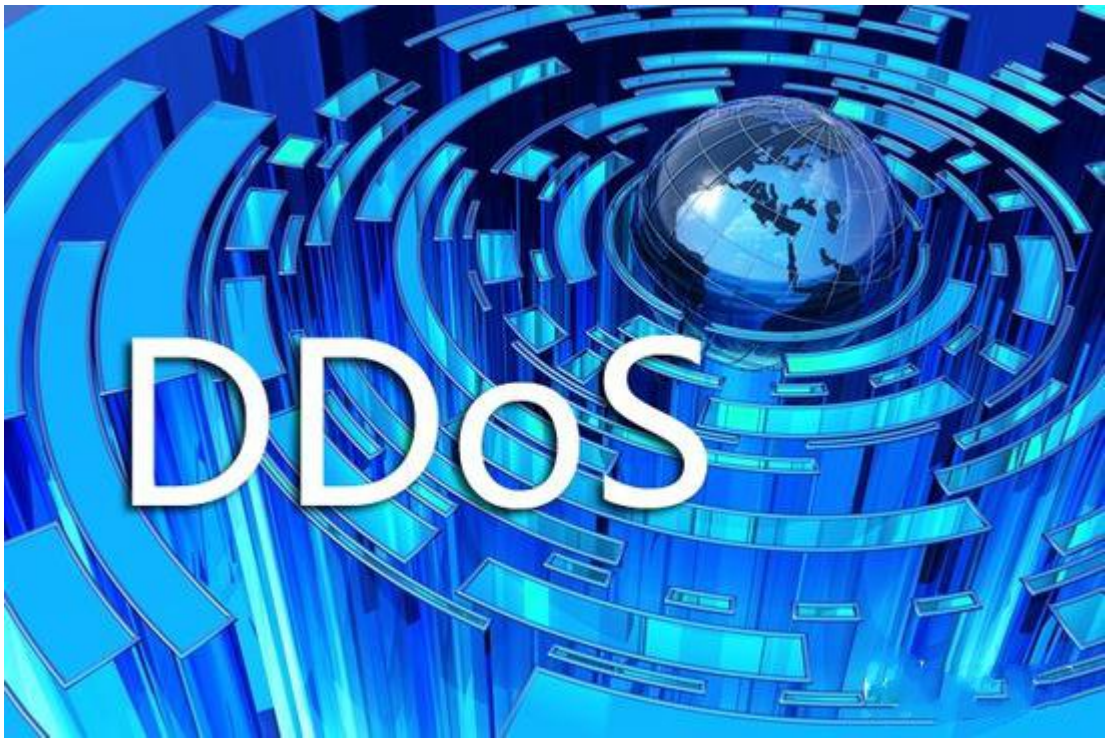

作为破坏力较强的黑客攻击手段，DDoS是一种形式比较特殊的拒绝服务攻击。作为一种分布、协作的大规模攻击方式，它往往把受害目标锁定在大型Internet站点，例如商业公司、搜索引擎或政府部门网站。由于DDoS攻击的恶劣性(往往通过利用一批受控制的网络终端向某一个公共端口发起冲击，来势迅猛又令人难以防备，具有极大破坏力)难以被侦测和控制，因此也广泛受到网络安全业界的关注。从最初的入侵检测系统(IDS)到目前新兴的全局安全网络体系，在防范DDoS攻击的过程中先进的网络安全措施发挥作用，使对抗黑客攻击的手段日益提升，向着智能化、全局化的方向大步迈进。

知己知彼:全面解剖DDoS攻击

分布式攻击系统和我们日常生活中司空见惯的客户机/服务器模式非常相象，但是DDoS系统的日趋复杂性和隐蔽性使人难以发现。入侵者控制了一些节点，将它们设计成控制点，这些控制点控制了Internet大量的主机，将它们设计成攻击点，攻击点中装载了攻击程序，正是由这些攻击点计算机对攻击目标发动的攻击。DDoS攻击的前奏是率先攻破一些安全性较差的电脑作为控制点主机。因为这些电脑在标准网络服务程序中存在众所周知的缺陷，它们还没有来得及打补丁或进行系统升级，还有可能是操作系统本身有Bug，这样的系统使入侵者很容易闯入。

典型的DDoS攻击包括带宽攻击和应用攻击。在带宽攻击中，网络资源或网络设备被高流量数据包所消耗。在应用攻击时，TCP或HTTP资源无法被用来处理交易或请求。发动攻击时，入侵者只需运行一个简单的命令，一层一层发送命令到所有控制的攻击点上，让这些攻击点一齐“开炮”——
向目标传送大量的无用的数据包，就在这样的“炮火”下，攻击目标的网络带宽被占满，路由器处理能力被耗尽。而较之一般的黑客攻击手段来说，DDoS的可怕之处有二:一是DDoS利用Internet的开放性和从任意源地址向任意目标地址提交数据包;二是人们很难将非法的数据包与合法的数据包区分开。

