宽带流量清洗解决方案技术白皮书

关键词：**DDoS**，流量清洗，**AFC**，**AFD**， 攻击防范

摘　　要：本文介绍了**H3C**宽带流量清洗解决方案技术的应用背景，描述了宽带流量清洗解决方案的业务实现流程以及关键技术，并对其在实际组网环境的应用作了简要的介绍

缩略语清单：

缩略语	英文全名	中文解释
DDoS	Distributed Deny of Service	分布式拒绝服务攻击
AFC	Anomaly Flow Cleaner	异常流量清洗设备
AFD	Anomaly Flow Detector	异常流量检测设备

杭州华三通信技术有限公司　　www.h3c.com.cn

目 录

1 技术背景 1
1.1 网络安全面临的挑战 1
1.2 流量清洗是运营商的新机会 1
2 宽带流量清洗解决方案介绍 2
2.1 方案总体介绍 2
2.2 流量检测防御技术 3
2.3 流量牵引技术 3
2.4 流量回注技术 4
2.4.1 策略路由方式 4
2.4.2 MPLS VPN方式 4
2.4.3 二层透传方式 5
2.5 丰富的业务报表 6
3 宽带流量清洗解决方案的典型组网 8
3.1 典型部署模式 1 8
3.2 典型部署模式 2 8
3.3 典型部署模式 3 9
4 方案总结 10

插图目录

图 1 流量清洗方案原理逻辑示意图.....2
图 2 流量牵引示意图.....3
图 3 采用策略路由技术实现流量回注.....4
图 4 采用MPLS VPN技术实现流量回注.....5
图 5 采用二层透传方式实现流量回注.....6
图 6 攻击TOP N统计表.....7
图 7 业务流量趋势图.....7
图 8 连接数趋势图.....7
图 9 典型部署模式 1.....8
图 10 典型部署模式 2.....9
图 11 典型部署模式 3.....9

1 技术背景

1.1 网络安全面临的挑战

随着网络技术和网络经济的发展，网络对企业和个人的重要程度在不断增加。与此同时，网络中存在的安全漏洞却也正在相应的增加，网络安全问题所造成的影响也越来越大。另一方面，网络黑金产业链也逐步形成。网络攻击的威胁越来越受经济利益驱使，朝着规模化、智能化和产业化发展。黑客攻击由原来的个人行为，逐渐转化为追求经济和政治利益的集体行为。有着严密组织的网络犯罪行为开始出现，给被攻击企业造成很大的损失，同时造成了恶劣的社会影响。越来越严重的城域网网络安全威胁，不仅影响了被攻击城域网接入大客户的业务质量，而且也直接影响着城域网自身的可用性。

近年来我国发生的大量安全事件和一系列安全威胁统计数据正以血淋淋的事实说明我国对城域网安全建设的重要性：

- 2007 年年底某省针对网吧的 DDoS 攻击敲诈勒索案件，导致网吧损失巨大。
- 2007 年 6 月完美时空公司遭受 DDoS 攻击损失数百万元。
- 2007 年 5 月某某游戏公司在北京、上海、石家庄 IDC 托管的多台服务器遭到 DDoS 攻击长达 1 月，经济损失达上百万元。
- 2006 年~07 年众多著名威客网络遭遇 DDoS 攻击，损失巨大
- 2006 年 12 月，针对亚洲最大的 IDC 机房 DDoS 攻击导致该 IDC 间歇性瘫痪
- 目前中国“黑色产业链”的年产值已超过 2 亿元，造成的损失则超过 76 亿元

