ICS 33.040.40
M 32

YD

中华人民共和国通信行业标准

YD/T 2272-2011

网络异常流量清洗系统技术要求

Technical requirements on network abnormal flow cleaning system

2011-06-01 发布　　2011-06-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言……II
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……2
4　概述……2
4.1　异常流量清洗系统构成……2
4.2　异常流量清洗方式……3
5　异常流量清洗工作流程……3
5.1　清洗启动流程……3
5.2　清洗及回注流程……3
5.3　清洗结束流程……4
6　物理接口要求……4
7　协议要求……4
7.1　检测部件……4
7.2　清洗部件……4
7.3　业务管理部件……5
8　性能要求……5
9　功能要求……5
9.1　异常流量检测部件……5
9.2　异常流量清洗部件……6
9.3　业务管理部件……9

前　言

本标准按照GB/T 1.1-2009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：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：唐　浩、万晓兰。

网络异常流量清洗系统技术要求

1 范围

本标准规定了网络异常流量清洗系统的技术要求，包括原理、功能、性能、协议、接口等方面的要求。

本标准适用于网络异常流量清洗系统。

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。

IEEE 802.3ab (1999)	用于操作在 4 对 5 类线平衡铜缆上的 1000Base-T 物理层参数和规范
IEEE 802.3ae	10G 以太网标准
IEEE 802.3u	百兆以太网标准（100Base-TX）
IEEE 802.3z（1998）	千兆以太网标准（1000Base-LX/1000Base-SX）

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文件。

3.1.1

分布式拒绝服务攻击 Distributed Denial of Service Attacks

一种以资源消耗（带宽、服务处理能力）为手段的攻击方式，目的就是要阻止合法用户对正常网络资源的访问，分布式拒绝服务攻击的特点是攻击者以较小的代价耗费被攻击者大量资源或控制大量傀儡主机同时发起攻击。

3.1.2

安全策略基线 Security Policy Baseline

指为满足网络安全的要求，使设备应具有的安全检查功能的策略和规则形成的集合。

3.1.3

被保护域 Protected Domain

指有可能遭到DDoS攻击的网络。

3.1.4

被保护对象 Protected Object

指被保护域中的具体受保护的服务器或者网络终端。

3.1.5

旁路设备 Bypass Device

指被保护域中距离网络出口最近的设备。

3.1.6

异常流量清洗　Abnormal Flow Cleaning

基于已形成的安全基线对采用带宽占用、服务处理能力消耗等方式的分布式拒绝服务攻击进行探测分析，发现有异常流量存在时，过滤异常流量和用户正常数据，将正常的用户数据回注到城域网中，从而保证带宽，保证正常业务的连续性。

3.2　缩略语

下列缩略语适用于本文件。

BGP	Border Gateway Protocol	边界网关协议
DDOS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
ICMP	Internet Control Message Protocol	互联网控制报文协议
IP	Internet Protocol	网际协议
Raw IP	Raw IP	原始 IP
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
UDP	User Datagram Protocol	用户数据包协议
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网

4　概述

4.1　异常流量清洗系统构成

异常流量清洗系统主要由异常流量检测部件、异常流量清洗部件及业务管理部件3部分组成。

4.1.1　检测、清洗部件形态及功能

检测部件、清洗部件既可以是一台设备的两个功能部件，也可以是两台不同的设备。检测部件也可以是专门的检测设备，甚至是一台有检测功能的主机或服务器。一个清洗部件可以对应多个检测部件。

异常流量检测部件通过镜像或者分光的方式把用户的流量复制过来，并实时进行攻击检测及异常流量分析。检测部件在网络中运行一段时间，可以根据实际网络中的流量情况，学习出一套与实际网络相似的流量分布情况并自动生成安全策略基线，学习到的安全策略基线上报给业务管理平台，由业务管理平台对此安全策略基线进行进一步加工处理后，再下发给检测部件或清洗部件，并应支持安全策略基线的配置。

攻击发生时，异常流量清洗部件通过更新旁路设备上的路由表项，将流经所有旁路设备上的被保护对象的流量动态地牵引到清洗部件进行清洗。清洗部件可通过BGP4或其他路由协议向旁路设备发布更新路由通告来实现旁路设备路由表更新。清洗部件把清洗后的流量回注给被保护对象，并向业务管理部件上报清洗日志以形成相应的报表。

