ICS 33.040
M 16

YD

中华人民共和国通信行业标准

YD/T 2668-2013

电信网络异常流量检测与控制技术要求

Abnormal traffic detection and control guideline for telecommunication network

2013-10-17 发布　　2014-01-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准按照 GB/T1.1-2009 给出的规则起草。

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：中国移动通信集团公司、华为技术有限公司、中兴通讯股份有限公司、工业和信息化部电信研究院、杭州华三通信技术有限公司。

本标准主要起草人：刘利军、何　申、王　静、任兰芳、王雨辰、刘利峰。

电信网络异常流量检测与控制技术要求

1 范围

本标准定义了电信网络面临的异常流量防护需求、检测技术、控制措施、监控产品部署方式，以及监控系统的性能和接口要求等。

本标准适用于对电信网络的异常流量的检测和控制。

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，仅所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。

IETF RFC 438，FTP的服务器与服务器交互（FTP server-server interaction）

IETF RFC 697，FTP的CWD命令（CWD command of FTP）

IETF RFC 775，面向目录的 FTP 命令（Directory oriented FTP commands）

IETF RFC 2228，FTP安全扩展（FTP Security Extensions）

IETF RFC 2349，TFTP休息间隔和传输大小选项（TFTP Timeout Interval and Transfer Size Options）

IETF RFC 2577，FTP安全考虑（FTP Security Considerations）

IETF RFC 3164，BSD Syslog 协议（The BSD Syslog Protocol）

3 术语和定义

下列术语和定义适用于本文件：

3.1

异常流量

电信网络中正常的业务和信令流量之外的、消耗网络资源的流量，如DDoS攻击、蠕虫、垃圾邮件等导致的流量。

3.2

异常流量检测系统

对异常流量检测和控制的软件系统或者硬件产品。

3.3

流量清洗

针对特定网络或服务系统，为其提供针对DDoS等异常流量攻击的监控、告警和过滤并保证业务正常运行的一种网络安全服务。

3.4

深度流检测　Deep Flow Inspection，DFI

通过对网络流特征而非数据包应用载荷进行分析从而进行异常流量检测的技术。

3.5

深度包检测　Deep Packet Inspection，DPI

通过深入解析数据包载荷进行异常流量的分析和检测的技术。

3.6

基于IP包的流量控制

根据定义好的控制规则审查每个IP数据包，以确定是否与某一控制规则匹配。

3.7

基于会话的流量控制

一种根据应用或传输协议的会话状态对协议流量进行控制的技术。

4 缩略语

下列缩略语适用于本文件：

AOI	Attribute oriented Induction	面向属性的归纳
ASIC	Application Specific Integrated Circuit	专用集成电路
ASPF	Application specific packet filter	应用层包过滤
CPU	Central Processing Unit	中央处理器
DDoS	Distributed Denial of Service	分布式拒绝服务
DFI	Deep Flow Inspection	深度流检测
DoS	Denial of Service	拒绝服务
DPI	Deep Packet Inspection	深度包检测
FTP	File Transfer Protocol	文件传输协议
HTTP	HTTP-Hypertext transfer protocol	超文本传输协议
ICMP	Internet Control Message Protocol	互联网控制消息协议
IDC	Internet Data Center	互联网数据中心
IM	Instant Messaging	即时消息
IP	Internet Proto	互联网协议
IPSec	Internet Protocol Security	IP安全协议
NBA	Network Behavior Analysis	网络行为分析
P2P	Peer to Peer	点对点
QoE	Quality of Experience	体验质量
QoS	Quality of Service	服务质量
RTP	Real-time Transport Protocol	实时传输协议
RTSP	Real Time Streaming Protocol	实时流传输协议
SLA	Service Level Agreement	服务等级协议
SOAP	Simple Object Access Protocol	简单对象访问协议
SSL	Secure Sockets Layer	安全套接层
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
UTM	Unified Threat Management	统一威胁管理
VPN	Virtual Private Network	虚拟专用网络

5 异常流量对电信网络的影响

5.1 概述

电信网络未来作为一个开放性的公众服务网络，面临着众多的安全威胁，异常流量作为一种重要的威胁严重影响着电信网络的安全平稳运营。攻击流量大量挤占移动通信网资源，极易造成网络不稳定和链路堵塞；同时商业利益的驱使，使得针对特定商业目标的异常流量攻击有愈演愈烈之势，对电信网络安全构成了严峻的挑战。有效遏制异常流量，缓解网络运营压力，成为电信运营商面对的一项十分紧迫的任务。

5.2 网络可用性影响

有些异常行为主要破坏网络可用性，导致网络设备、线路等基础设施无法正常提供服务，影响范围和程度相当巨大，其中破坏程度最大的当属DDoS及蠕虫所引发的流量型拒绝服务攻击。

DDoS攻击手段是在传统的DoS攻击基础之上衍生出来的一类攻击方式。传统的DoS攻击一般采用一对一方式。当攻击目标资源相对较少，如CPU相对处理能力低、内存较小或者网络带宽不大等情况下，DoS攻击会产生较为明显的影响。但随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存容量大大增加，网络带宽也逐渐向10GE级别发展，这使得需要消耗被攻击目标的资源大大增加，单靠一台主机的能力难以收到很好的效果。DDoS就是利用数量更多的傀儡机来发起进攻，以前所未有的攻击规模来扩大攻击效果。

蠕虫是一种能够自我复制的计算机程序，通常以执行垃圾代码以及发动拒绝服务攻击，令目标计算机的执行效率大大降低，从而破坏计算机的正常使用。目前很多蠕虫都利用网络进行相关传播，并且在传播过程中产生大量网络异常流量，经常堵塞电信网络关键核心设备的可用带宽和网络资源。

5.3 业务收入影响

一些非法的语音服务（如黑话吧），会对合法服务商的业务收入造成影响。此类应用可单独归纳为一种类型的异常流量，即非预期的业务应用。

5.4 用户感受影响

某些异常流量比如P2P下载、垃圾邮件等会占用了大量的网络带宽，使接入层网络设备长期工作在高负荷状态，严重影响了正常的Web、E-mail以及视频点播等业务用户的访问，对用户感受造成了极大的影响。

6 异常流量检测技术

6.1 检测算法

异常流量检测技术的相关检测算法，应支持异常检测和误用检测两种。

6.1.1 异常检测

异常检测方式首先需建立网络正常行为的模型，当发现被检测数据的实时行为模型与正常行为模型出现偏差时，即认为被检测数据存在异常。异常检测通常基于统计分析原理，其正常行为模型的建立与系统准确率紧密相关，不仅需要合理的参数选取，同时还要求智能化的自动学习能力。

由于不依赖对已知攻击行为的知识，因此该方式能有效检测未知的异常行为，但其缺点是误报率较高。

6.1.2 误用检测

误用检测方式的主要原理在于系统将被检测数据与预先确定的特征知识库进行逐一比较，如果发现匹配则判断有异常发生。特征知识库是把已知的攻击事件特征提取出来并进行集中存储的一个知识库。对误用检测来说，特征库是系统准确率的关键因素。

采用模式匹配，误用模式能明显降低误报率，但漏报率随之增加，攻击特征的细微变化都会导致误用检测无法检出。

6.1.3 综合分析

相比而言，误用检测原理简单，容易配置，特征知识库也便于扩充，误报率相对较低。但误用检测存在一个致命弱点，即只能检测到已知的攻击方法和技术，无法发现未知攻击行为。而异常检测能够检测已知或未知的攻击行为，漏报率较低，但检测特征不准确，误报率较高。

