DDoS攻击CC攻击防御流量过滤流量清洗原理

产品名称	DDoS攻击CC攻击防御流量过滤流量清洗原理
公司名称	一讯辽宁网推3部
价格	.00/个
规格参数	
公司地址	广州市天河区天河软件园A6栋08-12
联系电话	13825130039 13825130039

产品详情

DDoS攻击，CC攻击防御，流量过滤，流量清洗原理

攻击特征的匹配：

在发动DDoS攻击过程中是需要借助一些攻击工具的，比如僵尸网络等。同时网络犯罪分子为了提高发送请求的效率，攻击工具发出的数据包通常是编写者伪造并固化到工具当中的。

因此每种攻击工具所发出的数据包都有一些特征存在。那么流量清洗技术将会利用这些数据包中的特征作为指纹依据，通过静态指纹技术或者是动态指纹技术识别攻击流量。

静态指纹识别的原理是预先将多种攻击工具的指纹特征保存在流量清洗设备中的数据库，因此所有的访问数据都会先进行内部数据库比对，如果是符合的会选择直接丢弃。动态指纹识别清洗设备对流过的网络数据包进行若干个数据包学习，然后将攻击特征记录下来，后续有访问数据命中这些特征的直接丢弃。

IP信誉检查：

IP信誉机制是互联网上的IP地址赋予一定的信誉值.有一些经常用来当作僵尸主机的，会发送垃圾邮件或被用来做DDOS攻击的IP地址。会被赋予较低的信誉值.说明这些IP地址可能成为网络攻击的来源。

所以当发生DDOS攻击的时候会对网络流量中的IP信誉检查，所以在清洗的时候会优先丢弃信誉低的IP，一般IP信誉检查的极端情况是IP黑名单机制。

协议完整性验证：

为提高发送攻击请求的效率，大多数的都是只发送攻击请求，而不接收服务器响应的数据。因此.如果采取对请求来源进行交替严重，就可以检测到请求来源协议的完整性，然后在对其不完整的请求来源丢弃处理。在DNS解析的过程中，攻击方的工具不接收解析请求的响应数据，所以不会用TCP端口进行连接。所有流量清洗设备会利用这种方式区分合法用户与攻击方，拦截恶意的DNS攻击请求。

这种验证方式也适用于HTTP协议的Web服务器。主要是利用HTTP协议中的302重定向来验证请求，确认来源是否接收了响应数据并完整实现了HTTP协议的功能。正常的合法用户在接收到302 重定向后会顺着跳转地址寻找对应的资源。而攻击者的攻击工具不接收响应数据，则不会进行跳转，直接会被清洗拦截，WEB服务器也不会受到任何影响。