4.1.2　业务管理部件功能

业务管理部件主要负责流量清洗系统的集中管理。流量清洗相关业务配置可以由业务管理部件自动完成检测部件和清洗部件的软件配置，例如：添加被保护对象，为被保护对象配置安全策略基线等。业务管理部件还提供完善的流量清洗业务管理，支持手动清洗管理，自动清洗管理，手动关联，自动关联等异常流量处理方式；为异常流量提供多种方式的告警，例如：邮件告警、声音告警等。另外，业务管理部件还应为用户提供详细的流量日志分析报表、攻击事件分析处理报告等。

4.2 异常流量清洗方式

4.2.1 串接式

流量清洗系统直接串接到网络中，清洗部件实施对异常流量的检测，发现攻击，启动清洗，将异常流量过滤掉，然后将流量正常转发。这种方式组网简单，清洗部件本身的可靠性成为关键，而且实际组网使用不多，所以本标准暂不规定。

4.2.2 旁路式

流量清洗系统旁挂在城域网核心设备或者网络出口设备上，流量检测部件对被保护网络的流量进行检测，发现攻击后将事件报告业务管理部件，业务管理部件启动流量清洗，将出现异常的业务流量牵引到清洗部件上，流量清洗部件将攻击流量清洗干净后，再将正常流量回注到被保护网络，完成对网络的保护功能。实际网络应用中常常使用旁路式，本标准主要阐述旁路式的相关内容。

5 异常流量清洗工作流程

5.1 清洗启动流程

异常流量检测部件通过镜像或者分光的方式把被保护对象的流量复制过来，如图1所示，按照检测部件中的安全策略基线，判断是否有攻击发生，一旦发现有攻击发生，应立即通知业务管理部件。

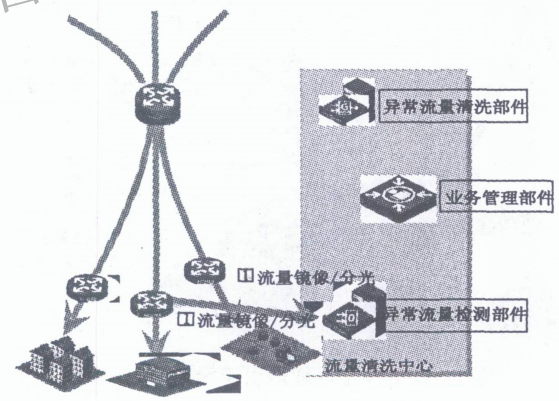

图1 正常时检测逻辑示意

5.2 清洗及回注流程

如图2所示，通过改变旁路设备路由表，将流量牵引至清洗部件。以利用BGP4协议实现流量牵引为例，清洗部件首先和被保护域的旁路设备（直连或者非直连均可）建立BGP Peer，攻击发生时，流量清洗部件通过BGP协议会向旁路设备发布BGP更新路由通告，更新旁路设备上的路由表项，将流经所有旁路设备上的被保护对象的流量动态地牵引到流量清洗部件进行清洗，并把清洗后的“干净”流量回注给被保护对象。流量的牵引方式及回注方式应该根据实际的网络环境和特点，择优选择。