针对异常检测与误用检测的技术差异，建议在异常流量的检测中对两者进行综合运用，在部署层次上，可采取以下方式：

1）异常检测：面向高带宽流量提供初级筛选，提供较高的处理性能并同时排除其中正常的访问流量以大幅度缩小进一步检测的目标范围，发挥高性能、低漏报率的优势；

2）误用检测：对异常检测所怀疑的可疑流量进行精确的特征匹配，发挥低误报率特点并回避性能较差的劣势。

6.2 检测方式

6.2.1 DPI

DPI不仅分析IP包的4层以下的内容，包括源地址、目的地址、源端口、目的端口以及协议类型，还对应用层的报文载荷内容进行深入分析。

DPI技术在分析IP包头的基础上，增加了对应用层的分析，它是一种基于应用层的流量检测和控制的技术。当IP数据包、TCP数据流或UDP包经过基于DPI技术的设备时，该系统通过深入读取IP包载荷的内容对应用层信息进行重组，从而得到整个应用程序的内容，这样可以有效检测出各种伪造业务流量的情况。例如，P2P下载业务可以采用80端口进行下载，而80端口通常传输的是HTTP协议报文，如果仅仅从80端口来区分业务，就会认为80端口的报文是HTTP业务，导致P2P流量不能被识别。通过采用DPI技术对报文的应用层信息进行分析，可以识别出企图通过知名端口掩护的P2P流。

6.2.2 DFI

DFI采用一种基于流量行为的应用识别技术，即不同的应用类型体现在会话连接或数据流上的状态各有不同。例如，网上IP语音流量体现在流状态上的明显特征包括：RTP流的包长相对固定，一般在130～220byte，连接速率较低，为20～84kbit/s，同时会话持续时间也相对较长；而基于P2P下载应用的流量模型的特点为平均包长都在450byte以上、下载时间长、连接速率高、首选传输层协议为TCP等。DFI技术正是基于这一系列流量的行为特征，建立流量特征模型，通过分析会话连接流的包长、连接速率、传输字节量、包与包之间的间隔等数据来与已知流量模型进行对比，从而实现鉴别应用类型。

从应用场景上说，DFI适合用于更大带宽的网络上，如10GE带宽以上的链路。DFI技术的核心是行为特征，而非内容特征，这决定了此类技术所固有的优势和缺点。

DFI的性能优势明显。DFI技术不需要对网络内容作分析，大幅度提高了处理性能，在相同的硬件平台的前提下，DFI技术可以实现更好的处理能力。以以太网为例，DFI只关注网络层、传输层的信息，只提取每个数据包的四层信息，不需要处理4~7层的信息，而且在现有代网络设备中，DFI的部分功能已经由网络设备分担，例如思科的netflow，已经有专用的ASIC芯片来维护数据流的产生和发送。

DFI可用于描述网络整体态势，通过对从更宏观的角度对网络的现状进行描述，如各种不同时段内各传输协议，应用协议，平均包长的变化情况，从网络整体的角度，来对网络的健康状态进行描述和监控。

但另一方面，DFI的应用识别粒度和准确率不如DPI，DFI只能通过有限的四层参数来描述，行为特征的描述和准确率上无法和DPI技术相提并论。

7 异常流量控制技术

7.1 控制方式

对网络异常流量应支持通过直路、旁路和直路-旁路联动三种方式进行部署和控制，三者在控制效果、系统性能以及对网络影响方面都各不相同。

7.1.1 直路控制

直路模式是较为常用的，其好处是控制非常直接和方便，缺点是一旦设备出现故障，可能影响网络的运行，即带来单点故障。为了解决单点故障的问题，通常采用双机冗余备份的方式，或者采用单机旁路（Bypass）开关的方式。

直路方式在技术上面临的两个主要困难：

一是单点故障的问题，即便采用旁路开关，也无法完全避免在软件故障检测失效或硬件故障情况下的单点故障。

二是性能和扩展性，异常流量控制设备类似于防病毒和IDS系统，需要随着应用和业务的更新而不断更新检测库，还需要随着新业务的出现而不断扩充业务功能，否则设备很快会失效。这都会使得设备的处理性能逐渐下降，并且可能需要更换设备，造成投资浪费。

如果需要在网络的核心层（例如城域网出口，通常可能会有10吉比特端口）大规模部署，上述问题会变得更为突出。

7.1.2 旁路控制

旁路控制设备往往通过端口镜像的方式获得流量的完整拷贝，然后进行复杂的分析。根据分析的结果，可以通过给其他直路设备发命令实现对流量的控制，也可以旁路发送控制包直接干预流量。

旁路部署最大的优点是不会对现有网络拓扑造成任何影响，旁路部署非常适合在网络的核心层部署，如果新业务增加导致监控设备性能不满足需求，只需要增加几台设备就可以了，原有设备仍可以继续使用，可以有效保护已有投资。

7.1.3 直路—旁路联动控制

直路-旁路联动部署方式介于直路部署和旁路部署之间，即旁路部署的检测设备，与直路部署的控制设备进行联动。例如检测设备为网络边缘的BRAS设备、防火墙设备、多业务网关设备下发控制命令。这样既不会增加新的故障点，又能够较好地实现后续业务的增值和扩展，还可以很好地利用直路设备强大的控制功能，是一种比较理想的部署方式。

采用七层分析的DPI技术增强了网络流量的检测识别能力，但是DPI技术对检测设备的性能要求很高，从而几乎没有直路设备能够提供精细的深度包检测。尽管部分防火墙产品已经支持部分DPI技术，但由于受到硬件体系结构的影响，DPI检测的扩展能力较差，因此深度包检测技术更多的应用在一些旁路设备上。旁路设备较直路设备降低了对系统处理实时性能的要求，不影响现有网络运行，但是旁路设备对网络流量的控制能力较弱。因此，为了弥补直路设备DPI检测能力不足和旁路设备控制能力有限的缺陷，需要将直路设备和旁路设备进行联动从而实现功能互补，形成一个完整的方案。

7.2 控制粒度

根据控制粒度的不同，流量控制技术应支持以下两类：

7.2.1 基于 IP 包的流量控制

基于IP包的控制技术根据定义好的控制规则审查每个IP数据包，以确定是否与某一控制规则匹配。控制规则基于数据包的报头信息，包括源IP地址、目的IP地址、源端口、目的端口和传输协议类型（TCP、UDP、ICMP等）进行定义。根据预定的控制规则，丢弃非法的数据包。

基于IP包的控制技术的主要优点是数据包的过滤速度快、效率高，但由于其只基于单个报文的信息进行控制，无法针对协议的交互状态进行细粒度的控制，控制粒度比较粗。同时，对于多通道的应用协议（如FTP协议）来说，由于在协议交互中需要动态协商一条甚至多条数据通道，配置控制规则时无法预知数据通道的信息，因此无法准确的配置控制策略实现这种场景下的流量控制。

7.2.2 基于会话的流量控制

基于会话的流量控制是一种根据应用或传输协议的会话状态对协议流量进行控制的技术。对于所有连接，其会话状态信息都将被维护并用来动态地决定数据包是否允许通过。例如，针对TCP连接，可以检测“TCP的三次握手的状态信息”和“拆除连接的握手信息”，对于非完整的TCP握手连接或者不符合当前的握手状态的报文会直接拒绝。通过检测握手和拆连接的状态，保证正常TCP访问的进行。

