◎网络、通信、安全◎

IPv6 安全网关的配置函数模型研究

江 勇,胡松华
JIANG Yong,HU Song-hua

清华大学 深圳研究生院,广东 深圳 518055
Graduate School at Shenzhen,Tsinghua University,Shenzhen,Guangdong 518055,China
E-mail:jiangy@sz.tsinghua.edu.cn

JIANG Yong,HU Song-hua.Research on configuration function model of IPv6 security gateway.Computer Engineering and Applications,2008,44(17):85-89.

Abstract: A new kind of functional model in configuration of security gateway has been put out to solve the problem after carefully study of question.After the implement of the model and result checking,this model has the benefit of easy and safe to configure.The research will help implement and configure the commercial security gateway.

Key words: IPV6;security gateway;service group;machine group;function model

摘 要:研究安全网关配置特点后提出一种新的安全网关模型-函数模型,并在此基础上提出了函数模型 IPv6 安全网关策略配置的结构。通过系统的实现与实际运行结果比较分析,证明这种方法能够起到配置简单、安全、配置重复利用等特点。对 IPv6 安全网关系统设计具有借鉴作用,同时提出服务元、服务域、主机元、主机域的概念,对现有的安全网关图形界面开发,配置与维护具有很大的启示。

关键词:IPv6;安全网关;服务组;主机组;函数模型
DOI:10.3778/j.issn.1002-8331.2008.17.026 **文章编号**:1002-8331(2008)17-0085-05 **文献标识码**:A **中图分类号**:TP393

1 引言

最初的互联网是力图建立一个健壮的通信平台,没有其它方面的要求,而现在的网络技术的发展要能够跟上现实的需求就必须在安全、计费、控制方面进行改进。流分类的提出和研究流分类就是在这样的形势下出现的。目前在四层交换机、安全网关、QOS 控制、RSVP、VPN、计费路由器中都需要使用流分类的研究成果[2,10]。

对于安全网关的研究主要集中在如何实现高速,实现代价的, 同时支持快速更新和适用于不同网络的流分类查找系统。在这方面比较突出的有 RFC[10],ETCAM[11]等研究方案。在这个领域的研究时存在的一个问题就是没有实际系统的例子来进行算法优化与结果分析,很多国内外研究者解决问题的方案就是采取 CLASSBENCH 软件来产生模拟数据。因此对于如何配置安全网关,如何优化人工配置一直研究比较少。

目前商业软件采取得方法主要是 ACL 手工输入法, 网络划分命名法,服务命名法。ACL 手工输入法是最早的商业安全网关[13]的配置方法,在终端使用文本方式来输入逐条 ACL。这种方法的最大问题是没有重复利用性,配置不安全同时复杂程度高。网络划分命名法在 ACL 手工输入法的基础上,将一些常用的网络进行命名代替,在配置时候直接使用名字代替。该方法直观,实现简单,但是依然存在 ACL 手工输入法没有重复利用性,配置不安全同时复杂程度高的问题。服务命名法常常辅助以网络划分命名法,最后的配置形式是:网络服务名网络处理方式。该方法较大程度的减少了安全性,减少了配置时发生错误的可能性。

由于安全网关的配置需要实际系统中开发经验,使用经验的总结, 对于安全网关的配置研究主要是从实际系统中产生。许政穆等人在其嵌入式系统上实现的 All IPv6 SOHO router 中采取了这种方法[8],清华紫光比威网络技术公司自主研发的双 NP 架构的千兆防火墙也采用了这种方法。在这个方面的研究比较少。比较接近的有王卫平等人的防火墙规则配置错误分析及其检测算法[15]中针对容易出现的配置错误提出算法进行分析,和本文提出的算法在不同层面减少配置错误。文献[16,17]也进行了类似的研究,提出算法分析了防火墙规则之间的冲突情况。在一些商业系统和试验系统中都以服务命名法作为默认的方法进行设计与开发[21],相关研究都集中在设备机构,

