ICS 33.030
M 21

YD

中华人民共和国通信行业标准

YD/T 2089-2010

局域网网关型
互联网内容过滤产品技术要求

Technical requirements for internet content control based on LAN gateway

2010-12-29 发布　　2011-01-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言……II
引　言……III
1　范围……1
2　规范性引用文件……1
3　术语、定义和缩略语……1
3.1　术语和定义……1
3.2　缩略语……1
4　局域网环境内不良信息防控概述……2
5　局域网网关型内容过滤产品架构……3
6　功能要求……4
6.1　基本功能……4
6.2　附加功能……7
7　性能要求……7
7.1　准确性……7
7.2　兼容性……7
7.3　安全性……7
7.4　网络数据处理性能要求……8

前　言

本标准是“绿色上网”系列标准之一。该系列标准预计的名称及结构如下：

1. YDN 138-2006　基于PC终端的互联网内容过滤软件技术要求
2. YDN 139-2006　基于PC终端的互联网内容过滤软件测试方法
3. 基于移动终端的互联网内容过滤软件技术要求
4. 基于移动终端的互联网内容过滤软件测试方法
5. YD/T 2054-2010　WAP网关内容过滤技术要求
6. YD/T 2055-2010　宽带网络接入服务器内容过滤技术要求
7. YD/T 2087-2010　WAP网关内容过滤测试方法
8. YD/T 2088-2010　宽带网络接入服务器内容过滤测试方法
9. YD/T 2089-2010　局域网网关型互联网内容过滤产品技术要求
10. YD/T 2090-2010　局域网网关型互联网内容过滤产品测试方法

随着绿色上网相关技术和业务的发展，还将制定后续的相关标准。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：国家计算机网络应急技术处理协调中心、中国互联网协会、深圳市任子行网络技术有限公司、郑州金惠计算机系统工程公司、西安邮电学院、工业和信息化部电信研究院。

本标准主要起草人：黄元飞、舒　敏、古　元、张　新、杨君佐、景晓军、汤怀礼、刘建华。

引　言

互联网给人们带来资源共享的同时，互联网上淫秽、色情等不良信息的存在对青少年的健康成长也造成极大隐患。目前在互联网上活动的黄色网站每天都在增长，由互联网不良信息引发的犯罪时有发生且呈上升趋势。近期即时通信、P2P共享、网络游戏等新的网络技术在互联网应用方面越来越广泛普及，许多不良信息也随之渗透进来，未成年人往往缺乏判断力和行为约束得以接触这些不良信息。如何实现对互联网有害内容的控制和网络访问行为管理，保护未成年人的健康上网，已成为整个社会、学校、家庭所关注的急需解决的问题。

制定绿色上网相关技术标准是从技术角度出发，规范绿色上网产品，指导和引导绿色上网相关技术的发展，为防范互联网不良信息侵扰，净化网络空间，营造绿色上网环境，推动绿色上网行动提供有效的技术手段。在实现技术方面包括内容过滤和网络行为管理两方面。目前，内容过滤技术国内外主要采用网址过滤、图像过滤、文本过滤、音频过滤、视频过滤等互联网内容过滤技术，对预先定义的互联网网址、文本或图像进行过滤和拦截，禁止或限制用户访问淫秽、色情等不良互联网内容，以达到防范互联网不良信息，为广大网民特别是青少年提供健康、安全、文明的网络环境的目的。网络行为管理方面主要包括上网身份认证，网络访问行为记录及分析，限制上网时间，限制访问网络范围，限制网络游戏，限制即时通讯，限制BT，限制音视频类服务等。但由于互联网的开放性、国际性和复杂性以及信息通信技术的迅速发展，互联网不良信息存储格式、传播方式、内容形式在不断变化，即使采用当前所有互联网内容过滤技术，也存在对互联网不良信息遗漏和错判现象。同时，为青少年健康成长创造绿色网络空间，实现绿色上网，又是一项复杂的、系统的社会工程，需要采用经济、法律、技术、行政等多种手段，对互联网进行综合治理，才能达到标本兼治的目的。

