009；

十四、《光缆通信工程网管系统验收规范》，编号为 YD/T 5179—2009；

十五、《移动通信直放站工程验收规范》，编号为 YD/T 5180—2009；

十六、《宽带 IP 城域网工程验收暂行规定》，编号为 YD/T 5181—2009；

十七、《第三代移动通信基站设计暂行规定》，编号为 YD/T 5182—2009。

以上规定由工业和信息化部负责解释并监督执行，由北京邮电大学出版社负责出版发行（联系电话：010-62285938，网址：www.buptpress.com）。

中华人民共和国工业和信息化部

二〇〇九年二月二十六日

前　言

本暂行规定是根据原信息产业部“关于安排 2007 年《通信工程建设标准》编制计划的通知”（信部规函〔2007〕176 号）的要求制定的。

本暂行规定主要包括网络拓扑结构、路由协议、高可靠性、边界完整性、入侵防范、网络访问控制、网络安全审计、灾难备份与恢复、安全运行管理中心等内容。

本暂行规定用黑体字标注的条文为强制性条文，必须严格执行。

本暂行规定由工业和信息化部通信发展司负责解释、监督执行。暂行规定在使用过程中，如有需要补充或修改的内容，请与部通信发展司联系，并将补充或修改意见寄部通信发展司（地址：北京市西长安街 13 号，邮编：100804）。

主编单位：北京电信规划设计院有限公司

主要起草人：夏俊杰 刘惠明 冯霄鹏 戴维 李磊 陈利兵 安超

参编单位：山西省信息工程设计院

参加人：张　辉　张　晟

目　次

1 总 则

1.0.1 本暂行规定适用于新建互联网网络安全工程设计，改扩建工程应在合理利用原有系统的基础上参照执行。

1.0.2 互联网网络安全设计应以明确的安全需求为基础，全面分析，确定分阶段的安全建设目标、建设内容和建设方案，要与互联网网络建设同步进行或分步骤、分阶段地落实各种安全措施。

1.0.3 互联网网络安全设计应遵循适度安全的原则，结合等级保护相关要求，对互联网网络风险进行合理评估，针对主要风险和威胁，有重点地部署安全措施。

1.0.4 工程中选用的安全产品应取得工业和信息化部（含原信息产业部）颁发的电信设备入网许可证，并满足有关主管部门的相关安全规定。

1.0.5 在特殊条件下，执行本暂行规定中的个别条款有困难时，设计中应充分论述理由，提出采取相应措施的报告，呈主管部门审批。

1.0.6 本暂行规定条款与国家有关标准、规范有矛盾时，应按国家标准、规范的规定执行。

2 术语和符号

英文缩写	英文名称	中文名称
AAA	Authentication Authorization Accounting	鉴别、授权、计费
ACL	Access Control List	访问控制列表
BFD	Bidirectional Forwarding Detection	双向转发检测
BGP	Border Gateway Protocol	边界网关协议
DDoS	Distributed Denial of Service	分布式拒绝服务攻击
DNS	Domain Name System	域名系统
EAP	Extensible Authentication Protocol	扩展认证协议
FRR	Fast Re-Route	快速重路由
GR	Graceful Restart	平稳重启
HIDS	Host Intrusion Detection Systems	基于主机的入侵检测系统
HIPS	Host Intrusion Prevention Systems	基于主机的入侵防御系统
IDC	Internet Data Center	互联网数据中心
IDS	Intrusion Detection Systems	入侵检测系统
IP	Internet Protocol	互联网协议
IPS	Intrusion Prevention System	入侵防御系统
IS-IS	Intermediate System to Intermediate System	中间系统到中间系统协议
LDP	Label Distribution Protocol	标签分发协议
MPLS	Multi-Protocol Label Switch	多协议标签交换
NAT	Network Address Translation	网络地址转换
NIDS	Network Intrusion Detection Systems	基于网络的入侵检测系统
NIPS	Network Intrusion Prevention Systems	基于网络的入侵防御系统
NSR	Non-Stop Routing	不间断路由
OSPF	Open Shortest Path First	开放最短路径优先协议
PPPoE	PPP over Ethernet	以太网上的点对点协议
RADIUS	Remote Authentication Dial In User Service	远端拨入用户验证服务