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60503053);国家高技术研究发展计划(863)(the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z209);广东省科技公关计划(the Key Technologies R&D Program of Guangdong Province,China under Grant No.0711011500047)。

作者简介:江勇(1975-),男,博士,副教授,主要研究领域为计算机网络体系结构;胡松华(1979-),男,硕士,主要研究领域为安全网关体系结构。

收稿日期:2007-11-07 **修回日期**:2008-01-21

安全,流分类方面,而对于配置模型设计成果较少。

在这方面研究处于领先水平的是 BELL 实验室的 Yair Bartal 根据实际系统 Firmato 提出了一种 MDL 的模型定义语言[1],在配置时使用高级语言来描述防火墙系统,然后进行编译。通过对该算法的分析发现该算法的结果相比现有的商业防火墙系统来说从配置效率上来说具有十分明显得优势(在配置语句条数,配置的可读性方面),但是该算法也存在实现与运行复杂度高,配置不易移植等问题。

在安全网关的研发过程中,针对安全网关的特点,同时结合国内外先进研究技术,提出了一种函数模型安全网关配置方法,通过实际产品的测试、运行后表明本方法在主要性能上能够接近国际水平,同时具有实现与运行复杂度低,配置利于理解,易于移植的特点。

2 安全网关配置的描述与评价指标

安全网关是指设置在不同网络或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口,能根据企业的安全政策控制(允许、拒绝、监测)出入网络的信息流,且本身具有较强的抗攻击能力。它是提供信息安全服务,实现网络和信息安全的基础设施,有效地监控了内部网和 Internet 之间的任何活动,保证了内部网络的安全[14]。常见的安全网关结构如图 1 所示。

图 1 常见的安全网关结构

图例中,IntranetA、IntranetB、Printer、DataBackup 构成了一个可信任网络,DMZ(Demilitarized Zone)向外网提供例公共服务,外网包含合法站点 LegalSite 与非法的站点 IllegalSite。

安全网关的内部逻辑结构如图 2 所示,其中规则匹配是安全网关相比路由器的特点。本文研究方向是如何制定策略配置逻辑,如何将这些配置转化成相应的规则,然后对规则进行适当的优化,最后将规则导入查找子系统来完成配置者所要求的任务。

图 2 安全网关的内部逻辑结构

2.1 安全网关配置的描述

安全网关的配置就是要提供人机配置接口,将配置转化为实际的安全网关硬件系统能够识别的元组[9]。

令 $F=\{f_1,f_2,\cdots,f_n\}$表示安全网关的规则集,令 $O=\{o_1,o_2,\cdots,o_n\}$表示规则集对应的操作结果。

表 1 中给出了这些维的定义,其每个域支持的类型有 3 种,掩码匹配、范围匹配与精确匹配的其中一种或者多种。

表 1 维的定义

名称	定义	类型
I	IPv6 地址	掩码匹配
P	端口	范围匹配,精确匹配
Pc	协议	精确匹配
M	MAC 物理地址	精确匹配
G	接口	精确匹配

这个多维空间 V 的维依次是 I,I,P,P,Pc,M,M,G,G,分别表示源 IP 地址,目的 IP 地址,源端口,目的端口,协议,源MAC 地址,目的 MAC 地址,源接口与目的接口。那么 f_i 是这个多维空间 V 的一个区域。对于任意一个到达安全网关的数据包,安全网关检测各个值是否在 f_i 表示的这个多维空间区域里面,是的时候称为匹配,否的时候称为不匹配。安全网关的规则查找功能就是找到最先匹配的规则 f_i 并返回 o_i。

令 $E=\{e_1,e_2,\cdots,e_m\}$表示安全网关配置人员所看到的配置结果,令 $G_{i/j}$ 表示规则 $f_i,\cdots,f_j$ 所有可能组合的一个集合,令 $\widehat{e}_i$ 表示由规则 e_i 翻译生成的规则集。本文研究的问题是如何找到一个对应关系 $\forall e_i,\widehat{e}_i\subseteq G_{1/n}$,同时$\neg\ \exists f_i,f_i\not\subset\{\widehat{e}_1,\widehat{e}_2,\cdots,\widehat{e}_m\}$。