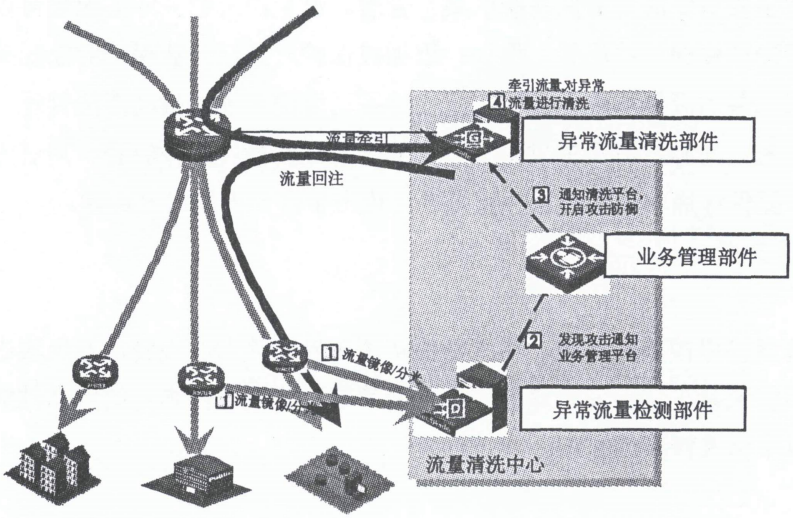

图2　攻击发生时引流清洗逻辑示意

5.3　清洗结束流程

如图3所示，当清洗过程启动后，清洗部件基于安全策略检测流量，当清洗部件判断攻击停止时，将攻击停止信息上报给业务管理部件，业务管理部件根据事先设置好的模式，选择自动或者手工联动清洗部件停止引流。

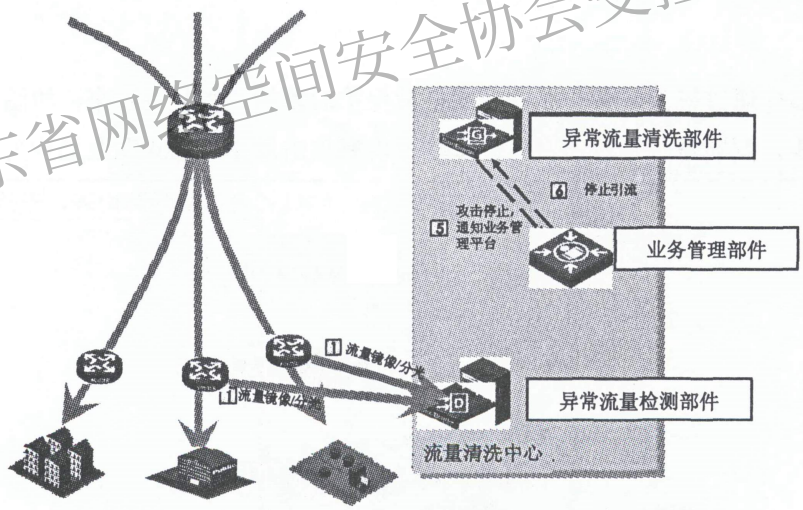

图3　攻击停止后取消引流示意

6　物理接口要求

流量清洗部件和流量检测部件应支持10/100/1000BASE-T接口、1000BASE-LX/SX接口、10GE等接口。百兆以太网接口应符合IEEE 802.3u，吉比特以太网接口应符合IEEE802.3z，1000Base-T接口应符合IEEE802.3ab、10G以太网接口应符合IEEE802.3ae。

7　协议要求

7.1　检测部件

应支持IP、TCP、UDP、ICMP、HTTP、DNS、FTP、TFTP等协议。

7.2　清洗部件

应支持不少于一种动态路由协议，如BGP4、OSPF、IS-IS等协议。应支持IP/TCP、UDP、ICMP、Raw IP、HTTP、DNS、FTP、TFTP等协议。

