

# 1. DDoS 攻击及防护技术

## 1.1 DDoS 攻击的起源

1988年11月2日，一个叫 Robert Morris Jr. 的大学生写了一个逻辑炸弹——蠕虫程序入侵 internet。这个蠕虫程序在 Internet 上快速传播，当时造成全网络中有 15%（大约 6000 个系统）都受到感染并停止运行。这就是第一次的 DoS 攻击，这次事件很有名的另外一个原因是此人的父亲——老 Morris 是个电脑专家，unix 系统的创始人之一，在政府专门负责对抗电脑犯罪的，所以后来很多分析文章认为此程序是老 Morris 写的。

从上世纪 90 年代到现在，DoS 技术主要经历大约阶段：

- 1) 技术发展时期。90 年代，Internet 开始普及，很多新的 DoS 技术涌现。90 年代末发明和研究过许多新的技术，其中大多数技术至今仍然有效，且应用频度相当高。绝大部分著名的 DoS 攻击方式，如 Ping of death, smurf, SYN flooding, 等等。
- 2) 从实验室向“产业化”转换。2000 年前后，DDoS 出现，Yahoo, Amazon 等多个著名网站受到攻击并瘫痪，还有 Codered, SQL slammer 等蠕虫造成的事件。
- 3) “商业时代”。最近一两年，宽带的发展使得接入带宽增加，个人电脑性能大幅提高，使 DDoS 攻击越来越频繁，可以说随处可见，而且也出现了出现了更专业的出租‘botnet’网络的‘DDoS 攻击经济’。可以说 DDoS 攻击的威胁已经无处不在。

## 1.2 DDoS 攻击的危害

DDoS（分布式拒绝服务攻击）是产生大规模破坏的武器。不象访问攻击穿透安全周边来窃取信息，DDoS 攻击通过伪造的流量淹没服务器、网络链路和网络设备（路由器，防火墙等）瘫痪来使得网络系统瘫痪。

DDoS 是作为黑客、政治黑客行为和国际计算机恐怖分子可选择的一种武器而出现。由于很容易对有限的防御发起进攻，DDoS 攻击目标并不仅仅是个人网站或其他网络边缘的服务器，他们征服的是网络本身。攻击明确地指向网络的基础设施，例如提供商网络中的集中或核心路由器、DNS 服务器。2002 年 10 月，一次拙劣的 DDoS 攻击影响了 13 个根 DNS (Domain Name Service) 服务器中的 8 个以及作为整个 Internet 通信路标的关键系统，这一事件预示了大规模攻击的到来。

服务提供商、企业和政府机关对因特网依赖的加剧，使得成功的DDoS攻击（经济和其它方面）能造成更加严重的破坏。新近以来，出现了更多功能更为强大的DDoS工具，使得将来的攻击破坏性更大。

因为DDoS攻击是最难防御的攻击之一，用合适的、有效的方法来响应它们，给依靠因特网的组织提出了一个巨大的挑战。网络设备和传统周边安全技术，例如防火墙和IDSs(Intrusion Detection Systems)无法提供足够的针对DDoS保护。面对当前DDoS的冲击，要保护因特网有效性，需要一个能检测和阻止日益狡猾、复杂、欺骗性攻击的下一代体系结构。

成功的DDoS攻击影响是很广泛的。网络站点的表现尤其受影响，可以造成客户和其它使用者访问失败。SLAs（服务水平承诺）被违反，促使服务信用损失惨重。公司名誉受损，有时甚至是永久的。收益下滑、生产率降低、IT开销增加、诉讼花销——这些损失在不断的增加。

损失的数目令人难以置信。来自Forrester、IDC和Yankee Group的评测估计一个象Cisco这样的公司网络中断24小时的代价大约是三千万美元。据Yankee Group估计，2000年2月，DDoS洪流攻击了Amazon、Yahoo、eBay和其它门户网站，造成的损失累计达到12亿美元。2001年1月，对Microsoft网站几天的DDoS攻击，损失大约为五千万。显然，商业公司必须采取措施来保护自己免遭恶意攻击。

由于DDoS攻击往往采取合法的数据请求技术，再加上傀儡机器，造成DDoS攻击成为目前最难防御的网络攻击之一。据美国最新的安全损失调查报告，DDoS攻击所造成的经济损失已经跃居第一。

DDoS攻击的一个致命趋势是使用复杂的欺骗技术和基本协议，如HTTP，Email等协议，而不是采用可被阻断的非基本协议或高端口协议，非常难识别和防御，通常采用的包过滤或限制速率的措施只是通过停止服务来简单停止攻击任务，但同时合法用户的请求也被拒绝，造成业务的中断或服务质量的下降；DDoS事件的突发性，往往在很短的时间内，大量的DDoS攻击数据就可是网络资源和服务资源消耗殆尽。

DDoS攻击主要是利用了internet协议和internet基本优点——无偏差地从任何的源头传送数据包到任意目的地。DDoS攻击分为两种：要么大数据，大流量来压垮网络设备和服务器，要么有意制造大量无法完成的不完全请求来快速耗尽服务器资源。有效防止DDoS攻击的关键困难是无法将攻击包从合法包中区分出来：IDS进行的典型“签名”模式匹配起不到有效的作用；许多攻击使用源IP地址欺骗来逃脱源识别，很难搜寻特定的攻击源头。

## 1.3 DoS 和 DDoS 攻击概述

DoS的攻击方式有很多种，最基本的DoS攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。单一的DoS攻击一般是采用一对一方式的，当攻击目标CPU速度低、内存小或者网络带宽小等等各项性能指标不高它的效果是明显的。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，内存大大增加，同时也出现了千兆级别的网络，这使得DoS攻击的困难程度加大了 - 目标对恶意攻击包的“消化能力”加强了不少，例如你的攻击软件每秒钟可以发送2,500个攻击包，但我的主机与网络带宽每秒钟可以处理10,000个攻击包，这样一来攻击就不会产生什么效果。

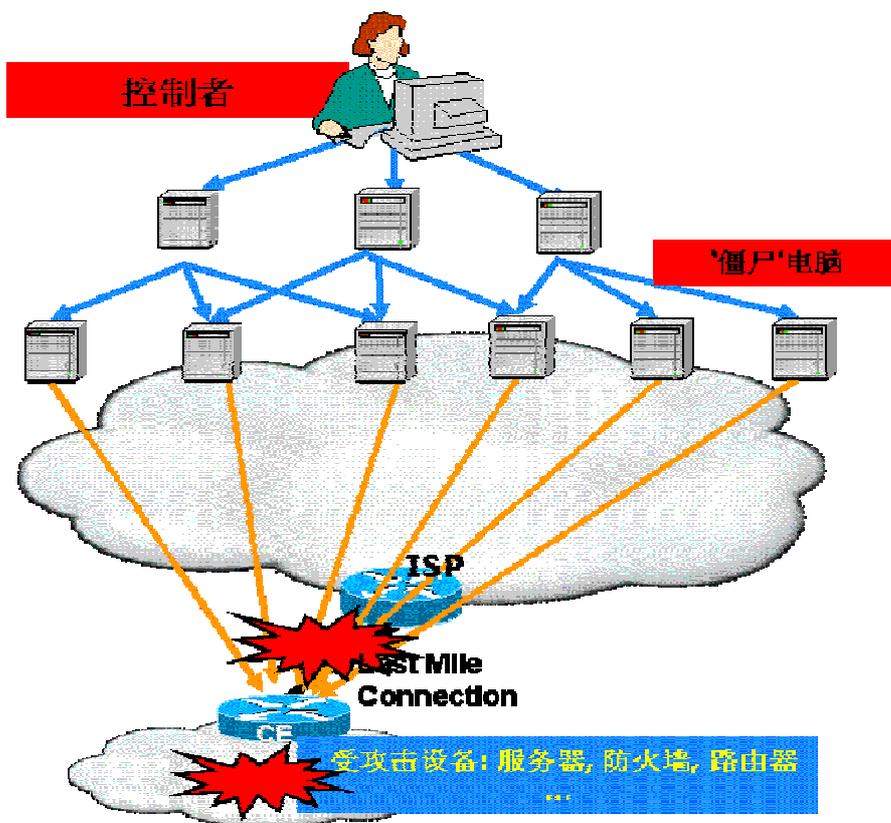
这样分布式的拒绝服务攻击手段（DDoS）就应运而生了，DDoS攻击手段是在传统的DoS攻击基础之上产生的一类攻击方式。如果说计算机与网络的处理能力增加了10倍，用一台攻击机来攻击不再能产生影响的话，攻击者使用10台或100台甚至上千上万台同时攻击的话，其效果自然大步一样了。DDoS攻击就是利用更多的傀儡机来发起进攻，以比从前更很多的规模来进攻受害者。高速广泛连接的网络给大家带来方便的同时，也为DDoS攻击创造了极为有利的条件。在低速网络时代时，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干节点之间的连接都是以千兆为级别的，这使得攻击可以从更远的地方或者不同的自治域发起，攻击者的傀儡机位置可以在分布在更大的范围或全球，选择起来更灵活了。

从技术角度讲，DDoS攻击包括威胁互联网计算机的安全和放置特洛伊木马程序。这是一种恶意的、不会自动复制的程序，它会伪装成良性程序，有意地执行一些用户并不希望的操作。众多的特洛伊木马程序会遵照一台由攻击者控制的主服务器的指示，在指定的时间以特定的方式共同发动攻击。DDoS攻击的一个致命趋势是使用复杂的欺骗技术和基本协议，如HTTP, Email等协议，而不是采用可被阻断的非基本协议或高端口协议，非常难识别和防御，通常采用的包过滤或限制速率的措施只是通过停止服务来简单停止攻击任务，但同时合法用户的请求也被拒绝，造成业务的中断或服务质量的下降；DDoS事件的突发性，往往在很短的时间内，大量的DDoS攻击数据就可网络资源和服务资源消耗殆尽，使服务停止。