局域网网关型互联网内容过滤产品技术要求

1 范围

本标准规定了局域网环境内对互联网内容进行过滤，禁止或限制用户访问预定义的互联网内容的网关型互联网内容过滤产品（以下简称内容过滤网关）的主要功能和性能要求。

本标准适用于局域网网关型互联网内容过滤产品，也可供部署在接入网的内容过滤产品参考。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

IETF RFC 1305　　网络时间协议

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

互联网内容过滤　*Internet Content Filtering*

通过技术手段实现内容过滤，对预先定义的互联网内容进行过滤和拦截，禁止或限制用户访问。

3.1.2

语义分析　Semantic Analysis

对语言单位的意义进行分析。

3.1.3

网址　Web Site

互联网信息资源的位置标志，这里指域名、URL和IP地址。

3.2 缩略语

下列缩略语适用于本标准：

CPU	Central Processing Unit	中央处理器
FAT	File Allocation Table	文件分配表
IDF	Inverse Document Frequency	倒文档频率
IP	Internet Protocol	网际协议
KFV	Keyword Frequency Vector	词频向量
NTFS	New Technology File System	NT文件系统
NTP	Network Time Protocol	网络时间协议
PC	Personal Computer	个人计算机
TF	Term Frequency	词频
URL	Uniform Resource Locator	统一资源定位器

USB　　Universal Serial Bus　　通用串行总线

4　局域网环境内不良信息防控概述

互联网上不良信息的表现形式主要有色情文学、黄色图像、色情动画、色情声音、成人电影等，基本覆盖了互联网上信息存在的所有形式：文本、图像、音频、视频，网址是各种形式的互联网信息的位置标志。局域网环境内不良信息的防控包括网络内容过滤和网络行为管理两大部分。

4.1　网络内容过滤

网络内容过滤的主要技术手段有网址过滤、文本过滤、图像过滤、音频过滤和视频过滤等，其中文本过滤主要有语义分析过滤、关键词过滤两种方式。在本标准中，文本过滤、图像过滤、音频过滤和视频过滤称为直接内容过滤技术，以区别于间接对互联网内容进行过滤的网址过滤技术。

—— 网址过滤

网址过滤的基本原理是基于既定的网址数据库，用户访问相关网页时，过滤产品根据网页对应网址的属性判断是否为不良网址，如果是则拦截。

网址数据库作为过滤产品判定一个网址是否有害的依据，其有效性的维护是网址过滤技术的关键。

—— 图像过滤

指对上网过程中的图像进行特征分析、特征提取，并利用模式识别和模糊匹配技术与图像特征数据库中的图像特征进行相似性匹配判决，对符合匹配条件的图像进行过滤。

相似性匹配判决的基础是图像特征库。图像特征库包括但不限于：淫秽、色情等图片特征集。图像格式，包括但不限于：JPG、JPEG、GIF、BMP、PNG、TIFF。

—— 语义分析过滤

指在访问互联网内容时，采用语义分析的方法对内容进行实时扫描，过滤被禁止访问的内容。

语义分析是指通过对所使用语言的语义倾向和所涉及的场景两个维度分析，来综合判断文本类型，其中语义倾向直接从词语的语义获得，场景从情景框架获得，即在敏感词语判断的基础上通过情景框架分析进行言语模式的判断，进而判定文本类型。