基于会话的流量控制技术能够支持多通道应用协议（即控制信息交互和数据传输是在不同的通道上完成的，例如FTP，RTSP）的流量控制。多通道应用协议使用约定端口初始化一个控制连接，然后会动态的选择另外的端口用于数据传输。由于数据传输端口的选择是不可预知的，所以基于IP包的流量控制技术无法正确的控制这样的流量。而基于会话的流量控制技术监视每个应用协议状态，根据数据通道的协商情况动态的添加控制策略，用于放行数据通道中的流量，并在数据通道关闭时关闭相应的控制策略，从而对多通道应用协议流量实施正确的流量控制。

8 监控系统部署模式

8.1 独立清洗部署模式

独立清洗部署模式如图1所示。

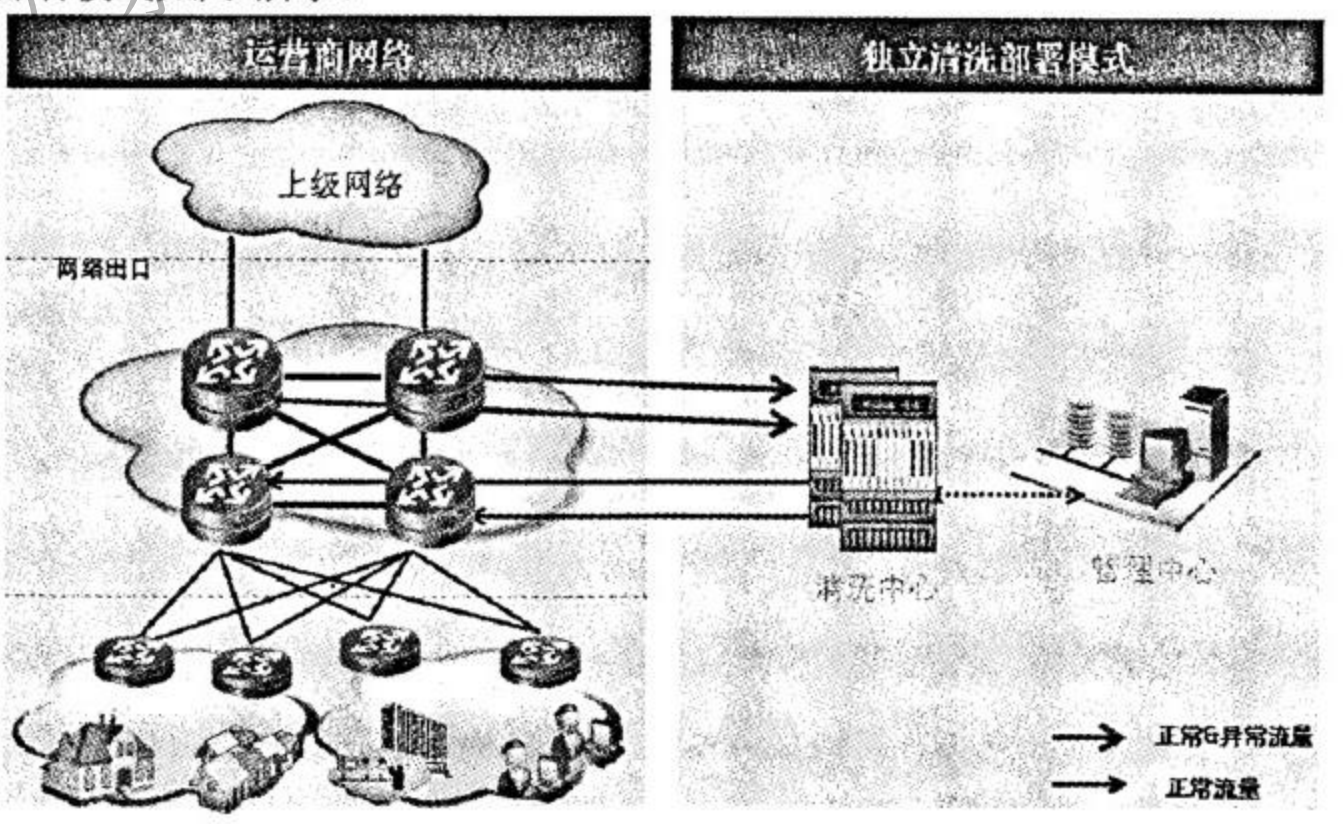

图1 独立清洗部署模式

模式描述：在核心路由器旁挂，根据管理中心下发的清洗策略对指定流量进行防护，清洗设备可以动态学习网络基线和检测网络异常，同时对异常流量进行清洗，通过报表系统向管理中心上报攻击事件和清洗情况。