2.2 评价指标

评价安全网关配置的指标和其它网络安全设备系统配置的指标接近。文献[12]中作者 Michael Carney 等人对于算法模型实现的评价进行了研究,认为灵活性,安全性,实现复杂度,运行性能是主要的评价指标。其中实现复杂度,运行性能可以结合为复杂度的实现复杂度,运行复杂度。在结合安全网关系统的特点后,通常的性能评价指标如下所示。

(1)配置扩散指数 Di_{eff},配置收敛指数 Co_{eff}

配置扩散指数 $Di_{eff}=(\sum_1^m e_i)/m$,配置收敛指数 $Co_{eff}=(\sum_1^m \hat{e}_i)/n$,当 Di_{eff} 越大时,配置时的规则生成的规则较多,完成功能会相对较多。当 Co_{eff} 越大时,同时生成的结果数量也比较少能够减少规则的条数,减轻安全网关查找的负荷。

(2)配置重复利用性

类似函数的重复利用特性,当一个比较好的配置有某个配置人员完成后,是否能够简单其它安全网关的配置上面。

(3)配置安全性

是否能够以某种方式避免配置的错误。这一点在实际的配置过程中非常重要,一个错误的配置可能会导致整个网络的瘫痪,造成严重的后果。

(4)复杂度

是否能够方便的实现开发,程序的实现复杂度,运行复杂度。

3 安全网关配置函数模型

在本章中展示把函数的思想引入安全网关的配置。从介绍一些定义的术语出发,然后在 3.1 节与 3.2 节中介绍层次化安全网关配置的基本思想模型,实现细节。

3.1 术语

安全网关技术在许多设备中引入,例如个人机器,安全网

关,路由器中使用,而且相应的称呼差异也比较大。这里给出一些定义说明。

(1)安全网关:引入安全网关技术的机器。

(2)安全网关客户:数据流经过安全网关的机器。

(3)接口:接口是安全网关的网口的描述。在 Linux 系统中以 lo,eth0 的形式描述。在硬件设备中可能会以 gi0,gi1 的形式给出。

(4)MAC 地址:安全网关客户的 MAC 地址。

(5)IP 地址:安全网关客户的 IP 地址。

(6)主机元:一个最基本的接口,MAC 地址,IP 地址的组合,任何安全网关客户同时满足这三点,那么这个安全网关客户属于主机组。

(7)协议:安全网关客户流经过安全网关数据使用的协议号。

(8)端口:安全网关客户流经过安全网关数据使用的端口。

(9)服务元:一个基本的协议,端口的组合,任何安全网关客户流经过安全网关数据同时满足这两点,那么这个数据属于这个服务元。

3.2 模型结构

本文提出的基本模型是主机域和服务域,主机域拥有一些主机元特性和从其它主机域继承的特性。服务域拥有一些服务元特性和从其它服务域继承的特性。在图 3 中描述了整个系统的各个关系。在图 4 中介绍了配置模型的逻辑结构。

图 3　整个系统中各个定义的关系

图 4　配置逻辑结构

主机域能够从主机域继承下来的层次化特性符合现实思维特点。例如有一个主机域定义为办公大楼 A,那么楼内的公司主机域 B 一定继承 A 的特点,同时又拥有自己的特点。相应的服务域也是一样。不同的是服务域由一些主机域组成,这些主机域是作为参数的形式出现的。例如 DMZ 服务的参数可能会有内网,外网,DMZ 这些主机域作为参数传给它。这样做的目的是利用函数的特性来完成配置的重复利用。

3.3 模型定义与实现

在定义中使用 XML 格式来定义各种格式,同时按照图 1 介绍的安全网关的基本模型给出一些例子来介绍定义方法。

3.3.1 主机元的定义

主机元由接口名、MAC 地址和 IP 地址段或者 IP 地址组成,这些成员之间的关系是或的关系,即主机元:=G|M|I。其中任意一项都可以以"*"号的形式来描述,表示匹配任意。

```
<主机元名>
  <G>接口名
  <M>MAC 地址
  <I>IP 地址段或者 IP 地址
</主机元名>
```