语义分析过滤技术通常以知识库体系作为支撑。通过知识库的扩充，可以实现对不同领域的过滤。

语义模型的表达式主要有 TF*IDF、词频向量（KFV）、语义本体（Semantic Ontology）等。

—— 关键词过滤

指在文本中匹配关键词，根据定义的关键词过滤规则认定是否为禁止的内容。

关键词过滤的作用范围包括但不限于：

— 对URL请求的域名、路径、查询部分分段过滤，拒绝符合关键词规则的URL请求；

— 对浏览器的窗口标题进行关键词过滤，关闭符合关键词规则的浏览器窗口；

— 对浏览器的显示内容进行关键词过滤，关闭符合关键词规则的浏览器窗口；

— 对应用程序的标题名称进行过滤，关闭符合关键词规则的应用程序。

—— 音频过滤

指对用户所访问的互联网音频信息进行识别，并利用特征匹配技术与音频特征数据库中的音频特征进行匹配判决，对符合匹配条件的音频进行过滤。

匹配判决的基础是音频特征库。音频特征信息包括听觉感知特征和听觉非感知特征，听觉感知特征包括音量、音调、音强等，听觉非感知特征即物理特征。

—— 视频过滤

指对用户所访问的互联网视频信息进行识别，并利用匹配技术与视频特征数据库中的视频特征进行匹配判决，对符合匹配条件的视频进行过滤。

匹配判决的基础是视频特征库。

4.2 网络行为管理

网络行为管理包含：

—— 即时通信管理

管理通过局域网网关的即时通信，决定是否允许用户使用 QQ、MSN、ICQ、YahooMessenger 等即时通信和进行文件传输。

—— 网络游戏管理

管理通过局域网网关的网络游戏。

—— P2P 下载控制

控制是否允许 P2P 下载、定义可以下载的文件类型。

—— 收发邮件控制

设置 WebMail 邮箱的 URL 控制列表，以实现禁止使用指定的 WebMail 收发邮件。

设置 POP3、SMTP 的邮件服务器控制列表，通过选择只封堵或只开放该列表中的邮件服务器来实现对收发邮件的控制。

—— 终端管理和账号管理

实现对局域网内 IP 地址和终端名的搜索，并对搜索到的终端信息进行分组管理；还可以设定部分或全部终端须用账号上网，通过对账号的分组管理，可实现在同一终端上不同用户具有不同的上网活动权限。

—— 实时查看网络状况

实时查看当天流量情况，查看正在进行网络活动的用户及活动情况，以获知当前网络流量比较大的用户及距当前某段时间内上网很活跃的用户。

5 局域网网关型内容过滤产品架构

内容过滤产品的过滤功能有网址过滤、文本过滤（包括语义分析过滤和关键词过滤）、图像过滤、音频过滤、视频过滤。过滤产品除具有内容过滤功能外，一般还具备即时通讯控制、网络游戏控制、P2P 下载控制、收发邮件控制、终端管理和账号管理、实时查看网络状况、上网时间管理、权限管理、日志管理、过滤等级设定、远程告知、远程控制、软件升级和帮助等辅助功能。