1.2 流量清洗是运营商的新机会

对 DDoS 攻击流量的清洗是目前最适合运营商来开展的业务。我们可以从两个角度来分析对 DDoS 流量清洗最适合运营商来开展业务的原因。

从城域网中接入的大客户的角度来看。在面临越来越严重的 DDoS 攻击的情况下，企业对 DDoS 攻击防御的需求越来越迫切。然而 DDoS 攻击自身的复杂性导致企业难以独立完成对 DDoS 攻击的防御。目前企业往往只能被动的采用服务器资源和带宽资源扩容的方式来保证自己的正常业务的资源能够得到满足。但随着 DDoS 攻击的规模越来越大，这种资源预留的作用越来越小。而运营商由于自身特点却是很好地 DDoS 攻击防御点。运营商自身具有充足的带宽资源，可以防止 DDoS 攻击流量不会将用户正常流量淹没，从而失去流量清洗的效果。另外，由于运营商同时面对城域网的众多用户提供服务，可以保证清洗设备的利用率，有效节约清洗成本，

从运营商的角度来看通过对城域网中大量的 DDoS 流量的过滤，可以有效减小城域网自身的负载，为城域网所承载的高价值业务提供有效的质量保障。可以在减小对城域网扩容压力的同

时保证高价值客户的网络业务质量，从而保持现有高价值客户的忠诚度，并且吸引新的高价值客户的接入。

综上所述，在城域网侧为企业客户开展流量清洗业务实现对 DDoS 攻击的防御，可以同时满足运营商和大客户的双重需要，已经成为目前运营商的必然需求。

2 宽带流量清洗解决方案介绍

2.1 方案总体介绍

宽带流量清洗解决方案提供的服务包括：网络业务流量监控和分析、安全基线制定、安全事件通告、异常流量过滤、安全事件处理报告等。“宽带流量清洗解决方案”的实施，减轻了来自于 DDoS 攻击流量对城域网造成的压力，提升带宽利用的有效性；保护企业网络免受来自互联网的攻击，提高网络性能，实现其核心业务的永续，保障其核心竞争力。

宽带流量清洗解决方案主要分为三个步骤。第一步，利用专用的检测设备对用户业务流量进行分析监控。第二步，当用户遭受到 DDoS 攻击时，检测设备上报给专用的业务管理平台生成清洗任务，将用户流量牵引到流量清洗中心。第三步，流量清洗中心对牵引过来的用户流量进行清洗，并将清洗后的用户合法流量回注到城域网。同时上报清洗日志到业务管理平台生成报表。其原理图如下：

