浅析在 ISG 1000如何实现策略路由

◆ 李宝军

摘要：策略路由可用于园区内有多条互联网出口的拓扑环境，充分利用现有设备的性能，根据不同源地址和不同目的地址将流量转发至相应接口，从而实现流量筛选转发的目的。

关键词：策略路由；PBR(Policy-Based Routing)

一、拓扑环境现状

根据神华宁煤集团的统一部署，集团公司的互联网出口仅对煤化工公司内部用户提供服务，对于在煤化工园区内办公的上海金山物流有限公司（以下简称金山物流公司）等外单位并不提供服务。上海金山物流有限公司作为煤化工公司的物流合作单位，在煤化工园区内分布广，在多个分厂内设有办公场所，与煤化工公司用户共用一个局域网。随着金山物流公司ERP业务的上线，需要全国各分公司通过互联网办理业务，更好地为煤化工公司提供服务。如果将所有办公场所接入互联网，需要租用多条互联网专线，不但重复建设，而且十分不经济，因此需要充分利用煤化工公司已经建成的局域网和网络设备，仅向中国移动公司（CMCC）申请一条10M互联网出口，与煤化工公司局域网边缘的ISG1000防火墙相连，在防火墙上实现对流量筛选转发，将金山物流公司用户的互联网流量转发至移动公司互联网出口，而同时保持金山物流用户对神华宁煤集团ERP系统（192.168.0.0/16）、上海AMEC公司CONVERO系统（10.160.0.0/16）的正常访问。

拓扑简图及流量转发方向如图1所示。

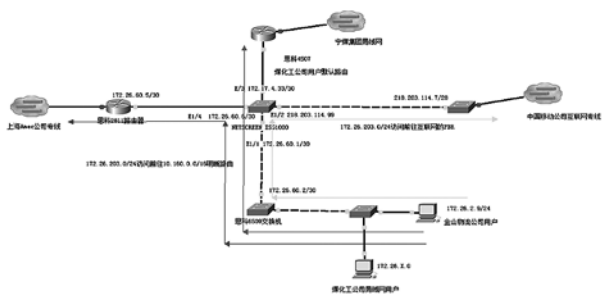

图1

二、策略路由（PBR）的应用分析

在ISG1000上有一条默认路由，用于煤化工公司内部用户通过神华宁煤集团局域网访问互联网。对于金山物流公司的用户来说无法通过该默认路由访问访问互联网，只能通过策略路由将互联网流量转发至E1/2出口。

一般情况下，PBR的优先级顺序是：

明晰路由>策略路由>默认路由

首先根据数据包中的目的地址去查找路由表中是否有最长匹配的明晰路由，如果没有，那么就去查找PBR，如果PBR中也没有，才会转发至默认路由所指向的E1/3接口。

然而ISG1000 ScreenOS中的路由条目转发的优先顺序却与以上顺序有所不同，具体如下：

策略路由>源端口路由>源地址路由>明晰路由>默认路由

可以看出PBR的优先级最高，因此只要符合PBR条件的路由都将被转发至PBR中设定的下一跳接口。

但新的问题产生了，如果将符合条件的源地址流量全部转发至互联网出口，那么金山物流公司的用户将无法访问连接ISG1000 E1/3接口所连的神华宁煤集团的EPR系统和E1/4接口所连的上海AMEC公司的CONVERO系统。

我们知道，策略路由可以根据扩展访问列表（Extended Accesslist）来结合匹配组（Match Group）和行为组（Action Group）设定的条件，将符合与扩展访问列表中源地址和目的地址匹配的流量转发至不同的出口方向，这就是我们解决以上流量转发问题的关键所在。

三、策略路由的实现方法

首先需要新建一个名称为CMCC的区域，在E1/2上设定相关属性，注意是Route模式，并划分到CMCC区域中。

```
set zone id 1000 "CMCC"
set interface ethernet1/2 ip 218.203.114.99/28
set interface ethernet1/2 route
set interface "ethernet1/2" zone "CMCC"
```

