DPtech 异常流量清洗

技术白皮书

杭州迪普科技有限公司

2016 年 3 月

目录

一、 概述

1.1. 背景

拒绝服务攻击（DoS, Denial of Service）是指利用各种服务请求耗尽被攻击网络的系统资源，从而使被攻击网络无法处理合法用户的请求。而随着僵尸网络的兴起，同时由于攻击方法简单、影响较大、难以追查等特点，又使得分布式拒绝服务攻击（DDoS，Distributed Denial of Service）得到快速壮大和日益泛滥。成千上万主机组成的僵尸网络为 DDoS 攻击提供了所需的带宽和主机，形成了规模巨大的攻击和网络流量，对被攻击网络造成了极大的危害。

随着 DDoS 攻击技术的不断提高和发展，ISP、ICP、IDC 等运营商面临的安全和运营挑战也不断增多，运营商必须在 DDoS 威胁影响关键业务和应用之前，对流量进行检测并加以清洗，确保网络正常稳定的运行以及业务的正常开展。同时，对 DDoS 攻击流量的检测和清洗也可以成为运营商为用户提供的一种增值服务，以获得更好的用户满意度。

1.2. 常见的攻击手段

大多数情况下，网络中的数据包利用 TCP/IP 协议传输，这些数据包遵循正常的协议规范，是无害的，但是如果出现过多的异常数据包，就会造成网络设备或者服务器过载；或者数据包利用了某些协议的缺陷，人为的不完整或畸形，就会造成网络设备或服务器无法正常处理，迅速消耗了系统资源，造成拒绝服务，这就是 DDoS 的工作原理。DDoS 攻击之所以难以防范，就在于攻击流和正常流混合在一起，很难有效地分辨出攻击流。

一般而言，DDoS 攻击主要分为以下几种类型：

带宽型攻击：这类 DDoS 攻击通过发出海量数据包，造成设备负载过高，最终导致网络带宽或是设备资源耗尽。

资源型攻击：这类 DDoS 攻击利用了诸如 TCP 或是 HTTP 协议的某些特征，通过持续占用有限的资源，从而达到使目标设备无法处理正常访问请求的目的。

二、 异常流量清洗解决方案

2.1 现有方案的不足

传统的 DDoS 防护手段采用防火墙或路由器等设备均是基于网络层的检测，而大多数 DDoS 攻击可以采用合法协议进行攻击，因此传统的防护手段无法正确识别并加以防护。同时，防火墙或路由器并非为 DDoS 攻击防护而设计，因此一旦启用此功能，性能将受到极大影响最终导致无法正常工作。

升级设备也是一个避免受到 DDoS 攻击影响的一个方法，但是随着现阶段 DDoS 攻击流的猛增，设备升级速度很难赶上 DDoS 攻击流量的增长。

2.2 迪普科技异常流量清洗解决方案

迪普科技 DDoS 攻击防护可支持简单的在线部署模式或者旁路部署模式，针对不同的用户、不同环境，采用不同的部署方式。

对于大型的运营商网络或大流量的网络，一般会采用单臂式旁路部署模式。单臂式旁路部署的优势是不需要改变原有网络拓扑，不会引起单点故障，方便扩容，更容易部署，以下为单臂式旁路部署方案介绍。

