第 35 卷 第 2 期 计 算 机 工 程 2009 年 1 月
Vol.35 No.2 Computer Engineering January 2009
·安全技术· 文章编号：1000—3428(2009)02—0164—03 文献标识码：A 中图分类号：TP393.08

一种防火墙规则配置异常分析方法

孙 云，罗军勇，刘 炎
（解放军信息工程大学信息工程学院，郑州 450002）

摘 要：从集合角度描述防火墙过滤规则及规则之间存在的异常类型，给出规则间异常类型判定方法。指出直接使用判定方法分析防火墙规则集时所存在的问题，提出一种基于规则顺序敏感性的防火墙规则配置异常分析方法，得到等效的不相关规则集，实现过滤规则的改写。
关键词：防火墙；过滤规则；异常；顺序敏感性

Analysis Method of Firewall Rule Configuration Anomalies

SUN Yun, LUO Jun-yong, LIU Yan
(College of Information Engineering, PLA Information Engineering University, Zhengzhou 450002)

【Abstract】 According to set theory, the method specifies the firewall filtering rules and various types of anomaly among them, brings forward a judgment method of anomaly types, points out the problems in the process of judgment which works directly on firewall rules. On the basis of order-sensitive characteristic of firewall rule configuration, the method finds out the equivalent irrelevance-rule set and modifies the filtering rule.
【Key words】 firewall; filtering rule; anomaly; order-sensitive characteristic

1 概述

网络数量的增长和网络应用的增加使防火墙的安全策略变得越来越复杂，具体表现为防火墙规则集包含规则的数量不断增加，再加上编辑规则时不可避免的人为错误等原因，几乎所有的规则集都会存在或多或少的错误和冗余[1]，导致预想的安全策略无法有效地实施。因此，有必要对规则集内存在的异常进行分析并研究发现异常的方法，为正确配置防火墙提供可靠的参考和指导。目前，人们针对防火墙规则集的特点研究出一些规则异常检测的模型和算法。防火墙的规则配置应该满足 3 个条件：一致性，完整性和紧密性，并采用防火墙决策图(Firewall Decision Diagram, FDD)来表示防火墙的最初配置，把一系列的算法应用到FDD上，从而保证了防火墙规则配置的一致性、完整性和紧密性[2]。Al-Shaer和H.Hamed分析了过滤规则之间的关系，定义了 5 种类型的规则异常，并提出一个用于检测防火墙规则设置中是否存在异常的模型。该模型主要基于策略树和状态机理论检测防火墙规则之间可能存在的异常，同时采用翻译树(translation tree)完成规则的高层翻译工作[3-5]。现有的方法大多忽略了防火墙规则的顺序敏感性，仅能检测 2 条规则之间存在的异常。本文根据防火墙规则的特点从集合的角度描述规则以及规则间的异常，给出 2 条规则间的异常判定方法，然后提出一种基于顺序敏感性的防火墙规则异常分析方法。

2 规则异常的分类

2.1 防火墙规则的形式化表示

不同厂商、不同型号的防火墙规则配置语句不同，其规则的表现形式也不尽相同。但其规则都可抽象成 3 部分：规则序号，过滤域和动作域。规则序号是一条规则在访问控制列表中的位置标识。过滤域可由多个子域组成，通常情况下子域有以下 5 类：协议类型，源 IP 地址，源端口号，目标 IP 地址和目标端口号。动作域只有 2 种选择：接受，即允许数据包通过防火墙；拒绝，即不允许数据包通过。所以，一条规则可以定义为一个七元组：