根据上面的流量转发方向分析，我们的基本思路已

经出来了，以IP 172.26.2.9的主机为测试地址，建三条访问列表，用于匹配不同的目的地址。

set access-list extended 1 src-ip 172.26.2.9/32 dst-ip 0.0.0.0/0 protocol any entry 1

set access-list extended 10 src-ip 172.26.2.9/32 dst-ip 192.168.0.0/16 protocol any entry 1

set access-list extended 10 src-ip 172.26.2.9/32 dst-ip 10.0.0.0/8protocol any entry 2

set access-list extended 20 src-ip 172.26.2.9/32 dst-ip 10.1.0.0/16 protocol any entry 1

set access-list extended 20 src-ip 172.26.2.9/32 dst-ip 10.2.0.0/16 protocol any entry 2

set access-list extended 20 src-ip 172.26.2.9/32 dst-ip 10.160.0.0/16 protocol any entry 3

建三个匹配组，与相应的访问列表相关联，再建三个行为组，并指定不同的数据转发出口。

set match-group name M-Amec

set match-group M-Amecext-acl 20 match-entry 1

set match-group name M-NCG

set match-group M-NCG ext-acl 10 match-entry 1

set match-group name M-CMCC

set match-group M-CMCC ext-acl 1 match-entry 1

set action-group name A-CMCC

set action-group A-CMCC next-hop 218.203.114.97 action-entry 1

set action-group name A-Amec

set action-group A-Amec next-hop 172.26.60.5 action-entry 1

set action-group name A-NCG

set action-group A-NCG next-hop 172.17.4.33 action-entry 1

建立一条名为：P-JinShanWuLiu的PBR，注意它有3条语句，每一条语句中匹配组和行为组之间的对应关系务必要一致，否则数据包的流向将不会按照我们期望的方向转发。

setpbr policy name P-JinShanWuLiu

setpbr policy P-JinShanWuLiu match-group M-Amec action-group A-Amec 1

setpbr policy P-JinShanWuLiu match-group M-NCG action-group A-NCG 2

setpbr policy P-JinShanWuLiu match-group M-CMCC action-group A-CMCC 3

另一个重点是这三条语句的顺序值得注意。为什么呢？我们回过头再来看一下刚才建立的访问列表：

在Extended Access list1的目的地址是任意地址，

图2

在Extended Access list 10的目的地址有一条10.0.0.0/8，在Extended Access list 20中的目的地址有一条10.160.0.0/16。

我们假设一下172.26.2.9的主机要访问上海Amec公司的Convero系统10.160.1.1/24的服务器。如果在P-JinShanWuLiu中按照1-10-20的顺序来匹配，首先匹配到Extended Access list 1，那么该数据包将会转发给E1/2接口的下一跳218.203.114.97，这显然不是我们想要的结果。如果按照10-1-20的顺序，首先匹配至Extended Access list 10，那么该数据包将会转发给E1/3接口的下一跳172.26.17.43，在神华宁煤集团公司局域网里显然也是找不到这台服务器的。如果按照20-10-1的顺序，首先匹配到Extended Access list 20，那么该数据包将会转发给E1/4接口的下一跳172.26.60.5，符合我们拓扑图中的描述，而访问互联网的流量会检查到 Ext-ACL 1才会匹配，这正是我们想要的结果。

下一步就是将建好的PBR条目与接口或区域绑定。根据PBR的原理，要把PBR策略应用在数据包的入向接口下。从拓扑图中看出，E1/1是连接煤化工公司局域网的接口，是172.26.2.9主机数据包向其他区域转发的入向接口，所以应用在该接口下。

set interface ethernet1/1 pbr P-JinShanWuLiu

最后一步，建立一个访问策略，否则上面的工作都还是徒劳，因为在默认条件下访问CMCC区域的流量都是被拒绝。因此新建一条从Trust到CMCC的访问策略，允许金山物流公司的主机地址可以访问CMCC区域，而其他主机则不允许访问，达到专线专享的目的，注意加上NAT源地址转换参数。

set policy id 29 from "Trust" to "CMCC" "172.26.2.9/32" "Any" "ANY" natsrc permit log

