网络优先数字出版时间:2014-2-18
网络优先数字出版地址:http://www.cnki.net/kcms/detail/45.1075.N.20140218.1416.002.html
广西科学院学报 2014,30(1):16~20
Journal of Guangxi Academy of Sciences Vol.30,No.1 February 2014

基于安全可靠的 DNS 系统构建
Constructing DNS System Based on Safety and Reliability

李 森,文 静
LI Sen,WEN Jing

(广西经济信息中心,广西南宁 530022)
(Guangxi Economic Information Center,Nanning,Guangxi,530022,China)

摘要:【目的】研究如何将策略路由技术应用到 DNS 系统的构建上,提出一种构建安全可靠的 DNS 系统的方法。**【方法】**从网络安全构架、系统安全和 BIND 安全等多方面,系统阐述如何增强 DNS 的安全可靠性,并将策略路由技术应用到 DNS 的构建上。**【结果】**提出一种构建安全可靠 DNS 系统的方法,在国际互联网双出口的网络环境下,策略路由技术由网络中的路由器和 DNS 服务器协同完成,可实现出口链路冗余及优化访问路径、DNS 解析业务冗余等功能。**【结论】**该方法可以解决 DNS 系统面临的安全威胁,提高 DNS 系统的可靠性,特别是策略路由技术的应用,在保证可靠性的基础上还优化了网络性能。

关键词:域名系统(DNS) BIND 策略路由
中图分类号:TP138 **文献标识码:**A **文章编号:**1002-7378(2014)01-0016-05

Abstract:【Objective】The application of Policy-Based Routing to DNS system construction is studied and the method of constructing safe and reliable DNS system is illustrated. **【Method】**From the network security, system security and BIND security aspects, the enhancement on the security and reliability of DNS is stated, and Policy-Based Routing technology is applied to the DNS construction. **【Result】**A method for constructing safe and reliable DNS system is illustrated. In the double ISP network environment, Policy-Based Routing is accomplished by cooperation of the router and DNS server, which can realize the function of Internet link redundancy, path optimization and domain name resolution redundancy. **【Conclusion】**The method can solve the security threats faced by DNS system and improve the reliability of the DNS system. Especially, the application of Policy-Based Routing can ensure the reliability and optimize the network performance.

Key words:domain name system(DNS),BIND,policy-based routing

【研究意义】域名系统(Domain Name System,DNS)用于 Internet 等 TCP/IP 网络中,通过用户的名称查找计算机和服务,当用户在应用程序中输入 DNS 名称时,DNS 服务器可以将此名称解析为与之对应的 IP 地址等信息。DNS 是网络应用最重要的基础平台之一,DNS 服务器一旦发生故障,网络将会瘫痪。建设安全、可靠的 DNS 系统是网络应用正常运行、发展的牢固基石。**【前人研究进展】**网络安全构架、系统安全、BIND(Berkeley Internet Name Domain)安全及策略路由技术都是成熟的技术和常见的应用,网络安全构架需要考虑和体现国家标准信息系统安全等级保护的要求[1];UNIX 操作系统本身存在不少安全漏洞,需要扬长避短;BIND 是最流行的 DNS 系统,灵活应用 BIND 本身的安全机制非常重要;策略路由可以使数据包按照用户指定的策略进行转发,可应用于某些路由必须经过特定的路径的管理目的[2]。**【本研究切入点】**目前,尚未见将网络环境、系统安全、应用安全及策略路由技术结合并应用到 DNS 上的报道。**【拟解决的关键问题】**本文简要介绍 DNS 存在的安全问题,从网络安全构架、系统安全和 BIND 安全等多方面系统阐述了如

收稿日期:2013-12-01
修回日期:2013-12-15
作者简介:李 森(1981-),男,工程师,主要从事计算机网络与信息安全研究。

何增强 DNS 的安全可靠性,研究如何将策略路由技术应用到 DNS 的构建上,从而在类 UNIX 系统下建立安全、可靠、灵活的域名服务体系。

1　DNS 的安全问题

现在绝大部分的 DNS 服务器均使用 BIND 系统。BIND 是一款开放源码的 DNS 服务器软件,由美国加州大学 Berkeley 分校开发,现由 ISC 机构维护[3]。常见的 DNS 安全问题有以下几种:

(1)DNS 规划和部署不当。主要体现在未能合理划分用户群,针对不同的用户群授予不同的访问权限等。

(2)单点故障。包括 DNS 服务器、网络关键设备、网络链路、网络出口等各方面的单点故障。

(3)DNS 恶意攻击。主要包括 DNS 欺骗和分布式拒绝服务(DDoS)攻击等。DNS 欺骗存在 DNS 劫持、DNS 重定向、DNS 缓存投毒等问题。分布式拒绝服务(DDoS)攻击是 DNS 面对的头号安全问题,该攻击容易阻塞 DNS 服务器的出口带宽,从而使 DNS 无法响应正常用户的请求。

(4)操作系统安全。DNS 服务器通常采用 UNIX/LINUX 操作系统,这些操作系统不可避免地存在安全漏洞,一旦非授权用户非法进入 DNS 服务器操作系统,就可以任意修改 DNS 配置文件,造成严重后果。

(5)BIND 配置不当。BIND 功能强大,配置灵活,如不能熟悉掌握并合理配置,不但不能充分发挥软件的性能,还会给网络攻击者留下安全漏洞。

(6)BIND 软件未及时更新。及时升级 BIND 版本和安装安全更新很重要,因为安全更新往往是针对安全漏洞发布的,更新版本的功能和性能都会有重大改进,长期不更新软件容易给攻击者可乘之机。

2　安全可靠的 DNS 系统的构建

针对 DNS 存在的安全问题,提出一系列增强系统可靠性、安全性的措施。从网络安全构架、操作系统安全和 BIND 安全等多方面加强安全防护,辅以持续的监控管理机制,从而建立安全可靠的 DNS 系统。另外,根据经验提出将策略路由技术应用到 DNS 构建上,以增强 DNS 的性能。

2.1　网络安全

网络安全构架为 DNS 提供安全可靠的网络环境,这是 DNS 安全防护的基础。网络安全构架在网络的可靠性和网络的安全防护两方面保障系统的安全。其中,网络的可靠性通过互联网出口冗余、关键设备冗余、链路冗余等多方面实现;网络的安全防护通过防火墙技术、入侵检测和防御技术、DDoS 攻击防护技术等实现。一般来说,在大型的网络环境中,网络安全构架基本得到保证。DNS 的网络安全构架[1]如图 1 所示。

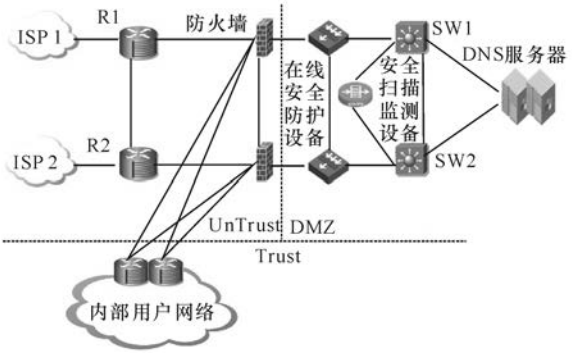

图 1　网络构架

2.2　操作系统安全

DNS 可建立在类 UNIX 系统上,这里选择用 FreeBSD 操作系统实现。FreeBSD 相对其他类 UNIX 系统的主要特点是系统稳定、网络性能更好、内存使用机制优秀,更适合于构架 DNS。

操作系统的安全通过如下的方法实现:安装最新稳定版本的操作系统,选择文本界面的最小化安装,关闭不需要开放的服务和端口,通过防火墙技术限制访问,安装需要的补丁等等。

2.3　BIND 安全

首先要选择安装最新、最稳定版本的 BIND。另外,可通过以下方式设置增强 BIND 安全。

(1)以最小权限运行 BIND。避免以超级用户的身份运行 BIND。在 UNIX 服务器中,可以用“-u”选项指定运行名字服务器进程的用户,赋予该用户完成 DNS 工作所需的最少权限。这样,即使有攻击者通过名字服务器闯进系统,也不可能获得超级用户的权限。具体操作时要使用 touch 或 chown 功能改变 BIND 进行读写操作的文件。