7.3 业务管理部件

应提供Browser-server模式的管理界面，应支持HTTP、HTTPS等协议。

应支持SNMP，ICMP，Telnet等协议。

8 性能要求

检测部件单机检测能力不低于10Gbit/s；

清洗部件单机清洗能力不低于10Gbit/s。

9 功能要求

9.1 异常流量检测部件

9.1.1 流量检测

应支持单向流检测。

单向流是指只对目的IP地址为被保护IP的流量进行检测，由被保护IP发出的流量不检测。

9.1.2 攻击检测

应支持攻击检测功能，能够识别表1和表2中所示的各种攻击。

表1 畸形报文攻击分类

畸形报文攻击类型	说　明
Fraggle	攻击者通过向目标网络发送UDP端口为7的ECHO报文或者UDP端口为19的Chargen报文，令网络产生大量无用的应答报文，占满网络带宽，达到攻击目的
ICMP Redirect	攻击者向用户发送ICMP重定向报文，更改用户主机的路由表，干扰用户主机正常的IP报文转发
ICMP Unreachable	某些系统在收到不可达的ICMP报文后，对于后续发往此目的地的报文判断为不可达并切断对应的网络连接。攻击者通过发送ICMP不可达报文，达到切断目标主机网络连接的目的
LAND	攻击者向目标主机发送大量源IP地址和目的IP地址都是目标主机自身的TCP SYN报文，使得目标主机的半连接资源耗尽，最终不能正常工作
Large ICMP	某些主机或设备收到超大的报文，会引起内存分配错误而导致协议栈崩溃。攻击者通过发送超大ICMP报文，让目标主机崩溃，达到攻击目的
Route Record	攻击者利用IP报文中的Route Record路由选项对网络结构进行探测
Smurf	攻击者向目标网络发送ICMP应答请求，该请求包的目的地址设置为目标网络的广播地址，这样该网络中的所有主机都会对此ICMP应答请求作出答复，导致网络阻塞，从而达到令目标网络中主机拒绝服务的攻击目的
Source Route	攻击者利用IP报文中的Source Route路由选项对网络结构进行探测
TCP Flag	不同操作系统对于非常规的TCP标志位有不同的处理。攻击者通过发送带有非常规TCP标志的报文探测目标主机的操作系统类型，若操作系统对这类报文处理不当，攻击者便可达到使目标主机系统崩溃的目的
Tracert	攻击者连续发送TTL从1开始递增的目的端口号较大的UDP报文，报文每经过一个路由器，其TTL都会减1，当报文的TTL为0时，路由器会给报文的源IP设备发送一个TTL超时的ICMP报文，攻击者借此来探测网络的拓扑结构
WinNuke	攻击者向安装（或使用）Windows系统的特定目标的NetBIOS端口（139）发送OOB（out-of-band）数据包，这些攻击报文的指针字段与实际的位置不符，从而引起一个NetBIOS片断重叠，致使已与其他主机建立连接的目标主机在处理这些数据的时候系统崩溃

表2 Flood攻击分类表

攻击类型	说 明
CC攻击	模拟多个用户（多少线程就是多少用户）不停地进行访问，访问那些需要大量数据操作,就是需要大量CPU时间的页面
DNS Query Flood	向被攻击的服务器发送大量的随即生成的或者不存在的域名解析请求，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
Fragment Flood	分片攻击
HTTP Get Flood	多是CC攻击
ICMP Flood	攻击者在短时间内向特定目标发送大量的ICMP请求报文（例如ping报文），使其忙于回复这些请求，致使目标系统负担过重而不能处理正常的业务
SYN Flood	由于资源的限制，TCP/IP 协议栈只能允许有限个 TCP 连接。SYN Flood 攻击者向服务器发送伪造源地址的 SYN 报文，服务器在回应 SYN ACK 报文后，由于目的地址是伪造的，因此服务器不会收到相应的 ACK 报文，从而在服务器上产生一个半连接。若攻击者发送大量这样的报文，被攻击主机上会出现大量的半连接，耗尽其系统资源，使正常的用户无法访问，直到半连接超时
TCP Flood	利用 TCP 协议漏洞制造的攻击
UDP Flood	攻击者在短时间内向特定目标发送大量的UDP报文，致使目标系统负担过重而不能处理正常的业务
Other Flood	其他攻击

9.1.3 安全策略基线配置

应支持安全策略基线配置的功能。由业务管理部件下发安全基线配置数据到检测部件，检测部件根据安全策略基线来判断是否发生攻击。安全基线的配置方式可以是系统自定义，也可以通过选择预先定义好的基线模板进行配置。

9.1.4 安全策略基线自学习

应支持安全策略基线自学习功能。可以根据实际网络中的流量情况，学习出一套与实际网络相似的流量分布情况并自动生成安全策略基线，学习到的安全策略基线上报给业务管理部件，由业务管理部件对此策略基线进行进一步加工处理后，再下发给检测部件或清洗部件。