被 DDoS 攻击时的现象

- 被攻击主机上有大量等待的 TCP 连接
- 网络中充斥着大量的无用的数据包，源地址为假
- 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯
- 利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求
- 严重时会造成系统死机

### 1.3.1 DDoS 攻击基本原理



如上图所示，一个完善的 DDoS 攻击体系分成几大部分，控制和实际发起攻击者，对被攻击者（服务器，路由器，防火墙）来说，DDoS 的攻击包是从攻击傀儡机（僵尸电脑）上发出的，控制者只发布命令而不参与实际的攻击。有控制权或者是部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自控制者的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些傀儡机器并没有什么异常，只是一旦黑客连接到它们进行控制，并发出指令的时候，攻击傀儡机就成为害人者去发起攻击了。

DDoS 发生的过程可以描述如下：

#### 1. 搜集了解目标的情况

- 被攻击目标主机数目、地址情况
- 目标主机的配置、性能
- 目标的带宽

从目标情况中找到可能成为傀儡机的机器

#### 2. 占领傀儡机

- 链路状态好的主机

- 性能好的主机
- 安全管理水平差的主机

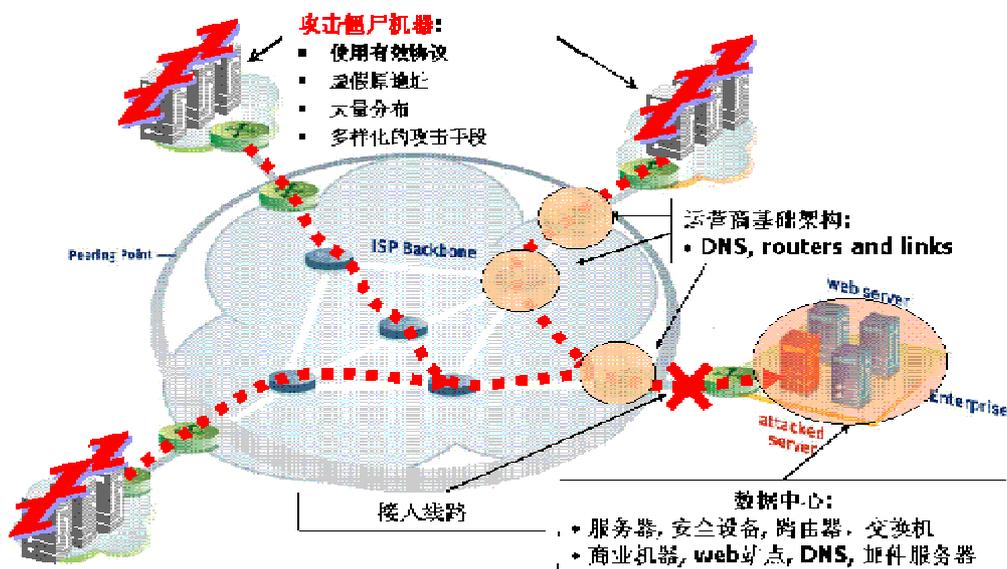
首先，一般采用扫描手段，随机地或者是有针对性地利用扫描器去发现互联网上那些有漏洞的机器，象程序的溢出漏洞、cgi、Unicode、ftp、数据库漏洞...等等，随后就是尝试入侵了，一旦入侵后，把 DDoS 攻击用的程序上载过去，一般是利用 ftp。在攻击机上，会有一个 DDoS 的发包程序，攻击者就是利用它来向受害目标发送恶意攻击包。

### 3. 实际攻击

经过前 2 个阶段的精心准备之后，就开始瞄准目标准备发射了。就象图示里的那样，攻击者登录到做为控制台的傀儡机，向所有的攻击机发出 DDoS 攻击命令，这时候埋伏在攻击机中的 DDoS 攻击程序就会响应控制台的命令，一起向受害主机或设备以高速度发送大量的数据包，导致服务停止，死机或连接线路拥塞中断。

## 1.3.2 DDoS 主要攻击类型

DDoS 攻击分为两种：要么大数据，大流量来压垮网络设备和服务器，要么有意制造大量无法完成的不完全请求来快速耗尽服务器资源。有效防止 DDoS 攻击的关键困难是无法将攻击包从合法包中区分出来：IDS 进行的典型“签名”模式匹配起不到有效的作用；许多攻击使用源 IP 地址欺骗来逃脱源识别，很难搜寻特定的攻击源头。



有两类最常见的 DDoS 攻击:

- **带宽攻击:** 这种攻击消耗网络带宽或使用大量数据包淹没一个或多个路由器、服务器和防火墙；带宽攻击的普遍形式是大量表面看合法的 TCP、UDP 或 ICMP 数据包被传

送到特定目的地；为了使检测更加困难，这种攻击也常常使用源地址欺骗，并不停地变化。这种攻击相对而言更加难以防御，因为合法数据包和无效数据包看起来非常类似

- **应用攻击：**利用 TCP 和 HTTP 等协议定义的行为来不断占用计算资源以阻止它们处理正常事务和请求。HTTP 半开和 HTTP 错误就是应用攻击的两个典型例子。

### 1.3.3 DDoS 攻击的常用技术和分类

#### ○ TCP/IP 协议层攻击

- **缓存溢出攻击**—试图在一个缓存中存储超出其设计容量的数据。这种多出的数据可能会溢出到其他的缓存之中，破坏或者覆盖其中的有效数据。
- **TCP SYN 泛洪攻击**—一个正常的 TCP 连接需要进行三方握手操作。首先，客户端向服务器发送一个 TCP SYN 数据包。而后，服务器分配一个控制块，并响应一个 SYN ACK 数据包。服务器随后将等待从客户端收到一个 ACK 数据包。如果服务器没有收到 ACK 数据包，TCP 连接将处于半开状态，直到服务器从客户端收到 ACK 数据包或者连接因为 time-to-live (TTL) 计时器设置而超时为止。在连接超时的情况下，事先分配的控制块将被释放。当一个攻击者有意地、重复地向服务器发送 SYN 数据包，但不对服务器发回的 SYN ACK 数据包答复 ACK 数据包时，就会发生 TCP SYN 泛洪攻击。这时，服务器将会失去对资源的控制，无法建立任何新的合法 TCP 连接。
- **UDP flooding** UDP 是没有连接状态的协议，因此可以发送大量的 UDP 包到某个端口，如果是个正常的 UDP 应用端口，则可能干扰正常应用，如果是没有正常应用，服务器要回送 ICMP，这样则消耗了服务器的处理资源，而且很容易阻塞上行链路的带宽。
- **ICMP 泛洪攻击**—当 ICMP ping 通过多个响应请求而造成系统过载时，就会发生 ICMP 泛洪攻击。这将导致系统不断地保留它的资源，直到无法再处理有效的网络流量。
- **Smurf 攻击**—在进行这种攻击时，攻击者会向接收站点中的一个广播地址发送一个 IP ICMP ping（即“请回复我的消息”）。Ping 数据包随后将被广播到接收站点的本地网络中的所有主机。该数据包包含一个“伪装的”源地址，即该 DoS 攻击的对象的地址。每个收到此 ping 数据包的主机都会向伪装的源地址发送响应，从而导致这个无辜的、被伪装的主机收到大量的 ping 回复。如果收到的数据量过大，这个被伪装的主机就将无法接收或者区分真实流量。
- **蠕虫**—蠕虫是一些独立的程序，可以自行攻击系统和试图利用目标的漏洞。在成功地利用漏洞之后，蠕虫会自动地将其程序从攻击主机复制到新发现的系统，从而再次启动循环。蠕虫会将自身的多个副本发送到其他的计算机，例如通过电子邮件或者互联网多线交谈（IRC）。有些蠕虫（例如众所周知的红色代码和 NIMDA 蠕虫）具有 DDoS 攻击的特征，可能导致终端和网络基础设施的中断。
- **Land:** 采用目标和源地址相同的 UDP 包攻击目标。这种攻击到现在还是有效的。

- **Tear drop**: 也叫碎片攻击, 发出的包是经过 **fragement** 的, 而这些碎片的位移是相互重叠的, 这种畸形数据包会造成目标主机不知道如何处理。
- **应用程序级攻击**
  - 基于会话的攻击。例如简单的 HTTP 等 TCP 服务, 服务器会话的数量是影响给定应用程序性能的重要因素, 会话的数量是有限制的, 这个限制就是一个 DDoS 的攻击点。一次简单的攻击便可打开 TCP 会话并让这些会话保持打开状态, 从而可以迅速填满所有可用的会话槽, 阻止建立任何新的会话。
  - DNS 攻击。DNS 请求大多是基于 UDP 协议的, 而且不需要由客户机进行认证, 因此很轻易就可以将数千个请求从伪造的来源发送到服务器。另外对请求解析的地址做改动也能加大 DNS 服务器的负担。
  - 应用程序或数据库。SQL 也是易受攻击的目标, 在大型而复杂的表格上, SQL 查询可能在应用程序级生成不同的错误行为。例如如果没有正确的索引, 涉及对同一个表的多个列进行筛选和排序操作的 SQL 请求便会产生指数级数量的操作, 这会消耗大量 CPU 资源并显著增加应用程序响应时间。