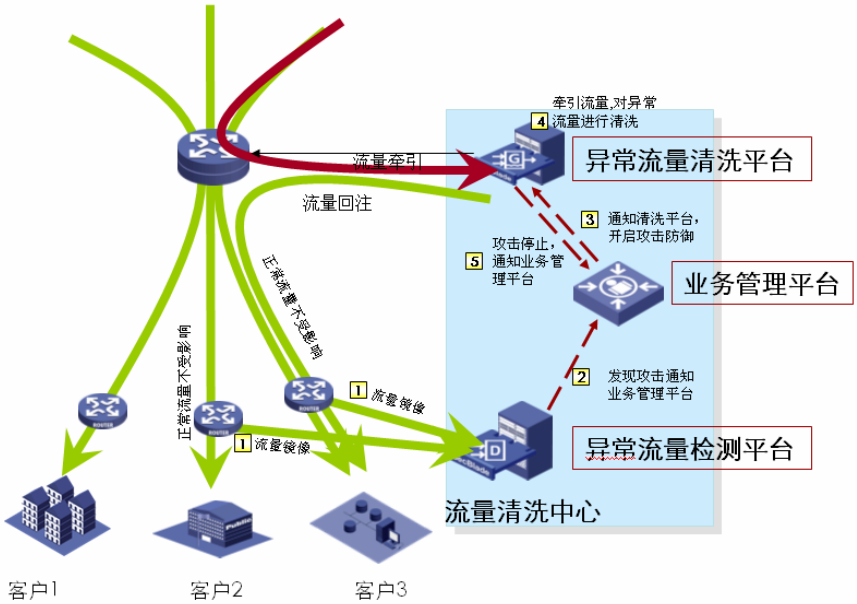

图1 流量清洗方案原理逻辑示意图

解决方案涉及的关键技术包括对 DDoS 攻击的检测防御，对被攻击用户的流量的牵引和清洗后的流量回注。其具体技术请见下面的描述。

2.2 流量检测防御技术

H3C 流量清洗宽带流量清洗解决方案，流量检测和防御功能由旁挂在城域网的专用探测和防御设备实现。

H3C DDoS 探测设备通过对城域网用户业务流量进行逐包的分析和统计，完成用户流量模型的自学习，并自动形成用户流量模型基线。基于该基线探测设备可以对用户的业务流量进行实时监测。当发现用户流量异常后，探测设备向专用的业务管理平台上报攻击事件。

H3C DDoS 防御设备通过静态漏洞攻击特征检查、动态规则过滤、异常流量限速和 H3C 独创的“基于用户行为的单向防御”技术，可以实现多层次安全防护，精确检测并阻断各种网络层和应用层的 DoS/DDoS 攻击和未知恶意流量。支持丰富的攻击防御功能，如，SYN Flood，UDP Flood，ICMP Flood、ACK Flood、RST Flood、DNS Query Flood、HTTP Get Flood 等常见攻击的防御。

2.3 流量牵引技术

为了在用户的业务遭受 DDoS 攻击时，将用户的流量动态的牵引到流量清洗中心来进行清洗。H3C 流量清洗中心利用 IBGP 或者 EBGP 协议，首先和城域网中用户流量路径上的多个核心设备（直连或者非直连均可）建立 BGP Peer。攻击发生时，流量清洗中心通过 BGP 协议会向核心路由器发布 BGP 更新路由通告，更新核心路由器上的路由表项，将流经所有核心设备上的被攻击服务器的流量动态的牵引到流量清洗中心进行清洗。同时流量清洗中心发布的 BGP 路由添加 no-advertise 属性，确保清洗中心发布的路由不会被扩散到城域网，同时在 H3C 流量清洗中心上通过路由策略不接收核心路由器发布的路由更新。从而严格控制对城域网造成的影响。下图所示：

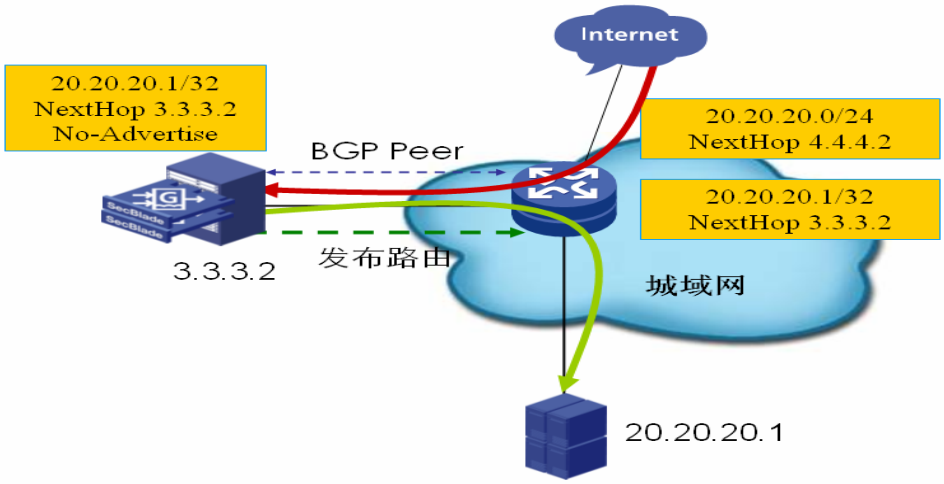

图2 流量牵引示意图

2.4 流量回注技术

H3C 流量清洗系统支持丰富的网络协议和多种物理接口来实现将清洗后的流量重新注入到城域网。可以提供策略路由、MPLS VPN、二层透传、双链路等多种方式进行用户流量的回注。下面以前三种方式为例详细介绍具体方案。