根据上述互联网内容过滤产品的主要功能，过滤产品架构如图1所示。

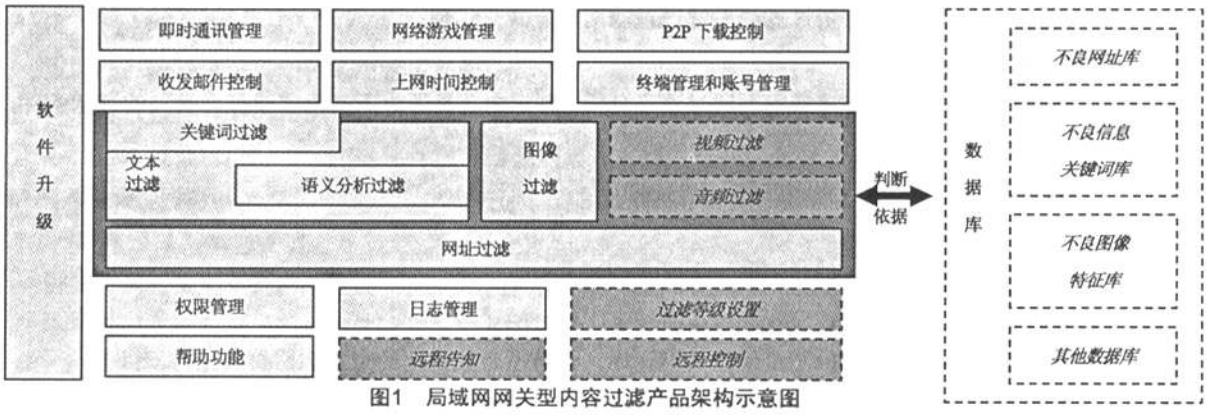

图1 局域网网关型内容过滤产品架构示意图

在上述软件架构中，过滤产品将与不良网址库、不良信息关键词库、不良图像特征库等数据库交互，以获得过滤的判断依据。

6 功能要求

6.1 基本功能

6.1.1 网址过滤

过滤产品应提供对网址（域名、URL或IP地址）进行过滤的功能，拦截对不良网址的访问请求。

（1）默认方式

过滤产品能将所访问的网址同不良网址数据库进行比对、判断，拦截淫秽、色情等不良网址。

过滤产品应配备一个较完备的不良网址数据库。网址数据库应记录完整的域名、URL、IP地址等网址信息，采用符合相关要求的加密格式存储和处理。网址数据库应按照国家有关规定支持在线升级，或以同步方式更新网址信息。

（2）自定义方式

自定义方式的网址过滤可以采用但不限于以下三种手段，且可以通过多种手段协作实现：

a）黑名单：管理员可以通过人工添加网址的办法设定一些网址禁止用户访问；

b）白名单：管理员可以通过人工添加网址的办法设定一些网址永远不被信息过滤产品过滤和拦截；

c）只允许访问：管理员可以开启此选项，使得只能访问“只允许访问名单”中的网址，其他网址禁止用户访问。

过滤产品如采用黑白名单进行网址过滤，应提供如下黑白名单管理功能：

— 管理员应可以人工添加、删除和修改黑白名单，可以将单个或多个网址（网页）添加至黑（白）名单；

— 黑白名单冲突时，系统应有告警信息，且提供优先选择设置，且默认方式为黑名单优先。

6.1.2 直接内容过滤

过滤产品应提供对文字、图像等互联网内容进行直接过滤的功能，拦截对不良信息的访问请求，以禁止或限制用户访问不良的互联网内容。

过滤软件应支持文本过滤和图像过滤功能，宜支持视频过滤和音频过滤功能。

（1）文本过滤

过滤产品应对互联网上的文本信息内容进行分析、识别，拦截淫秽、色情等不良文本信息。

文本过滤主要采取语义分析过滤或关键词过滤两种方式来实现：

a）语义分析过滤

— 过滤产品对访问的文本或网页通过语义分析，判定内容是否为不良内容或符合设定的过滤条件，如果是则禁止访问；

— 能够准确判断文本内容的性质；

— 具备完善的知识库；

— 具有良好的扩展性，能够不断扩大过滤领域。

b）关键词过滤

— 过滤产品具备较完善的不良信息关键词库，含有不良关键词的文本和网页禁止访问；

— 管理员可以添加、删除和修改关键词。

（2）图像过滤

过滤产品应能对互联网上的图像内容进行分析、识别，拦截淫秽、色情等不良图像。

过滤产品应配置一个较完备的不良图像特征库。

不良图像特征库至少应含有淫秽、色情图像相关的特征信息。

（3）视频过滤

利用图像识别技术，对屏幕上出现的视频（包括流媒体）进行分析计算，通过计算结果判断该当前画面是否含有不良信息，如含有不良信息则进行拦截。

（4）音频过滤

利用音频识别技术，对播放的声音进行分析计算，通过计算结果判断是否含有不良信息，如含有不良信息则进行拦截。

6.1.3 即时通讯管理

过滤产品应提供下列即时通信管理功能：

— 可对常见的即时通信工具设置开放、封堵策略；

— 可依据策略禁止或限制相应的即时通信及文件传输；

常见的即时通信工具包括但不限于：QQ、MSN、ICQ、Yahoo Messenger、UC、AOL Messenger、网易泡泡、搜Q、UU通、Google Talk、Skype等。