表 2 描述了图 1 中部分安全网关主机元的定义。在以后的介绍中使用这些定义进行描述。

表 2　安全网关主机元的定义

<IntranetA> <G>eth0 <M>* <I>2001:210:3000:1::/64 </IntranetA>	<IntranetB> <G>eth0 <M>* <I>2001:210:3000:2::/64 </IntranetB>
<Printer> <G>eth0 <M>00-0F-1F-CA-6B-CF <I>2001:210:3000:3::1 </Printer>	<DataBackup> <G>eth0 <M>00-53-45-00-00-00 <I>2001:210:3000:3::2 </DataBackup>
<DMZ> <G>eth1 <M>0E-1A-00-BA-12-BA <I>2001:210:3000:4::/64 </DMZ>	<LegalSite> <G>eth2 <M>* <I>www.legal.com www.yahoo.com </LegalSite>
<IllegalSite> <G>eth2 <M>* <I>www.illegal.com </IllegalSite>	

3.3.2 主机域的定义

主机域是一个能够继承的概念,它包含一些已定义的主机元与一些已定义的其它主机域,这些成员之间的关系是或的关系,即主机域:=El|El|…|Er|Er|….下面介绍它的描述格式。

```
<主机域名>
    <El>主机元
    …
    <Er>主机域
    …
</主机域名>
```

表 3 描述了图 1 中部分安全网关主机域的定义,介绍一个可信内网主机域定义。这个可信内网主机域包括两个主机元。在以后的介绍中使用这些定义进行描述。

表 3　安全网关主机域的定义

<TrustOfficeNet> <El>IntranetA <El>IntranetB </TrustOfficeNet>	<TrustNet> <El>Printer <El>DataBackup <Er>TrustOfficeNet </TrustNet>
<DMZ> <El>DMZ </DMZ>	<UntrustNet> <El>LegalSite <El>IllegalSite </UntrustNet>

3.3.3 服务元的定义

主机元由协议号、端口和处理方式组成,其中协议号、端口可以以"*"号的形式来描述,表示匹配任意.端口的表示方法有:[a,b]表示从端口 a 到 b,[a,*]表示大于等于 a 的端口,[*,

a]表示小于 a 的端口,[a]表示端口等于 a。

<服务元名>
<Pc>协议号
<P>端口
<W>处理方式
</服务元名>

表 4 描述了图 1 中部分安全网关服务元的定义,这些服务元在服务域中被应用。

表 4 安全网关服务元的定义

<SSHService> <Pc>TCP <P>[22] <W>accept </SSHService>	<DenySSHService> <Pc>TCP <P>[22] <W>drop </DenySSHService>
<FTPService> <Pc>TCP <P>[21] <W>accept </FTPService>	<DenyFTPService> <Pc>TCP <P>[21] <W>drop </DenyFTPService>
<HIGHPortAccess> <Pc>TCP,UDP <P>[256,] <W>accept </HIGHPortAccess>	<DenyHIGHPortAccess> <Pc>TCP,UDP <P>[256,] <W>drop </DenyHIGHPortAccess>
<MonitorMailService> <Pc>TCP <P>[25],[110] <W>monit</Monitor MailService>	<AccessAccept> <Pc>TCP,UDP,ICMP <P>* <W>accept </AccessAccept>
<AccessDrop> <Pc>TCP,UDP,ICMP <P>* <W>drop </AccessDrop>	

3.3.4 服务域的定义

服务域是由一系列服务元组成的集合,同时它有一个参数列表$1,$2….这些参数在使用的时候被赋予相应的主机组值。

<服务域名>
<explanation>
<Sl param=$1,param=$2,…>服务元名
…
<Sr param=$1,param=$2,…>服务域名
…
</服务域名>