当然 DDoS 攻击的手段不止这些。但 DDoS 攻击和病毒攻击的方式完全不同: 病毒是要求用最新的代码, 以绕过防病毒软件, 一旦被反病毒软件识破, 病毒就失去了生命力, 而 DDoS 可以说不需要‘新’技术, 一个 10 年前发明的 TCP SYN 照样造成今天的网站瘫痪。这也是 DDoS 非常难于防范的原因: DDoS 的请求表面上和正常的请求没有什么不同, 大量的请求因为无法区分而无法拒绝。

### 1.3.4 新型 DDoS 攻击目标-基础网络

并不是所有的 DDoS 攻击的目的都是导致特定终端 (例如 Web 服务器) 停止运行, 最新的攻击者可能会将网络基础设施本身作为攻击目标, 会造成更大的威胁, 网络大面积瘫痪。这种攻击包括导致连接带宽达到饱和, 耗尽路由器和交换机的资源, 中断路由器上的某项服务等。连接饱和与 CPU 耗尽型 DDoS 攻击可能会拒绝为动态路由协议提供保持相邻关系所必需的带宽。当路由器失去与相邻设备的连接时, 它会清空从这个中断的相邻设备获得的所有路由。随后它必须将所有发往这些被清空的路由的流量转向一个替代路由, 或者丢弃所有这些流量。因为它必须连续地重新计算新的路由 (清除中断的路由和更新路由), CPU 资源最终将被大量占用。无论如何, 结果都是会发生 DoS。伪装控制流量的 DDoS 攻击会劫持动态路由协议流量, 恶意地重置所有相邻关系, 或者用错误的信息更新相邻关系, 从而导致 DoS。

用 DoS (拒绝服务) 来攻击路由器将对整个因特网造成严重影响。因为路由协议遭到直接攻击, 从而在大范围内带来严重的服务器的可用性问题。路由器攻击会对网络造成毁灭性的后果。因为路由器常常集成了 VPN 服务或者防火墙, 因而使其成为更吸引黑客的目标。一旦路由器岌岌可危, 整个网络便立刻变得十分危险了。防火墙和入侵检测系统 (IDS) 的目的在于检测针对个别网络服务器或主机的攻击, 而不是对网络基础设施进行保护的。

## 1.3.5 DDoS 常见攻击工具

DDoS 攻击实施起来有一定的难度，要求攻击者必须具备入侵他人计算机的能力。但是一些傻瓜式的黑客程序的出现，这些程序可以在几秒钟内完成入侵和攻击程序的安装，使发动 DDoS 攻击变成一件轻而易举的事情。主要的攻击工具有 JOLT, WINNUKE, TRINOO, TFN, Targa3, Naphta, Trash, fawx,...

下面我们介绍一下这些常用的黑客程序和工具，其中重点介绍 TFN2K。

### ○ Trinoo

Trinoo 的攻击方法是向被攻击目标主机的随机端口发出全零的 4 字节 UDP 包，在处理这些超出其处理能力的垃圾数据包的过程中，被攻击主机的网络性能不断下降，直到不能提供正常服务，乃至崩溃。它对 IP 地址不做假，采用的通讯端口是：

攻击者主机到主控端主机：27665/TCP

主控端主机到代理端主机：27444/UDP

代理端主机到主服务器主机：31335/UDP

### ○ TFN

TFN 由主控端程序和代理端程序两部分组成，它主要采取的攻击方法为：SYN 风暴、Ping 风暴、UDP 炸弹和 SMURF，具有伪造数据包的能力。

### ○ Stacheldraht

Stacheldraht 是从 TFN 派生出来的，因此它具有 TFN 的特性。此外它增加了主控端与代理端的加密通讯能力，它对命令源作假，可以防范一些路由器的 RFC2267 过滤。Stacheldraht 中有一个内嵌的代理升级模块，可以自动下载并安装最新的代理程序。

### ○ TFN2K

TFN2K 是由德国著名黑客 Mixer 编写的同类攻击工具 TFN 的后续版本，在 TFN 所具有的特性上，TFN2K 又新增一些特性，TFN2K 通过主控端利用大量代理端主机的资源进行对一个或多个目标进行协同攻击。当前互联网中的 UNIX、Solaris 和 Windows NT 等平台的主机能被用于此类攻击，而且这个工具非常容易被移植到其它系统平台上。

TFN2K 由两部分组成：在主控端主机上的客户端和在代理端主机上的守护进程。主控端向其代理端发送攻击指定的目标主机列表。代理端据此对目标进行拒绝服务攻击。由一个主控端

控制的多个代理端主机，能够在攻击过程中相互协同，保证攻击的连续性。主控端和代理端的网络通讯是经过加密的，还可能混杂了许多虚假数据包。整个 TFN2K 网络可能使用不同的 TCP、UDP 或 ICMP 包进行通讯。而且主控端还能伪造其 IP 地址。所有这些特性都使发展防御 TFN2K 攻击的策略和技术都非常困难或效率低下。

- ◆ 主控端通过 TCP、UDP、ICMP 或随机性使用其中之一的数据包向代理端主机发送命令。对目标的攻击方法包括 TCP/SYN、UDP、ICMP/PING 或 BROADCAST PING (SMURF) 数据包 flood 等。

- ◆ 主控端与代理端之间数据包的头信息也是随机的，除了 ICMP 总是使用 ICMP\_ECHOREPLY 类型数据包。

- ◆ 与其上一代版本 TFN 不同，TFN2K 的守护程序是完全沉默的，它不会对接收到的命令有任何回应。客户端重复发送每一个命令 20 次，并且认为守护程序应该至少能接收到其中一个。

- ◆ 这些命令数据包可能混杂了许多发送到随机 IP 地址的伪造数据包。

- ◆ TFN2K 命令不是基于字符串的，而采用了"++"格式，其中是代表某个特定命令的数值，则是该命令的参数。

- ◆ 所有命令都经过了 CAST-256 算法 (RFC 2612) 加密。加密关键字在程序编译时定义，并作为 TFN2K 客户端程序的口令。

- ◆ 所有加密数据在发送前都被编码 (Base 64) 成可打印的 ASCII 字符。TFN2K 守护程序接收数据包并解密数据。

- ◆ 守护进程为每一个攻击产生子进程。

- ◆ TFN2K 守护进程试图通过修改 argv[0] 内容 (或在某些平台中修改进程名) 以掩饰自己。伪造的进程名在编译时指定，因此每次安装时都有可能不同。这个功能使 TFN2K 伪装成代理端主机的普通正常进程。因此，只是简单地检查进程列表未必能找到 TFN2K 守护进程 (及其子进程)。

- ◆ 来自每一个客户端或守护进程的所有数据包都可能被伪造。

由于所有的控制通讯都是单向的，这使得实时监测 TFN2K 额外困难。因为其随机性地使用 TCP、UDP 和 ICMP 数据包，同时进行了加密，数据包过滤和其它被动式防御策略都显得不切实际和效率低下的。伪造的数据包更会增加追踪参与拒绝服务攻击的代理端主机的难度。

幸运的是，TFN2K 仍然有弱点。可能是疏忽的原因，加密后的 Base 64 编码在每一个 TFN2K 数据包的尾部留下了痕迹 (与协议和加密算法无关)。可能是程序作者为了使每一个数据包的长度变化而填充了 1 到 16 个零 (0x00)，经过 Base 64 编码后就成为多个连续的 0x41 ('A')。添加到数据包尾部的 0x41 的数量是可变的，但至少会有一个。这些位于数据包尾部的 0x41 ('A') 就成了捕获 TFN2K 命令数据包的特征了。对 TFN2K 客户端程序 (tfn) 和守护程序文件 (td) 的简单搜索也可能会找到 TFN2K。

目前仍没有能有效防御 TFN2K 拒绝服务攻击的方法。最有效的策略是防止网络资源被用作客户端或代理端。

## TFN2K 预防

- ◆ 只使用应用代理型防火墙。这能够有效地阻止所有的 TFN2K 通讯。但只使用应用代理服务器通常是不切合实际的，因此只能尽可能使用最少的非代理服务。

- ◆ 禁止不必要的 ICMP、TCP 和 UDP 通讯。特别是对于 ICMP 数据，可只允许 ICMP 类型 3（destination unreachable 目标不可到达）数据包通过。

- ◆ 如果不能禁止 ICMP 协议，那就禁止主动提供或所有的 ICMP\_ECHOREPLY 包。

- ◆ 禁止不在允许端口列表中的所有 UDP 和 TCP 包。

- ◆ 配置防火墙过滤所有可能的伪造数据包。

- ◆ 对系统进行补丁和安全配置，以防止攻击者入侵并安装 TFN2K。

#### TFN2K 监测

- ◆ 扫描客户端/守护程序的名字。

- ◆ 根据前面列出的特征字符串扫描所有可执行文件。

- ◆ 扫描系统内存中的进程列表。

- ◆ 检查 ICMP\_ECHOREPLY 数据包的尾部是否含有连续的 0x41。另外，检查数据侧面内容是否都是 ASCII 可打印字符（2B，2F-39，0x41-0x5A，0x61-0x7A）。

- ◆ 监视含有相同数据内容的连续数据包（有可能混合了 TCP、UDP 和 ICMP 包）。

#### TFN2K 响应

一旦在系统中发现了 TFN2K，最好立即通知安全公司或专家以追踪入侵进行。因为 TFN2K 的守护进程不会对接收到的命令作任何回复，TFN2K 客户端一般会继续向代理端主机发送命令数据包。另外，入侵者发现攻击失效时往往会试图连接到代理端主机上以进行检查。这些网络通讯都可被追踪。

