完善域名安全防护 提供优质网络服务

刘守东　王晓峰
中国联合网络通信集团有限公司吉林省分公司

摘要　随着我国互联网业务迅猛发展，用户对网络服务的要求越来越高，域名服务是互联网最基本的网络服务之一，在互联网中几乎每个用户的每次访问都会使用到域名解析。域名系统的安全、解析的准确程度和响应速度是影响整个网络服务质量的重要因素。如何保证域名管理和解析安全、及时、准确，成为运营商最关注的问题之一。文中介绍了吉林联通域名解析系统的现状，阐述了如何完善域名系统安全防护，及时提供优质的网络服务。

关键词　域名系统 安全防护 网络服务

1 前言

随着我国互联网业务迅猛发展，用户对网络服务的要求越来越高，在互联网中几乎每个用户的每次访问都会使用到域名解析。2009年5月19日，黑客恶意攻击导致暴风影音DNS域名服务器工作异常，由于暴风影音客户端软件存在缺陷，导致安装该软件的上网终端频繁发起域名解析请求，引发运营商的递归域名解析DNS服务器拥塞和瘫痪，造成大面积的移动和固定互联网用户访问网站慢或打不开网页，影响范围波及我国东部数个经济发达省份。

域名解析的过程就是当应用过程需要将一个主机域名映射为IP地址时，调用域名解析函数，解析函数将待转换的域名放在DNS请求中，以UDP报文方式发给本地域名服务器。本地域名服务器查到域名后，将对应的IP地址放在应答报文中返回，同时还必须具有连向其他服务器的信息以支持不能解析时的转发。若域名服务器不能回答该请求，就暂成为DNS中的另一个客户，向根域名服务器发出请求解析，根域名服务器一定能找到下面的所有二级域名的域名服务器，以此类推，一直向下解析，直到查询到所请求的域名。

2 吉林联通域名系统现状

2.1 吉林联通DNS结构

吉林联通DNS域名系统分为DNS解析系统和DNS管理系统，其中，DNS解析系统包括授权DNS和Cache DNS。作为通信定级业务系统，DNS解析系统采用异地冗余/负载分担式部署，DNS管理系统为DNS解析系统的日常运维管理和监控平台。

2.2 DNS解析系统

2.2.1 授权DNS

授权DNS包括两台非递归DNS服务器,异地布置在长春和吉林节点。长春节点作为主域名服务器，吉林节点为辅助域名服务器，主域名服务器定期地把授权域的更新数据传送给辅助域名服务器。

授权DNS服务器前端均通过汇聚路由器的访问控制列表（ACL）实现系统的网络层安全防护。在系统服务层面，当主机服务进程异常时，后台监控程序自动重新启动BIND解析进程，保证服务的可用性。

授权DNS的服务对象为Internet上的Cache DNS服务器，当任一授权服务器发生故障或服务异常时，请求方会自动向另一台域名服务器发送解析请求。

2.2.2 Cache DNS

Cache DNS采用Anycast分布式组网方式，分为长春、吉林两个一级核心节点和四平、通化、延边州3个二级节点。每个核心节点的配置容量可以单独承载全省的流量；各地市节点正常情况下主要承载本城域网内用户的域名解析工作，出现故障的时候，可以自动实现节点间的切换。长春和吉林核心节点各有5台服务器，二级节点各有两台服务器。每个节点内服务器均双上联两台接入交换机，交换机再双上联省网或城域网路由器。交换机通过OSPF动态路由实现设备/链路的冗余。DNS主机之间通过Anycast机制实现负载分担和实时热备份。系统总解析能力满足3倍于任一节点访问量的要求，而且可满足未来2年的使用需求。

(1)节点服务策略

两个一级节点负责节点内和其他没有本地DNS节点的地市用户的服务，二级节点承担区内普通用户解析请求。外网用户流量只能到达两个一级节点，即在省网骨干路由器上，只能看到核心节点广播的DNS服务地址路由。