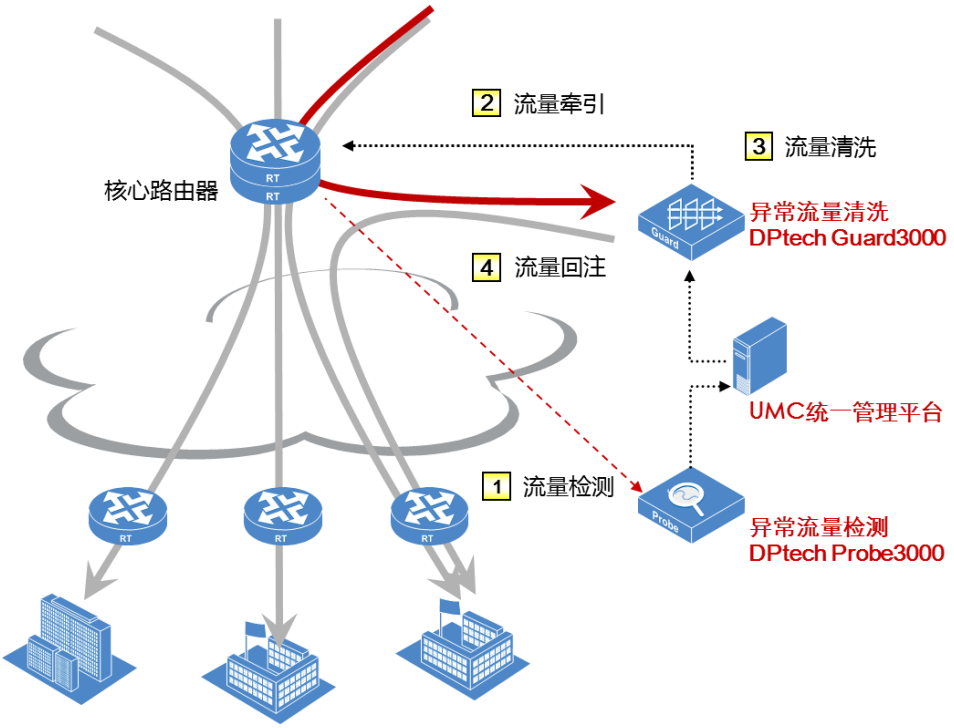

图 1 异常流量清洗单臂式旁路部署典型组网

如上图所示，异常流量清洗的单臂式旁路部署模式主要由流量检测、流量牵引、流量清洗、流量回注 4 个阶段组成：

1) 流量检测：异常流量检测设备 Probe3000 可通过镜像、分光、NetFlow/NetStream/nFlow 流日志等方式，对指定的流量进行检测，把这些目标的流量信息反馈给管理平台供用户参考，当发生攻击时，可及时发送告警给 UMC 统一管理平台。
2) 流量牵引：当收到告警日志后，UMC 将给异常流量清洗设备 Guard3000 下发防护策略，Guard3000 与核心网络设备进行交互，通过 BGP 动态路由协议将需要保护的用户流量牵引到 Guard3000 上进行防护。
3) 流量清洗：Guard3000 收到牵引过来的流量后进行攻击识别，采用专业的 DDoS 防护技术对攻击报文进行流量清洗。
4) 流量回注：完成清洗后，Guard3000 将清洗后的用户合法流量回注到用户网络中，同时上报清洗日志到 UMC 生成流量清洗报表。

单臂式旁路部署方式适合于大型网络，而对于 1G 左右流量的小型网络，也可采用在线部署模式。在线部署模式的优点是检测和防护一体化，而且可以检测到双向流量。但是串接方式的问题是灵活性不够，增加了故障节点，而且由于所有流量都经过设备，对于设备的可靠性要求非常高，典型组网如下图所示：

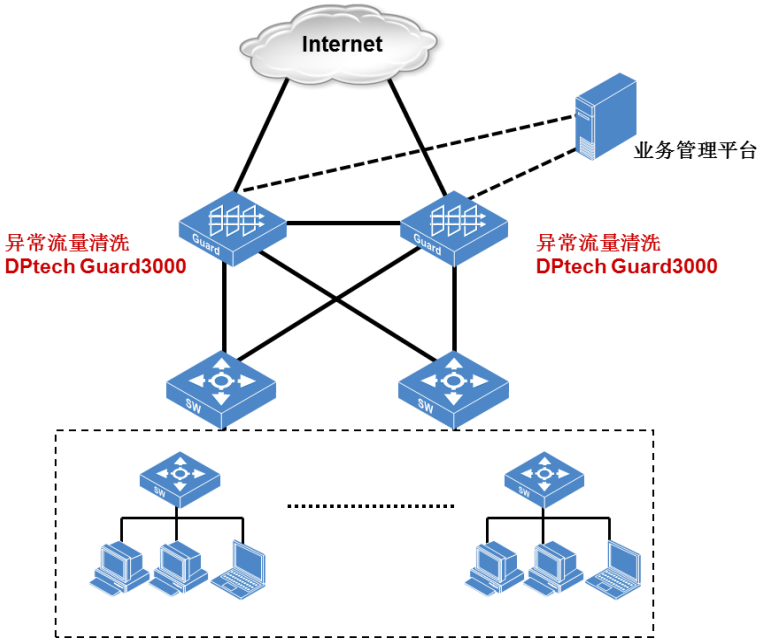

图 2 异常流量清洗在线部署典型组网

2.3 技术特色及优势

1)．高效的异常流量检测和清洗技术

既支持深度数据包检测技术（DPI），也可以通过分析网络设备输出的 NetFlow/NetStream/nFlow 流信息（DFI），从而深入识别隐藏在背景流量中的攻击报文，以实现精确的流量识别和清洗。采用先进的分布式多核硬件结构，并且可以通过智能集群方式实现多设备集群，从而打造超万兆级异常流量清洗平台。

2)．高可用性

可以采用在线或旁路部署的方式进行 DDoS 攻击的防护。当采用旁路部署的方式时，可以实现对流量的按需清洗，在任何情况下都不会影响正常流量。良好的网络协议适应性，能够支持 ARP、VLAN、链路聚合等网络层协议以及静态路由、RIP、OSPF、BGP、策略路由等路由协议，满足各种组网应用。当采用在线部署模式下，可以实时对威胁流量进行清洗。

3)．多层次的安全防护

通过静态漏洞攻击特征检查、动态规则过滤、异常流量限速和先进的“智能流量检测”技术，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，包括 SYN Flood、UDP Flood、ICMP Flood、DNS Query Flood、HTTP Get Flood、CC 攻击等各种攻击。