## 1.4 传统 DDoS 攻击防护技术

### 1.4.1 基于主机的防护

采用主机配置，软件补丁和应用程序优化的手段，DDoS 的目标通常是主机，因此防范也并非单单是网络的事。很多 DDoS 攻击能成功主要是利用了主机操作系统或应用系统的漏洞，特别是应用层面的攻击，因此，选用健壮的操作系统，和良好设计的应用都是非常重要的，特别是软件补丁和应用程序的优化。但由于诸多原因，就像防护病毒一样，此方法并不容易实施，同时对针对网络的 DDoS 攻击也无法提供有效保护

升级操作系统以及各种网络应用程序，及时安装各种补丁，对 WEB 等应用采用 DNS 轮询或者负载均衡方式增加抗拒绝服务能力；在条件不许可的情况下，可以使用多 IP 主机的方式。优化服务器或者应用程序本身，比如 Windows 2000 和 Windows server 2003 操作系统，就具备一定的抵抗拒绝服务攻击的能力，只是默认状态下没有开启，开启的话自身就可以抵御 10000 个 SYN 攻击包，若没有开启仅能抵御数百个攻击包。

对于 WEB 服务，应尽量避免使用数据库连接，必须使用数据库时，应在调用数据库的脚本中拒绝使用代理的访问，防止针对数据的连接耗尽型攻击。把网站做成静态页面，不仅能大大提高抗攻击能力，同时也大大减少了服务器的负荷开销。

## 1.4.2 基于网络的防护

传统流行的 DDoS 防护技术主要有以下几种，

- 1) IPS 提供一些检测功能，可以有限防御 DoS 攻击，但难于真正缓解 DDoS 攻击。
- 2) 防火墙提供的保护：一般防火墙是要保持连接状态的，因此性能会受到限制，防火墙也成为 DoS 攻击的目标。
- 3) 路由设备也能提供一些的包过滤或限制速率的措施，或者用黑洞路由的方式，但这些做法使但合法用户也被拒绝了，结果是服务中断，攻击者（黑客）取得了胜利。
- 4) 还有一种办法是大量供应，提供足够的带宽或处理能力，这种方式并未提供足够保护来防止更大攻击，而且作为阻止 DDoS 攻击的策略代价太高。

不管哪种 DDoS 攻击，，当前的防护技术都不足以提供完善的抵御。

### ○ 黑洞技术

黑洞技术描述了一个服务提供商将指向某一目标企业的包尽量阻截在上游的过程，将改向的包引进“黑洞”并丢弃，以保全运营商的基础网络和其它的客户业务。但是合法数据包和恶意攻击业务一起被丢弃，所以黑洞技术不能算是一种好的解决方案。被攻击者失去了所有的业务服务，攻击者因而获得胜利。

### ○ 路由器

许多人运用路由器的过滤功能提供对 DDoS 攻击的防御，但对于现在复杂的 DDoS 攻击不能提供完善的防御。

路由器只能通过过滤非基本的不需要的协议来停止一些简单的 DDoS 攻击，例如 ping 攻击。这需要一个手动的反应措施，并且往往是在攻击致使服务失败之后。另外，现在的 DDoS 攻击使用互联网必要的有效协议，很难有效的滤除。路由器也能防止无效的或私有的 IP 地址空间，但 DDoS 攻击可以很容易的伪造成有效 IP 地址。

基于路由器的 DDoS 预防策略——在出口侧使用 uRPF 来停止 IP 地址欺骗攻击——这同样不能有效防御现在的 DDoS 攻击，因为 uRPF 的基本原理是如果 IP 地址不属于应该来自的子网网络阻断出口业务。然而，DDoS 攻击能很容易伪造来自同一子网的 IP 地址，致使这种解决方案无效。

本质上，对于种类繁多的使用有效协议的欺骗攻击，路由器 ACLs 是无效的。包括：

- SYN、SYN-ACK、FIN 等洪流。
- 服务代理。因为一个 ACL 不能辨别来自于同一源 IP 或代理的正当 SYN 和恶意 SYN，所以会通过阻断受害者所有来自于某一源 IP 或代理的用户来尝试停止这一集中欺骗攻击。
- DNS 或 BGP。当发起这类随机欺骗 DNS 服务器或 BGP 路由器攻击时，ACLs——类似于 SYN 洪流——无法验证哪些地址是合法的，哪些是欺骗的。

ACLs 在防御应用层（客户端）攻击时也是无效的，无论欺骗与否，ACLs 理论上能阻断客

户端攻击——例如 HTTP 错误和 HTTP 半开连接攻击，假如攻击和单独的非欺骗源能被精确的监测——将要求用户对每一受害者配置数百甚至数千 ACLs，这其实是无法实际实施的。

### ○ 防火墙

首先防火墙的位置处于数据路径下游远端，不能为从提供商到企业边缘路由器的访问链路提供足够的保护，从而将那些易受攻击的组件留给了 DDoS 攻击。此外，因为防火墙总是串联的而成为潜在性能瓶颈，因为可以通过消耗它们的会话处理能力来对它们自身进行 DDoS 攻击。

其次是反常事件检测缺乏的限制，防火墙首要任务是要控制私有网络的访问。一种实现的方法是通过追踪从内侧向外侧服务发起的会话，然后只接收“不干净”一侧期望源头发来的特定响应。然而，这对于一些开放给公众来接收请求的服务是不起作用的，比如 Web、DNS 和其它服务，因为黑客可以使用“被认可的”协议（如 HTTP）。

第三种限制，虽然防火墙能检测反常行为，但几乎没有反欺骗能力——其结构仍然是攻击者达到其目的。当一个 DDoS 攻击被检测到，防火墙能停止与攻击相联系的某一特定数据流，但它们无法逐个包检测，将好的或合法业务从恶意业务中分出，使得它们在事实上对 IP 地址欺骗攻击无效。

### ○ IDS/IPS 入侵监测防御

IDS/IPS 解决方案将不得不提供领先的行为或基于反常事务的算法来检测现在的 DDoS 攻击。但是一些基于反常事务的性能要求有专家进行手动的调整，而且经常误报，并且不能识别特定的攻击流。同时 IDS 本身也很容易成为 DDoS 攻击的牺牲者。

作为 DDoS 防御平台的 IDS 最大的缺点是它只能检测到攻击，但对于缓和攻击的影响却毫无作为。IDS 解决方案也许能托付给路由器和防火墙的过滤器，但正如前面叙述的，这对于缓解 DDoS 攻击效率很低，即便是用类似于静态过滤串联部署的 IDS 也做不到。

### ○ DDoS 攻击的手动响应

作为 DDoS 防御一部份的手动处理太微小并且太缓慢。受害者对 DDoS 攻击的典型第一反应是询问最近的上游连接提供者——ISP、宿主提供商或骨干网承载商——尝试识别该消息来源。对于地址欺骗的情况，尝试识别消息来源是一个长期和冗长的过程，需要许多提供商合作和追踪的过程。即使来源可被识别，但阻断它也意味同时阻断所有业务——好的和坏的。

### ○ 其他策略

为了忍受 DDoS 攻击，可能考虑了这样的策略，例如过量供应，就是购买超量带宽或超量的网络设备来处理任何请求。这种方法成本效益比较低，尤其是因为它要求附加冗余接口和设备。不考虑最初的作用，攻击者仅仅通过增加攻击容量就可击败额外的硬件，互联网上上千万台的机器是他们取之不净的攻击容量资源。

## 1.4.3 Cisco 网络设备上防护 DDoS 攻击

在传统防护 DDoS 攻击技术和手段中，在基础网络层面进行一定的防护在某些时候还是比较高效的手段。思科网络设备上可以采取相应的手段，对大多数的 DDoS 攻击可以进行有效的

防护。

- 反向地址查询 uRPF

单播逆向路径转发，Unicast Reverse Path Forwarding（单播 RPF）主要应用在路由器和高端交换机中，目的是网络设备可以检查数据包的源地址，在 FIB 表中查找该源地址是否与数据包的来源接口相匹配，如果没有匹配表项将丢弃该数据包，其目的是预防 IP 欺诈，特别是对于伪造 IP 源地址的拒绝服务（DoS）攻击非常有效。

在 DDoS 攻击中，往往有很多攻击包是虚假地址，在网络中可以根据路由过滤这些虚假地址，在思科网络设备上使用 `ip verify unicast reverse-path` 网络接口命令，执行反向地址查询功能，这个功能检查每一个经过路由器的数据包。在路由器的 CEF（Cisco Express Forwarding）表该数据包所到达网络接口的所有路由项中，如果没有该数据包源 IP 地址的路由，路由器将丢弃该数据包。例如，路由器接收到一个源 IP 地址为 1.2.3.4 的数据包，如果 CEF 路由表中没有为 IP 地址 1.2.3.4 提供任何路由（即反向数据包传输时所需的路由），则路由器会丢弃它。

- 使用访问控制列表（ACL）过滤 RFC 1918 中列出的所有地址

参考以下配置：

```
interface xy
ip access-group 101 in
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 permit ip any any
```

- 参照 RFC 2267，使用访问控制列表（ACL）过滤进出流量

ISP 端边界路由器应该只接受源地址属于客户端网络的通信，而客户端网络则应该只接受源地址未被客户端网络过滤的通信。

如果使用单一地址反向路径转发（Unicast RPF），能够充分地缩短访问控制列表（ACL）的长度以提高路由器性能。

- 使用 CAR（Control Access Rate）限制 ICMP 数据包流量速率

参考以下配置：

```
interface xy
rate-limit output access-group 2020 3000000 512000 786000 conform-action
transmit exceed-action drop
```

```
access-list 200 permit icmp any any echo-reply
```

- 设置 SYN 数据包流量速率

参考以下配置:

```
interface {int}  
rate-limit output access-group 153 45000000 100000 100000 conform-action  
transmit exceed-action drop  
rate-limit output access-group 152 1000000 100000 100000 conform-action  
transmit exceed-action drop
```

```
access-list 152 permit tcp any host eq www  
access-list 153 permit tcp any host eq www established
```