2.4.1 策略路由方式

通过在旁挂路由器上配置策略路由，将流量清洗中心回注的流量指向受保护设备相对应的下一跳，从而绕过旁挂设备的正常转发，实现该用户的流量回注。为了简化策略路由的部署，可以将城域网的用户分组，仅为为每组用户配置一条策略路由指向该组用户所对应的下一跳设备。这样既可实现针对该组用户的流量回注。而且在初期实施完成后不需要在修改城域网设备的配置。方案的可维护性和可操作性得到了很大的增加。其组网如下图所示：

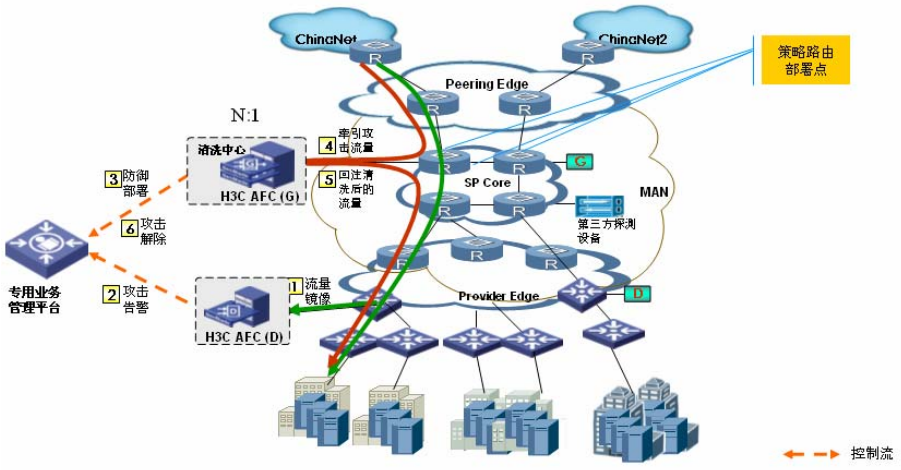

图3 采用策略路由技术实现流量回注

- 采用策略路由方式进行流量回注的优点是：
  部署简单，对城域网影响的设备点较少；
  一次部署后续无需改动；
- 采用策略路由方式进行流量回注的局限是：
  直接影响城域网核心设备；

2.4.2 MPLS VPN 方式

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，从而绕过旁挂设备的正常转发，实现该用户的流量回注。其组网如下图所示：

