协 办

DNS安全防护解决方案

杭州迪普科技有限公司

1 引言

国际著名网络安全专家Roland Dobbins曾说过，DNS就像空气，平时我们感觉不到它的存在，但是一旦出现问题，其影响可能“致命”。作为一项互联网基础业务，DNS的安全直接关系到整个互联网应用能否正常使用。近年来，“163.net域名劫持”、“Google域名劫持”、“百度域名劫持”、“暴风影音断网门”等事件都说明DNS安全性面临巨大风险，在安全性遭到破坏时将会导致巨大损失。

2 DNS安全防护面临的威胁

DNS作为全球最大、最复杂的分布式层次数据库系统，由于其开放、庞大、复杂特性，设计之初对于安全性考虑不足，再加上人为攻击和破坏，DNS面临非常严重的安全威胁。因此，如何解决DNS安全问题，并寻求相关解决方案是当今亟待解决的问题。

2.1 DDoS攻击

DDoS（Distributed Denial of Service）攻击通过僵尸网络，利用各种服务请求耗尽被攻击网络的系统资源，造成被攻击网络无法处理合法用户请求。针对DNS的DDoS攻击可按攻击发起者和攻击特征进行分类。

按攻击发起者进行分类可分为两类：一是僵尸网络，即控制大批僵尸网络利用真实DNS协议栈发起大量域名查询请求；二是模拟工具，即利用工具软件伪造源IP发送海量DNS查询。

按攻击特征进行分类可分为Flood攻击，即发送海量DNS查询报文导致网络带宽耗尽而无法传送正常DNS 查询请求；资源消耗攻击，即发送大量非法域名查询报文引起DNS服务器持续进行迭代查询，从而达到较少的攻击流量消耗大量服务器资源的目的。

2.2 DNS欺骗

DNS欺骗是最常见的DNS安全问题之一。当一个DNS服务器由于自身的设计缺陷，接收了一个错误信息，那么就将做出错误的域名解析，从而引起众多安全问题。例如将用户引导到错误的互联网站点，甚至是一个钓鱼网站；发送电子邮件到未经授权的邮件服务器。

攻击者通常通过以下3种方式进行DNS欺骗：缓存污染，攻击者采用特殊的DNS请求，将虚假信息放入DNS的缓存；DNS信息劫持，攻击者监听DNS会话，猜测DNS服务器响应ID，抢先将虚假响应提交给客户端；DNS重定向，将DNS名称查询重定向到恶意DNS服务器。

2.3 系统漏洞多

BIND（Berkeley Internet Name Domain）是最常用的DNS服务软件，具有广泛的使用基础，Internet的绝大多数DNS服务器都基于这个软件。BIND提供高效服务的同时，也存在很多安全性漏洞。CNCERT/CC在安全报告中指出：2009年7月底被披露的“Bind9”高危漏洞，影响波及全球数万台域名解析服务器，我国有数千台政府和重要信息系统部门、基础电信运营企业以及域名注册管理和服务机构的域名解析服务器受到影响。

DNS服务器的自身安全性非常重要。目前，主流的操作系统如Windows、UNIX、Linux均存在不同程度的系统漏洞和安全风险，补丁管理是安全管理工作中非常重要和困难的一个组成部分，因此针对操作系统的漏洞防护是DNS安全防护工作中的重点。

3 现有DNS安全手段不足

3.1 系统扩容

利用提高DNS服务器的性能或

者增多DNS服务器数量的方法改善每秒处理DNS请求的能力，这种扩容应对用户访问量的增加是有效的，但是面对现有的DNS攻击能力，请求流量甚至可以到达千万QPS，只依靠系统扩容远远不够，而且如果对所有部署DNS服务器进行性能提升，其成本高，耗费大量人力、财力。

3.2 DNSSEC

DNSSEC的确可以提高DNS安全性，但DNSSEC的全面部署是一个很困难的任务，难以在短时间内完成，而且DNSSEC本身很消耗性能，这有可能成为DNS的新隐患。

3.3 防火墙

防火墙本身并没有专门针对DNS的防护手段，面对多种多样的DNS攻击，显得束手无策。

3.4 流量阈值判断攻击

采用判断DNS请求流量阈值的方法判断攻击，利用防护设备配置针对源IP、Domain的过滤策略，使用此种方法，针对热点事件产生的正常DNS请求流量超限的情况会产生误报，对通过非法域名以小博大的攻击方法由于其流量未超限会产生漏报。