- 搜集证据并联系网络安全部门或机构

如果可能, 捕获攻击数据包用于分析。常用的数据包捕获工具包括 TCPDump 和 snoop 等, 将这些捕获的数据包和日志作为证据提供给有关网络安全部门或机构。

## 1.5 新型 DDoS 攻击防护技术

随着 DDoS 攻击的危害性越来越大, 各行业对 DDoS 的有效防护也越来越重视。由于传统的防护方法其不可避免的局限性, 使得 DDoS 攻击防护技术的革新变得重要, 目前新型的 DDoS 攻击防护技术主要有两类:

- 基于传统识别的防护技术
- 基于 MVP 技术的数学模型技术

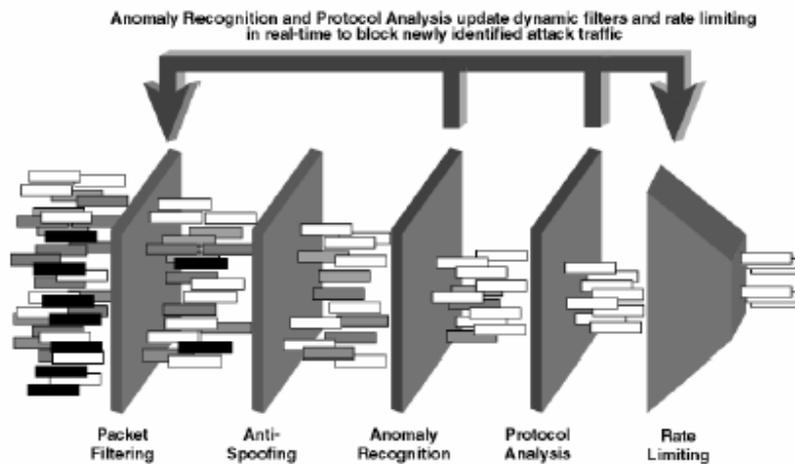
### 1.5.1 基于传统识别的防护技术

基于传统识别的防护技术, 主要是从防火墙技术和内容交换机技术演变而来, 主要采用串行模式, 所有流量通过该设备, 通过对通过流量的分析来判断攻击流量, 并将攻击流量直接丢弃。一般采用桥接技术, 不涉及路由的改变, 比较简单易用。此种技术由于是网关模式, 性能有限, 主要应用于企业网络中

### 1.5.2 基于 MVP 技术的数学模型技术

DDoS 攻击防御中, 最关键的技术是如何分辨合法业务流量和恶意业务流量, 业界领先的 Multi-Verification Process(MVP) architecture 技术是专门针对 DDoS 攻击的独特的、申请专

利的多验证过程技术，就是将各种验证、分析和实施技术结合在一起用来从合法业务中识别和分离恶意业务。这个净化的过程由五个模块（步骤）组成：



**Figure 2:** Riverhead Networks' Multi-Verification Process (MVP) architecture

图示说明：

- Multi-Verification Process(MVP) architecture: 多验证过程(MVP)体系结构
- Anomaly Recognition and Protocol Analysis update dynamic filters and rate limiting in real-time to block newly identified attack traffic: 反常事件识别和协议分析实时更新动态过滤器和速率限制，阻断最新被识别的攻击业务
- Packet Filtering: 数据包过滤
- Anti-spoofing: 反欺骗
- Anomaly Recognition: 异常识别
- Protocol Analysis: 协议分析
- Rate Liming: 速率限制

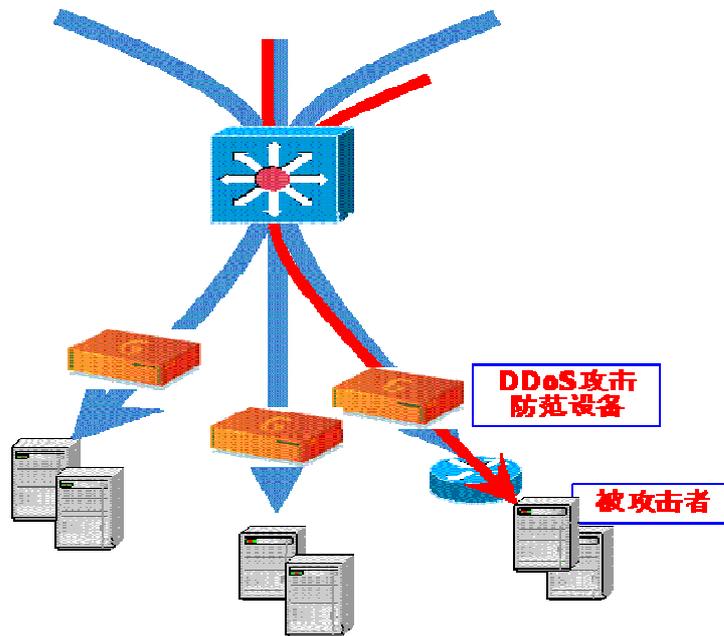
- 过滤：该模块包括静态和动态的 DDoS 过滤器。静态过滤器用来阻断非必要的业务到达受害目标，用户可对其进行配置的并且已预先设定缺省值。动态过滤器由其它模块根据观测到的行为和对业务流的详细分析动态嵌入，它能提供实时的升级来提高对可疑流的验证级别以及阻断被确定为恶意的源头和数据流。
- 反欺骗：该模块用以核实进入系统的数据包没有欺骗信息。攻击保护卫士使用许多独特的源鉴定机制来阻止欺骗的数据包到达受害者。反欺骗模块还提供一些机制用来确保合法业务的正确识别，在事实上消除了有效包被抛弃的危险。
- 异常识别：该模块监测所有通过了过滤器和反欺骗模块的业务，并将其与随时间纪录的基准行为相比，搜寻那些有偏差的业务，识别恶意包的来源。该模块工作的基本原理用来识别攻击源和类型，提供阻断业务的警戒线或对可疑数据实施更详细的分析。
- 协议分析：该模块处理反常事件识别模块发现的可疑数据流，目的是为了识别特定的应用攻击，例如 http-error 攻击。然后，协议分析模块检测任何不正确的协议处理，包括不完全处理或错误处理。
- 速率限制：该模块提供了另一个执行选项，并且通过更详细的监测来防止不正当数据流攻击目标。该模块实施每个数据流业务的修整，处罚长时间消耗大量资源的源头。

在攻击间隙，攻击防御处于“自学习”模式，被动监测不同来源的业务模型和数据流，了解正常行为，建立基准配置文件。该信息被用来调整策略，用以在实时网络活动中识别和过滤已知、未知和以前从未见过的攻击。

## 1.6 DDoS 攻击防御模式

### 1.6.1 串行部署防御 DDoS 攻击

串行部署防御模式主要应用在企业网络中，在网络的出口或要保护的目标地址前进行部署，提供串行的保护形势。如下图所示



此种部署模式不需要 DDoS 攻击检测器，直接将防护设备部署在需要保护的设备前面，利用设备的识别能力，直接过滤攻击流量。

此种部署模式实施比较简单，但也有以下几个较为明显的弱点

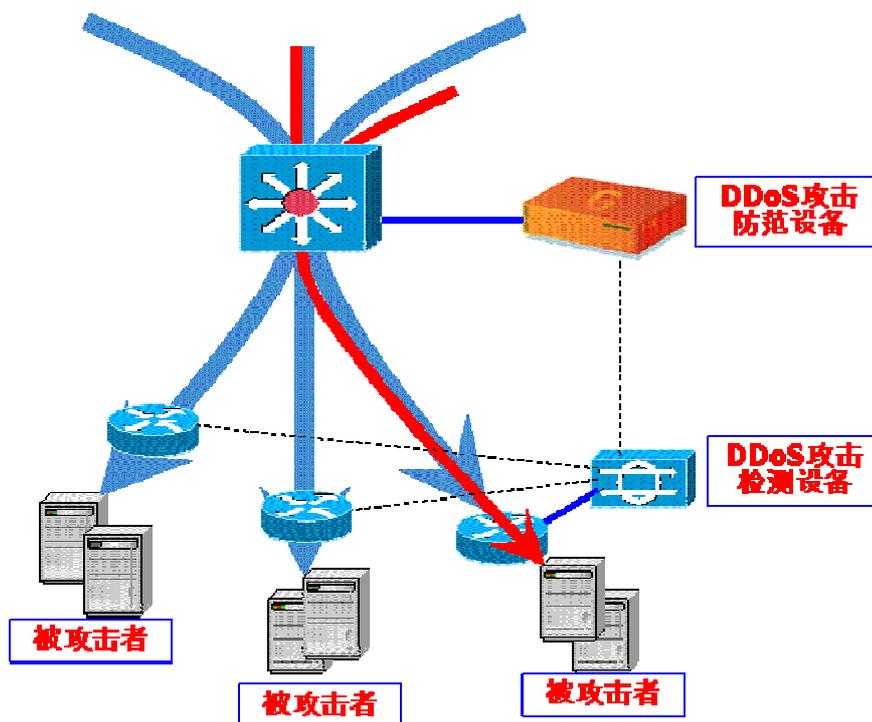
- 可能会成为性能瓶颈，任何时候流量都经过防范设备
- 在需要保护的目標设备比較多的情況下，投資較高
- 对来自上游的基于带宽的 DDoS 攻击无法提供有效保护

## 1.6.2 旁路部署防御 DDoS 攻击

完整的 DDoS 保护围绕四个关键主题建立：

- 要缓解攻击，而不只是检测
- 从恶意业务中精确辨认出好的业务，维持业务继续进行，而不只是检测攻击的存在
- 内含性能和体系结构能对上游进行配置，保护所有易受损点
- 维持可靠性和成本效益可升级性