优势：部署简单，技术复杂度低，适用于小型网络，对特定保护用户同时做检测和清洗防护。

劣势：静态防护流量，扩容时需同步扩容清洗设备，对于特定时期的人为控制有要求。

8.2 采样清洗部署模式

采样清洗部署模式如图2所示。

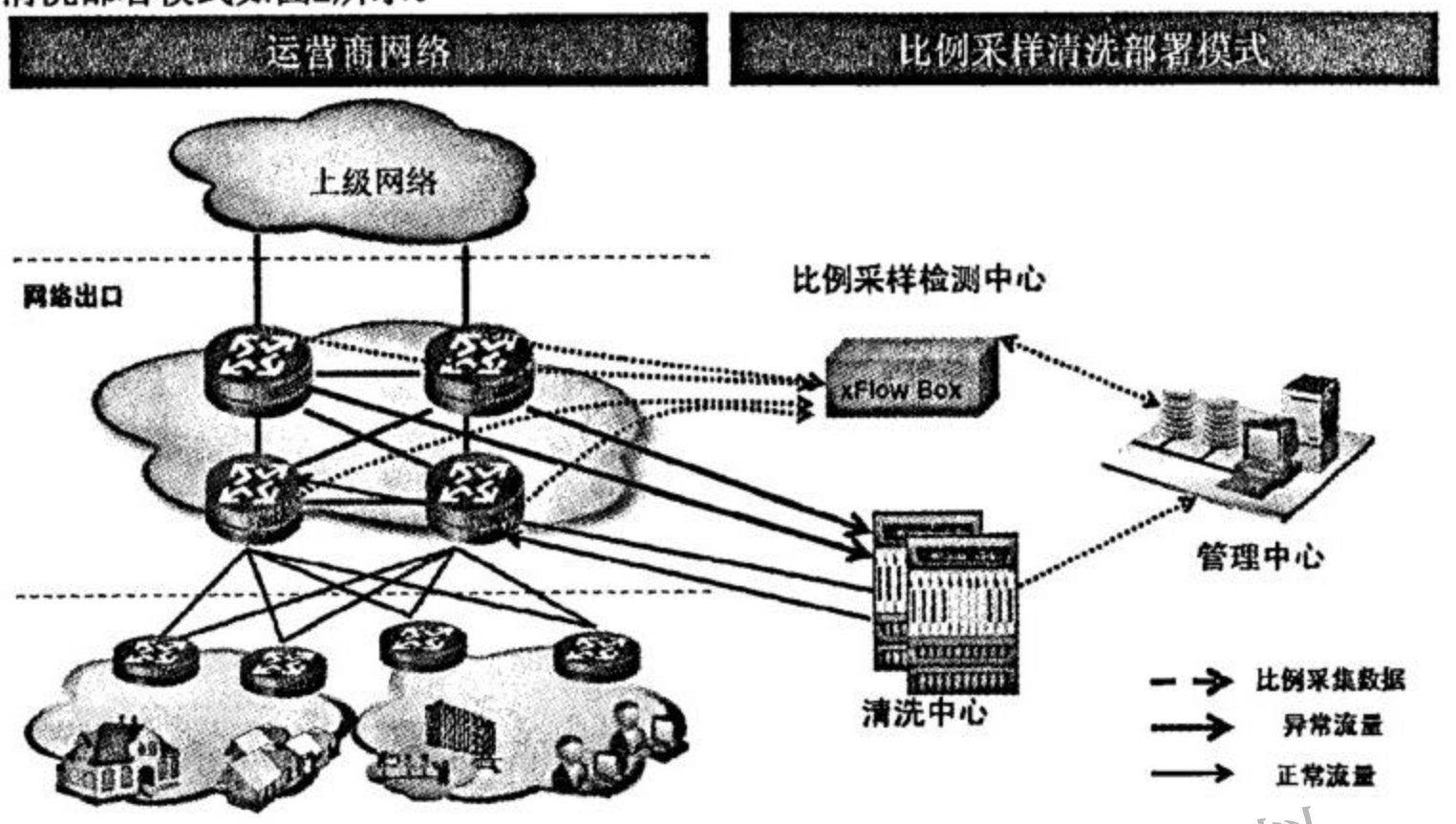

图2 采样清洗部署模式

模式描述：xFlow设备通过采样流量分析网络异常，检测到异常后可通过清洗设备自动下发引流策略到核心路由设备，将异常流量引入清洗设备进行清洗，通过报表系统向管理中心上报攻击事件和清洗情况。

优势：部署复杂度低，采用流量比例取样容易实现全网流量分析，同时可借助骨干网或者大型城域网已经部署的xFlow设备。

劣势：基于xFlow的技术限制，检测攻击的时延比较大，同时对现网网络设备的xFlow特性有一定需求，只针对流量型攻击，而对小流量攻击和应用层攻击无法识别。

8.3 深度检测清洗部署模式

深度检测清洗部署模式如图3所示。

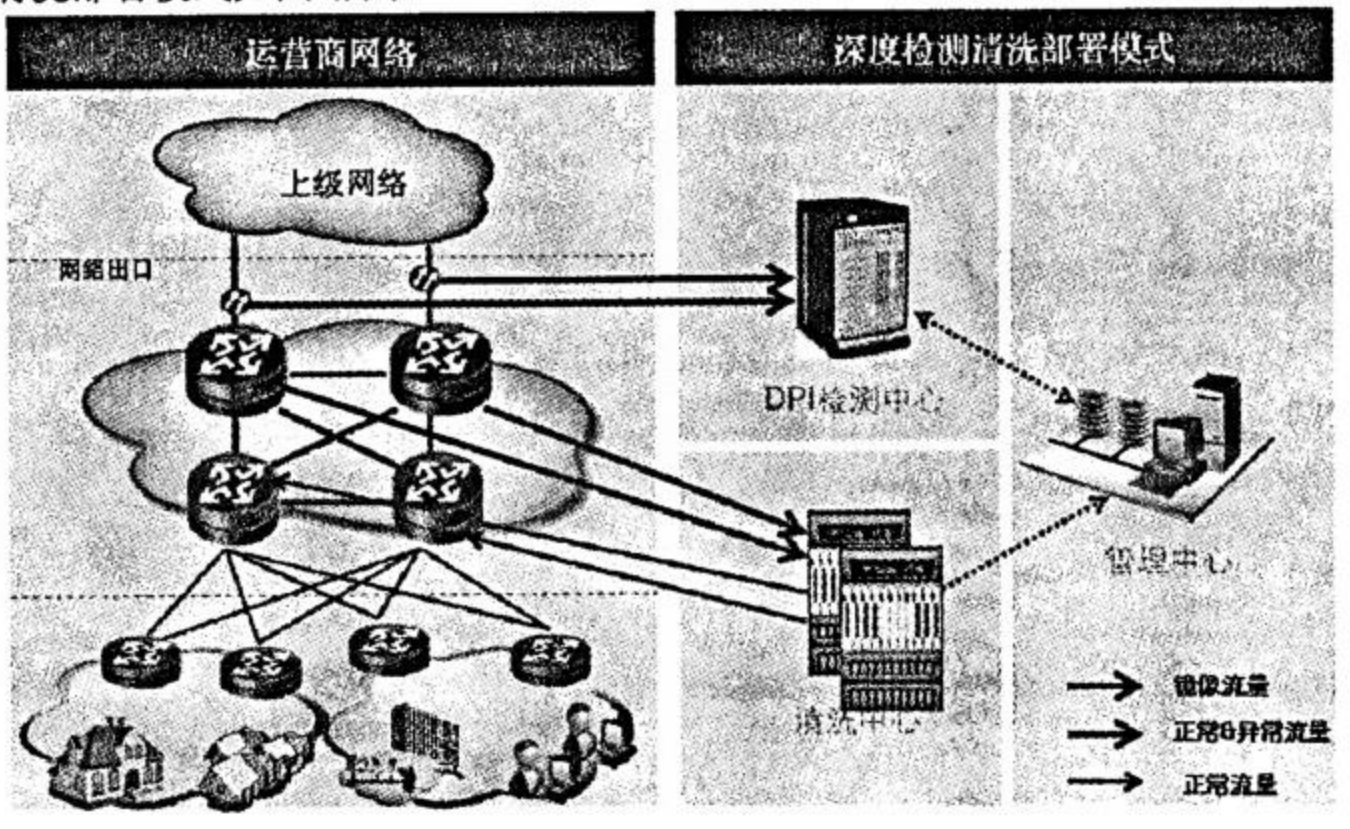

图3 深度检测清洗部署模式

模式描述：DPI攻击检测设备通过全流量全报文检测网络异常，产生异常后可通过清洗设备自动下发引流策略到核心路由设备，将异常流量引入清洗设备进行清洗，通过报表系统向管理中心上报攻击事件和清洗情况。

优势：可以检测小流量攻击和应用层攻击，动态识别应用层攻击特征，同时可提供网络流量分析，用户行为分析，P2P，VoIP等业务检测能力，精细的检测和防护可向最终用户开展安全增值业务。

劣势：技术复杂度高，多用于城域网、重点IDC或大客户出口。

8.4 部署模式对比

	独立清洗部署模式	比例采样清洗部署模式	深度检测清洗部署模式
部署说明	在核心路由器旁挂，静态的对指定流量进行防护，清洗设备可以动态学习网络基线和检测网络异常，同时对异常流量进行清洗，通过报表系统上报攻击事件和清洗情况	xFlow 设备通过采样流量分析网络异常，产生异常后可自动下发引流策略到核心路由设备，将异常流量引入清洗设备进行清洗，通过报表系统上报攻击事件和清洗情况	DPI 流量分析设备通过全流量分析网络异常，产生异常后可自动下发引流策略到核心路由设备，将异常流量引入清洗设备进行清洗，通过报表系统上报攻击事件和清洗情况
部署优势	部署简单，成本低，适用于小型网络或者初期试验网络，对特定保护用户同时做检测和清洗防护	部署成本低，大多骨干网，大型城域网已经部署了 xFlow 设备，针对仅解决流量型攻击性价比高	可以检测应用层攻击，同时可提供网络流量流向分析，用户行为分析，共享接入防护，应用层协议分析等
部署劣势	静态防护流量，扩容时需同步扩容清洗设备，对于特定时期的人为控制有要求	基于xFlow的技术限制，检测攻击的时延比较大，同时对现网的xFlow采集有一定需求，只针对解决流量型攻击，而对应用层攻击无法识别	成本高