也可以用“-t”选项让 BIND 运行在指定的环境中(chroot( )),这种方法可以提高系统的安全性,使系统遭到破坏时降低损失。该功能也称为“沙箱”。

(2)使用访问控制列表。访问控制列表(ACL)是地址的匹配列表,使用访问控制列表可以使配置简单而清晰,首次定义之后可以在后续的 allow-notify, allow-query, allow-recursion, blackhole, allow-transfer 等配置中使用。使用 ACL 可以对访问域名服务器的用户实施良好的控制,而不会使配置文件因为

大量的 IP 地址而变得混乱。例如,ACL 表中的 bogusnets 列表和 blackhole 语句可以防止用户对域名服务器的欺骗和 DDoS 攻击,具体的用法如下:

```
    acl bogusnets {
    0.0.0.0/8;  10.0.0.0/8;  172.16.0.0/12;
};
options {
    … …
    blackhole { bogusnets; };
    … …
}
```

(3)限制查询。根据 IP 地址创建访问列表。访问列表可以应用于特定的区,也可以应用于服务器收到的任何查询,通过这些访问列表,可以指定允许哪些 IP 地址向名字服务器发送查询。利用这一特性,根据需要对不同用户隐藏域名空间中的特定部分,但对一些特殊用户开放。限制所有查询的配置如下:

```
    options {
    … …
    allow-query { address_match_list; };
    … …
}
```

限制特定区的查询的配置如下:

```
zone "example.com" {
   type master;
   file "example.com";
   allow-query { address_match_list; };
}
```

(4)限制区文件传送。主辅 DNS 的一致性要求一旦主域名服务器的内容有变化,就需将新的域文件传到辅服务器,BIND 默认配置是允许所有 IP 地址进行区文件传送,显然,这给攻击者提供了机会,可以通过 nslookup、dig 等工具获取所有区的数据。

限制区文件传送可以利用 BIND 提供的 allow-transfer,因为 allow-transfer 作为 zone 的子语句,可以限制某个特定区的传送,作为 options 的子语句,则可以限制所有的区传送。全局方式的区文件传送有时并不需要,它会增加不必要的传输数据量和时间,特别是对大型 DNS 系统。此外,辅域名服务器也要限制区文件传送,否则,攻击者可以轻易地从辅域名服务器获得区的数据。

实现限制所有区的传送的语句格式如下:

```
    options {
    … …
allow-transfer { address_match_list;/IP 地址; };
    … …
}
```

实现限制特定区的传送的语句格式如下:

```
    zone "example.com" {
   type master;
   file "example.com";
   allow-transfer { address_match_list; /IP 地址; };
}
```

实现限制辅域名服务器区的传送的语句格式如下:

```
    options {
   … …
   allow-transfer { none; };
   … …
}
```

(5)分离 DNS。域名服务器实际上有 2 个主要功能:回答来自远程域名服务器的反复查询和回答来自本地解析器的递归查询。前者对应“为 Internet 用户访问内部服务器提供域名解析”服务,此时,该域名服务器是内部服务器名字解析的“授权”域名服务器,它只需回答来自其他域名服务器的查询,可以关闭它的递归查询,防止 DNS 欺骗攻击。后者一般称为“解析”域名服务器,将它开放给内网可信用户或 forwarding 主机,允许递归查询。

分离 DNS 就是在一台 DNS 服务器上实现“授权”域名服务器和“解析”域名服务器,可以满足用户在 Internet 上与内网上对同一服务器公布不同的区数据的要求。

分离 DNS 借助访问控制列表、视图(view)和 recursion 语句实现:

```
    view "internal" {
  match-clients {our-nets; };  // 匹配内网客户的访问
  recursion yes;  // 对内网客户允许执行递归查询
  zone "example.com" {  // 定义内网客户可见的区声明
       type master;
       file "example.com.hosts.internal";
   }
}

   view "external" {
```

```
    match-clients { any; };    // 匹配 Internet 客户的访问
    recursion no;    // 对 Internet 客户不允许执行递归查询
    zone "example.com" {// 定义 Internet 客户可见的区声明
        type master;
        file "example.com.hosts.external";
    }
}
```