旁路式部署防御模式可以完全围绕这几个关键主题进行，没有串行模式的几大弱点，可以应用在各种网络中，对网络设备，服务器等提供保护。如下图所示



此种部署模式是在原有网络的基础上实施，对原有网络没有任何改变。此方式需要 DDoS 攻击检测器或流量异常检测手段，当检测器发现 DDoS 攻击后，直接通知 DDoS 防范器将流量引导到 DDoS 防范器进行过滤，然后将过滤完后正常的流量继续传送到目标地址。

这种模式基于检测、转移、验证和转发的基础上实施一个完整 DDoS 保护解决方案来提供完全保护，通过下列措施维持业务不间断进行：

- 实时检测 DDoS 停止服务攻击攻击。
- 转移指向目标设备的数据业务到特定的 DDoS 攻击防护设备进行处理。
- 从好的数据包中分析和过滤出不好的数据包，阻止恶意业务影响性能，同时允许合法业务的处理。
- 转发正常业务来维持商务持续进行。

此种部署模式具有如下的特点

- DDoS 攻击检测和防范过程可以完全自动实现
- DDoS 防范设备不会成为性能瓶颈，只有当攻击发生的时候，流量才会经过 DDoS 防范设备
- 适合运营商和大型企业
- 不仅可以防范面向 CPU 的 DDoS 攻击，也可以防范面向带宽的攻击
- DDoS 防范设备是旁路的，同时又是共享设备，可以对众多的保护目标提供保护又不会使性能瓶颈
- 在需要保护的目標设备比較多的情況下，平均投資明顯下降
- 對來自上游的基於帶寬的 DDoS 攻擊可以提供有效保護
- 在運營商網絡環境中，可以很容易將其轉變成安全服務產品，銷售給企業用戶

- 可以适用于复杂的网络环境，IP，MPLS，MPLS VPN，GRE Tunnel 等

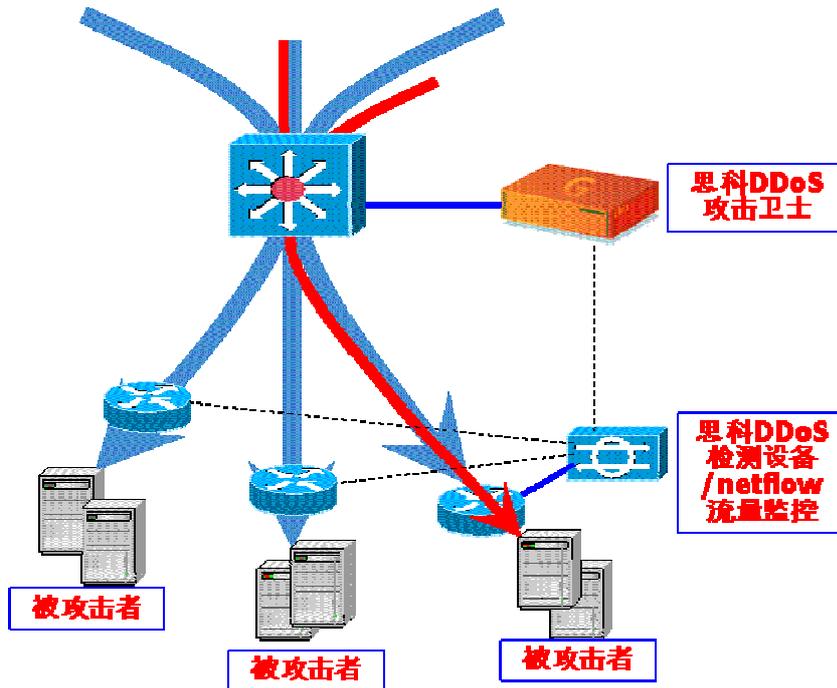
此种部署模式对 DDoS 防御具有以下保护性质：

- 通过完整的检测和阻断机制立即响应 DDoS 攻击，即使在攻击者的身份和轮廓不断变化的情况下。
- 与静态路由过滤器或 IDS 签名相比，能提供更完整的验证性能。
- 提供基于行为的反常事件识别来检测含有恶意意图的有效包。
- 识别和阻断个别的欺骗包，保护合法商务交易。
- 提供能处理大量 DDoS 攻击但不影响被保护资源的机制。
- 攻击期间能按需求布署保护，不会引进故障点或增加串联策略的瓶颈点。
- 内置智能只处理被感染的业务流，确保可靠性最大化和花销比例最小化。
- 避免依赖网络设备或配置转换。
- 所有通信使用标准协议，确保互操作性和可靠性最大化。

### 1.6.3 思科 DDoS 防护解决方案实现

思科 DDoS 防护解决方案是典型的旁路式 DDoS 防御方案，提供完整保护来防御各种 DDoS 攻击，甚至包括那些还未出现过的 DDoS 攻击。以积极缓解性能为特色，快速检测攻击，从合法业务中分离出恶意数据包，提供以秒计而不是以小时计的快速 DDoS 响应。该方案容易布署在关键路由器和交换机附近，可升级的选项来消除任何单个故障点，并且不影响任何现存的网络部件的性能和可靠性。

思科 DDoS 防护解决方案套件有两个独立的组件——Detector 攻击探测器和攻击防护卫士，两部分系统协同工作，能为任何环境提供 DDoS 保护。如下如所示

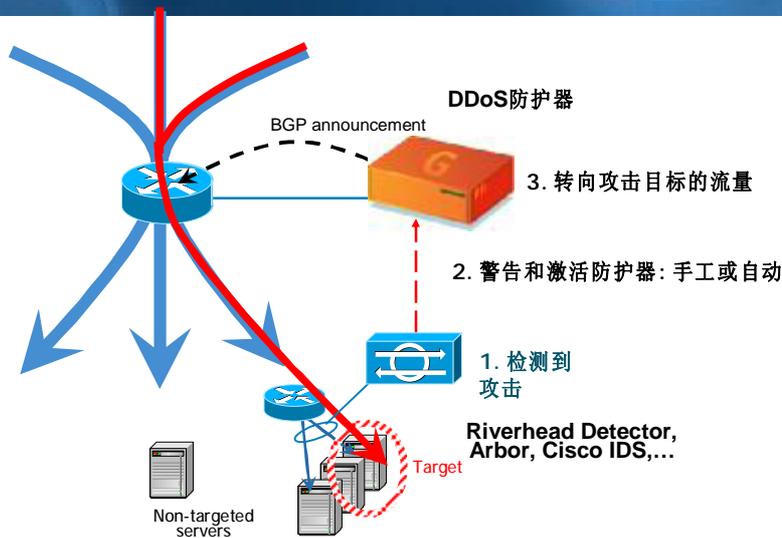


- 攻击检测器：作为早期报警系统，探测器提供对最复杂 DDoS 攻击的深入分析。探测器被动监测网络业务，搜寻与“正常”行为的偏差或 DDoS 攻击的基本行为。攻击被识别后，检测器发警报给攻击保护卫士，提供详细的报告和具体警报来快速响应该威胁。例如，即使在没有超出全面界限的情况下，检测器也需要能观测到从单个源头来的 UDP 包速率超出了范围。检测器可以是专用的 DDoS 检测器，也可以是 IDS 入侵检测器或 Netflow 流量异常监控系统
- 攻击保护卫士：攻击保护卫士是完善 DDoS 解决方案套件的基石——它是一个高性能 DDoS 攻击缓解设备，不仅能部署在上游的 ISP/数据中心，还能部署在一个大企业内部来保护网络和数据中心资源。

当攻击保护卫士被通知有一个目标处于被攻击状态时，攻击卫士通过发布 BGP 路由协议的宣告，指向目标的业务流量将被转移到与该目标设备相连的防护卫士。然后，业务将通过五个阶段的分析和过滤，过滤所有恶意业务，使得好的数据包能继续传送。攻击保护卫士位于一个单独网络接口处的路由器或交换机附近，在不影响其他系统的数据业务流情况下实现按需保护。攻击保护卫士可同时保护多个可能的目标，包括路由器、Web 服务器、DNS 服务器、LAN 和 WAN 带宽。

具体实现过程请参见下图

## 思科DDoS防护解决方案简介



4

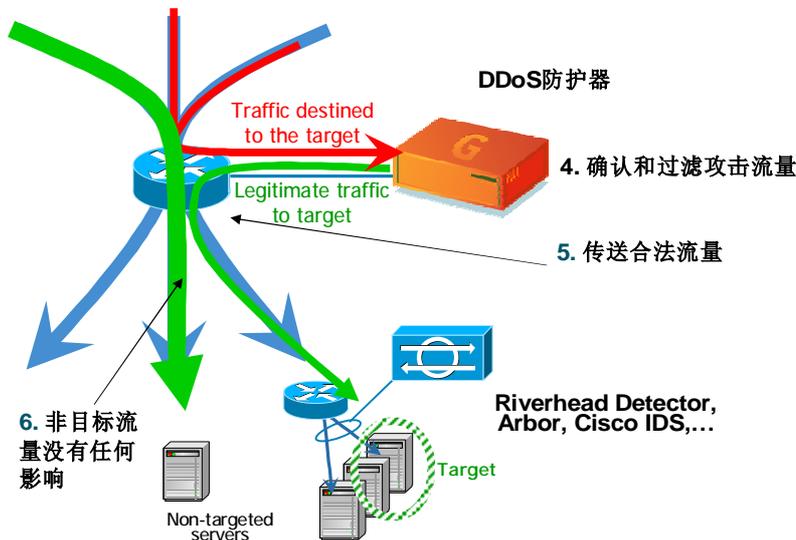
首先看看网络的部署情况，左边是原有网络结构，不受任何影响。将思科 DDoS 防护器部署在上层路由器旁边，一般是 PoP 点，DDoS 防护器和此路由器有 BGP 的连接；再靠近需要保护的受保护对象网络区域，部署 DDoS 监测器，或 IDS 入侵检测，或流量检测等设备，用以发现 DDoS 攻击的发生