表 5 是部分安全网关服务域的定义。

3.3.5 安全网关配置

在定义完毕 3.3 节介绍的各个模块后,安全网关的配置选择服务域然后配置相应的参数,如果想要配置 DMZ 访问,那么选择 SetDMZ 服务域, 然后根据它的解释选择 DMZ,UntrastNet,TrastNet 分别作为参数 1、参数 2、参数 3。这样就完成了一个配置(见表 6)。

3.4 模型翻译与优化

策略的翻译就是将用户高层配置转化成实际系统能够识别的规则。如果不管实际的性能,只管功能的实现,那么上面的配置翻译功能只要将主机组包含的主机域,服务组包含的服务元进行一个笛卡儿的乘积运算得到一个最终的多元组匹配。这里的翻译可以使用编译函数的方法进行。图 5 流程图介绍了编译方法。

表 5 安全网关服务域的定义

<SetSSH> <explaination>将参数 1 设置为 SSH 访问允许 <severelem param=$1>SSHService </SetSSH>
<SetFTP> <explaination>将参数 1 设置为 FTP 访问允许 <severelem param=$1>FTPService </SetFTP>
<SetDMZ> <explaination>将参数 1 设置为 DMZ,允许不可信网络参数 2访问,不允许信任网络参数 3 访问 <Sl param=$2 param=$1>AccessDrop <Sl param=$3 param=$1>AccessAccept <Sr param=$1>SetSSH <Sr param=$1>SetFTP </SetDMZ>

表 6 安全网关配置

服务域	参数 1	参数 2	参数 3	解释
SetDMZ	DMZ	UntrastNet	TrastNet	将 DMZ 设置为 DMZ,允许不可信网络 UntrastNet 访问,不允许信任网络 TrastNet 访问
SetSSH	UntrastNet			将 UntrastNet 设置为 SSH 访问允许

Sl?

图 5 翻译流程图

进行翻译后的规则表现形式就是以多元组的方式来描述。表 7 中给出了一条元组的信息。

表 7 一条元组

I_s	P_s	Pc_s	M_s	G_s
2001:250:3000:3::1/62	*	TCP	*	Eth0
I_d	P_d	M_d	G_d	W
*	23	*	Eth2	Drop

3.5　实验方法与实际运行结果

清华大学深圳研究生院的 IPv6 安全网关项目中实现了模型提供的方法,并容易地实现了对应的图形配置界面。通过对大学城现有安全网关配置的移植和运行,经过实际网络使用后的数据随机取样如表 8。

表 8　随机取样结果

m(函数配置配置个数)	$\sum_{1}^{m}\hat{e}_i$(中间结果条数)	n(优化最终元组数目)
27	1 468	938
38	1 723	1 211
35	1 598	1 056
30	1 245	965
51	1 682	1 134
53	1 764	1 341

从上面的结果计算配置效率指标得出 Di_{eff}=32.98~54.37,Co_{eff}=1.29~1.57。

在安全网关的移植过程中对服务元,服务域的修改很少,只需要重新定义主机元,主机域就能快速配置安全网关,因此配置重复利用性比较高,利于经验的代码形式积累。

4　评价

在表 9 中给出了目前存在的各种方法的评价性能比较,其中 Di_{eff}和 Co_{eff}是在清华大学深圳研究生院的 IPv6 路由安全网关实际运行数据的平均值。

表 9　各种方法评价比较

算法	Di_{eff}	Co_{eff}	重复利用性	安全性	实现复杂度	运行复杂度
ACL 手工输入法	1.00	1.00	低	低	低	低
网络划分命名法	1.00	1.00	低	中	低	低
网络划分命名法	23.12	1.00	中	高	低	低
Firmato	17.34	1.30	低	高	高	高
函数模型	43.68	1.43	高	高	低	较低

通过上面的比较分析,本文提出的函数模型安全网关配置方法能够很好提高配置效率,同时方法建立在函数模型的基础上,因此容易理解和经验的交流。在实际的实现过程中也发现开发简单,运行复杂度较低的特点。