RSTP	Rapid Spanning Tree Protocol	快速生成树协议
TE	Traffic Engineering	流量工程
uRPF	unicast Reverse Path Forwarding	单播反向路径查找
UTM	Unified Threat Management	统一威胁管理
VPN	Virtual Private Network	虚拟专用网络
VRRP	Virtual Router Redundancy Protocol	虚拟路由器冗余协议

3 网络拓扑结构

3.0.1 网络层级应根据网络建设规模、网络维护组织结构、网络服务质量要求划分为两级或三级结构，通过层级划分进行流量汇聚，并对风险影响范围进行限制。

3.0.2 网络中接入节点与边缘汇接节点之间可采用双星形或环网结构，边缘汇接节点与核心汇接节点连接的拓扑形式可采用双星形结构。核心汇接节点之间的拓扑形式可采用网状结构、不完全网状结构或者是多平面结构。

3.0.3 网络中同一区域内的多台核心汇接节点设备应放置在间隔一定距离的不同通信楼。

3.0.4 核心汇接节点之间必须设置2个或2个以上不同局向的中继电路，不同局向的中继电路必须由不同的传输系统开通。

3.0.5 应合理设置与其他网络的互联互通节点，宜在网络边界处部署专用网络互联设备，并通过中继电路设置或协议设计保证对等和穿透业务流量的合理拓扑结构。

4 路由协议

4.0.1 互联网自治域内的域内路由协议应选用动态路由方式，目前可采用OSPF或IS-IS；自治域之间的域间路由协议可采用BGP-4。

4.0.2 必须保证路由协议自身的安全性，在OSPF、IS-IS、BGP等协议中启用校验和认证功能，保证路由信息的完整性和已授权性。

4.0.3 在域内路由协议中，应根据网络规模和网络拓扑合理规划路由层次，在使用OSPF路由协议情况下划分不同区域，在使用IS-IS路由协议情况下划分不同层级，限制路由规模并将路由震荡的影响限制在一定范围之内。

4.0.4 在网络节点设备中，尤其是域内的层级边界和域间的网络边界设备，应接收路由信息并根据路由策略进行路由信息的宣告。应制定清晰明确的路由信息注入策略，对路由信息的交互进行严格控制，网络节点设备以及业务系统设备路由的宣告和接收应限制在明确界定的范围之内。

4.0.5 域内路由协议与域间路由协议应相互配合，防止路由环回和路由黑洞的产生。

4.0.6 在网络关键节点，可根据源地址/端口、目的地址/端口以及协议类型等参数实施ACL，可根据路由表中的网段和物理接口实施uRPF。

5 高可靠性

5.0.1 通过相关协议参数的设置，在网络中部署路由协议快速收敛技术，实现路由变化时的快速收敛；在网络中部署 RSTP 技术，实现二层链路的快速恢复。

5.0.2 通过 BFD 技术，对核心汇接节点之间、边缘汇接节点之间、业务设备与边缘汇接节点之间的通路进行快速故障检测。当网络中存在多个厂商设备时，应确保 BFD 的互通。

5.0.3 通过 TE FRR 等快速重路由技术，在核心汇接节点之间进行链路保护，提高核心层网络可靠性；也可通过其他专有 FRR 技术（如 IP FRR、VPN FRR），对端口和通路等层级进行保护。在同时部署多种 FRR 机制时，应合理规划，明确各个层级 FRR 之间的关系和功能。当网络中存在多个厂商设备时，应确保 FRR 的互通。

5.0.4 通过 VRRP 技术，以主备方式保障业务系统接入的可靠性并实现故障快速恢复。

5.0.5 通过 GR、NSR 技术，在不间断转发的情况下对 OSPF、IS-IS、BGP、MPLS LDP 等协议进行重启。当网络中存在多个厂商设备时，应确保 GR、NSR 的互通。

5.0.6 核心汇接节点设备必须实现主控板卡、交换板卡、电源模块、风扇模块等关键部件的冗余配置。

5.0.7 可在核心汇接节点和边缘汇接节点部署带外网管系统。

6 边界完整性

6.0.1 本暂行规定中描述的网络边界是指一个网络同其他网络的分界线，互联网边界主要包括不同电信业务经营者互联网之间的分界线、互联网同其他异构网络之间的分界线以及互联网内各安全域之间的分界线。