<规则序号，协议类型，源 IP 地址，源端口，目标 IP 地址，目标端口，动作>

记为：$R<R[1],R[2],R[3],R[4],R[5],R[6],R[7]>$。其中，

$R[1]\in\{1,2,3,4,5,6,7\}$，表示规则序号；

$R[2]\subseteq\{\text{TCP,UDP,ICMP,IP,IGMP}\}$，表示协议类型集合；

$R[3]\subseteq\{0.0.0.0,1.1.1.1,\cdots,255.255.255.255\}$，表示源 IP 地址集合；

$R[4]\subseteq\{0,1,2,\cdots,65\ 535\}$，表示源端口号集合；

$R[5]\subseteq\{0.0.0.0,1.1.1.1,\cdots,255.255.255.255\}$，表示目标 IP 地址集合；

$R[6]\subseteq\{0,1,2,\cdots,65\ 535\}$，表示目标端口号集合；

$R[7]\in\{Accept,Deny\}$，表示动作。

防火墙配置的多条过滤规则形成了防火墙的访问控制列表(Access Control List , ACL)，如表 1 所示。

表 1 防火墙访问控制列表

规则号	协议类型	源 IP 地址	源端口	目的 IP 地址	目的端口	动作
1	UDP	224.0.21.0 (255.255.255.0)	any	209.165.202.128 (255.255.255.192)	100~200	*Accept*
2	TCP	139.66.0.0 (255.255.0.0)	any	209.165.202.128 (255.255.255.192)	<100	*Deny*
3	UDP	224.0.21.0 (255.255.255.0)	any	209.165.202.128 (255.255.255.192)	201~300	*Accept*
4	TCP	139.66.0.0 (255.255.0.0)	any	209.165.202.128 (255.255.255.192)	<50	*Accept*
5	TCP	139.66.11.0 (255.255.255.0)	any	209.165.202.128 (255.255.255.192)	>30	*Accept*
6	UDP	224.0.21.0 (255.255.255.0)	any	209.165.202.128 (255.255.255.192)	140~270	*Deny*
7	UDP	224.0.21.0 (255.255.255.0)	any	209.165.202.128 (255.255.255.192)	150~250	*Deny*

作者简介：孙 云(1981－)，男，硕士研究生，主研方向：计算机软件，网络安全；罗军勇，教授；刘 炎，硕士
收稿日期：2008-06-09 **E-mail：**sunyun1981@sina.com

2.2 规则异常的分类

定义 1 规则 R 过滤域中所有子域的笛卡儿积称为规则 R 所匹配的数据包集合。记为

$$\{R\} = R[2]\times R[3]\times R[4]\times R[5]\times R[6]$$

定义 2 若 $\{R_x\}\cap\{R_y\}\neq\phi$，则称规则 R_x 与规则 R_y 是相关的，否则称规则 R_x 与规则R_y不相关。

规则异常是指防火墙访问控制列表中 2 条规则所匹配的数据包集合出现交叠或覆盖，可能导致规则无法体现预先设定的安全策略。定义以下 4 类异常：

定义 3 屏蔽异常 如果 $\{R_y\}\subseteq\{R_x\}$，$R_x[1]<R_y[1]$ 且 $R_x[7]\neq R_y[7]$，则称规则R_y被规则R_x屏蔽。表1中规则4被规则2屏蔽。

定义 4 冲突异常 如果规则R_x与规则R_y相关，$\{R_y\}\not\subset\{R_x\}$ 且 $R_x[7]\neq R_y[7]$，则称规则 R_x 与规则R_y是冲突的。表 1 中规则 3 与规则 7 冲突。

定义 5 冗余异常 如果 $\{R_y\}\subseteq\{R_x\}$，$R_x[1]<R_y[1]$ 且 $R_x[7]=R_y[7]$，则称规则R_y是冗余的。表1中规则7对于规则6是冗余的。

定义 6 重叠异常 如果规则R_x与规则R_y相关，$\{R_y\}\not\subset\{R_x\}$ 且 $R_x[7]=R_y[7]$，则称规则 R_x 与规则R_y是重叠的。表 1 中规则 4 与规则 5 是重叠的。

3 防火墙规则异常判别方法

3.1 相关性判定

考虑 2 条规则

$$R_x<R_x[1],R_x[2],R_x[3],R_x[4],R_x[5],R_x[6],R_x[7]>$$

$$R_y<R_y[1],R_y[2],R_y[3],R_y[4],R_y[5],R_y[6],R_y[7]>$$

令 $R_{\text{inter}}[k]=R_x[k]\cap R_y[k]$，$2\le k\le 6$，$\{R_{\text{inter}}\}=\{R_x\}\cap\{R_y\}$。

由定义 1 和集合的性质可得

$$\{R_{\text{inter}}\}=R_{\text{inter}}[2]\times R_{\text{inter}}[3]\times R_{\text{inter}}[4]\times R_{\text{inter}}[5]\times R_{\text{inter}}[6]$$

所以，由定义 2 可知：$\forall k(2\le k\le 6)$，若 $R_{\text{Inter}}[k]\neq\phi$，则$R_x$与$R_y$相关；否则$R_x$与$R_y$不相关。

3.2 异常类型判定

根据异常类型的定义判断 2 条规则之间存在的异常类型，实际上是判别 2 条规则所匹配的数据包集合间的包含关系。可以通过 2 条规则所对应过滤子域的包含关系判定它们匹配数据包集合的包含关系，简化问题的规模。那么 $\{R_x\}$ 与 $\{R_y\}$ 之间的关系可用以下方法判断：