4). 自动流量牵引和灵活的流量回注

在发现 DDoS 攻击时，流量监测设备与流量清洗系统联动实现自动清洗功能，异常流量清洗设备 Guard3000 向邻居的路由器/交换机发布 BGP 更新路由通告，自动、迅速地将被攻击用户的流量牵引到 Guard3000 上来对其进行清洗。同时，Guard3000 可通过策略路由、MPLS VPN、GRE VPN、二层透传等多种方式，将清洗后的干净流量回注给用户，用户正常的业务流量不受任何影响。

5). 详尽的分析统计报表

针对检测和清洗的各种威胁流量，提供丰富的攻击日志和报表统计功能，包括攻击前流量信息、清洗后流量信息、攻击流量大小、时间及排序等信息以及攻击趋势分析等各种详细的报表信息，便于了解网络流量状况。

三、 异常流量清洗关键技术

3.1 异常流量检测技术

异常流量检测设备 Probe3000 通过与 UMC 统一管理平台的配合完成对于网络异常流量的监控和管理。对于超负荷流量及 DDoS 攻击做出判断并告警，帮助网络管理员生成网路监控图并完成日志报表的制作，在发现 DDoS 攻击时，流量监测设备与流量清洗系统联动实现自动清洗功能。

Probe3000 目前可支持两种检测方式：

1). 基于 DPI 检测

可以通过接收真实流量(可通过镜像或分光方式)进行 DPI 深度包检测功能，对流量做出最真实的分析。利用镜像作分析的好处是可以获取到原始报文的所有信息，统计数据比较完整，但是缺点是当需要检测的流量非常大时，对设备的性能要求太高。

2). 基于 DFI 检测

可以通过接收 NetFlow/NetStream/nFlow 等流信息进行流量统计分析，这种方法非常适合大流量的统计，缺点是统计数据比较粗糙，信息有延迟。

Probe3000 通过聚合用户的流量信息，根据设定的阈值对流量进行实时检测，定期上报流量日志。当判断存在异常流量后，会及时向 UMC 发送启动防护的告警日志，由 UMC 操作引流清洗任务。

Probe3000 同时具备智能识别攻击的能力，基于三四层报文信息以及常见的应用统计信息建立自动学习模型，会根据最新流量信息进行自动更新，通过这些学习模型，设备可以迅速发现存在的异常流量。这种智能学习对于发现未知攻击有很有效的作用。

Probe3000 支持多种 DDoS 攻击的检测，包括网络型攻击 SYN Flood、UDP Flood、DNS Query Flood、ICMP Flood、(M)Stream Flood、Ping of Death、Connection Flood、Land、Tear Drop、WinNuke 等，应用型攻击 HTTP Get 攻击、CC 攻击、DNS 攻击等。

3.2 异常流量清洗技术

异常流量清洗设备 Guard3000 通过异常流量限速，动态规则过滤，以及基于迪普科技自主研发的独特的指纹识别智能防护系统，可以实现多层次安全防护，精确过滤各种网络层和应用层的攻击和未知恶意流量。

3.2.1针对网络层的攻击防护

对于各种 Flood 攻击，除了提供最常见的限速功能外，迪普科技针对一些特殊的攻击提供专门的防护算法。

1）速率限制

根据用户配置的不同防护策略对流量进行汇聚统计，通过这些汇聚数据与用户设置阈值进行对比，对超过阈值的汇聚流进行限速。

2）SYN Cookie 防护

异常流量清洗设备Guard3000对TCP新建连接的协商SYN报文进行拦截处理，通过连接信息计算出一个 cookie 值，作为 SYN/ACK 报文的初始序列号（seq number）返回给客户端，再对客户端回应的 ACK 报文中携带的 cookie 信息来进行报文有效性确认。如果确认是合法请求，Guard3000 将作为代理会向服务器端发送 SYN 报文建立连接，客户端与服务器间关于此次连接的后续报文都将通过 Guard3000 进行代理转发。当攻击者向服务器发起 SYN Flood 攻击时，由于无法发送有效的 cookie 信息，因此无法与服务器建立连接并造成资源的消耗。在整个过程中，Guard3000 作为代理服务器和客户端交互，同时也模拟客户端与服务器进行交互，为服务器过滤掉恶意连接，保证了业务的正常稳定运行。