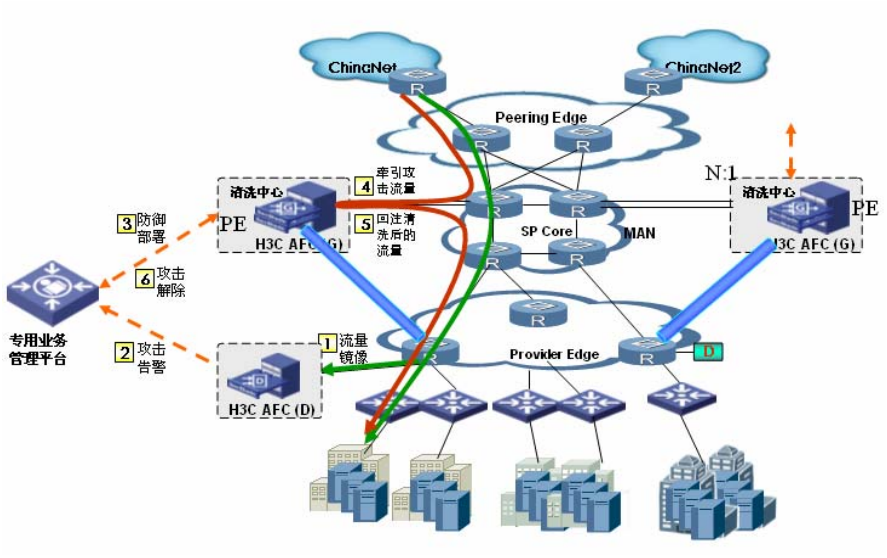

图4 采用 MPLS VPN 技术实现流量回注

- 采用 MPLS VPN 方式进行流量回注的优点是：

  部署完成之后，后续用户业务开展工作量很小；

  对网络拓扑的修改主要是城域网边缘，对核心层拓扑的冲击很小；

- 采用 MPLS VPN 方式进行流量回注的局限是：

  依赖城域网设备支持 MPLS VPN 功能；

  需要在全网部署清洗 VPN，对城域网改动范围大；

2.4.3 二层透传方式

流量清洗中心旁挂在城域网汇聚设备或者 IDC 核心或者汇聚设备上，旁挂设备作为受保护服务器的网关，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、城域网设备、受保护服务器置于相同 VLAN 中，通过在流量清洗系统上做三层转发，城域网设备上做二层透传，从而绕过旁挂设备的正常转发，实现该用户的流量回注。其组网如下图所示：

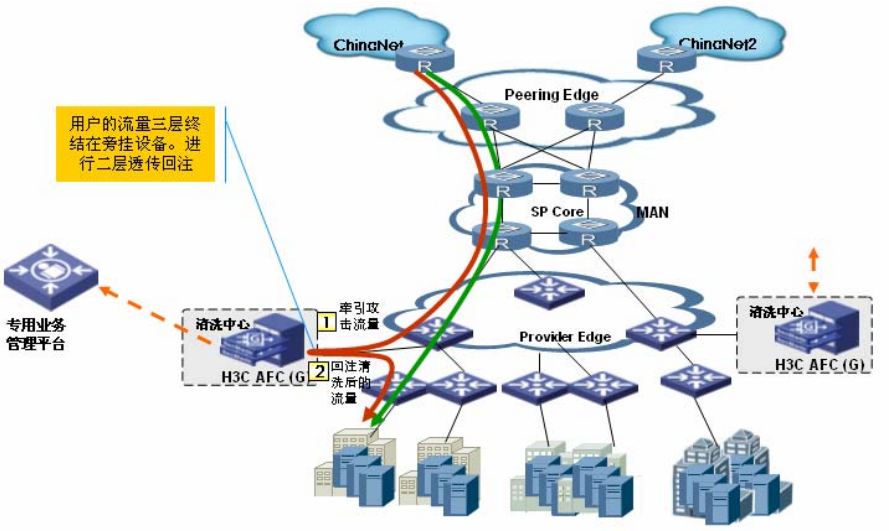

图5 采用二层透传方式实现流量回注

- 采用二层透传方式进行流量回注的优点是：

  方案部署简单，对城域网的影响很小。

- 采用二层透传方式进行流量回注的局限是：

  比较合适旁挂设备为交换机的情况

2.5 丰富的业务报表

宽带流量清洗方案作为一种安全服务，增强最终用户的安全感受，让用户能够及时直观的了解受保护业务的实时状况、攻击状况和清洗状况是一件非常重要的事。H3C 利用专用的业务管理平台——SecCenter 实现了城域网中的统一的设备、业务管理，并可以为用户提供专用的业务状况、攻击状况和清洗状况报表输出。在对受保护服务器进行异常流量监控和异常流量清洗的过程中，H3C 流量清洗系统的清洗模块和探测模块定时向 SecCenter 发送多种流量日志、攻击清洗日志。专用的业务管理平台 SecCenter 对安全模块上报的这些安全日志进行汇总、归纳和分析，输出多张用户业务、攻击清洗状况报表。可以很方便的给最终用户提供多维度的宽带流量清洗业务状况报表和提供安全事件处理报告，从而让最终用户实时直观的了解当前的业务状况和历时状况回溯。部分报表举例如下：