6.0.2 边界完整性设计应明确安全域的划分。根据需求划分合理的安全域，对于安全级别较高的安全域应重点保护。不同安全域之间，常用的网络边界安全组件和技术有防火墙、VPN 网关、UTM、网闸、数据交换区等。

6.0.3 电信业务经营者的互联网互联边界应采用路由协议的校验和认证等安全机制保障边界完整性。

6.0.4 应根据网络安全等级的需求选择部署包过滤防火墙、应用代理网关防火墙和状态检测防火墙。防火墙宜应用于中小型网络接入公用互联网或应用系统接入公用互联网等场合。

6.0.5 VPN 网关的部署应结合设备的特点、网络状况及主要应用需求灵活选择串联模式、并联模式等部署模式。

6.0.6 UTM 可集成防火墙、IPS、防病毒网关、防拒绝服务攻击网关、内容过滤网关、垃圾邮件过滤网关等各种安全网关的功能，宜应用在客户及小型系统网络边界或不同的网络分区或用户组之间。

6.0.7 网闸设备宜部署在要求物理隔离的网络之间。

6.0.8 数据交换区技术宜用于有频繁的、较大的业务量互通要求或高密级网络对外网互联的应用场合。数据交换区可根据安全级别和功能不同划分不同的逻辑区域。

7 入侵防范

7.0.1 常见的入侵防范的主要措施包括入侵检测、入侵防御和流量监测与清洗等系统。

7.1 入侵检测系统

7.1.1 入侵检测系统包括 HIDS 和 NIDS。HIDS 的数据采集部分应部署在其所监测的主机上，NIDS 的数据采集部分应部署在其所监测的网络上。

7.1.2 部署 HIDS 时，应在考虑系统检测功能实现的同时，充分考虑其对所在主机的性能影响。

7.1.3 NIDS 通常部署在受保护的网络中或被监控的链路上，宜部署在网络的进出口处或数据交换区域，对关键链路或数据交换区进行安全检测。NIDS 的部署方式可采用链路旁路方式部署在被检测的链路中，也可利用网络设备的端口镜像功能以旁挂方式部署在数据交换区域。

7.1.4 NIDS 可与防火墙配合使用，由 NIDS 实现安全检测功能，由防火墙实现安全控制功能，通过两者联动来实现自动安全检测和控制。为避免 NIDS 产生海量告警，宜放置在防火墙内侧。

7.2 入侵防御系统

7.2.1 入侵防御系统可对网络威胁进行主动和实时的防御，宜部署入侵防御系统进行风险控制。

7.2.2 入侵防御系统包括 HIPS 和 NIPS。HIPS 可部署在服务器上，NIPS 宜部署在网络的进出口位置，对入侵活动和攻击流量进行拦截，以最大程度地减少损失。