SYN Cookie 防护技术如下图所示：

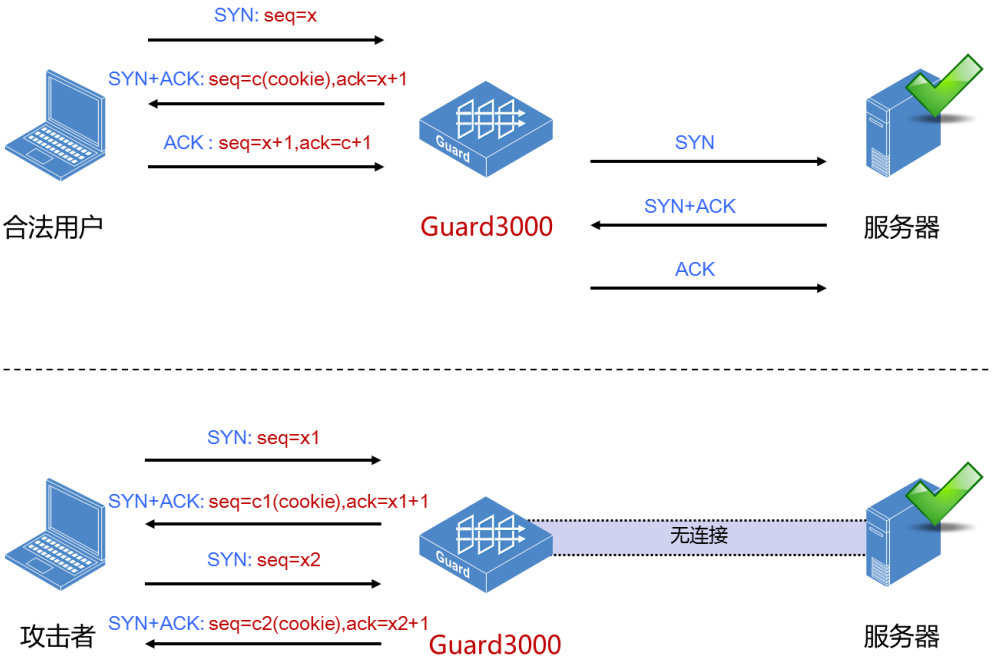

图 3 SYN Cookie 防护图示

3）SYN Reset 防护

SYN Cookie 技术能较为有效的防护 SYN Flood 攻击，但是这种技术由于需要清洗设备一直作为代理进行转发，因此对于设备的性能要求较高。SYN Reset 技术在 SYN Cookie 基础上做了进一步的优化。

当客户端发起新建连接 SYN 报文时，异常清洗设备 Guard3000 会先丢弃这个 SYN 报文，然后模拟服务器向客户端回应一个 SYN/ACK 报文，其中的确认序列号（ack number）未按协议规定要求生成，而是通过特殊算法计算的 cookie 值，与客户端的期望值不一样。正常请求的客户端获取到这个 SYN/ACK 报文后，发现确认序列号和预期的不一致，从而会向服务器回应一个序列号为 cookie 信息的 RST 报文，终止这条连接。Guard3000 提取这个报文中的 cookie 信息，随后与设备中的防护表项中的信息进行校验。如果校验通过，则连接被认为是可信的，然后就记录这个客户端 IP 到设备白名单中，随后的报文可以直接通过。由于攻击者一般不会处理回应的 SYN/ACK 报文，所以它不会回应 RST 报文进行验证，也就无法加入到 IP 地址白名单中，从而无法与服务器建立连接从而造成攻击。由于 SYN Reset 防护技术中清洗设备只需验证客户端的合法性，不需要作为代理进行转发，因此对于清洗设备的性能消耗非常小。

SYN Reset 防护技术如下图所示：

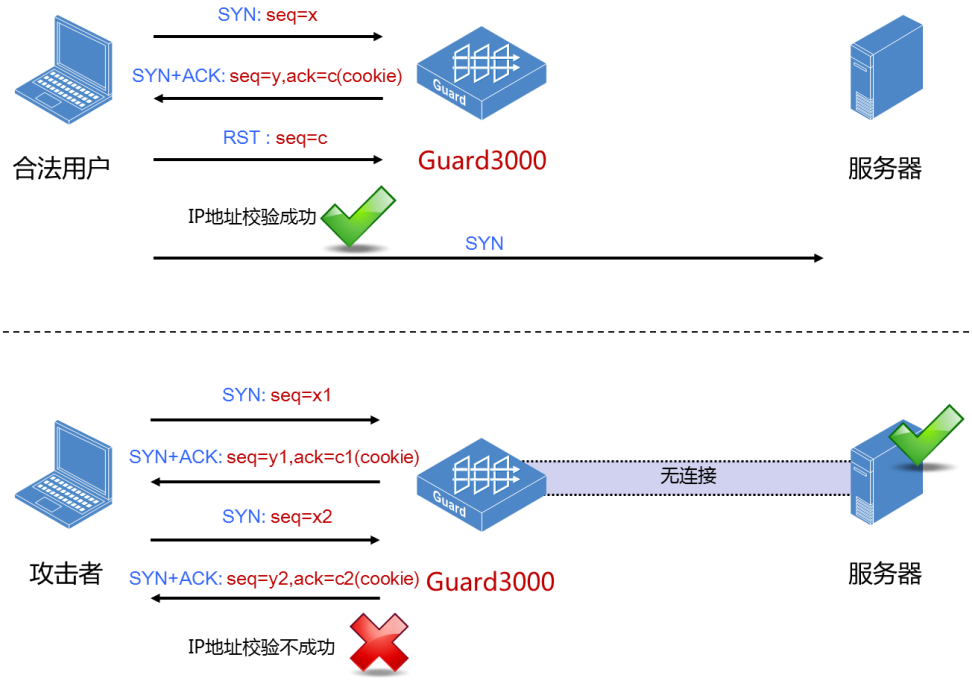

图 4 SYN Reset 防护图示

4）TCP 状态防护

正常客户端利用合法的协议栈进行通信，TCP 有相应的状态变迁模型，但是攻击者为了节省攻击资源没有使用合法协议栈，因此可通过一个简单的状态检测表项对 TCP 进行全状态检测，对于状态不全的报文进行丢弃，达到了屏蔽攻击的目的。例如，正常 TCP 请求是通过 3 次握手的方式连接的，它符合 TCP 的状态变迁模型，而一些 ACK flood，FIN flood 由于没有正常的 3 次握手，状态变迁模型是不完整的，所以这些报文会被直接过滤掉。