6.1.4 网络游戏管理

过滤产品应提供下列网络游戏管理功能：

— 可对常见的在线网络游戏设置开放、封堵策略；

— 可依据策略禁止或限制相应的网络游戏联网；

常见的在线网络游戏包括但不限于：QQ游戏、联众、中国游戏中心、边锋、远航、浩方、魔兽世界等。

6.1.5 P2P 下载控制

过滤产品应提供下列P2P下载控制功能：

— 可对常见的P2P下载设置开放、封堵策略；

— 可依据策略禁止或限制P2P下载；

常见的P2P下载工具包括但不限于：BitComet、BitTorrent Deadman Walking、比特精灵（Bit Spirit）、TurboBT等。

6.1.6 收发邮件控制

过滤产品应提供下列邮件应用管理功能：

— 可以设置WebMail邮箱的URL控制列表，以实现禁止使用指定的WebMail收发邮件。

— 可以设置POP3、SMTP的邮件服务器控制列表，通过选择只封堵或只开放该列表中的邮件服务器来实现对收发邮件的控制。

6.1.7 终端管理和账号管理

过滤产品应提供下列网络管理功能：

— 可以实现对局域网内IP地址和终端名的搜索，并对搜索到的终端信息进行分组管理；

— 可以设定部分或全部终端须用账号上网；

— 通过对账号的分组管理，可实现在同一终端上不同用户具有不同的上网活动权限；

— 按终端或账号对上网行为进行监管。

6.1.8 实时查看网络状态

过滤产品应可实时查看当天流量情况，查看正在进行网络活动的用户及活动情况，以获知当前网络流量比较大的用户及某段时间内上网很活跃的用户。

6.1.9 上网时间管理

过滤产品应具备对上网时间进行管理的功能。用户可根据需要设定上网的时间表，在设定的时间单元内中断网络访问。设置单元应包括但不限于：小时、天、周。

过滤产品应具备自动时间校正功能，以防止修改系统时间规避管理。网络对时协议宜采用IETF RFC 1305。

6.1.10 权限管理

过滤产品应设置有管理员，以对过滤产品进行配置和管理。

过滤产品应提供对管理员进行身份鉴别的功能。身份鉴别方式可采用但不限于口令字、USB钥匙等。

6.1.11 日志管理

内容过滤产品应具备日志功能。

— 日志数据生成

应至少能对下列事件生成日志：

a） 网络访问，包括但不限于HTTP、HTTPS、SMTP、POP3、Telnet、FTP等；

b） 网络流量，特别是单个用户的流量；

c） 对不良网址或不良内容的过滤和拦截；

d） 所拦截的即时通信；

e） 所拦截的网络游戏；

f） 所拦截的P2P下载；

g） 过滤规则的修改；

h） 管理和控制策略的修改；

i） 过滤产品的启动、关闭和更新。

应在每一个日志记录中记录事件发生的时间、事件描述，必要时保留相关的证据。

— 日志查询

过滤产品应提供对日志记录的查询功能，且只允许管理员查询日志记录。

— 日志导出或存档

过滤产品应提供对日志记录的导出、存档功能，且只允许管理员导出、存档日志记录。

— 日志删除或清空

过滤产品应提供对日志记录的删除、清空功能，且只允许管理员删除、清空日志记录。

— 日志的统计功能

可以对上述日志信息进行统计，以表格、图表的形式提供统计报表。

— 日志保存设置功能

用户可自行设定日志保留的天数及磁盘限额。

— 日志报表和趋势分析图

提供各种上网活动的排名、统计、趋势分析图。可对分组、对人员进行网络活动排名，对访问资源进行统计，对各网络活动进行访问趋势分析。

6.1.12 帮助功能

过滤产品应提供完备的帮助功能。

6.1.13 升级功能

过滤产品应具备在线升级功能，升级的内容包括但不限于：主过滤引擎、关键词库、不良网址库、图像特征库等。

过滤产品应具有升级告知功能。

软件的升级可通过但不限于以下两种方式实现：