当网络发生变化，已有的安全策略基线不适合现有的环境时，应支持安全策略基线重新学习功能，以确保安全策略基线的准确性。

9.1.5 流量监控数据上报

应支持流量监控数据上报给业务管理部件的功能。

9.1.6 攻击检测数据上报

应支持攻击检测数据上报到业务管理部件的功能。

9.1.7 检测能力扩展

应支持检测能力平滑扩展，多个检测部件并联完成检测任务。

9.1.8 互为备份、负载分担

当保护对象业务流量较大、多个检测部件共同完成检测任务时，各个检测部件应支持互为备份、负载分担。

9.2 异常流量清洗部件

9.2.1 攻击流量处理

1）清洗

应支持攻击流量清洗功能，应能清洗掉如下常见攻击：

畸形报文：见表1；

对于此类攻击，根据报文的协议特征和交互特征准确识别出攻击报文从而进行有效过滤拦截。

Flood攻击：见表2；

对于此类大流量攻击，当报文流量超过安全策略基线设定的门限值时，自动触发更高级的防护机制，其中包括对虚假源IP的识别（对于TCP连接，利用SYN Cookie机制），UDP方式的DNS转换为TCP方式DNS进行虚假源IP识别，HTTP Get Flood（CC攻击）利用HTTP重定向机制对源IP进行合法性识别等。对于识别为虚假源IP的报文流直接进行过滤拦截。

2）流量限制

对于未知异常流量采取限制流量措施，主要根据安全策略基线对未知异常流量进行限制，对于超过安全策略基线的报文进行过滤拦截。

3）自定义过滤

应支持抓包功能，即通过设定设备接口、协议类型、端口等条件来抓取异常流量清洗部件报文的功能。抓取攻击报文，通过分析报文特征，提取攻击特征等信息，以便制定自定义过滤攻击策略。

应支持自定义过滤功能，当现有的防御策略不能完全防御攻击时，可以根据抓包的报文分析得到的攻击特征、攻击类型（IP头、TCP头、TCP载荷、UDP头以及UDP载荷等）、攻击源IP、源端口、目的IP、目的端口等信息来定制精确化的过滤策略，过滤攻击报文的功能。

9.2.2 流量回注

9.2.2.1 策略路由方式

应支持策略路由的流量回注。通过在旁路路由器上配置策略路由，将流量清洗部件回注的流量指向被保护对象对应的下一跳，从而绕过旁路设备的正常转发，实现该被保护对象的流量回注，组网如图4所示。

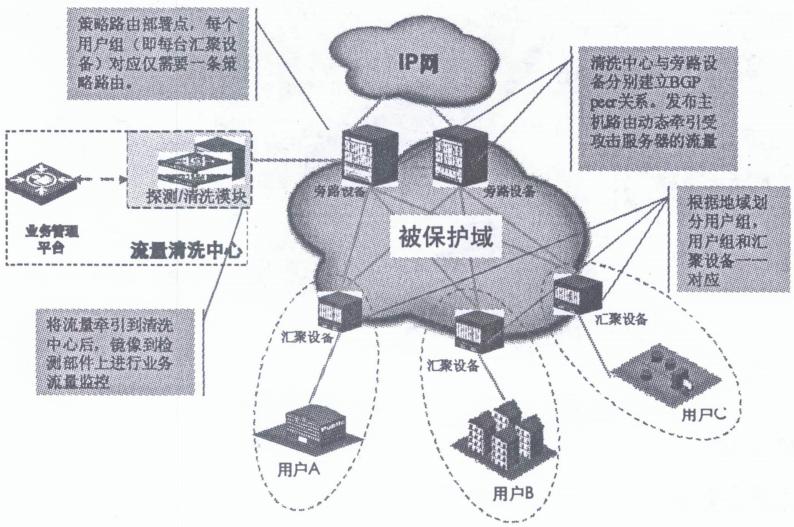

图4 采用策略路由实现流量回注

9.2.2.2 二层透传方式

宜支持二层透传流量回注。流量清洗部件旁路在城域网汇聚设备或者数据中心核心或者汇聚设备上，此时利用二层透传的方式来回注用户的流量，这种透传方式为特定组网环境下的回注方法。将流量清洗

系统、旁路设备、旁路设备正常三层转发的下一跳置于相同VLAN中，通过在流量清洗系统上做三层转发，旁路设备上做二层透传，从而绕过旁挂设备的正常转发，实现该用户的流量回注，组网如图5所示。