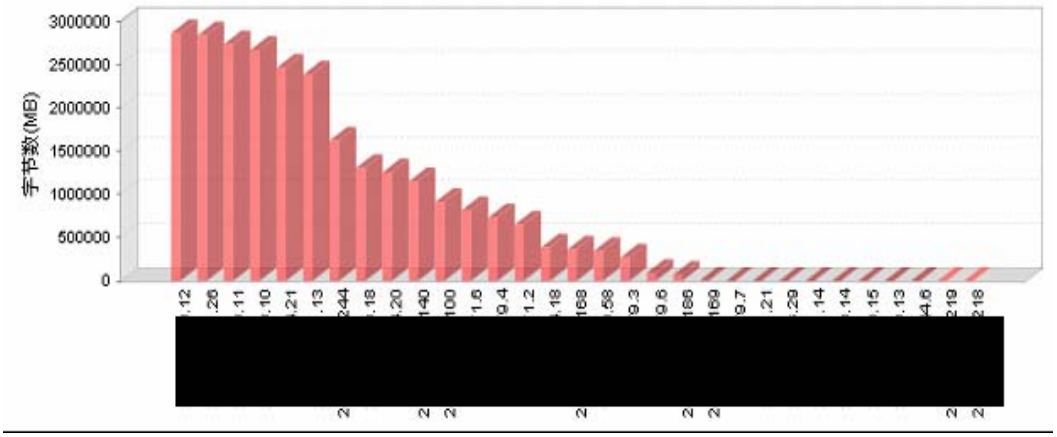

图6 攻击 TOP N 统计表

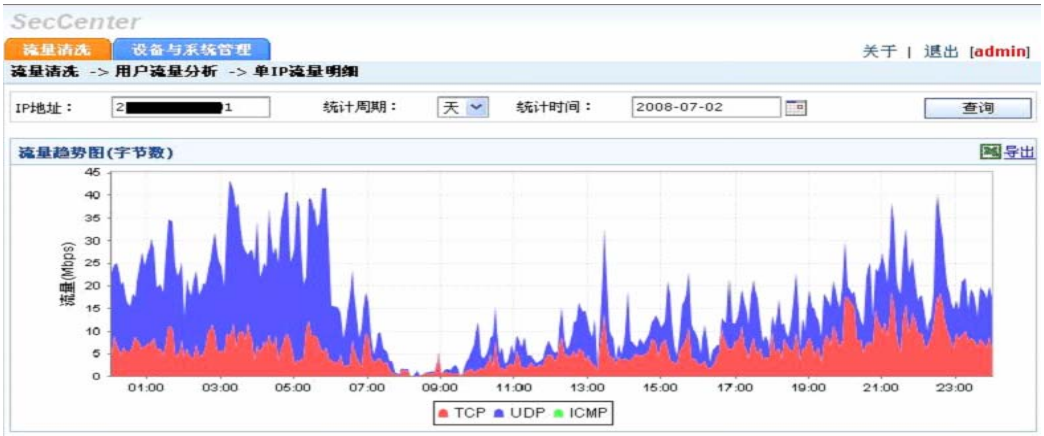

图7 业务流量趋势图

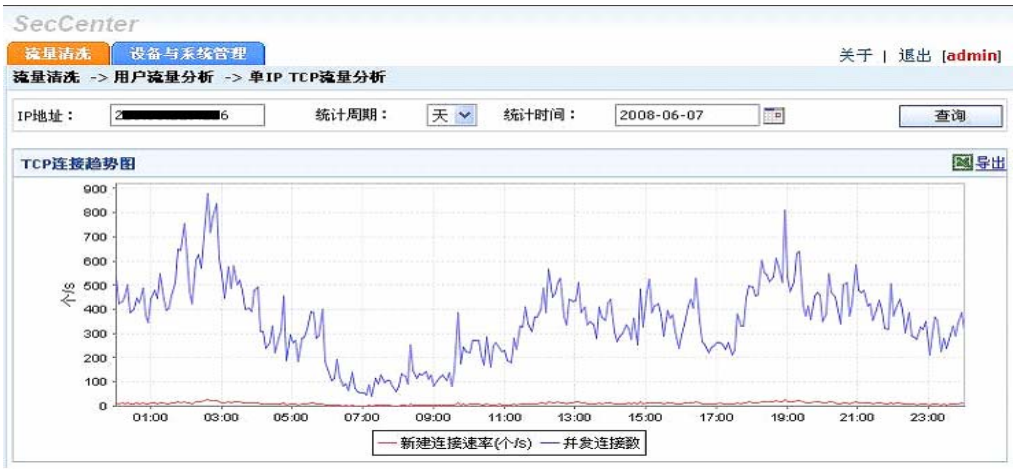

图8 连接数趋势图

3 宽带流量清洗解决方案的典型组网

3.1 典型部署模式 1

在城域网核心旁挂部署清洗模块。在靠近汇聚设备或者用户侧接入设备部署探测设备。这种组网模式，清洗模块对城域网覆盖面广，有利于支撑城域网内新增用户业务的开展。