— 自动在线升级：用户在接入互联网状态下，软件自动搜索是否有升级包，发现升级包自动下载并安装，用户没有提示界面；

— 手动在线升级：用户通过手动方式连接升级服务器，通过界面提示自动下载升级程序，并进行安装。

6.2 附加功能

6.2.1 远程告知

访问符合设定过滤条件的网址或内容时，宜自动形成告警并告知远程的管理员或指定人员。

6.2.2 过滤等级设定

过滤产品宜对过滤等级（过滤灵敏度）进行设定，禁止访问符合设定条件的文本、图像。

管理员应能够对过滤等级（过滤灵敏度）进行调节，从而改变内容信息过滤的粒度。

过滤产品过滤等级（过滤灵敏度）的缺省级别应为最高级别。

6.2.3 远程控制

过滤产品宜允许管理员远程察看日志或者远程修改过滤产品的过滤设置等。

7 性能要求

互联网内容过滤产品性能指标主要包括四类：准确性指标、兼容性指标、安全性指标和网络数据处理性能指标。

7.1 准确性

准确率、漏判率、误判率是评价准确性的常用指标：

— 对不良信息的准确率是指过滤产品正确判断不良互联网内容的概率。

— 对不良信息的漏判率是指过滤产品将不良互联网内容错误判断为合法互联网内容的概率。

— 对合法信息的误判率是指过滤产品将合法互联网内容错误判断为不良互联网内容的概率。

过滤产品对不良信息判断的准确率应不低于90%，对不良信息的漏判率和对合法信息的误判率应不高于10%。

7.2 兼容性

过滤产品应兼容十、百、千、比特每秒兆以太网络环境。

过滤产品应能兼容防火墙、网络代理模式环境。

7.3 安全性

过滤产品的本身不应留有安全漏洞，并具备自身安全防护功能。

过滤产品宜具备故障检测和故障略过机制。

过滤产品的配置规则、相关数据库等关键信息应采用加密格式存储。

在使用网址过滤时，过滤产品应保证不能通过代理服务器回避过滤限制。

未经用户许可，过滤产品不得收集用户信息。

7.4 网络数据处理性能要求

7.4.1 吞吐量

吞吐量视不同速率的网关有所不同，具体指标要求如下：

a） 网关在只有一条允许规则和不丢分组的情况下，应达到的吞吐量指标：

1） 对64字节短分组，十兆和百兆比特每秒网关应不小于线速的20%，吉比特每秒及吉比特每秒以上网关应不小于线速的35%；

2） 对512字节中长分组，十兆和百兆比特每秒网关应不小于线速的70%，吉比特每秒及吉比特每秒以上网关应不小于线速的80%；

3） 对1518字节长分组，十兆和百兆比特每秒网关应不小于线速的90%，吉比特每秒及吉比特每秒以上网关应不小于线速的95%。

b） 在添加200条不同的访问控制规则的情况下，网关的吞吐量下降应不大于原吞吐量的3%。

7.4.2 延迟

延迟视不同速率的网关有所不同，具体指标要求如下：

a） 十兆比特每秒网关的最大延迟不应超过1ms；

b） 百兆比特每秒网关的最大延迟不应超过500μs；

c） 吉比特每秒及吉比特每秒以上网关的最大延迟不应超过90μs；

d） 在添加200条不同的访问控制规则的情况下，网关延迟所受的影响应不大于原来的3%。

7.4.3 最大并发连接数

最大并发TCP连接数视不同速率的网关有所不同，具体指标要求如下：

a） 十兆比特每秒网关的最大并发连接数应不小于1000个；

b） 百兆比特每秒网关的最大并发连接数应不小于10000个；

c） 吉比特每秒及吉比特每秒以上网关的最大并发连接数应不小于100000个。

7.4.4 最大连接速率

最大TCP连接速率视不同速率的网关有所不同，具体指标要求如下：

a） 十兆比特每秒网关的最大连接速率应不小于每秒500个；

b） 百兆比特每秒网关的最大连接速率应不小于每秒1500个；

c） 吉比特每秒及吉比特每秒以上网关的最大连接速率应不小于每秒5000个。