四种不同的部署模式分别都有各自的优缺点,不存在绝对意义上的优劣。在实际使用中需要结合网络规模、复杂度以及部署成本等多种因素来综合权衡。

9 管理中心与清洗系统接口要求

管理中心确认异常后开始引流，清洗系统负责流量清洗。异常流量清洗系统接口的功能、性能、管理接口的信息模型和所采用的接口协议及安全都需要满足一定的要求。

9.1 接口功能要求

管理中心通过接口实现对流量清洗系统的管理，接口的功能包括单点登录、配置管理、引流管理、告警管理、安全管理、报表数据管理。

9.1.1 单点登录

管理中心通过URL链接接口可以直接登录到下级流量清洗系统的首页，不需要再输入用户名和密码，下级节点根据预先配好的用户分配权限。

9.1.2 心跳管理

管理中心心跳感知下级清洗节点的状态，从而决定流量异常时是否引流。下级清洗节点定时（5s）上报自身状态（busy或normal）。如果管理中心连续2次收不到心跳，认为下级节点出现故障。如果下级节点正在进行流量清洗，则不需要上报自身状态，同时取消引流。

9.1.3 配置管理

管理中心通过接口对流量清洗系统进行配置，配置信息包括大客户基本信息、IP信息和策略信息。在管理中心对这些信息进行配置，通过接口下发到下级的流量清洗系统，原则上以上级下发的信息为主，不在下级进行配置，避免配置冲突。发生冲突时，以上级下发的配置为主。不同的节点可以配置不同的策略。

所有的配置下发应返回成功或失败，失败应包含失败原因。

9.1.4 引流管理

管理中心通过接口控制下级流量清洗系统或宽广流控系统进行引流和取消引流。

9.1.5 清洗管理

异常流量管理中心对于DDoS攻击，可以设置自动清洗和手动清洗两种方式。

自动清洗方式：清洗系统检测到攻击后直接进行清洗，不需要管理员手动确认。

手动清洗方式：清洗系统检测到攻击后，上报告警，待管理员确认清洗后开始清洗。管理员可以手动启动和停止基于IP粒度的清洗。

无论是自动清洗还是手动清洗，清洗系统都应上报攻击告警及相关清洗信息。

9.1.6 告警管理

异常引流告警：数据业务系统检测发现大客户的流量超过阈值，发送引流告警到集中管理平台。集中管理平台收到引流告警后，根据预订的策略进行自动或手动引流。

清洗系统攻击告警：引流开始后，流量经过清洗系统，清洗系统发现异常或攻击后，向管理中心发送的异常/攻击告警。管理中心接收到来自被管清洗节点的告警后，根据预订的策略进行自动清洗或手动清洗处理。

攻击的详细信息和确认过程应被记录到数据库，备案查询。

9.1.7 报表数据管理

报表数据管理接口主要描述上下级之间的数据接口要求，具体报表的格式和定义请参见管理平台的技术要求。报表数据接口内容主要包括：

1）IP入流量日志；
2）IP丢弃流量日志；
3）大客户入流量日志；
4）大客户丢弃流量日志；
5）节点入流量日志；
6）节点丢弃流量日志；
7）当前攻击日志；
8）结束攻击日志；
9）攻击源IP日志。

9.2 接口协议要求

管理中心和下级流量清洗系统及流控系统的接口包括下面几种协议类型：

9.2.1 Syslog

Syslog用于下级清洗系统上报异常/攻击日志。Syslog接口协议及报文格式应符合IETF RFC 3164的要求。

9.2.2 FTP

FTP用于上下级的报表数据传输。FTP接口协议应符合IETF RFC 438、IETF RFC 697、IETF RFC 775、IETF RFC 2228、IETF RFC 2349、IETF RFC 2577的要求。

9.2.3 SOAP

SOAP是一种轻量的、简单的、基于XML的协议，它被设计成在 WEB上交换结构化的和固化的信息。SOAP可以和现存的许多因特网协议和格式结合使用，包括超文本传输协议（HTTP），简单邮件传输协议（SMTP），多用途网际邮件扩充协议（MIME）。它还支持从消息系统到远程过程调用（RPC）等大量的应用程序。

SOAP主要用来下发用户信息、用户策略、引流策略等数据。

9.2.4 HTTP

HTTP是互联网的标准协议，单点登录使用HTTP协议登录到下级OMC。

9.3 接口安全性要求

9.3.1 网络安全性

通过安全的网络能根本保证接口数据的安全性，建议上下级清洗系统之间建立安全隧道（如IPSEC VPN或TLS），保证通信安全。

9.3.2 SOAP 安全性

SOAP基于HTTP或HTTPS进行数据传输，如果网络层通过IPSEC VPN通讯，建议基于HTTP提供SOAP服务，可以减少安全认证加密解密的开销。如果网络层不能提供IPSEC VPN，基于HTTPS提供SOAP服务，通过SSL保证数据的安全性。

9.3.3 单点登录安全性

单点登录应采用安全的机制，保证用户名、密码不在网上明文传输。

9.3.4 数据一致性

数据一致性指标指管理中心下发的用户名策略信息和下级收到的一致，采集到的流量数据与实际数据应保持一致，不出现重复和错误现象。

该指标验证三类数据的一致性：配置数据的一致性、报表数据的一致性以及告警数据的一致性。

9.3.5 FTP 安全性

可选项。可选择性支持标准FTP、安全文件传送协议（sFTP）或者SSL加密的FTP（FTPs）。

9.4 接口性能要求

9.4.1 处理能力

9.4.1.1 操作响应时间

操作响应时间指管理中心通过上下级接口执行某项操作后，收到被管OMC响应的延迟时间。正常情况下，单条操作响应时间应小于5s。

9.4.1.2 心跳间隔时间

下级清洗节点每隔5s上报自身状态（busy或normal）。如果管理中心连续2次收不到心跳，认为下级节点出现故障，如果下级节点正在进行流量清洗，则取消引流。

9.4.1.3 告警时延

告警时延指标包括两个场景：

1）告警上报时延：从实时告警发生（清洗设备判断攻击开始或判断异常开始）到被管OMC接口发出告警的延迟时间。实时告警应有较小的时延。正常运行情况下，告警时延小于5s。

2）告警处理时延：从下级被管OMC发出告警，到管理中心完成处理告警的延迟时间。正常情况下，告警处理时延小于5s。因为告警展示依赖Web界面的刷新，刷新间隔可配，所以界面的展示时延不列入性能指标。后台处理完成后，Web界面随时刷新即可获得最新的告警。

9.4.1.4 报表数据准备时延

报表数据的准备时延是对下级OMC的要求，指从统计周期的结束时间至统计数据准备完成，可供管理中心采集的时间点之间的时长。不同统计粒度下对统计时延的要求如下：

统计周期	最大统计时延
5min	1min
1h	5min
24h	10min

例如，对于统计周期是5min的统计汇总，整点开始新的统计周期，那么8:00至8:05的统计数据，在统计周期结束之后1min内，也就是在8:06之前，下级OMC应当准备完毕可供管理中心采集。