第一步：DDoS 检测器发现有 DDoS 攻击发生，而且确认被攻击对象的地址或网段；

第二步：DDoS 检测器通过 SSH 发出告警信息给 DDoS 防护器，DDoS 防护器知道哪段 IP 地址被攻击了。DDoS 防护器可以自动启动防护，也可以是管理员人为干涉启动防护；

第三步：DDoS 防护器一旦启动对于相应网段的防护功能，将向旁边的路由器广播一条关于被攻击网段的 BGP 路由，支出下一跳地址是 DDoS 防护器的地址。由于 BGP 路由的优先级高于 OSPF/ISIS 等 IGP 路由，这时路由器中关于被攻击网段的路发生变化，下一跳不再是原来的下一跳地址，而变成了 DDoS 防护器的地址；

## 思科DDoS防护解决方案简介



5

第四步：这时所有面向被攻击者的流量被路由器转向到了 DDoS 防护器，如上图的红色的流量表示。红色的流量是混合流量，包含有攻击流量和正常用户请求流量；混合流量送达 DDoS 防护器后，DDoS 防护器拥有 MVP 多级验证体系结构，具有识别攻击流量和正常流量的能力（具体技术细节参见下段的 MVP 多级验证体系结构），将 DDoS 攻击流量区分和过滤掉；

第五步：DDoS 防护器将合法流量再转发到原有的网络中，因此合法流量可以到达被攻击的服务器。这时，我们可以知道，DDoS 攻击已经被有效防止了，不管是哪一种攻击，对于服务器而言，基本没有感觉到被攻击了，网络实现自动防护；

第六步：其他的非被攻击流量的路由没有任何改变。

### 完善 DDoS 攻击防御布署

完善的 DDoS 保护提供灵活的、可升级的布署来保护数据中心（服务器和网络设备）、ISP 链接或骨干网（路由器和 DNS 服务器）。

#### ○ 提供商

攻击保护卫士可布署在服务提供商的基础设施上有战略意义的节点上，来保护核心路由器、下游边缘设备、链接以及客户。也可以布署在边缘路由器来提供特定的客户保护。攻击探测器可以靠近提供商的边缘或在客户内部。



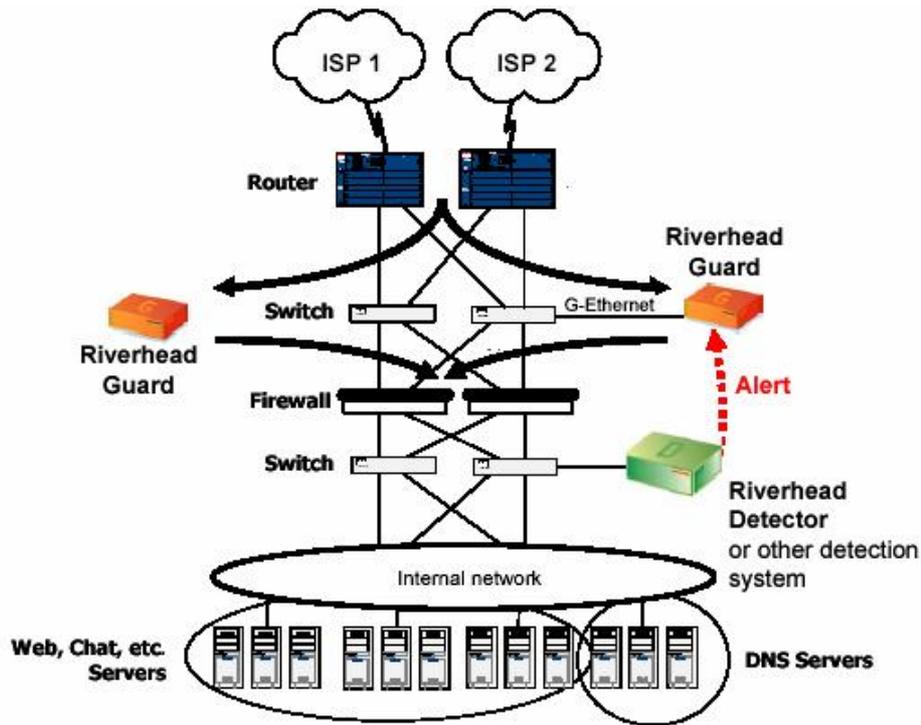
**Figure 4:** Riverhead protection in an ISP environment. Traffic destined for targeted device is diverted to Riverhead Guards; clean traffic is returned to the system.

图示说明:

- Traffic for targeted device diverted through Guard: 到目标设备的业务通过攻击防护卫士转向
- “clean” traffic returned to system: 返回到系统的干净业务
- DDoS protection in an ISP environment: ISP 环境的 DDoS 保护部署
- Traffic destined for targeted device is diverted to Riverhead Guards, clean traffic is returned to the system: 到特定目标设备的业务转移到攻击保护卫士，返回干净的业务到系统

#### ○ 企业和数据中心

在企业数据中心，攻击保护卫士被布署在数据中心的分发层，保护下游的低速链接和服务。攻击保护卫士能连接到分发交换机并且支持冗余配置（见图 5）。



**Figure 5:** Riverhead protection in an enterprise environment. Only traffic destined for the targeted device is diverted to the Guard, which returns “clean” transactions back to the system.

图示说明:

- Alert: 报警
- Riverhead protection in an enterprise environment : 企业环境下的攻击防护卫士
- Only traffic destined for the targeted device is diverted to the Guard, which returns “clean” transactions back to the system: 只有到特定目标设备的业务转移到攻击防护卫士, 返回干净业务到系统

在 DDoS 防护器部署的选择上, 从上图可见, 一般建议在防火墙的上层, 这样可以有效防护外部防火墙阻断并引起防火墙连接拥塞的可能性; 如果部署在防火墙后面, 就可能引起防火墙已经瘫痪, 从而失去保护的意义。

## 1.6.4 电信级 DDoS 攻击检测-Arbor

### Arbor Networks Peakflow 电信级DDoS攻击检测

Arbor Networks Peakflow SP (<http://www.arbornetworks.com/>) 是一个可扩展的平台, 可以提供一个全面的解决方案, 为电信运营商及其客户提供强大的DDoS检测防御、流量和路由功能。Peakflow SP能让电信运营商可以为他们的企业客户

提供可扩展的DDoS检测防御和流量管理工具，也可以帮助网络管理人员主动地检测和清除整个网络中的异常情况，例如DDoS攻击和蠕虫。Peakflow SP的流量和路由功能可以分析流量网络，让操作人员可以及时地针对路由、传输、合作伙伴和客户制定业务决策。

Peakflow SP可以利用它的双层收集器架构进行扩展。这些收集器可以从多个路由器和一个控制器获取NetFlow统计数据。控制器可以协调事件关联和对事件进行追溯。当Peakflow SP与Cisco Guard结合提供DDoS防御功能时，一旦通过收集器获得某个区域的异常信息，控制器就会建立SSH连接，启用Cisco Guard，将受攻击区域置于保护模式。

在思科的DDoS防御解决方案，Peakflow SP可以为DDoS攻击检测、追溯和消除提供一个简便的方法。它首先会利用来自于网络中已有的路由器的数据流，构建一个覆盖整个网络的正常行为模式。与内嵌式数据收集方法相比，Peakflow SP可以从思科路由器收集基于数据流的Cisco NetFlow统计数据。这使得Peakflow SP可以随着网络规模的扩大而进行扩展。或者，Peakflow SP可以利用不支持Netflow的路由器上的数据包获取功能。它还可以使用光分离器，或者来自于相邻路由器或交换机的端口镜像流量。无论是NetFlow还是数据包获取都不会对网络的性能或者可靠性产生影响；即这种数据收集方式是不影响运行的。系统可以实时地将这些流量与基本模式进行对比，标记异常情况和找出受到影响的接口、严重性等。异常情况随后会被用来与网络进行对比，追溯来源和找出输入节点。最后，根据异常情况的特性，Peakflow SP会为保持服务的正常运行建议合适的威胁消除措施，例如启动Cisco Guard XT清除恶意数据包，或者启用远程触发黑洞（RTBH），在远程路由器上丢弃无用流量。

## 1.7 DDoS 防御安全服务模型

电信运营商可以将DDoS防御模式作为一种服务，提供给他们企业客户。同时也可以被电信运营商用于防止他们自己的基础网络和关键业务遭受DDoS攻击。

下列是DDoS防御安全服务模式，以及它们的功能和主要作用。

DDoS 防御安全服务模式

DDoS 防御模式	核心功能	主要作用
托管网络	为SP客户提供最后一英里带宽保护	新的SP收入模式，主要功能在于提高客户的业务连续性，保护关键的最后一英里带宽，确保在数据连接上连续地提供增强的服务
主机托管	保护由运营商托管的数据中心资产	新的SP收入模式，确保电信运营商托管的关键资产的正使用，区分托管服务

托管对等连接点	为下游 ISP 提供批量的无 DDoS 连接	新的 SP 收入模式，提供批量清洁连接，更好地推广一个无 DDoS 的环境
基础设施保护	针对 SP 的保护模式可以保护他们的网络和保护服务供应	保护数据中心的关键资产，消除针对关键路由基础设施的攻击（对等节点、运营商边缘和核心路由器），通过在昂贵的跨海连接上减少无用流量，降低运营开支，降低附带损害的影响