5）指纹识别防护

数据包的网络层、传输层中有很多字段，包括报文长度、TTL、源目的端口等信息，甚至包括数据段的一些信息，在不同的网络中，都是具有自己的统计特征的，这些信息就是指纹。指纹识别防护的基本思想在于根据正常网络流量的指纹建立防护模型，当网络异常的时候，提取出异常指纹和防护模型进行对比，对超过防护模型的数据包进行过滤。

例如针对报文长度，可在清洗设备 Guard3000 接收到报文后，提取出报文长度，将报文长度字段进行离散化存储，然后定时统计出当前网络下报文长度的分布模型。当网络出现异常的时候，会有某一种指纹分布出现波动，超过我们建立

的分布模型值，这时就可以根据这个指纹特征对异常报文进行过滤。

仅采用单个指纹特征的进行防护的效果有时可能不理想，所以可采用多个报文特征聚合成一个指纹特征的方法，例如源 IP 和 TTL 组合成一个整体，作为一个指纹进行统计过滤，这样对于一些复杂的异常流量攻击会有更好的效果。

3.2.2 针对应用层的攻击防护

应用层的攻击不同于网络层攻击，它往往是一种非对称的攻击，即客户端只需要耗费很小的带宽和主机资源，而服务器端则要消耗很大的带宽或者主机资源，这种攻击的破坏性更大。应用层攻击主要集中在 DNS 攻击以及 HTTP 攻击上。

1） DNS 域名限速

支持按照 DNS 的每个域名进行单独限速。这个限速还可以支持通配符，以支持域名部分随机的情况。

2） DNS 重传校验

当清洗设备检测到有攻击后，会把后续收到的第一个 DNS 请求报文缓存在本地，不直接转给服务器。正常主机在一段时间(2-5 秒)没有收到响应报文后会重发 DNS 请求报文，但是攻击报文依然会在短时间内不停的发送请求，通过这个特性，就可以马上丢弃这些不符合重传时间间隔的攻击报文。

3） DNS TC 反弹防护

几乎所有的 DNS 攻击都是用 UDP 报文，可以利用这个特性来防护一些离散的 DNS 攻击，当检测到 DNS 攻击时，设备会回应给客户端一个带有 TC 标示位的应答报文。这时正常的主机会重新发起基于 TCP 的 53 端口的请求，设备接到 TCP 的请求后，转化为 UDP 请求送给 DNS 服务器，以免 DNS 服务器由于处理大量 TCP 报文负载过大。但是，由攻击软件发送的模拟攻击报文不会重发 TCP 的 DNS 请求报文，因此所有的 DNS 攻击都会被设备丢弃而不会到达 DNS 服务器。

4） HTTP Cookie 验证防护

HTTP Cookie 技术主要原理就是按照 HTTP 协议的规范来认证 HTTP 请求数据包是不是来自一个合法的客户端。防护设备截获客户端发给服务器 URL 的 GET 请求，然后构造一个重定向报文发送给客户端，让客户端重新请求重定向的地址，在这个重定向报文中，添加了需要验证的 cookie 字段，这个 cookie 的添加通常

有两种方法：一个是通过 HTTP 头的 set-cookie 字段设置，要求下次 HTTP 请求需要携带指定的 cookie 字段；另一个是通过在重定向的 URL 后端添加一个 cookie 参数，要求用户访问这个带 cookie 参数的 URL 地址。当正常客户端接收到重定向报文后，会按照要求携带 cookie 字段访问指定的 URL 地址，防护设备验证通过后，会去掉添加的 cookie 字段然后透传给服务器，如果是攻击请求的话，由于它无法添加指定的 cookie 字段访问，在防护设备验证无法通过被直接丢弃。