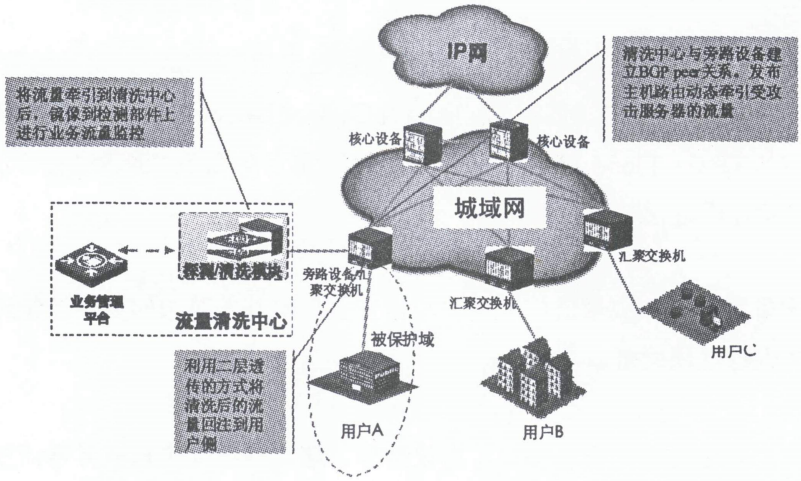

图5　采用二层透传方式实现流量回注

9.2.2.3　MPLS VPN方式

宜实现MPLS VPN方式流量回注。利用流量清洗系统做PE与城域网汇聚设备建立MPLS VPN隧道，清洗后的流量进入VPN内进行转发，在旁路设备上直接进行标签转发，从而绕过旁路设备的正常三层转发，实现该用户的流量回注，组网如图6所示。

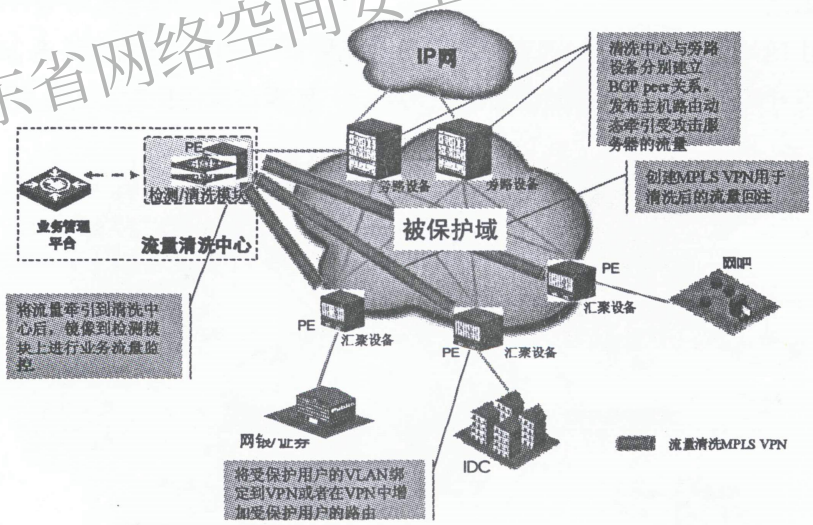

图6　采用MPLS VPN实现流量回注

9.2.3　流量监控数据上报

系统应支持流量监控数据上报给业务管理部件的功能。

9.2.4　攻击清洗数据上报

系统应支持攻击清洗数据上报到业务管理部件的功能。

9.2.5　清洗能力扩展

清洗部件应支持清洗能力平滑扩展，多个清洗部件并联完成清洗任务。

9.2.6　互为备份、负载分担

当保护对象业务流量较大、多个清洗部件共同完成清洗任务时，各个清洗部件应支持互为备份、负载分担。该功能的实现原理如下：

在各个清洗部件上运行虚拟路由冗余协议（VRRP），使得各个清洗部件成为一个VRRP组。

将各清洗部件的上一级设备的（如果清洗部件是模块，那么上一级设备就是清洗模块所在设备）向清洗部件转发业务流的端口聚合在一起，形成聚合端口组，该聚合端口组基于流进行负载分担。

为了与同网段其他设备通信，各个清洗部件之间应配置ARP表项一致。

9.3 业务管理部件

9.3.1 清洗业务管理功能

系统应支持清洗业务管理功能，包括：

提供策略模板功能。按照清洗所保护的对象的特点，将清洗业务分类为两种类型：上网业务类型和服务器业务类型。上网业务类型，提供对网络出口的保护，应用于无特定软件应用的网络保护。检查网络的全部TCP，UDP及其他应用的特征并进行保护。应针对不同带宽的上网业务类型提供预定义的策略模板。服务器业务类型，提供对网络应用服务器的定向保护，应用于各种网络服务器的保护。应能够自动学习、检查网络服务器提供的应用，并应能够针对这些应用的特征提供更加专业的保护。应提供对不同应用在不同环境下的策略模板，以便简化配置。