7.2.3 HIPS 宜部署在被保护主机上，用于监听用户的访问行为，其部署应充分考虑其对所在主机性能的影响。

7.2.4 NIPS 宜采取串行部署方式，应保证所有需要保护的网络数据都经过 NIPS 设备。NIPS 应具备故障倒换功能，避免因为设备或电源故障对网络造成影响。NIPS 也可采用旁挂方式进行部署以减少对网络结构的影响。

7.3 流量监测与清洗系统

7.3.1 流量监测系统设计应结合网络设备能力以及实际网络情况，灵活选择流采样、链路分光或端口镜像等部署方式。

7.3.2 流量清洗系统可部署在省网、城域网等被保护网络的边界，也可部署在 DNS、认证计费系统等重要支撑系统以及 IDC 网络出口等重要位置。

7.3.3 流量清洗系统的部署应结合网络实际情况制定合理的引流、过滤、回注策略，避免引流、回注过程中大规模流量调度影响网络中正常业务流量转发。

7.3.4 流量监测系统与流量清洗系统之间应能够实现系统之间的联动，必要时建立联动接口，在发现攻击流量后以手动或自动方式实现攻击流量的清洗过滤。

8 网络访问控制

8.0.1 通过网络访问控制设计，防止对于网络设备的未授权访问及对于网络资源的未授权使用。

8.0.2 网络访问控制设计应首先分析访问控制需求，明确用户或用户组、资源、操作和限制条件等访问控制要素。

8.0.3 网络访问控制设计应根据保护对象需求按照自主访问控制、强制访问控制、角色访问控制等级别进行分类，并在此基础上合理制定访问控制策略。

8.0.4 宜采用配置路由器、交换机等网络设备的访问控制列表，或者部署防火墙设备、代理服务器、专用访问控制设备等手段来实现访问控制。访问控制设备可部署在网络的边界或用户网络及系统的出口位置。

8.0.5 访问控制的实现应以用户身份识别与认证为前提。用户接入网络时应通过 PPPoE、802.1x/EAP、DHCP＋Web Portal 等宽带接入认证技术进行认证后才能有效接入网络。实现用户身份识别宜采用基于用户名/口令、智能卡或证书等通用方式。

8.0.6 用户应在受控情况下使用各类网上应用，应经过 AAA 系统的鉴权、认证和计费。互联网上针对公众用户的 AAA 系统可基于 RADIUS 或 DIAMETER 认证服务器来实现。

9 网络安全审计

9.0.1 网络安全审计应由专用审计系统或相关安全设备来实现。部署专用审计系统时宜重点考虑日志采集、主机审计、网络审计、审计中心等部分；部署相关安全设备时宜选取网络漏洞扫描、防火墙、IDS/IPS、互联网行为监控等产品。

9.0.2 网络安全审计的对象应包括路由器和交换机等网络设备、服务器、网络安全设备等。所有审计对象应开启日志记录功能，日志信息宜统一存储在审计中心。

9.0.3 应结合用户的定制化审计需求，明确各类审计对象的审计重点，可选择日志审计、主机审计、网络审计等审计方法。可采取分层模式建设日志采集代理、审计客户端、网络审计服务器、审计中心等。

10 灾难备份与恢复

10.0.1 灾难备份及恢复应以等级保护和风险评估为基础，灾难备份与恢复的等级应与安全等级保护确定的安全等级一致。

10.0.2 互联网网络自身的灾难备份与恢复相关设计可参见本暂行规定“网络拓扑结构”和“高可靠性”章节要求。应用系统及物理层面的灾难备份与恢复应参见其他相关标准。

10.0.3 应建立网络安全监测机制，制定灾难备份策略和恢复方案，并通过加强安全管理落实相关策略和流程。

11 安全运行管理中心

11.0.1 安全运行管理中心应具有安全事件管理、安全策略管理、安全预警管理、安全日志审计、知识库管理、流程管理、关联分析、风险管理等功能。

11.0.2 安全运行管理中心应具有时间同步功能，保证安全事件计时的一致性，实现安全事件分析和日志审计。

11.0.3 安全运行管理中心应支持对各类被管理对象的多种数据采集方式，实现安全事件收集、安全日志收集等功能。应提供与邮件、工单、短信平台等系统的接口，实现安全预警、安全响应等功能。

11.0.4 安全运行管理中心可采取分级建设模式，多级安全运行管理中心之间应制定明确合理的上下级接口规范。

附录A　本规定用词说明

本暂行规定条文严格程度的用词，采用以下写法：

A.0.1　表示很严格，非这样不可的用词；

正面词采用“必须”；

反面词采用“严禁”。

A.0.2　表示严格，在正常情况下均应这样做的用词：

正面词采用“应”；

反面词采用“不应”或“不得”。

A.0.3　表示允许稍有选择，在条件许可时首先应这样做的用词：

正面词采用“宜”；

反面词采用“不宜”；

表示允许有选择，在一定条件下可以这样做的，采用“可”。

中华人民共和国通信行业标准

互联网网络安全设计暂行规定

Provisional Specification of Design for Internet Network Security

YD 5177—2009

条 文 说 明

前　言

按照等级保护、风险评估、灾难备份与恢复方面的相关要求，互联网网络安全框架总体上可包括安全技术和安全管理两个体系。其中，安全技术体系分为物理安全、网络安全、信息传递与业务提供安全、应用安全不同的层面。网络安全包含网络自身安全性和网络安全防护两个方面，网络自身的安全性一般包含网络拓扑结构安全、路由协议安全、高可靠性等方面，网络安全防护包括边界完整性、入侵防范、网络访问控制、网络安全审计等方面。在保障网络安全的基础上，可通过安全运行管理中心和完善的安全管理措施，来最大化地提高网络的安全防护能力和安全管理水平，通过灾难备份与恢复保障网络在出现故障时的快速切换与恢复。