9.4.2 可靠性

9.4.2.1 平均故障发生间隔

平均故障发生间隔指网管接口故障发生间隔时间的平均值。要求平均故障发生间隔大于 180 天。

9.4.2.2 平均故障修复时间

平均故障（不可用）修复时间指网管接口在出现故障后修复的平均时间。要求网管接口的由软件引发的故障一年内平均修复时间小于 1h。

9.4.2.3 容错能力

容错能力指当管理中心向下级清洗系统或流控系统接口输入非法数据时，下级系统对接口错误的处理能力。被管业务系统应不会因为输入的非法数据导致被管设备故障。

10 监控及清洗系统性能要求

10.1 清洗系统容量要求

系统应能对容量为10吉比特链路上的双向流量进行过滤。

10.2 清洗系统性能指标要求

清洗系统的性能应符合以下要求：

1）系统能够全部满足周知的流量型拒绝服务的安全攻击识别（见附录A），对于新发现的攻击应在5个工作日内完成特征更新和清洗功能。

2）实际待清洗流量模型在系统额定吞吐和连接数、新增连接数等条件内，生效规则数变化对系统性能影响小于1%，流量模型变化对系统性能影响小于10%。对于超过额定流量模型流量能够做到实时转发。

3）系统在长时间运行情况下，性能变化不超过1%。

4）其他性能参数包括（本标准中对下列性能参数指标不做限定，仅作为重要指标以附录B的形式列出供参考）：

a）系统转发延迟；

b）异常流量清洗系统的误差率；

c）支持的白/黑名单数量；

d）单机或单板吞吐处理能力；

e）策略生效时间；

f）最大并发连接数；

g）单机或单板每秒新增连接数；

h）单个流控制粒度；

i）多个流聚合控制粒度；

j）包速率。

10.3 流量监测设备性能要求

DPI/DFI设备的性能参数包括：

1）总体业务数据流识别误差率；

2）单业务识别性能参数：单业务数据流识别误差率（包括误识别率和漏识别率）、单业务数据流识别时间；

3）总体业务数据流控制误差率；

4）单业务控制性能参数：单业务数据流控制误差率、业务控制策略生效时间；

5）在连接干扰/信令干扰的业务数据流控制方式下，业务性能参数还包括干扰流量总带宽；

6）交换性能参数：吞吐量、时延和最大并发连接数，其中并联接入方式不包括吞吐量和时延。

本标准中对上述所有性能参数指标不做限定，仅作为重要指标以附录C的形式列出供参考。

附 录 A
（规范性附录）
拒绝服务攻击的种类

表A.1 需支持的拒绝服务攻击列表（包含但不限于）

攻击类型	类别	攻击名称	攻击描述
拒绝服务攻击	针对 TCP 协议字段类的攻击	TCP Floods	使用设置各种标志位的 TCP 洪水包消耗目标设备的 CPU 周期，导致链路拥塞、目标资源 CPU 耗尽，拒绝为合法用户提供服务
		TCP SYN flood	SYN Flood 是当前最流行的 DoS 与 DDoS 的攻击方式之一，SYN 攻击利用 TCP 协议三次握手的原理，大量发送伪造源 IP 的 TCP SYN 半连接请求，从而使得被攻击方资源耗尽（CPU 满负荷或内存不足）的攻击方式
		TCP FIN flood	使用假冒的源地址、端口和 FIN 标志位淹没目标。如果攻击者猜测到已有连接的序列号、端口和源地址，这条连接将被终止。由于成功猜测的可能性比较低，攻击者的目标可能是使用过量的包去压垮（overwhelm）网络或者端主机，并且通过设置标志位去绕过可能阻止其他包类型的安全系统
		TCP RST flood	使用假冒的源地址、端口和 RST 标志位淹没目标。描述同 TCP FIN flood
		TCP ACK flood	使用设置 ACK 标志的包淹没目标
		TCP URG Flood	这个威胁使用带有随机的、假冒的地址和 URG 标志位的 TCP 包淹没目标。如果攻击者碰巧猜测到现有连接的参数，目标将立即传递数据到应用去执行。但这种可能性比较低，因此更可能的是使用大量的包去耗尽资源
		TCP CWR Flood	这个威胁使用带有随机的、假冒的地址和 CWR （Congestion Window Reduced）标志被打开的 TCP 包，淹没用户指定的目标。为了阻碍性能，导致对合法流量的慢速响应，并可能出现 DoS，这个攻击企图使用错误的包淹没目标
		TCP ECE flood	这个威胁使用带有随机的、假冒的地址和 ECE 标志被打开的 TCP 包，淹没用户指定的目标。为了阻碍性能，导致对合法流量的慢速响应，并可能出现 DoS，这个攻击企图使用错误的包淹没目标
		TCP NULL flood	使用没有任何 flag 被设置的 TCP 包淹没目标
		TCP Erroneous Flags Flood	在攻击包中，TCP 标志的错误结合被打开
		TCP Xmas	使用带有 FIN、URG 和 PUSH 标志的 TCP 包淹没目标。经常地（frequently）用于 OS 识别（fingerprinting），但可以摧毁一些 OS
	针对 TCP 协议流程的攻击	stream	使用假冒的源地址、端口和 RST 标志位淹没目标。描述同 TCP FIN flood
		DRDOS	发动 DRDoS 的攻击者冒充受害者的 IP 地址向路由器们发送 syn request，也就是 TCP 三次握手的第一步，路由器们以为受害者要和自己建立 tcp 连接，所以返回 ack 应答，由于源 IP 的伪造，所有的 ack 应答全部都涌向了受害者

表A.1（续）

攻击类型	类别	攻击名称	攻击描述
拒绝服务攻击	针对 TCP 协议流程的攻击	Low-rate TCP-based attacks	低速脉冲（Low-rate pulsating）攻击，它调整 TCP 拥塞控制和流管理参数
		Eyenetdee	这种攻击工作类似 Land attack，但它以低包速发送 SYN flood 到 telnet、FTP、pop、finger 或者 inetd 服务。这些服务以 shut down 作为响应
		NAPTHA	NAPTHA 忽略（bypass）在代理机器上的 TCP 协议栈，参与连接，基于接收到的包构建回复 -> 填充在主机上的 TCP 连接队列
	针对 UDP 协议的攻击	UDP Floods	使用 UDP 洪水包淹没目标链路，导致链路拥塞
		Fraggle attack	Smurf attack 的 UDP 变种。假冒源 IP（受害者 IP）的 UDP 包被发送到 port 7（echo port）的广播地址，回复到受害者地址
		UDP Port 0 DoS	这个威胁通过发送一个 UDP 包到目标主机的端口 0，导致或者防火墙或者远程主机崩溃
		NetBIOS Denial of Service（WinNuke）, oob	这个威胁发送大量的数据到 UDP 137 端口（NetBIOS 名字服务的 UDP 端口。）上。导致较早的 Windows 版本耗费 CPU 达到 100%，并且使 NetBIOS service 崩溃
		Papasmurf attack	通过结合 Smurf 和 Fraggle 的混合（Hybrid） attack
		DB2 Discover Service Denial of Service	IBM DB2 提供了一个 UDP 发现服务，它在端口 523 监听。这个服务期待具有 20 字节或者更少的有效载荷的包被发送到它。这个威胁发送长度远大于 20 字节的 UDP 包到这个服务，导致服务崩溃，最终导致对合法用户的拒绝服务
		MS02-039 MS SQL Server 2000 UDP Ping Flood	MS SQL Server 2000 使用 UDP Port 1434 用于外部主机进行连通性 ping 检查。发送一个具有特定载荷的 UDP 包到这个端口，将导致服务器 ping 应答响应。可以通过发送具有伪造（伪造的）源的 UDP 洪水包执行威胁。或者发现另一台脆弱的 MS SQL Server，并使用它作为源，导致两台服务器相互 ping，最终导致拒绝服务
	针对 IP 报文分片的攻击	Frag flood	产生新的 IP 分片。端点尽力去重组包，但从来不会完成，因为后面的分片没有被发送。而导致目标端点崩溃
		opentear	产生新的 IP 分片。端点尽力去重组包，但从来不会完成，因为后面的分片没有被发送。而导致目标端点崩溃
		Nestea	产生重叠的 IP 分片，导致目标崩溃或者重启
		TearDrop	产生重叠的 IP 分片，导致目标崩溃或者重启
		Jolt	产生重叠的 IP 分片，导致目标崩溃或者重启
		Boink	产生导致在目标的一个太大的包的重组，最终导致目标崩溃或者重启
		Bonk	产生导致在目标的一个太大的包的重组，最终导致目标崩溃或者重启
		Ping of death	攻击者发送一个大于 2^{16} 字节的 ICMP 包，将引起分片并在接收者进行重组。这些攻击是瞄准特定的操作系统版本，在重组大于 2^{16} 字节的包期间，它们将崩溃或者重启。攻击使用 ICMP 包，也许是因为可以通过命令行 ping 容易地产生 ICMP 包，但攻击可以使用任何 IP 包