建立清洗任务功能。保护对象受到攻击后，应能够自动建立一个清洗任务，用于跟踪、监控本次攻击和清洗的过程并实时展示，也应支持手动为保护对象建立一个清洗任务。

引流功能。针对攻击，应根据预先配置的策略来决定是自动执行引流清洗，还是等待用户来决定是否开始清洗。

告警功能。对于清洗任务的各个阶段应提供告警，通知用户清洗任务的进程，用户也可以定制告警的阶段、内容和形式。

自动配置功能。对于清洗业务配置，业务管理部件将自动完成将配置下发到检测部件和清洗部件，在清洗任务中自动与相关设备进行联动，进行BGP路由引流，回注等配置。

9.3.2 报表功能

系统应支持报表功能，报表不仅仅是提供统计的数据，还要在统计数据的基础上进行分析，提供统计分析图。报表功能包括：

基于被保护对象的关键元素分析做出统计分析报表，例如新建会话数、连接数、并发会话数、流量、报文数等。

根据被保护对象实时流量，提供精确的流量分析报告。

统计数据应保存400天以内的记录，并能提供保存数据时间内任意时长的统计报表。

统计报表应支持导出功能，应支持统计分析图的导出。

检测流量分析报表。针对被保护对象的检测流量，业务管理部件应支持Top IP流量统计、IP流量明细统计、IP分片流量统计、TCP流量统计、HTTP流量统计、DNS流量统计。

清洗业务分析报表。记录被保护对象受到的攻击和执行的清洗任务。提供清洗任务的统计报表。提供清洗任务的时间、攻击流量信息等。针对清洗部件清洗的流量还需要支持清洗流量统计、Top具体定义服务器流量统计、攻击类型分布和TOP攻击源统计。

9.3.3 设备管理

系统应支持设备管理功能，即集中对流量检查部件和流量清洗部件的管理，能够自动完成清洗被保护对象及其策略的同步配置。业务管理部件能够监控流量检测部件和流量清洗部件的运行状态，并在相应部件上自动完成业务需要的配置。应支持对流量检测部件和流量清洗部件上报的事件进行分析联动。

业务管理部件应支持负载分担的组网方式。将各部件按逻辑功能和组网方式组织为一个清洗系统进行逻辑管理，提供对清洗系统的用户管理，能够动态为清洗部件扩容，同步配置，应支持多清洗部件的管理。

9.3.4 被保护对象管理

系统应支持用户，业务，保护IP的三级管理。对被保护用户的业务进行分类管理。针对业务类型的不同，上网业务和服务器业务分别进行管理。应支持保护对象的状态查看，手动进行清洗任务管理。

针对上网业务，提供在不同的网络情况下的预定义策略模板。还支持手动对策略进行细节调整。

针对服务器业务，可以自动学习被保护服务器提供的网络应用的信息。针对不同的网络应用提供专项的检查，也可以通过预定义的策略模板进行配置，需要提供不同应用的不同网络情况下的预置策略模板，也可以手动对策略继续细节调整。

9.3.5 实时流量数据分析、监控

系统应支持被保护对象实时流量数据分析、业务攻击状况和设备负载状况实施监控等功能。针对清洗任务，实时提供清洗前的流量信息、清洗后的流量信息；攻击流量和正常流量的分布和趋势；各种攻击类型的分布和趋势等信息。

9.3.6 告警功能

系统应支持安全事件任务告警功能。对清洗任务的不同时间阶段及时提供告警，以便于用户及时对攻击进行了解和处理。应支持对于告警的时间、阶段、告警的内容及告警的形式的配置并应支持提供多种告警方式，应支持邮件告警和声音告警。

中华人民共和国
通信行业标准
网络异常流量清洗系统技术要求
YD/T 2272-2011
*
人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
宝隆元（北京）印刷技术有限公司印刷

开本：880×1230 1/16 2011年9月第1版
印张：1 2011年9月北京第1次印刷
字数：25千字
ISBN 978-7-115-2386/11-337
定价：10元