(6)TSIG 与 DNSSEC。TSIG 称为“事务签名”(transaction sigature),是一种保护 DNS 消息的机制,通过共享密钥方式对通信双方进行认证。BIND 主要支持服务器对服务器之间通信的 TSIG,可以利用 TSIG 保护域传送(zone transfer)、通报(notify)、递归查询信息和动态更新。

更强的可靠域名服务是应用 DNS 安全扩展(DNSSEC),它用数字签名的方法确保 DNS 内部信息的安全,并在提供权限认证功能的同时保证信息的完整。它同时使用非对称与对称式的加密模式对资源记录(RR)和区域传输模式分别进行处理。理论上,DNSSEC 是可靠的域名建立和解析方法,对防止域名欺骗等攻击行为是有效的。但是由于 DNSSEC 的复杂性、配置的繁琐和性能的羸弱,DNSSEC 并未得到广泛应用。

2.4　DNS 监控及管理

DNS 的安全问题没有一劳永逸的解决方案,不存在某个措施可以将威胁完全消除,需要做一系列工作来持续提供保护。同时,需要在日常使用中不松懈地进行监控和管理。监控和管理对象包括但不限于:实时监控 DNS 防护设备,分析其日志报告;使用 PF 防火墙观察 DNS 服务器连接状况;使用 ifstat 工具观察 DNS 服务器网卡流量;使用 rndc 工具,统计分析域名解析情况;对 DNS 服务器日志进行备份和分析;定期更新系统和 DNS 软件补丁,加固系统安全;定期对 DNS 系统进行安全评估等。

2.5　策略路由技术

策略路由一般应用在网络中,可以使数据包按照用户指定的策略进行转发。本研究的策略路由技术由网络中的路由器和 DNS 服务器协同完成。下面结合具体网络环境(如图 2 所示)阐述策略路由技术在 DNS 系统上的构建方法。

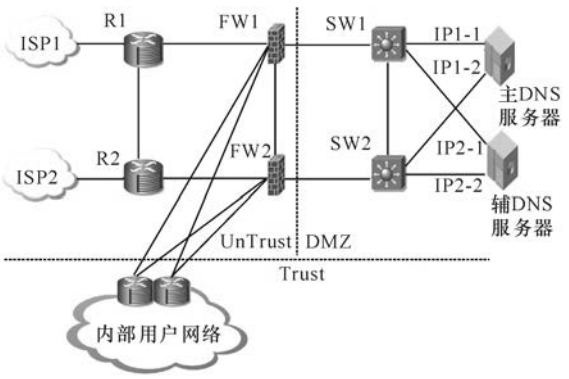

图 2　DNS 部署网络示意图

如图 2 所示,网络结构为全冗余方式,任一互联网出口、链路或设备发生意外都可以避免单点故障。其中,SW1 和 SW2 使用堆叠方式(2 台交换机虚拟为 1 台逻辑交换机)部署;主辅 DNS 服务器均为双网卡,分别同时接入 SW1 和 SW2,设置 IP1-1 为对应 ISP1 互联网出口的 IP 地址段,设置 IP2-1 为对应 ISP2 互联网出口的 IP 地址段,设置 IP1-2 和 IP2-2 为面向内部用户访问的同一个 IP 地址段。

(1)路由器上的策略路由。通过配置路由器上的策略路由和 NAT,将主 DNS 服务器的 IP1-1 映射为 ISP1 的公网地址,将辅 DNS 服务器的 IP2-1 映射为 ISP2 的公网地址,可以实现主、辅 DNS 服务器分别走不同电信运营商(ISP)互联网出口,避免单点故障。

(2)DNS 服务器上的策略路由。这里以支持 PF 防火墙的操作系统,包括 FREEBSD/ OPENBSD/ NETBSD 等为例子,实现 DNS 服务器上的策略路由。