本暂行规定主要规定了网络安全方面的相关设计要求，包括网络拓扑结构、路由协议、高可靠性、边界完整性、入侵防范、网络访问控制、网络安全审计、灾难备份与恢复、安全运行管理中心等内容。本暂行规定不包括与物理安全、信息传递安全、业务提供安全以及应用安全相关的工程设计要求，这部分内容的设计应参见相关的标准、规范。

目　次

6 边界完整性

6.0.1 互联网边界存在的安全威胁主要有用户的非法访问、黑客及病毒的入侵、网络攻击等，强化互联网边界的完整性是有效实现网络安全的必要手段。边界完整性设计的目的是将安全风险和威胁限定在一定的安全范围内，避免安全风险的大范围扩散，保障不同区域的安全性，实现对网络的分级分域防护。

6.0.2 在进行边界完整性设计时应重点考虑以下内容：

1. 应明确安全域的划分。根据需求划分合理的安全域，对于安全级别较高的安全域应重点保护；

2. 应明确边界控制重点的安全保护等级，如重点是控制边界的入侵行为还是防范外部的攻击，是仅对外部进行访问控制还是严格要求物理隔离等；

3. 应保持网络原有的性能特点，对网络上的应用、协议和数据传输具有透明性；

4. 边界完整性建设不应影响网络的扩展和网络上承载系统的部署方式及系统功能实现。

6.0.3 运营商的互联网互联边界不宜部署防火墙、UTM 等网络边界安全组件。

6.0.5 VPN 是提供远程访问内部网络功能的主要部件。

7 入侵防范

7.0.1 入侵防范是指从IP网络的若干关键点收集信息并对其进行分析，从中发现网络中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定的安全措施。入侵检测主要检测端口扫描、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、网络蠕虫攻击等入侵行为，发现是否有违反安全策略的行为或遭到入侵的迹象；入侵防御则是一种主动的入侵防范、阻止系统，检测到攻击企图后，会自动丢弃非法包或采取其他阻断措施。

1. 通过入侵检测系统的设计和部署，实现对网络或主机中的信息探测、拒绝服务、蠕虫病毒、权限获取和可疑网络活动等威胁进行检测和识别，必要时提供安全记录和告警，为了解安全状况和阻断非法访问提供依据。

2. 通过入侵防御系统的设计和部署，实现对网络或主机中的信息探测、拒绝服务、蠕虫病毒、权限获取和可疑网络活动等威胁进行检测和识别，并主动、实时地采取措施对攻击或恶意数据包进行限制和阻断。

3. 通过部署流量监测系统，对网络中的路由设备发出的流信息进行采集分析，关联网络的路由信息，发现定位网络中的DDoS等攻击流量，保证网络的安全性和可用性，为网络优化改造提供依据。

7.3.1 采用流(Flow)采样方式部署时，应合理设置被监测路由设备的流(Flow)采样比例，确保路由设备开启流采集不影响正常流量转发。

8 网络访问控制

8.0.1 访问控制技术通常包括入网访问控制、网络权限控制、目录级控制、属性控制等级别，本暂行规定规范了入网访问控制和网络权限的访问控制。

9 网络安全审计

9.0.1 网络安全审计的设计目标就是要实现对系统的记录及活动进行独立地复查与检查，以便监测系统控制是否充分，确保系统控制与现行策略和操作程序保持一致，探测违背安全性的行为，并通告控制、策略和程序中所显示的任何变化，为事后取证和安全策略调整提供依据。

11 安全运行管理中心

11.0.1 安全管理中心是实现安全管理的技术平台，通过安全运行管理中心的设计和部署，实现对防火墙、入侵检测等安全设备（系统）的统一安全管理，实现对风险和安全状况的集中呈现和管理。