表A.1（续）

攻击类型	类别	攻击名称	攻击描述
拒绝服务攻击	针对 IP 协议报文字段的攻击	Land attack	Land attack 使用 IP 欺诈（spoofing），结合打开一个 TCP 连接。在 Land 中，两个 IP 地址——源和目的地址，被修改成相同的，结果，内核进入面对自己的 ACK 战争
		IP non-existing protocol attack	使用在 protocol 字段中带有保留值的 IP 包淹没目标
	通过恶意软件发起的攻击	trash2	Trash2 是一种属于 DoS 的恶意软件（malware）。DoS 攻击针对 Windows98/95/2000/NT 机器。使用随机的、假冒的源地址转发随机的、假冒的 ICMP/IGMP 包，导致用户的机器冻结或者 CPU 使用达到定点（roof）
		IGMP of death	Igmp of death 是属于 DoS 的间谍软件(spyware)。Igmpofdeath.c 是 trash2.c 的修改版，它也转发随机的 type 2 igmp 包
		IGMP syn	Igmp syn 是属于 DoS 的恶意软件。Igmpsyn.c 使用随机的源地址转发 type 1 IGMP 请求。该攻击 Windows 95 / 98 有影响
		Twinge	Twinge 循环使用所有的 ICMP 类型和代码组装成 ICMP 报文并发送，将使一些 Windows 主机崩溃。 Trash 使用随机的类型/代码发送 ICMP 消息
		trash	Trash 属于 DoS 间谍类别。它的出现表明你的计算机感染了恶意软件，并且是不安全的。简单的 DoS 攻击针对 Windows98/95/2000/NT 机器。使用随机被选择的 ICMP 错误代码转发随机的、假冒的 ICMP 包。结果：冻结（freeze）用户机器，或者 CPU 使用将增加到极限值（extreme lag）
		trash2	Trash2 是一种属于 DoS 的恶意软件（malware）。DoS 攻击针对 Windows98/95/2000/NT 机器。使用随机的、假冒的源地址转发随机的、假冒的 ICMP/IGMP 包，导致用户的机器冻结或者 CPU 使用达到定点（roof）。
针对 ICPM/IGMP 协议的攻击		Smack	发送来自随机 IP 地址的随机 ICMP unreachable 包
		Winfreez	Winfreez DoS 攻击卷入位于同样的 LAN 的攻击者，使其成为受害者。从路由器到受害者主机，发送假冒的 ICMP 重定向主机包风暴。基于 Microsoft Windows 的机器将收到 ICMP 重定向主机包，并改变它们的网络路由表，因此在攻击期间变得僵化（frozen）、操作非常慢、或者失败去执行正常的应用
		ICMP Source Quench Denial of Service	这个利用使用在主机路由表中已知的、用户指定的网关发送假冒的 ICMP 抑制包（ICMP Quench Packets）。ICMP 抑制包是信息性消息（informational messages），由于网络问题、可用的系统资源比较低，或者一正经历的 DoS 攻击，由网关设备发送到主机的消息，为了建议主机限制包加载或者查找可选的资源。这个利用的结果将减慢网络流量
		ICMP Floods	发送大量 ICMP 包到目标网络，导致链路拥塞
		Smurf attack	ICMP 放大（amplification）攻击，也称为反射（reflection）攻击。发送 Ping 请求到一个广播地址，机器回复到在请求中冒充的受害者的地址。导致链路拥塞、端点资源耗尽

表A.1（续）

攻击类型	类别	攻击名称	攻击描述
拒绝服务攻击	针对ICPM/IGMP协议的攻击	Papasmurf attack	通过结合 Smurf 和 Fraggle 的混合（Hybrid）attack
		ICMP p-smash Flood	这个威胁使用 ICMP type 9 消息（路由器通告，router advertisement）去淹没远程目标机器
		Moyari13	这个攻击和死亡之吻（kiss of death）攻击相似。它发送非法的 ICMP 时戳包，使一些 Windows 版本崩溃
		IGMP flood	使用随机的 IGMP 消息淹没目标
		IGMP Win attack （Kiss of death）, IGMP Nuker	一个特别的精心制作（crafted）IGMP 包将使一些版本的 Windows 崩溃。 这个 nuker 使用一个利用（exploit）去毁坏 Win 95, 98 和 NT 3.x 平台。它转发 IGMP 包以后，大多数目标脆弱性平台将做 windows 知道的最好去做的事情，显示蓝屏并阻止计算加，或者重启系统。如果受害者使用一个更高版本的 Windows 或者使用 Linux，已经为防止 nuke 给 windows 打了补丁，nuke 对它不将有任何影响
		IGMP membership attacks	IGMP 使用报告抑制（suppression）机制去防止重复的（redundant）IGMP 成员报告被发送到路由器查询器（querier router）。收到单播成员报告的主机将相信另一个成员是在它的子网内，并将抑制它自己的成员报告。这台主机然后被从多播树中排除了
连接耗尽型攻击		Connection flood, Connection Exhausted	称为连接耗尽攻击，顾名思义就是将服务器上可用的连接数占满直至无法正常响应。连接耗尽攻击使用真实的 IP 地址与服务器建立连接。攻击者操控了大量的傀儡主机或者使用代理服务器来发起大规模的连接。当连接数达到一定规模，超过了服务器的能力时，正常的连接请求将无法建立。通过不断地与服务器建立大量的连接，最终服务器的内存资源将被耗尽
基于 HTTP 协议的攻击		HTTP-Get flood	针对 Web 服务的 DoS 攻击被称为 HTTP-GET flood 攻击，这样的攻击逐日上升。在这种类型的攻击中，恶意（malicious）客户端自动地发送大量的 HTTP-GET 请求到目标 Web 服务器。由于 HTTP-GET 请求具有合法的格式，并且通过正常的 TCP 连接进行发送，所以入侵检测系统（Intrusion Detection System, IDS）无法检测到它们
	针对访问查询协议的攻击	CC attack	CC 主要是通过多个代理来攻击页面，通过模拟多个用户（多少线程就是多少用户）不停的进行访问（访问那些需要大量数据操作，就是需要大量 CPU 时间的页面）。通过代理一方面隐藏自己的身份，另一方面也可以绕开所有的防火墙，因为基本上现有防火墙都会检测并发的 TCP/IP 连接数目，超过一定数目一定频率就会被认为是 Connection-Flood。同时也可能出现通过恶意仿冒形式散布虚假文件发布消息，对于目标站点的特定文件例如（mp3\ram\rar）等文件进行恶意下载来达到拖垮服务器系统资源的目的
	针对数据库的攻击	Fatboy	FATBOY 就是通过请求动态页面的数据库查询，达到拖死数据库的目的，针对静态的页面效果相对要小得多