HTTP Cookie 验证技术如下图所示：

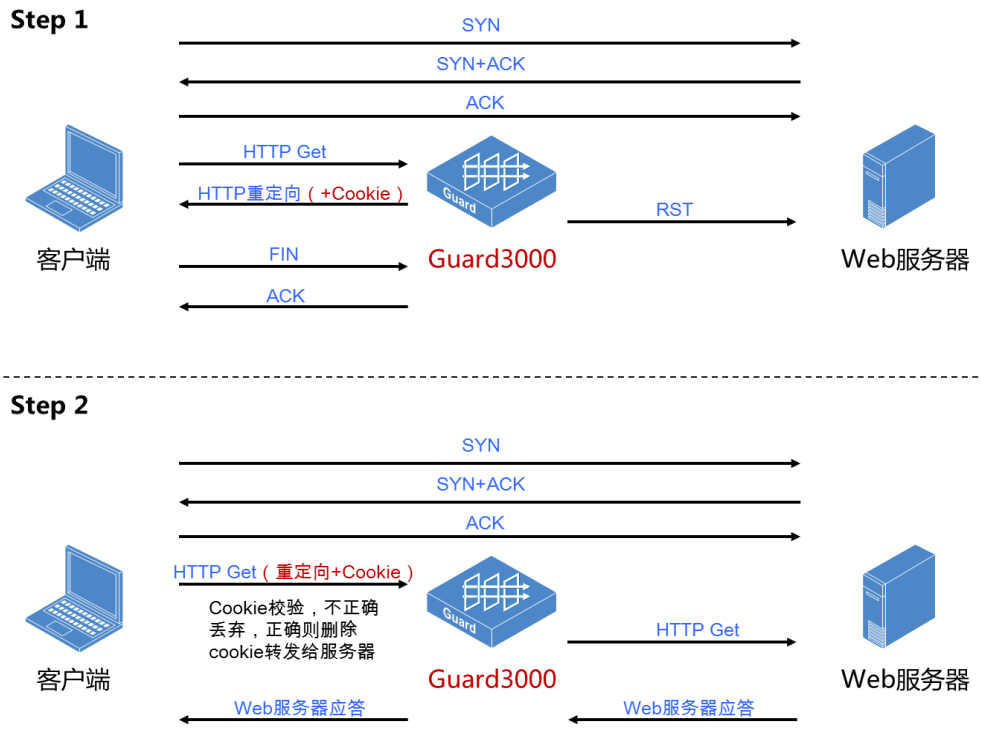

图 5 HTTP Cookie 防护图示

3.3 流量牵引

当检测到某个 IP 遭到攻击的告警日志时，这个 IP 的流量将被牵引到异常清洗设备 Guard3000 进行过滤。攻击结束后，异常流量检测设备 Probe3000 会发送攻击结束的告警日志，将这个 IP 的流量恢复原路径。

流量牵引技术可使用 BGP、OSPF、策略路由、MPLS 等，通常情况下，采用 BGP 作为流量牵引的方式。

攻击发生时，Guard3000 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清洗中心进行清洗。同时清洗设备发布的 BGP 路由添加 no-advertise 属性，确保清洗设备发布的路由不会被扩散到整个网络。

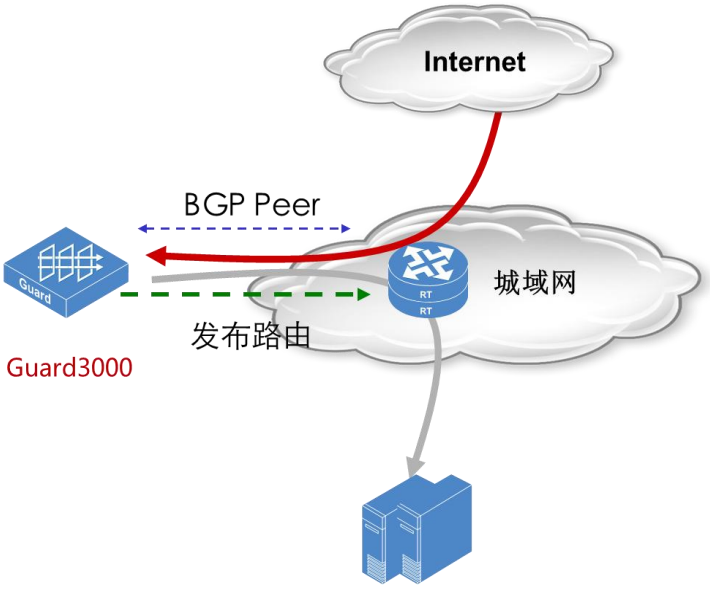

图 6 流量牵引示意图

3.4 流量回注

3.4.1策略路由回注方式

利用策略路由可以根据报文入接口指定转发下一跳的功能，通过在核心交换机（设备 A）上配置策略路由，将从接口 2 收到的从防护设备回注的流量转发给受保护设备相对应的下一跳（设备 B），由于策略路由优先于普通路由，因此在核心交换机（设备 A）收到回注流量时会优先命中策略路由而不会命中之前用于牵引流量的普通路由，因此不会再将回注流量发回给防护设备，从而避免环路。

