proxy\_arp实验

Linux 2.4内核下的代理ARP和透明防火墙   
  
一: 操作环境   
  
Redhat 7.X, iptables, iproute2   
  
  
二: 为什么需要Proxy ARP?   
  
目前而言，为了添加防火墙，重新布署网络结构主要有如下方法：   
  
a. 防火墙两端分别使用真实地址和私有地址，用NAT或者端口转发实现对外服务，缺点是不能支持所有协议。   
b. 把现有从ISP得到的IP地址分段成两个子网在防火墙两端使用，缺点是需要更改服务器默认网关及子网掩码等设置   
c. 用代理ARP技术构建透明防火墙，可以Linux 2.4内核中轻易实现，它能保持现有的IP地址、 网关和子网掩码设置，加上使用真实IP地址，所以支持所有协议。   
  
三: 典型应用图例   
  
下面我们来考虑一个典型的小型企业网络环境：   
  
1> 公司有专线连结互联网，为了保护DMZ区内的服务器，我们想架设一台防火墙直接连接路由器，下面再连结所有向外提供服务的各种WEB,Mail,DNS服务器,如下图：   
  
  
                            Internet   
  
                                |   
  
                                | DDN   
  
                            \_\_\_\_|\_\_\_\_   
  
                           |  Router |   
  
                           |\_\_\_\_\_\_\_\_\_|e0: a.b.c.1   
  
                                |                
  
                              \_\_|\_\_ eth0: a.b.c.2                                 
  
                             |     |   
  
                             |  F  | 用Proxy ARP技术的透明防火墙 (gw: a.b.c.1)   
  
                             |\_\_\_\_\_|   
  
                                |   eth1: a.b.c.2 (两边可以用同一个IP，节省IP地址)   
  
                                |   
  
                   \_\_\_\_\_\_\_\_\_\_\_\_\_|\_\_\_\_\_\_\_\_\_\_\_\_   
  
                  |                 |        |           
  
                \_\_|\_\_              \_|\_      \_|\_   
  
     mail relay|  A  |ip:a.b.c.3  | B |    | C |   
  
     web proxy |     |gw:a.b.c.1  |\_\_\_|    |\_\_\_|   
  
               |\_\_\_\_\_|             WEB      DNS   
  
                  |             ip:a.b.c.4  IP:a.b.c.5   
  
\_\_ Intranet\_\_\_\_\_ \_|             gw:a.b.c.1  gw:a.b.c.1    
  
  192.168.1.0/24  |   
  
                \_\_|\_\_   
  
               |  D  |   
  
               |Mail |    
  
               |\_\_\_\_\_|   
  
  
注：   
1. 一台防火墙F保护整个DMZ区和内部网络，两边可以用同一个IP地址a.b.c.2 。   
2. 透明防火墙F两边在同一网段，且被保护的机器的IP和网关设置与同没有透明防火墙时一样，对被保护的服务器和外部用户而言都是透明的。当拿掉防火墙F时整个网络仍然能工作。   
3. 服务器A连结内部网络作代理服务器共享上网，且配置Sendmail为内部网上的邮件服务器D作邮件relay。   
4. 服务器A也可以直接连接到Router，和服务器F一样，这样要单独为服务器A设置防火墙规则。   
5. 如果只有服务器F连接路由器，则只需用一个交叉电缆连结即可，不用HUB或者Switch 。   
6. 你也可以合并A到F中，这样需要在F上有三块网卡同时连结DMZ和内部网络。   
  
四: 如何设置Proxy ARP?   
  
Redhat 7.2已经带有iproute2，用 #ip route命令而不是以前用的#route命令   
假定从ISP得到的IP地址为a.b.c.0/28 即可有a.b.c.0-15 共16个IP可用，但a.b.c.0(网络地址)和a.b.c.15(广播地址)不可用，故实际可用IP为a.b.c.1-14共14个IP地址。   
  
a. 安装时先设置eth0和eth1的IP地址都是a.b.c.2，且默认网关为a.b.c.1 。   
b. 启动后运行下面的命令或者放入/etc/rc.d/rc.local   
ip route del a.b.c.0/28 dev eth0   
  
ip route add a.b.c.1 dev eth0   
  
echo 1 > /proc/sys/net/ipv4/conf/eth0/proxy\_arp   
echo 1 > /proc/sys/net/ipv4/conf/eth1/proxy\_arp   
  
echo 1 > /proc/sys/net/ipv4/ip\_forward   
  
  
最后当你运行ip route命令时你应该看到类似下面的输出。   
  
a.b.c.1 dev eth0 scope link   
a.b.c.0/28 dev eth1 proto kernel scope link src a.b.c.2   
127.0.0.0/8 dev lo scope link   
default via a.b.c.1 dev eth0   
  
c. 我从防火墙F ping DMZ区的所有机器和路由器，再确保你能从web,DNS上能够ping路由器，   
如果你是后来添加的透明防火墙，你可能要等一段长的时间让路由器知道现在你在用代理ARP，   
最终路由器会清除自身的ARP cache的，如果可能，关掉路由器电源再打开以使更快地清除ARP cache.   
  
d. 不同的Linux 内核响应新的ARP cache的时间不同，用Linux 2.4内核比较快。   
  
e. 当然你也可以在透明防火墙F两端用不同的IP地址。   
  
  
五: 其它应用   
  
  
下面是另一种情况的代理ARP应用。   
  
在公司局域网上，有两台数据库服务器你需要单独保护，你可以添加一个透明防火墙，同样不需要改动任何现有的IP地址设置，类似上面的道理，如下图。   
  
  
  
  
        ip:192.168.1.201   
  
  
  
        gw:192.168.1.1   
  
  
  
        | database1 |         \_\_\_\_                  \_\_\_   
  
              |\_\_\_\_\_\_\_\_\_\_eth1| F2 |eth0\_\_\_\_\_\_\_\_\_\_\_\_|F1 | 公司防火墙      
  
              |              |\_\_\_\_|                |\_\_\_| 192.168.1.1   
  
        | database2 |   内部代理ARP防火墙   
  
  
  
       ip:192.168.1.202   
  
       gw:192.168.1.1   
  
  
  
  
设置步骤如下：   
1. 为F2两端设置相同的IP为192.168.1.200,默认网关为192.168.1.1   
  
2. 启动后运行   
ip route del 192.168.1.0/24 dev eth1   
  
ip route add 192.168.1.201 dev eth1   
ip route add 192.168.1.202 dev eth1   
  
echo 1 > /proc/sys/net/ipv4/conf/eth0/proxy\_arp   
echo 1 > /proc/sys/net/ipv4/conf/eth1/proxy\_arp   
  
echo 1 > /proc/sys/net/ipv4/ip\_forward   
  
3. 保证从database服务器能ping通代理ARP防火墙另一端的服务器，然后开始在F2上设置具体的防火墙规则。

在windows系统中有如下结论：   
  
总结：   
主机不设默认网关－－－－从不向本网段外的地址arp请求，不会发生代理arp   
  
主机设本网段其他地址为网关－－－－－－如果目的是非本网段地址，则向所设 的网关arp请求不会发生代理arp   
  
主机将网关设为非本网段地址－－－－－－－－向外网发包时，会arp请求所设网关的mac，如果此时真网关开启代理arp，代理就会发生   
  
主机将网关设为自己－－－－－－－－可以对任何地址（你的目的地址，不管是多少）发arp请求，如果真网关开启代理arp，代理就会发生。