吉林联通现有的两个Cache DNS服务地址，按照服务器策略设计原则，二级节点发生故障时，由一级节点提供备份服务。两个一级节点之间为负载分担和冗余互备的关系，保证了DNS服务的连续性。

(2)节点路由策略

DNS服务器将服务地址作为Loopback地址配置到本地，同时运行动态路由软件，与接入交换机运行OSPF路由协议，将服务地址广播到DNS接入交换机。通过Anycast方式实现节点内的DNS服务的负载分担和冗余互备。

节点内DNS接入交换机与上联的城域网汇聚路由器运行OSPF路由协议，将服务地址广播到城域网汇聚路由器，城域网汇聚路由器通过重新分布，将服务地址广播至整个城域网内，对区内用户提供DNS服务。

DNS服务器上同时运行服务监控程序，定期检测系统服务状态，当服务器服务状态异常时，监控程序自动停止将服务地址广播到DNS接入交换机。DNS接入交换机收到停止服务地址广播的路由更新后，将该路由更新广播到上联的城域网汇聚路由器，并同步到整个城域网。

2.3 DNS网管系统

DNS网管系统主要针对DNS解析系统提供基本的管理功能，包括数据制作、性能监测、解析监控、重点域名拨测、报表管理、攻击监测等。

数据制作模块方便管理员对BIND配置文件、数据文件进行操作及数据下发。

性能监测包含对各台主机进程状态、性能、解析量的监测，监测间隔为5 min。

解析监控模块根据系统中的解析日志，生成域名及源IP排行榜，通过该功能可进行入侵企图分析，并形成报告。

报表管理模块包含主机性能报表、业务统计报表、解析时延报表等，根据报表内容每月由维护人员形成月报分析。

攻击监测模块对DNS服务器的flood攻击行为进行监测，包括防攻击模板配置及告警查询。目前防攻击模板配置的阈值为500Qps，超过阈值的IP来源将被列入ACL列表，屏蔽时间为1 min。

3 DNS安全防护

吉林联通按照工业和信息化部与中国联通集团的相关要求部署了各项安全防护策略。2010年8月进行了系统改造，改造后系统性能明显改善，稳定性和抗攻击能力均得到很大提升，各项安全防护指标已完全符合标准。

3.1 系统安全

按照规范的要求，将操作系统参数进行安全加固，并形成统一的模板。

(1)用户账号和口令限制

- 加锁与设备运行维护无关的默认系统账号，例如：daemon、bin、sys、lp等。
- 用户密码需大于8位，并且必须由大小写字母及非字母字符构成。
- 用户口令生存周期为90天，修改密码时不能与最近3次使用过的密码重复。

(2)用户登录限制

- 维护人员只能通过ssh2方式登录，用户登录需要鉴权。
- root用户不能远程直接登录，只能通过普通用户转换。
- 当5次输入密码失败后，失败记录到日志：/var/admn/sulog。