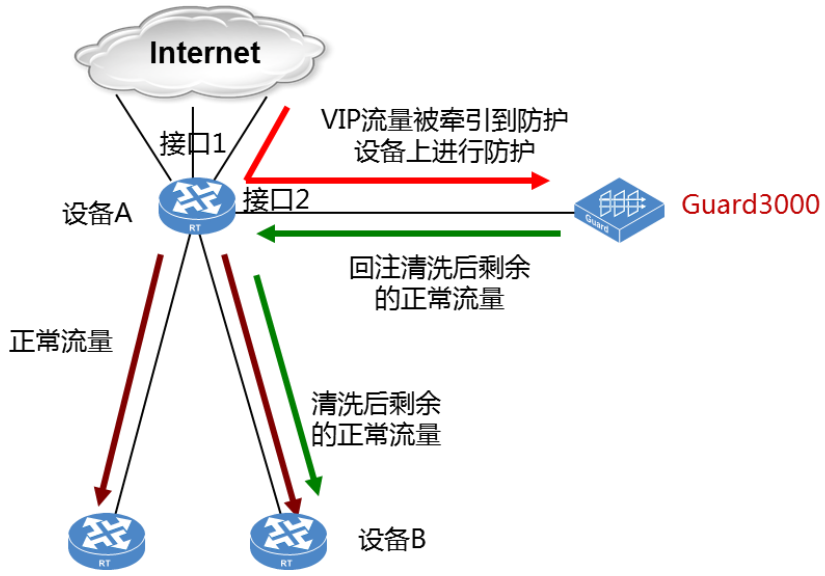

图 7 策略路由回注

3.4.2GRE 回注方式

在防护设备与受保护设备相对应的下一跳（设备 B）之间建立 GRE 隧道，防护设备在回注流量时将流量封装成 GRE 报文后送往设备 A，而这些 GRE 报文的目的地址是设备 B，因此设备 A 收到这些 GRE 报文后不会命中之前用于牵引流量的普通路由，而是会直接转发给设备 B，在设备 B 上进行 GRE 解封装然后发送给真实客户网络，从而避免环路。

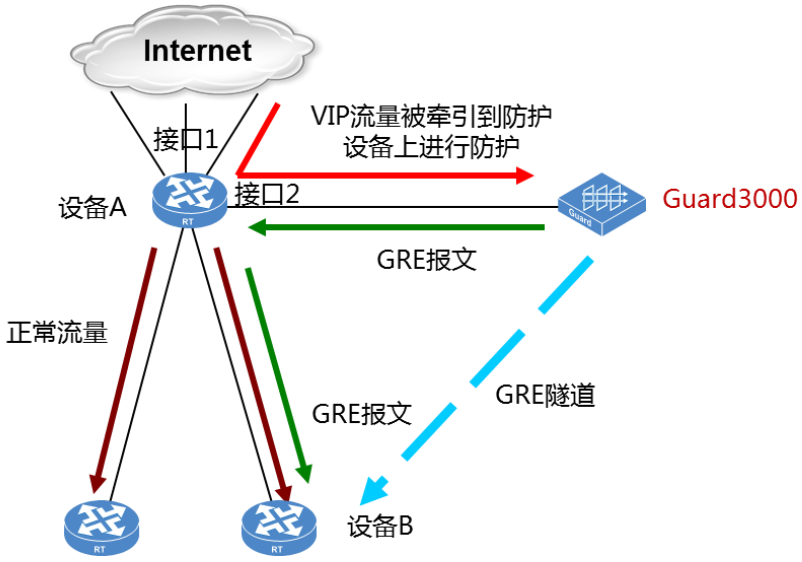

图 8 GRE 回注

3.4.3VLAN 二层回注方式

将防护设备与受保护设备相对应的下一跳（设备 B）部署在同一个 VLAN 中，即在核心交换机设备 A 上将接口 2 和接口 3 配置到同一个 VLAN 中，这样防护设备在回注流量时可以直接通过 VLAN 内的二层转发送往设备 B，即回注流量到达设备 A 时不用进行三层转发，而是通过二层转发送往设备 B 并最终到达真实客户网络，因此不会命中之前用于牵引流量的普通路由，从而避免环路。

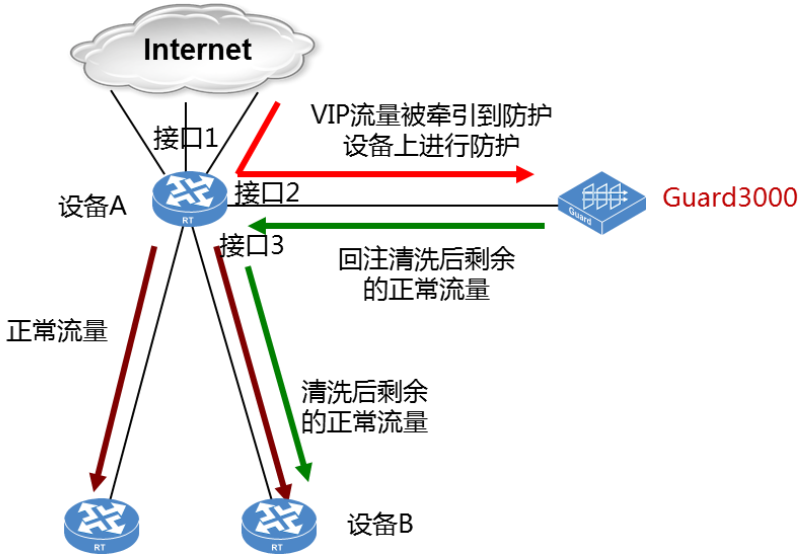

图 9 VLAN 二层回注

3.4.4MPLS 回注方式

与 GRE 方式类似，在防护设备与受保护设备相对应的下一跳（设备 B）之间建立 MPLS 隧道，防护设备在回注流量时进行 MPLS 封装，封装后的报文到达设备 A 之后会直接转发给设备 B，在设备 B 上进行 MPLS 解封装然后发送给真实客户网络，此时经过设备 A 的回注流量是 MPLS 报文因此不会命中之前用于牵引流量的普通路由，从而避免环路。