探测设备在靠近用户侧的汇聚或接入设备旁挂，通过分光或者镜像的方式将流量复制到探测设备进行逐包的监控，及时准确的发现用户的异常流量状况。同时，利用业务管理平台实现集中式的设备管理，业务管理和专用报表输出。

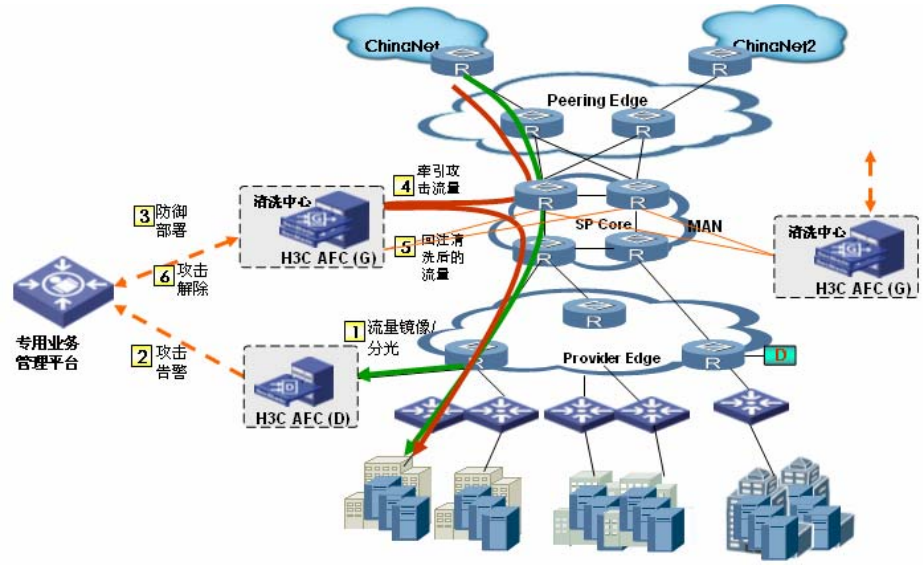

图9 典型部署模式 1

3.2 典型部署模式 2

在城域网核心同时旁挂部署清洗和探测设备。这种组网模式，能够很好的节约端口、光纤资源。清洗和探测模块对城域网覆盖面广，有利于支撑城域网内新增用户业务的开展。同时，利用业务管理平台实现集中式的设备管理，业务管理和专用报表输出。