4 DPtech DNS防护方案

4.1 DNS系统DDoS攻击防护

采用智能的DNS DDoS攻击识别技术，通过实时分析DNS解析失败率、DNS响应报文与请求报文的比例关系等方法，能准确、有效识别各种针对DNS的DDoS攻击，避免产生漏报和误报，并能通过专业的线性DNS攻击防御技术和离散DNS攻击防御技术有效防御DNS DDoS攻击。

同时，还能通过流量异常检测、SYN Cookie、SYN Proxy、连接限制、连接速率限制等技术实现全面的TCP Flood、UDP Flood、SYN Flood、ICMP Flood、HTTP Get、CC等DDoS攻击防御，全面确保DNS服务器免受DDoS攻击。

4.2 DNS报文预处理

网络中经常会出现一些不符合规范的DNS报文（域名超长，非法字符等），虽然这些报文量不大，但是由于报文内容不规范，可能导致服务器出现未知问题。一般情况下，DNS防护模块无法区分不规范报文和正常报文，因此，我们专门添加了预处理模块，对于DNS报文，严格按照RFC1034、RFC1035、RFC2181规定，对于不符合的报文直接丢弃。

此外，还可以添加DNS访问控制，用户可以根据需要设置域名、IP以及DNS类型的黑白名单，对报文进行过滤。例如，如果出现一些IP或者域名经常发动攻击，则可以让这部分报文不经过后续的识别和防护模块，而是直接过滤，提高整个系统运行效率。同理，对于一些可信的IP或者域名，也可以不经过后续模块而是直接交给DNS服务器处理，这样可以提高用户访问速度。

4.3 DNS检测和预警

根据设置请求流量阈值的方法判断是否发生攻击，具有一定局限性。例如，在发生一些热点事件（如世界杯，“十八大”会议等）时，产生的正常DNS请求流量会超过平时配置的防护阈值，这样肯定会发生误报。还有一种情况，攻击者只发送不多的虚假域名DNS请求，这些请求会造成频繁逐级递归查询，造成资源耗尽，但是这种攻击的流量可能小于阈值，必然产生漏报。这些都是传统DNS攻击识别的缺陷。我们采用以下两种更准确的方法来识别攻击。

(1)实时分析DNS解析失败率。也就是请求域名不存在，导致服务器回应“no such name”，如果解析失败率增加，则说明有大量无法解析的请求产生（超过指定阈值），可能存在攻击，即使攻击流量不大，也可以直观通过解析失败率发现攻击行为。

(2)实时分析DNS响应报文与请求报文的比例关系。如果攻击流量很大，导致服务器瘫痪，这样服务器将无法回应报文，也就不会产生“no such name”报文，这时我们采用和上述方法互补的检测方式。既然服务器瘫痪无法回复报文，那么必然存在DNS服务器响应报文与请求报文之间比例的失衡，当这个比值不断缩小时，就认为服务器出现了问题，有可能遭到攻击。

通过以上两种方法，无论采用怎样的攻击方式，都可以被迅速发现，然后采取进一步防护手段。

4.4 DNS防护

(1)DNS每源IP限速

支持按每源IP限速、每源IP范围限速，可以为不同的源IP设置不同的限速阈值，支持访问量TOP *N*源IP的识别与展示。

(2)DNS每域名限速

支持按每Domain限速，可以为不同的Domain设置不同的限速阈值，支持访问量TOP *N* Domain的识别与展示。

(3)DNS多级域名限速

以上方法对于域名离散的攻击没有办法进行防护，但是经过观察，域名离散通常不是全离散，而是部分离散。因此，可以把域名分为多级进行防护（.com属于顶级域名，baidu.com属于二级域名，以此类推），对每一个域级进行单独统计并观察，例如，如果产生*.baidu.com针对百度子域进行攻击的报文，采用传统的全域名方法进行统计无法进行防护，但是针对

二级域名就可以轻松发现并丢弃这种攻击。目前，可以支持8级域的检测防护，能很好地针对这种部分子域进行随机DNS攻击的情况。

(4)TCP反弹防护

几乎所有的DNS攻击都采用UDP报文，因此可以利用这个特性来防护一些离散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标识位的应答报文，这时正常的主机会重新发起基于TCP的53端口请求，设备接到TCP请求后，转化为UDP请求送给DNS服务器，避免DNS服务器由于处理大量TCP报文负载过大的情况，但是攻击报文不会重发TCP的DNS请求报文，因此所有DNS攻击都会被设备丢弃，不会到达DNS服务器。