(3)对默认权限进行限制

修改umask值，给文件所有者读写权限，只给组成员和其他用户读权限。

(4)启用时钟同步功能

- 网管服务器与中国联通集团增值系统时钟服务器同步。
- 其他DNS服务器与网管服务器同步。

(5)关闭启动项中不需要的服务

• 关闭自启动服务：sendmail、lp、rpc、snmpdx、keyserv、nscd、volmgt、uucp、dmi、autoinstall。

• 关闭默认服务：ftp、telnet、smtp、finner等。

(6)设置屏幕保护时间为3 min，即3 min无交互自动退出

(7)禁止系统堆栈可执行

3.2 BIND软件安全设置

服务器均安装解析软件BIND9.6.1-p1版本。

在Named.conf文件中进行安全设置：

(1)配置域名黑名单，方便处理针对单域名的攻击。

(2)授权服务器禁止递归解析。

(3)缓存服务器关闭数据传输功能。

(4)缓存服务器只为本省用户提供递归服务，最大递归解析数限定为10万。

3.3 网络设备安全

(1)交换机启用Tacacs认证授权，所有登录用户和口令由Tacacs服务器统一管理，并进行命令授权和审计。

(2)交换机均开启了访问控制功能，只开放53端口提供域名解析服务，除此之外不提供其他服务。

(3)启用登录访问控制，只有授权的维护终端可以登录，对维护终端的IP地址与MAC地址进行了绑定，预防地址欺骗。

3.4 网管安全防护系统

(1)切换管理模块

如果DNS发生网络中断，Anycast软件将捕获到这类故障并自动切换。

若DNS进程出现异常，Anycast软件不能处理这种故障。DNS管理系统的切换管理模块，会定期轮巡DNS进程和解析是否正常，如果检测到异常，则关闭本地DNS的路由，主动将解析切换到别的分系统，并将告警信息发送给管理系统的故障管理模块及维护人员。该功能可以保障DNS业务的可用性。

(2)模拟拨测模块

模拟拨测模块提供重点域名的监控功能。管理员预先设定好重保域名及IP地址。网管会定期将拨测的解析结果与配置的基准结果进行比较，如果一致则认为正常，如果不一致则还会再比较授权DNS的解析结果；如果与授权的也不一致，则清空Cache并产生告警信息；如果与授权的一致但与配置基准结果不一致，则可能是基准配置有问题，发出轻微告警。该功能能方便管理员及时处理系统隐患，避免重保域名被劫持，保证重保网站的安全运行。

(3)防攻击监控模块

防攻击监控模块可以实现针对DNS服务器的DDOS攻击防护。

基于源IP的防攻击模块，可以预先设置查询阈值，现设置阈值为500Qps，对超出阈值的查询视为flood攻击，形成告警记录的同时将攻击源自动阻断1 min。在源IP的请求量正常后，再允许其访问请求。

基于解析域名的DNS防攻击模块，可以解决类似暴风影音的单域名解析故障。监控模块监测主机的CPU性能指标，并结合对域名解析量和失败量的分析，将超出门限的域名加入黑名单。当域名解析恢复时，会自动删除黑名单。

3.5 日志管理

服务器和交换机均开启了日志功能，包括用户登录访问日志、维护日志、状态监测日志和故障告警日志。每月对日志进行审计分析，以便发现安全隐患。在安全事件发生后，可根据日志提供的信息进行定位。

3.6 漏洞评估制度

根据漏洞评估制度，每月检查服务器操作系统及应用软件版本，进行漏洞检测，打补丁或升级软件版本时需要提出申请，并且在升级后形成记录表。另外每月检测维护人员使用的主机操作系统，检查安装防火墙和杀毒软件、病毒库更新情况，并形成相关报表。

3.7 备份与恢复

在多个地市缓存DNS中布置了节点，实现了异地全业务热备份。服务器本身都具备双电源、双网卡，磁盘作RAID1全镜像。每台服务器双上联两台交换机，为系统提供了安全保障。

当本地授权域名分别授权两台服务器时，任一授权服务器发生故障或服务异常时，请求方会自动向另一台域名服务器发送解析请求，对用户解析注册域名没有影响。两台服务器在结构上均属于单点，因此授权系统的应急恢复采用冷备份恢复的方式。长春和吉林节点各有一台服务器，用作冷备份服务器。当授权服务器硬件出现故障时，使用冷备份服务器作为临时替代服务器，配置成故障服务器的IP地址，即可恢复服务。

根据数据备份规定要求，每10 min对解析日志进行备份，每天对BIND配置文件、数据文件进行备份，每个月对解析软件、监控数据进行备份，备份文件保存在异地专用的备份存储介质上，保存周期为3个月。当服务器出现故障时，可利用备份文件快速恢复系统及数据。

4 结束语

通过完善域名系统的安全防护措施，并定期组织有针对性的域名系统安全应急演练，吉林联通已经将域名系统的人为安全隐患降至最低，可保障系统的安全稳定运行，为用户提供优质的服务。ttm

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