屡战屡败:防范手段失效溯源

既然了解DDoS攻击的起源结果，为什么还会让它如此肆虐呢?平心而论，以往所采用的几种防御形式的被动和片面，是DDoS攻击难以被遏止的真正原因。

在遭遇DDoS攻击时，一些用户会选择直接丢弃数据包的过滤手段。通过改变数据流的传送方向，将其丢弃在一个数据"黑洞"中，以阻止所有的数据流。这种方法的缺点是所有的数据流(不管是合法的还是非法的)都被丢弃，业务应用被中止。数据包过滤和速率限制等措施同样能够关闭所有应用，拒绝为合法用户提供接入。这样做的结果很明显，就是"因噎废食"，可以说是恰恰满足了黑客的心愿。

既然"因噎废食"不可取，那么路由器、防火墙和入侵检测系统(IDS)的功效又怎样呢?从应用情况来看，通过配置路由器过滤不必要的协议可以阻止简单的ping攻击以及无效的IP地址，但是通常不能有效阻止更复杂的嗅探攻击和使用有效IP地址发起的应用级攻击。而防火墙可以阻挡与攻击相关的特定数据流，不过与路由器一样，防火墙不具备反嗅探功能，所以防范手段仍旧是被动和不可靠的。目前常见的IDS能够进行异常状况检测，但它不能自动配置，需要技术水平较高的安全专家进行手工调整，因此对新型攻击的反应速度较慢，终究不是解决之道。

全局安全:充分遏制DDoS魔爪

深究各种防范措施对DDoS攻击束手无策的原因，变幻莫测的攻击来源和层出不穷的攻击手段是症结所在。为了彻底打破这种被动局面，目前业界领先的网络安全技术厂商已然趋于共识:那就是在网络中配置整体联动的安全体系，通过软件与硬件技术结合、深入网络终端的全局防范措施，以加强实施网络安全管理的能力。

以锐捷网络2004年底推出的GSN??全局安全网络解决方案为例，它在解决DDoS方面给出了自己独特的见解。首先，GSN??在网络中针对所有要求进行网络访问的行为进行统一的注册，没有经过注册的网络访问行为将不被允许访问网络。通过GSN??安全策略平台的帮助，管理员可以有效的了解整个网络的运行情况，进而对网络中存在的危及安全行为进行控制。在具体防范DDoS攻击的过程中，每一个在网络中发生的访问行为都会被系统检测并判断其合法性，一旦发觉这一行为存在安全威胁，系统将自动调用安全策略，采取直接阻止访问、限制该终端访问网络区域(例如避开网络内的核心数据或关键服务区，以及限制访问权限等)和限制该终端享用网络带宽速率的方式，将DDoS攻击发作的危害降到最低。

在终端用户的安全控制方面，GSN
??能对所有进入网络的用户系统安全性进行评估，杜绝网络内终端用户成为DDoS攻击来源的威胁。从当用户终端接入网络时，安全客户端会自动检测终端用户的安全状态。一旦检测到用户系统存在安全漏洞(未及时安装补丁等)，用户会从网络正常区域中隔离开，并自动置于系统修复区域内加以修复，直到完成系统规定的安全策略，才能进入正常的网络环境中。这样一来，不仅可以杜绝网络内部各个终端产生安全隐患的威胁，也使网络内各个终端用户的访问行为得到了有效控制。通过在接入网络时进行自动"健康检查"，DDoS再也不能潜藏在网络中，并利用网络内的终端设备发动攻击了。

对于用户来说，正常业务的开展是最根本的利益所在。随着人们对Internet的依赖性不断增加，DDoS攻击的危害性也在不断加剧。不少安全专家都曾撰文指出:及早发现系统存在的攻击漏洞、及时安装系统补丁程序，以及不断提升网络安全策略，都是防范DDoS攻击的有效办法。而先进的全局安全网络体系的出现，实现了将系统层面和网络层面相结合来有效的进行安全解决方案的自动部署，进一步提高了对于DDoS这类"行踪飘渺"的恶性网络攻击的自动防范能力。尽管目前以DDoS为代表的黑客攻击仍旧气焰嚣张，但是在可以预见的将来，广大用户手中握紧的安全利刃必定可以斩断DDoS的魔爪。