(5)DNS重传校验

当设备检测到攻击后，会把后续收到的第一个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(2～5s)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发送请求，利用该特性，就可以马上丢弃这些不符合重传时间间隔的攻击报文。

(6)智能指纹识别

当IP以及域名都随机时，DNS报文的其他字段可以成为识别DNS攻击的重要手段。我们可以对报文的三层以及四层进行指纹特征识别，这些字段必然存在一些雷同的指纹特征（例如，其源端口可能雷同），并根据这些雷同指纹特征对DNS请求报文进行防护，这样就可以避开域名全随机的难题。只要攻击报文不是所有字段全随机，利用指纹识别的方法都可以有效防护DNS攻击。

(7)DNS投毒防护

收到请求报文后，根据源目的IP，源目的端口以及DNS ID五元组建立DNS会话，这时没有会话的DNS回应报文全部作为恶意投毒攻击丢弃，只有建立会话的回应报文才递交给后端DNS服务器，这样攻击者就很难将投毒的攻击报文发送到DNS服务器。

(8)DNS 重点域名监控

对一些经常受到攻击的热点域名进行重点检测，把这些域名和指定的IP组进行配置，当某个时刻IP出现变化且变化范围不在IP组内时，就发出告警，由管理员向权威服务器确认这个变化，判断服务器是否遭到攻击。利用这个检测机制，可以及时发现DNS欺骗攻击。

(9)DNS回复报文过滤

这种方法主要是为了对设备收到的回复报文进行检测，然后按照指定的规则进行过滤。如果应答中的IP包括内网地址、特殊用途地址或者用户自定义地址，则将DNS解析结果中的这些IP地址进行过滤，保留正常地址，然后再对回复报文进行转发。如果解析结果中的所有IP都为非法地址，则将整个报文丢弃，这样就可以使含有非法地址的回复报文无法到达DNS服务器。

4.5 DNS Cache

代替DNS服务器进行回复，可以有效降低DNS服务器负荷。当遭到DNS离散攻击时，DNS请求报文首先匹配DNS Cache中的表项。如果命中则直接由DNS Cache回复这个请求，如果未命中，则需要上送DNS 服务器进行递归请求。由于DNS Cache已经回复了大多数DNS请求，倘若递归请求依然较大，则可能是攻击流量，对这些递归请求进行限速处理，以免DNS服务器受到影响。

通常情况下，DNS Cache模块会和DNS防护模块配合使用。首先通过DNS Cache对大多数常用请求进行回复，然后通过DNS防护模块对剩下的递归请求进行过滤。这样到达DNS服务器的流量就非常小，既可以保证用户的正常上网，又大大减轻了DNS服务器负担。

设备可以通过导入或者自学习方式填充DNS Cache表项，当前我们的DNS Cache表项可以达到200万。

4.6 利用DNS备份中心防护攻击

如果某个地区DNS服务器遭到攻击，我们可以将超过阈值的请求全部转发到备份中心，由备份中心代替DNS服务器应答请求。由于备份中心的性能非常高，完全可以处理大多数DNS攻击，避免了DNS服务器遭到攻击宕机的情况。即使当多个DNS服务器遭到攻击，也可以同时把流量引到备份中心进行处理，一个备份中心可以供很多DNS服务器共享资源，节省了建设成本。考虑到备份中心可能在同一时间收到很大的攻击流量，可以适当地在备份中心部署DNS防护设备协助防护。

4.7 DNS协议异常防护与漏洞防护

针对DNS欺骗和系统漏洞，最有效的方法是能够准确识别各种协议异常和攻击行为。

传统的攻击识别方式是通过定义攻击行为的特征来实现对已知攻击检测。这种方式实现简单，但是会导致误报较多，无法准确地识别攻击。

识别攻击最有效的方式是通过分析攻击产生原理，定义攻击类型的统一特征。这种方式不受攻击变种影响，有较高技术门槛，但是可以有效降低误报率。

专业的漏洞库应该为DNS服务提供“虚拟系统补丁”功能，即使DNS服务器未能及时更新补丁程序，仍然能有效地阻挡所有企图利用特定漏洞进行的攻击，可以在几分钟完成部署，保护DNS免遭攻击。

如对本文内容有任何观点或评论，请发E-mail至editor@ttm.com.cn。