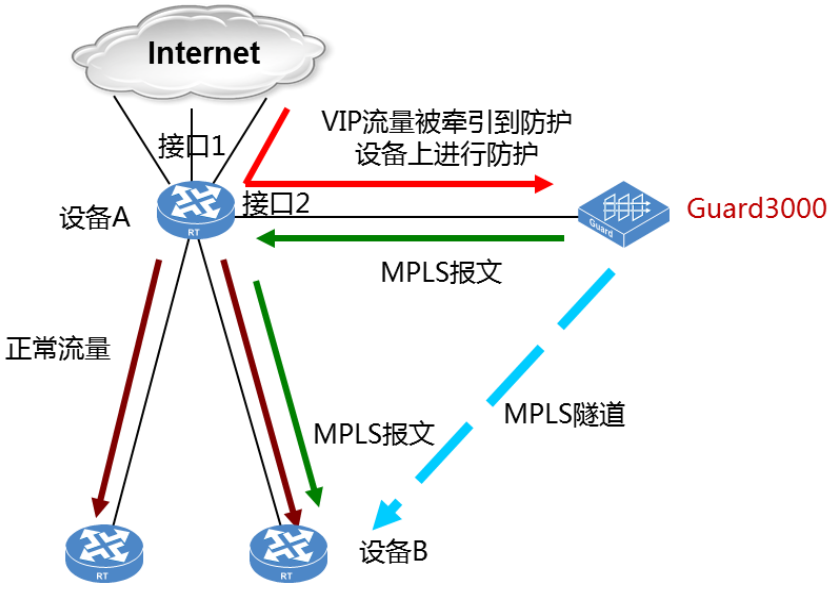

图 10 MPLS 回注

3.5 统计信息和日志

异常流量清洗解决方案作为一种安全服务，不仅要提供异常流量清洗的功能，同时也要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。通过 UMC 统一管理平台可实现对异常流量检测 Probe3000 以及异常流量清洗 Guard3000 的管理，并可为用户提供专业的流量状况，清洗效果，历史日志等报表输出。通过这些丰富的报表，可以让最终用户实时直观的了解当前的业务状况和历史状况回溯。

UMC支持详细报表功能，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：

- 基于清洗业务分析，攻击流量类型分析做出统计分析报表，例如 SYN Flood、UDP Flood 等。
- 根据被保护对象实时流量，提供精确的流量趋势图。
- 统计数据可根据服务器存储容量保持清洗记录，并能提供保持数据时间内任意时差的统计报表。
- 报表支持自动导出功能。当设置自动导出周期后，系统将按照报表任务指定的周期和报表格式自动导出报表，并将报表发送至指定的收件人。

图 11 异常流量清洗效果图

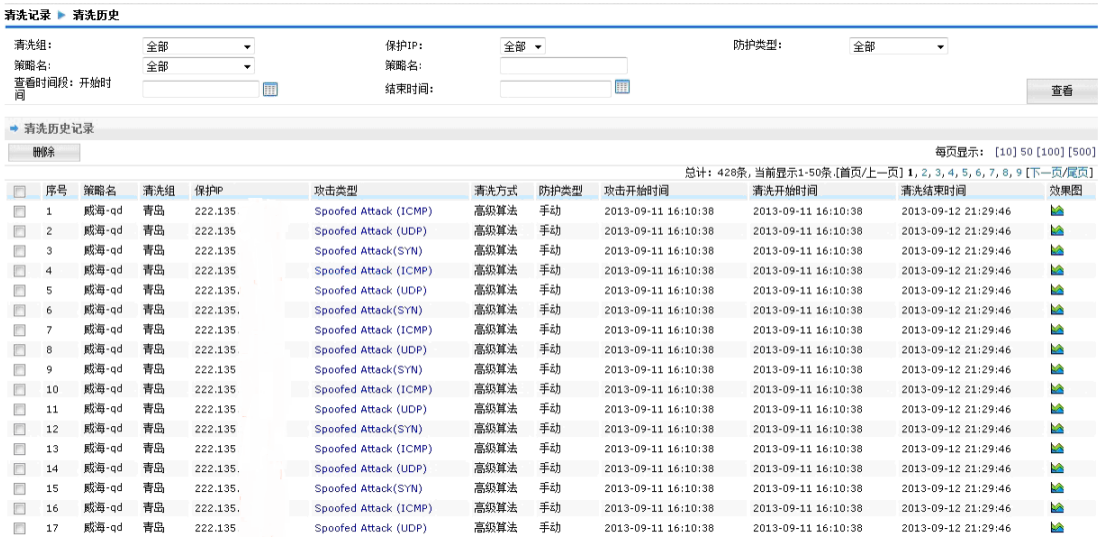

图 12 异常流量清洗报表