### 1.7.1 托管网络服务模式

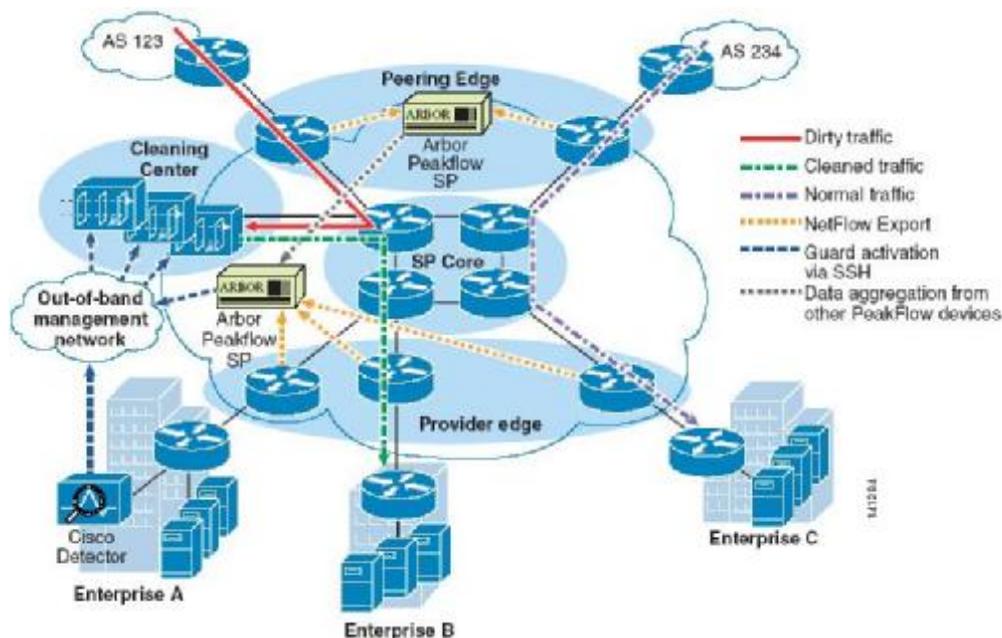
这种服务模式让电信运营商可以防止企业客户的网络遭到来自互联网的 DDoS 攻击。这些攻击不仅会影响主机和上面的应用，而且——更加严重的是一——还会导致电信运营商和客户网络之间的连接带宽达到饱和。对于金融和电子商务客户而言，这种攻击可能导致客户的流失、声誉的下降和其他损失。

如果能够及早检测到 DDoS 攻击，并尽可能地在网络上游阻止它们，就可以有效地消除 DDoS 攻击的影响。一般而言，电信运营商可以利用思科 DDoS 解决方案，在两个服务层次为企业客户提供 DDoS 防御功能，如图所示：

专用服务——这种高级服务适用于那些在线服务对业务的持续发展至关重要的客户。这种服务用于为客户终端设备提供承诺的流量清洁容量，策略学习和定制，以及可选的 DDoS 检测和清洁启用功能。

共享服务——这种服务面向对的是其他一些需求并不是特别迫切的企业客户。因此，这项服务用于提供“尽力而为的”、由其他客户共享的流量清洁容量，标准的 DDoS 检测策略，并且不提供基于 CPE 的 DDoS 检测和清洁启用功能。

图 托管网络服务模式



专用服务的架构设计包括在 SP 的网络清洁中心为每个客户专门设置一个 Cisco Guard XT 设备或者 Cisco Anomaly Guard 服务模块。这些设备的数量取决于客户希望防御的 DDoS 攻击的最大规模。SP 可以建立多个清洁中心，具体取决于 SP 与互联网其他部分之间存在多少个对等节点，以及它们之间的距离。设计目标是在尽可能靠近攻击进入的对等节点的位置处消除攻击流量。

为了检测 DDoS 攻击，专用服务可以在客户端部署思科流量异常检测器 XT，或者通过在电信运营商网络部署 Peakflow SP 获取来自于核心路由器的 NetFlow 统计数据。客户也可以同时采用这两种手段。通过安装思科流量异常检测器，可以帮助客户灵活地在设备上定制策略。

在共享服务的设计中，清洁中心将包含由多个客户共享的 Cisco Guard XT 设备或者 Cisco Anomaly Guard 服务模块。因为该服务只提供“尽力而为的”DDoS 净化功能，所以当所有设备的全部容量都被用于消除现有攻击时，SP 将无法再接受额外的 DDoS 攻击消除请求。

单独部署 Peakflow SP 是共享服务检测 DDoS 的首选方法。Peakflow SP 可以提供一种可扩展的检测方法，因为它能够同时从多台路由器收集 NetFlow 统计数据，发现其中的异常情况。这是一种非常经济的方法，因为如果客户不需要高度精确的 DDoS 检测功能，就无需购买终端检测设备。

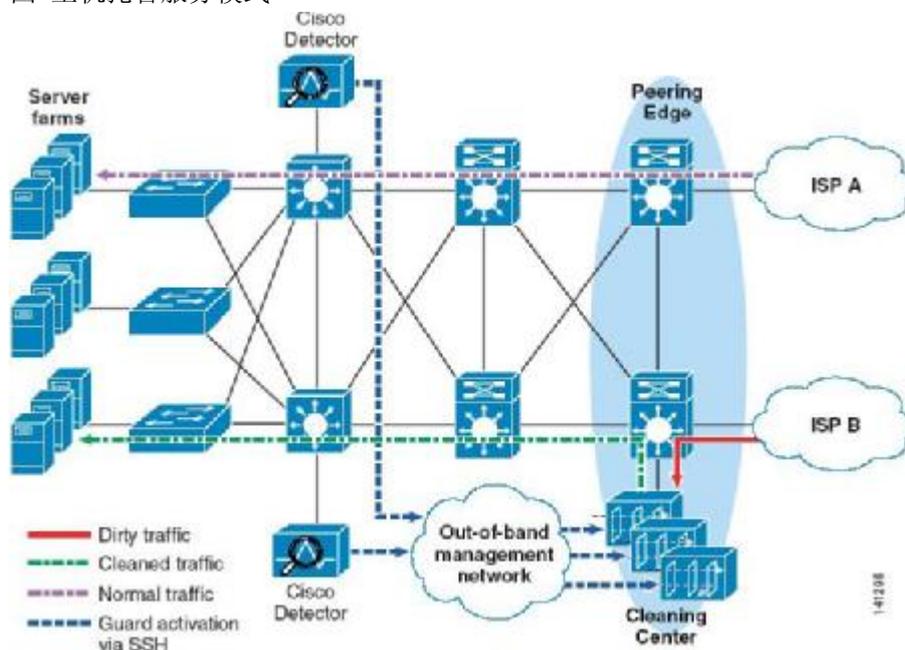
对于这两种服务等级，都可以在检测到 DDoS 攻击之后，通过手动或者自动的方式启用 Cisco Guard XT，以保护区域安全。手动启用允许 SP 或者客户在启用区域保护之前，验证攻击是否属实。

## 1.7.2 主机托管服务模式

这种服务模式让主机托管电信运营商可以为使用他们的 Web 托管和应用模式的客户提供 DDoS 防御功能。该服务将以对 SP 现有的托管服务的增值改进的形式提供。它是一种“尽力而

为的” DDoS 防御服务，可以为检测和消除攻击提供缺省的策略模板，类似于前面介绍的托管网络 DDoS 防御服务中的共享服务。

图 主机托管服务模式



这种服务的架构设计包括用于 DDoS 检测的思科流量异常检测器 XT 或者 Peakflow SP, 但是两者不宜同时使用。为了消除 DDoS 攻击，共享式 Cisco Guard XT 设备或者 Cisco Anomaly Guard 服务模块应当被放置在靠近托管电信运营商网络的对等节点的清洁中心，以防止攻击流量导致它的核心网络带宽达到饱和。

### 1.7.3 托管对等服务模式

这种模式可以防止 DDoS 攻击导致 SP 对等节点或者网络接入节点发生带宽饱和。如果不采用思科的解决方案，DDoS 攻击可能会中断对等节点之间的连接。这种服务可以用托管 DDoS 防御服务的形式提供，或者作为一个有效的 DDoS 防御系统提供，以保护 SP 基础设施。例如，作为一项托管服务，它可以包含对与下游 ISP 的连接的保护。SP 可以在内部部署该解决方案，保护层次化网络中两个区域之间的连接，自治系统之间的跨海连接，或者两个属于同一个 SP 的自治系统之间的连接。

图 针对跨海连接的对等节点 DDoS 防御服务



在这种模式的设计中，Peakflow SP 可以提供一种可扩展的 DDoS 防御方法。它可以充当一个集中的平台，汇集来自于不同对等节点的路由器的 NetFlow 统计数据。为了消除 DDoS，清洁中心应当位于源对等节点附近，以便在 DDoS 攻击数据包导致与目的地对等节点的连接饱和之前，滤除这些数据包。如果需要为两个对等节点之间的连接中的双向流量都提供 DDoS 防御功能，就需要在网络的每一段都建立清洁中心。

### 1.7.4 基础设施保护模式

这种服务模式可以提供对 SP 基础设施网络资产的保护，实现统一、可靠的服务供应。它不是一项可以直接创造收入的服务；但是，它可以防止 DDoS 攻击的影响，从而保持可用性和服务供应。SP 可以在内部部署该解决方案，保护层次化网络中两个区域之间的连接，自治系统之间的跨海连接，或者两个属于同一个 SP 的自治系统之间的连接。

图 基础设施保护服务