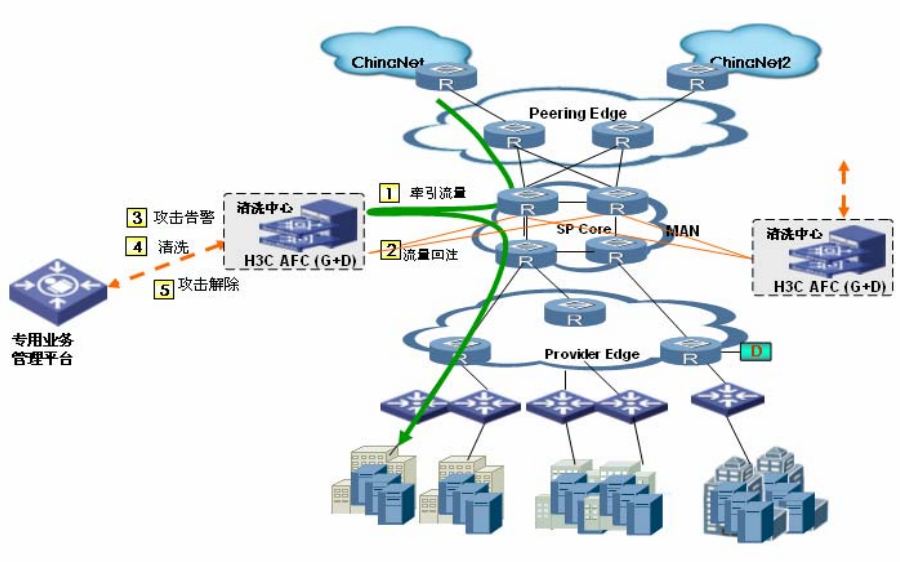

图10 典型部署模式 2

3.3 典型部署模式 3

随着流量清洗业务的发展。面对高价值用户的特殊需求，可以将对 DDoS 探测和防护部署位置合一，实现 VIP 客户流量的就地清洗。这种部署模式更加灵活，简单；同时可以利用业务管理平台实现对这些清洗设备的集中式管理和统一报表输出。

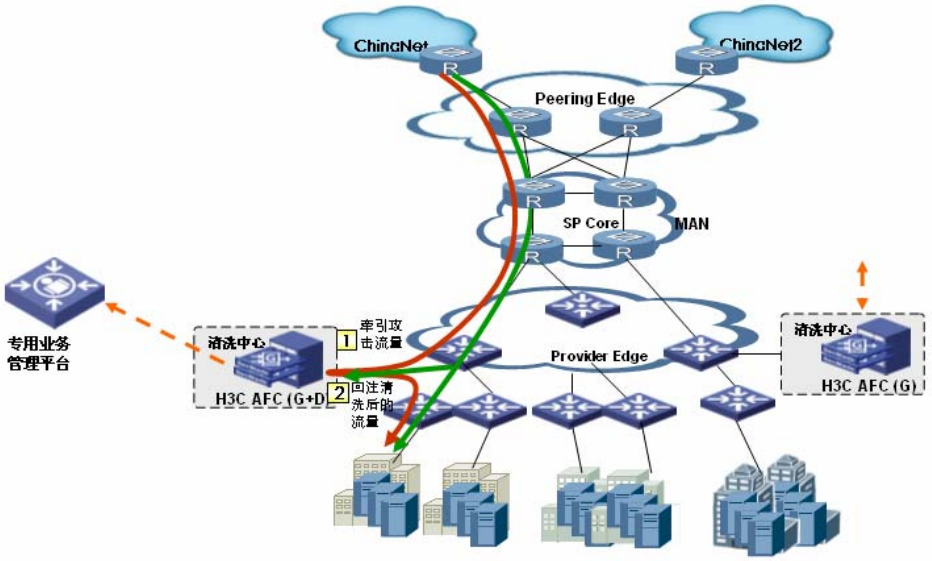

图11 典型部署模式 3

4 方案总结

H3C“宽带流量清洗解决方案”可以针对城域网中现在常见的 DDoS 攻击流量进行过滤，实现对城域网和大客户网络业务的保护。可以有效的兼顾城域网接入用户和运营商双方的利益，为建设安全可用的网络环境贡献自己的力量。

Copyright ©2008 杭州华三通信技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
本文档中的信息可能变动，恕不另行通知。