表A.1（续）

攻击类型	类别	攻击名称	攻击描述
拒绝服务攻击	针对DNS服务器的攻击	DNS Query Flood, DNS Amplification Attacks	DNS Query Flood 攻击采用的方法是向被攻击的服务器发送大量的域名解析请求，通常请求解析的域名是随机生成或者是网络世界上根本不存在的域名，被攻击的 DNS 服务器在接收到域名解析请求的时候首先会在服务器上查找是否有对应的缓存，如果查找不到并且该域名无法直接由服务器解析的时候，DNS 服务器会向其上层 DNS 服务器递归查询域名信息。域名解析的过程给服务器带来了很大的负载，每秒钟域名解析请求超过一定的数量就会造成 DNS 服务器解析域名超时并瘫痪
		DNS Resolver Denial of Service	这个威胁发送一个包含所有可以得到的事务 ID 的 DNS 应答包作为 DNS 应答。这导致一些 Windows DNS Resolver 的实现失败去解析（resolve）进一步的名称。目的端口应被设置为 DNS 解析器（DNS resolver）监听的端口，典型情况下，为第一个或者第二个低特权端口（1026, 1027）。为了确保威胁到达正确的 DNS 解析器端口，可以指定一个端口范围，例如 1025~1035
		Symantec Firewall DNS Response Denial of Service	这个威胁发送一个 DNS 包，在 DNS 包中，压缩的名称指针指回它本身，这导致各个 Symantec Firewall 应用去引起内核进入一个无限的循环
针对特定系统或软件的攻击		Mail Bombs	攻击者发送大量的邮件到一台邮件服务器，导致邮件服务器崩溃，或者导致它对其他合法用户拒绝服务
		Microsoft Windows BOOTP Denial of Service	这个威胁发送具有最大长度主机名和 FQDN（Fully Qualified Domain Name）的 BOOTP 包。如果 BOOTP 被启用，将导致在 Windows DHCP 服务上的异常（aberrant）行为
		Samba SWAT Denial of Service	这个威胁利用在 Samba SWAT HTTP daemon 中的一个弱点。导致服务崩溃，拒绝合法用户的访问
		IMail LDAP Denial of Service	这个威胁发送大量的数据到随 IMail 5.0 带的 LDAP 服务。这个威胁将导致 LDAP 服务去使用 90%以上的 CPU，因此导致一 DoS 条件
	利用 SIP 消息发起的攻击	SIP Flood	这个威胁发送 SIP INVITE 消息洪水，企图导致在 SIP 设备上的拒绝服务。SIP 典型情况下在端口 5060 上监听
		Cisco SNMPv3 Denial of Service	这个威胁发送一个 SNMPv3 message 到目标上的 162 端口上
利用型攻击	针对DNS服务器的攻击	DNS Cache poisoning attacks	利用在 BIND 的事务 id 分派中的缺点（flaw），结果导致受害者缓存一个假冒的记录。终端用户可能被重定向到攻击者指派的站点
	利用缓冲区漏洞的攻击	SQL Slammer	利用在 SQL Server 和 MSDE 代码中存在的缓冲区溢出漏洞（vulnerability）
		ISC DHCP Buffer Overflow	这个威胁攻击在 ISC DHCP Sersion 3.0.1rc8 和更早期版本存在的缓冲区溢出。影响多个 Linux 发行版

表A.1（续）

攻击类型	类别	攻击名称	攻击描述
利用型攻击	利用 BGP 协议的攻击	BGP 攻击	边界网关协议（Border Gateway Protocol, BGP）的攻击可以分为2大类：（1）针对建立 BGP 连接的 TCP 协议的攻击；（2）针对 BGP 协议自身漏洞的攻击。 1、基于 TCP 协议的漏洞 BGP 是基于 TCP 的 179 端口来建立连接的，会话时间比较长，BGP 会话的发起者选择随机端口和邻居的 TCP 端口进行通信。因此，开放的 BGP 端口容易被攻击者发现、侦听和攻击。基于 TCP 方式的攻击有 SYN Flooding 攻击、序列号预测、DDoS 攻击等。BGP 协议不使用自身的序列号而依靠 TCP 的序列号来代替，就存在发起 BGP 欺骗、序列号猜测、BGP 会话劫持等攻击。对于这种攻击的防范可以在邻居会话之间配置认证手段，如果认证方案不够强健，攻击者可通过发送 UPDATE 信息来插入、删除路由，通过修改路由表而发起远程攻击。 2、BGP 的漏洞和脆弱性 BGP 报文包括 4 种报文：OPEN, UPDATE, KEEPALIVE, NOTIFICATION。对于这些 BGP 报文，外部源端可通过使用伪造的 OPEN, UPDATE, KEEPALIVE, NOTIFICATION 消息来中断对等体之间的连接，并能使用伪造的 UPDATE 报文来破坏路由，也能通过注入伪造的 TCP 包来中断 BGP 对等体间的连接。BGP 对等体允许在任何时候断开对等体之间的连接，也能够通过发送伪造的 UPDATE 消息来破坏路由。特别是，在 UPDATE 消息中伪造原子聚合、下一跳、AS 路径属性和网络层可达信息可以达到破坏路由的目的。另外，在默认情况下，BGP 没有使用任何认证机制，攻击者就会发送 UPDATE 信息来修改路由表（撤销、增加、删除），也可以传播伪造的路由信息

附 录 B
（资料性附录）
清洗系统性能参数参考值

性能参数	参考值
转发延迟	小于 80us
异常流量清洗系统的误差率	漏判率应小于 1%，误判率应小于 0.1%
支持的白/黑名单数量	不小于 3000 个
单机或单板吞吐处理能力	不低于 10G
策略生效时间	小于 10 秒
最大并发连接数	不低于 1000 万
每秒新增连接	不低于 50 万
单个流，控制粒度	10kbit/s
多个流聚合的控制粒度	1Mbit/s
包速率	100 包/秒

附 录 C
（资料性附录）
DFI/DPI 设备性能参数参考值

性能参数	参考值
总体业务数据流识别误差率	0~10%
单业务数据流识别误差率	−10%~10%
单业务数据流识别时间	<60s
总体业务数据流控制误差率	0~10%
单业务数据流控制误差率	0~10%
单业务控制策略生效时间	<30s
干扰流量总带宽	<被监控链路带宽的 5%（千分之五）
交换吞吐量	被监控链路线速的 90%
交换时延	<200μs
最大并发连接数	>150 万

中华人民共和国
通信行业标准
电信网络异常流量检测与控制技术要求
YD/T 2668–2013
*
人民邮电出版社出版发行
北京市丰台区成寿寺路 11 号邮电出版大厦
邮政编码：100064
宝隆元（北京）印刷技术有限公司印刷

*
开本：880 × 1230　1/16　　2014 年 9 月第 1 版
印张：1.75　　2014 年 9 月北京第 1 次印刷
字数：45 千字
15115 • 368
定价：20 元
本书如有印装质量问题，请与本社联系　电话：(010)81055492