通过应用 PF 策略路由技术,改变 DNS 服务器上双网卡默认数据串流的工作方式,实现数据从哪里流进(请求),从哪里流出(响应),保证了双网卡独立工作,即内网用户和互联网用户各自通过不同网卡,走不同的路由访问 DNS 服务器,这样起到 2 个作用:第一,实现路由隔离作用,增强系统安全性;第二,两台 DNS 服务器总共有 2 块内网网卡和 2 块外网网卡,配合使用 DHCP 地址分发和路由器策略路由功能(包括路由器上和 DNS 服务器上设置的策略路由)后,实现 DNS 业务的高度冗余,即任一互联网出口链路,任何一台 DNS 服务器,任何一块网卡发生故障都不会影响内外网的 DNS 解析服务,从而大大提高 DNS 的可靠性。另外,还可以应用 PF 防火墙技术,增强对内部用户的安全防护,即通过设置 PF 使 DNS 服务器只对用户开放域名解析 53 端口,仅信任管理网络的几个管理端口(如 22 端口),阻

断来自非可信域的端口扫描或者 DDOS 攻击和入侵,进一步提高 DNS 系统的安全性。

以图 2 的主 DNS 服务器为例,PF 策略路由技术实现的关键语句如下:

```
int_if = "bce0"
ext_if = "bce1"
int_gw="IP1-2"
ext_gw="IP1-1"
pass in quick on $int_if reply-to ( $int_if $int_gw)
proto {tcp,udp} to any port 53 keep state
pass in quick on $ext_if reply-to ( $ext_if $ext_
gw) proto {tcp,udp} to any port 53 keep state
```

3 结束语

DNS 在网络应用中具有重要作用,确保 DNS 的正常运转和安全可靠具有重大意义。本文针对常见的 DNS 的安全问题进行分析,提出了构建安全可靠 DNS 系统的一些方法和途径。这些方法适用于任何中大型企业以及组织机构的应用环境,并可根据各自的具体情况以较为低廉、合理的成本建设安全可靠的 DNS 系统。

广西互联网络中心的域名系统按照本文所阐述的技术进行构建,已经成功稳定运行数十年,为各级政务部门应用提供免费域名解析服务,同时为广西互联网络中心约 5 000 名用户访问互联网提供域名解析服务。事实验证,将策略路由技术应用到 DNS 构建上,具有零投资而效果显著的特点,值得推广应用。

参考文献:

[1] 李森,李陶深,洪茹. 电子政务网络安全防护体系构建[J]. 广西科学院学报,2009,25(04):350-352.

[2] 廖淑华,钟怀蓉. 策略路由技术在城域网中的应用[J]. 农业网络信息,2010,4:87-91.

[3] Paul Albitz,Cricket Liu. DNS 与 BIND[M]. 雷迎春,龚弈力,译. 北京:中国电力出版社,2002:20-21.

(责任编辑:尹 闯)

广西苦苣苔科植物杂交品种获国际认证

新闻时间:2013-12-31

近日,广西植物研究所温放博士和韦毅刚研究员历时 3 年培育的苦苣苔科报春苣苔属植物两个种间杂交品种“紫月”Primulina “Purple Moon”和“古铜小伙”Primulina “Tan Boy”喜获国际苦苣苔科植物新品种登录权威认证机构——世界苦苣苔科植物协会(The Gesneriad Soceity)授予的认证证书,其品种名已经获得了国际认证。其中,新品种“古铜小伙”得到了认证证书签署负责人 Irina Nicholson 博士的高度评价,她在邮件中写道:“‘古铜小伙’这一新品种的花色如此特别、华丽灿烂,我非常荣幸能为它进行登录,这是极不寻常的成果,你们育成的杂交品种是如此让人震惊! 她实现了苦苣苔花卉爱好者的梦想!”

这两个杂交品种是中国大陆地区育成的苦苣苔科植物新品种首次获得国际植物新品种登录证书,表明植物所在培育具有自主知识产权的苦苣苔科植物新品种方面迈出了可喜的一步,为今后深入开展这方面的育种工作奠定了扎实的基础。这对提升植物所在苦苣苔科植物育种、开发和保育方面的研究的国际地位,以及推动广西乃至我国苦苣苔科植物观赏园艺化、产业化方面具有重要的意义。

(摘自广西植物研究所网页)