某数据中心反击DDOS攻击典型案例 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022__E6_9F_90_E6_95_B0_E6_8D_AE_E4_c101_181840.htm 某互联网公司作为一个知名的网站，时时都有受到攻击的威胁。目前该互联网公司非常大的安全隐患是来自外网的拒绝服务公司（Denial of Service Attacks），包括以SYN Flood和Ping Flood为主的技术，其主要方式是通过使关键系统资源过载，导致网络或服务器的资源被大量占用，甚至造成网络或服务器的全面瘫痪。 世纪互联针对该互联网公司网络和业务的实际情况，采用了防火墙、路由器、IDS相结合的办法，提出了一套以防范拒绝服务攻击为主的安全服务解决方案。 方案实施 该互联网公司在遭受拒绝服务攻击时，单纯地使用防火墙并不能进行有效地防护。因此，世纪互联在部署该互联网公司防范拒绝服务攻击的配置时，运用了将防火墙与路由器相结合的方式。 世纪互联针对该互联网公司的拒绝服务攻击的安全解决方法是，在该互联网公司和IDC的接口使用Cisco 7206路由器，在南楼和北楼分别加防火墙，利用这种防范措施相结合，共同抵制拒绝服务攻击。 路由器的部署 为阻止拒绝服务攻击，世纪互联将该互联网公司原来的2948路由器换为Cisco7206路由器。这种Cisco的72系列路由器的优势在于：能有效执行TCP截取和封掉源地址等功能。 TCP截取特性，通过截取和验证TCP连接请求的合法性来防止SYN的报文洪水。在截取模式下，TCP截取软件截取从客户到服务器并与扩展访问列表匹配的TCP同步（SYN）分组。其中，软件代表目标服务器与客户建立连接，以便于客户与服务器进行连接，并且透明地将

两个半连接结合起来，使来自不可抵达主机的连接请求不能到达服务器。同时，在连接期间，软件继续转发和分组。 如果出现非法请求，软件在半打开连接上的主动超时功能以及TCP连接请求设置阀将保护目标服务器，使其继续准许合法请求。 灵活使用TCP截取建立安全策略，可选择截取所有请求或只截取来自特定网络或目标为特定服务器的请求，也可以配置连接速率和未解决连接数目的阀值。 采用在监视模式下运行TCP截取，与截取模式不同的是，在监视模式下，软件的被动监视通过路由器的连接请求，如果在配置的时间内没能建立连接，软件将干预并终止该连接请求。 路由器设置步骤 一旦发现对给互联网公司的拒绝服务攻击，世纪互联的安全服务工程师首先会在监控中心检测到这种攻击行为，并且会在第一时间通知该互联网公司。同时，在授权的情况下，世纪互联在路由器上的设置将以如下步骤进行： 1、启用TCP截取； 2、设置TCP截取模式； 3、设置TCP截取删除模式； 4、更改TCP截取定时器； 5、更改TCP截取主动阀值； 6、监控和维护TCP截取。 根据世纪互联的测试情况，在该互联网公司遭受Flood攻击时，可字7206路由器上做 如下配置： 1、设置TCP截取模式为watch； 2、配置扩展IP访问列表101，截取发送给受攻击子网中所有的TCP包； 3、设置TCP截取的定时器时间值； 4、可以随时显示TCP截取的信息。 防火墙的部署 由于该互联网公司的网络分布在南楼和北楼两个物理位置，因此世纪互联分别在两个2914之前安装了2台Netscreen防火墙，均采用透明的工作模式。 Netscreen的策略由世纪互联和该互联网公司的技术人员共同配置，对SYN Flood、Ping Flood、UDP Flood等拒绝服务攻击都设置为阻断

。 综上所述，世纪互联为该互联网公司提供的拒绝服务攻击的安全防护包括可交换机、防火墙层。通过这层防护，极大限度地降低了该互联网公司所受到的拒绝服务攻击的危害。同时，世纪互联提供的入侵检测服务，可以为该互联网公司提供网络违规的预警。 应用优势 世纪互联为该互联网公司定制的整体网络安全解决方案的优势在于：在网络改动较少的前提下，有效地阻止DDOS的攻击；同时，由于使用了IDS的服务，使该互联网公司具备预警的功能，从而能及时根据网络攻击事件制定紧急响应对策，充分体现了经济性和高效性。 