这是建成后的访问策略，可以点击日志查看是否有匹配的用户数据流量。

图3

（下转44页）

3.结语

通过对烟草行业近12年科技查新报告的统计分析，可以看出烟草行业科技查新有以下几个特点：

（1）查新委托项目基本呈逐年递增趋势，这在一定程度上体现了大环境下烟草行业重视科技创新，科技创新已经成为烟草行业发展进步的核心动力。

（2）查新委托单位主要以烟草行业内的单位为主，其他行业单位所占比例极小；烟草行业内单位所占比例从高到低依次为：各省级中烟工业公司（包括其下属的卷烟厂），烟草科研机构和省级局（省级烟草公司）；烟草机械公司与各大高校、烟叶公司及其他行业企业共同占据了剩余的部分。体现了烟草行业属于专业性较强的行业，各省级中烟工业公司是烟草行业生产实践的主力军。

（3）省级中烟工业公司查新委托项目量随年份呈较高幅度的增长，烟草科研机构查新委托项目数量随年份波动幅度呈较为平稳的缓慢上升趋势，体现了近年来中国烟草总公司高度重视科技创新工作，以科技创新带动行业发展。

（4）烟草化学、烟草工艺和烟草农业等类的查新委托项目自2004年以来有明显增长的趋势，说明烟草化学、烟草农业、烟草工艺作为烟草行业的主要研究方向，仍然是烟草行业主要的科技创新领域。

（5）烟草行业在烟草化学和烟草工艺方面，积极围绕减害降焦开展科研工作，充分体现了国家烟草专卖局自觉践行国家利益至上、消费者利益至上的“两个至上”行业共同价值观，积极履行烟草控制框架公约；同时，烟草行业生产企业和科研机构也对国家决策层面控烟做出了积极的正向反馈。在烟草农业方面，加强了对农药重金属残留的研究，体现出烟草行业非常重视食品安全，积极从源头上控制食品安全。

参考文献

[1]傅淑英.烟草科技查新咨询服务工作的回顾与展望[J]. 图书馆工作与研究,2001(6):47.

[2]程彪,付淑英,张仕华.烟草科技情报查新质量的保证和提高[J].黑龙江烟草,1999(8):23-24.

[3]程彪,高琳.加强情报查新工作、促进行业科技进步[J].烟草科技,1995(6):44-45.

[4]谢玉森.浅谈科技项目查新工作是科技管理的重要环节[J].河南烟草研究,1997(3):31-32.

（作者单位：中国烟草科技信息中心）

（上接36页）

四、结论测试

从172.26.2.9主机上分别测试一下三个方向的流量，根据下图的跟踪结果可以确认，数据包是按照预期

图4

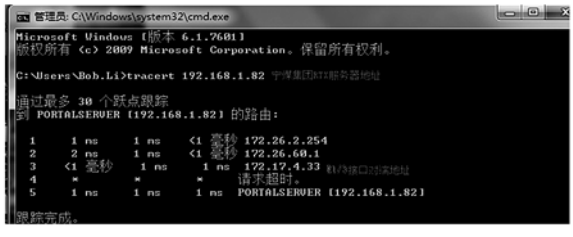

图5

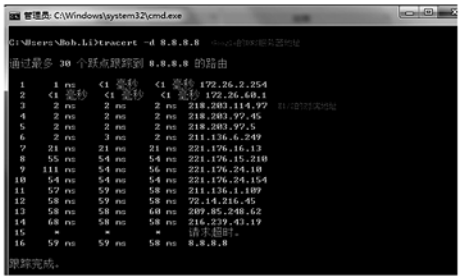

图6

方向进行了转发。

（作者单位：神华宁夏煤业集团煤炭化学工业分公司）