5　结论

函数模型安全网关配置策略是一种易于思维理解,方便应用界面设计,同时方便配置的重复利用,方便配置经验描述积累的新型配置模型。在实际的配置过程中发现了安全性较高,运行复杂度低的特点。但是该模型存在的问题是实际系统中的服务定义往往较多,系统提供的基础预设服务不能在简捷与高效之间较好权衡。同时该模型没有较好与之对应的地址指导分配、规则压缩方法,将进一步研究该领域的较好方法。

6　结束语

本文提出一种高层的安全网关配置逻辑与方法,解决了目前安全网关手工配置存在的要求高,难度大,复杂繁琐的问题。尤其是服务域的概念提出,能够很好地建立一个扩展性非常好的安全网关配置方法,甚至可以用几个甚至一个配置来完成安全网关的配置。同时对于好的服务组配置能够做到定义的重用,不同的企业,单位可以借鉴别人写的好的服务组配置来完成自己安全网关的配置。

参考文献:

[1] Bartal Y,Mayer A,Nissimy K,et al.Firmato:a novel firewall management toolkit [C]//Proc of 20th IEEE Sym on Security and Privacy,Oakland,CA,1999:17-31.

[2] 徐恪,吴建平,徐明伟.高等计算机网络——体系结构、协议机制、算法设计与路由器技术[M].北京:机械工业出版社,2003.

[3] Comeb D E.用 TCP/IP 进行网际互联第一卷:原理、协议与结构[M].4 版.北京:电子工业出版社,2004.

[4] Hinden R.RFC 2374 An IPv6 aggregatable global unicast address format[S].1998-07.

[5] Hinden R.RFC2373 IP Version 6 addressing architecture[S].1998-07.

[6] Deering S,Hinden R.RFC 2460 Internet Protocol,Version 6(IPv6) Specification,Internet Engineering Task Force[S].1998-12.

[7] IEEE Computer Society.A quantitative study of firewall configuration errors[J].IEEE,2004.

[8] Hsu J M,Hsu C F,Huang C M.Design of an IPv6 SOHO router based on embedded linux system [C]//Proceedings of the 19th International Conference on Advanced Information Networking and Applications,IEEE,2005.

[9] Al Shaer E S,Hamed H H.Firewall policy advisor for anomaly discovery and rule editing[J].IEEE,2003.

[10] Gupta P,McKeown N.Packet classification on multiple fields[J]. ACM Sigcomm,1999.

[11] Spitznagel E,Taylor D,Turner J.Packet classification using extended TCAMs [C]//Proceedings of IEEE International Conference on Network Protocols(ICNP),2003.

[12] Carney M,Loe B.A comparison of methods for implementing adaptive security policies [C]//Proceedings of the 7th USENIX Security Symposium (SECURITY 98),Berkeley,Usenix Association,26-29 Jan 1998:1-14.

[13] Cisco's PIX firewall series and stateful firewall security[EB/OL].(1997).http://www.cisco.com/warp/public/751/pix/nat wp.pdf.

[14] Yazaki T,Kanetake T,Akahane S,et al.High speed IPv6 router/switch architecture [C]//Proceedings of the 2004 International Symposium on Applications and the Internet Workshops,IEEE,2004.

[15] 王卫平,陈文惠.防火墙规则配置错误分析及其检测算法[J].计算机应用,2005.

[16] 赵启斌,梁京章.防火墙过滤规则异常的研究[J].计算机工程,2004.

[17] 高峰, 许南山. 防火墙包过滤规则问题的研究 [J]. 计算机应用,2003,23(6).

[18] 段海新,吴建平.防火墙在传输网络中的吞吐量与管理问题及解决方案[J].计算机工程与应用,2002,38(11):8-11.

[19] 王家业,荆继武.包过滤防火墙的安全研究[J].计算机科学,1999,26(8):34-36.

[20] 胡继琴,苗春峰.论防火墙技术的应用与开发[J].中州大学学报,2002,(1):88-89.

[21] 张磊,卿斯汉.一个基于 Agent 的防火墙系统的设计与实现[J].软件学报,2000,11(5):642-645.