(1) $\exists k(2\le k\le 6)$，使得 $R_x[k]\cap R_y[k]=\phi$，则 $\{R_x\}\cap\{R_y\}=\phi$；

(2) $\forall k(2\le k\le 6)$，如果 $R_x[k]=R_y[k]$，则 $\{R_x\}=\{R_y\}$；

(3) $\forall k(2\le k\le 6)$，如果 $R_x[k]\subseteq R_y[k]$，则 $\{R_x\}\subseteq\{R_y\}$；

(4)若 $\{R_x\}\cap\{R_y\}\neq\phi$，且 $\exists k(2\le k\le 6)$，使得 $R_x[k]\not\subset R_y[k]$，则 $\{R_x\}\not\subset\{R_y\}$。

4 防火墙规则配置异常分析方法

将上述规则异常判别方法的直接应用于规则集中规则之间的异常分析存在 2 大问题：

(1)如表 1 中规则 2 与规则 4 是屏蔽异常；规则 2 与规则 5 是冲突异常；规则 4 与规则 5 是重叠异常。由于规则的顺序敏感性，规则 4 与规则 5 的重叠异常无意义，它已被前面 2 个异常所替代，这里称其为无效异常。

(2)如表 1 中规则 1 与规则 7 是冲突异常；规则 3 与规则 7 也是冲突异常。然而规则 1 和 3 所匹配的数据包集合完全涵盖了规则 7 所匹配的数据包集合，由于规则的顺序敏感性，规则 7 永远都不会产生作用，这种情形称为组合屏蔽。

产生这 2 种情形的根本原因在于忽视了防火墙规则的顺序敏感性，使规则匹配数据包集合在多次比较中被重复使用。

4.1 解决的方法

基本思想：将规则两两进行比较，消去匹配数据包集合中的交集。

首先说明如何计算 2 条相关规则匹配数据包集合的差集并写出与差集相匹配的新规则。为方便讨论，假设相关规则间只有 2 个过滤域出现部分重叠(非包含关系)，其余过滤域都是包含关系。若只写出部分重叠的过滤域，那么可将规则简单表示如下：

$R_A<A_1,A_2>$ 和 $R_B<B_1,B_2>$

令 $A_1\cap B_1=m$，$A_2\cap B_2=n$；

则

$$R_B<B_1,B_2>=R_B<(B_1-m)\cup m,(B_2-n)\cup n>$$

所以

$$\{R_B\}=[(B_1-m)\times(B_2-n)]\cup[(B_1-m)\times n]\cup[m\times(B_2-n)]\cup[m\times n];$$

根据 3.1 节推论可知：

$$\{R_{\text{in ter}}\}=\{R_A\}\cap\{R_B\}=m\times n$$

因为

$$(B_1-m)\cap m=\phi,\ (B_2-n)\cap n=\phi$$

所以

$$\{R_B\}-\{R_A\}=\{R_B\}-\{R_{\text{inter}}\}=[(B_1-m)\times(B_2-n)]\cup[(B_1-m)\times n]\cup[m\times(B_2-n)]$$

因此，与 $\{R_B\}-\{R_A\}$ 匹配的规则可写为如下 3 条子规则：$R_{B1}<B_1-m,B_2-n>$，$R_{B2}<B_1-m,n>$ 和 $R_{B3}<m,B_2-n>$。

现在假设规则总数为 W，则防火墙规则配置异常分析方法的伪代码表示如下：

```
int i, j;
for( i=1; i<W; i++)
{for( j=i+1; j<=W; j++)
{计算规则 i 与规则 j 匹配数据包集合的交集 {R_inter} ；
将 {R_j}-{R_inter} 作为新的匹配数据包集合；
根据 {R_j}-{R_inter} 写出与之匹配的新规则 R_j' ；
用 R_j' 取代 R_j ；
}}
```

上述过程结束后会出现 3 种情形：

(1)若某条规则的匹配数据包集合经修改后变为空，说明此规则是无效的。

(2)若某条规则的匹配数据包集合被修改但不为空，说明此规则与其前面的某些规则相关并且部分失效，详细情况可以参看 $\{R_{\text{inter}}\}$ 的记录信息。

(3)若某条规则的匹配数据包集合在整个考察过程中没有被修改，说明此规则完全有效，其余规则没有对其产生任何影响。

上述过程将规则集作为一个整体，考虑到防火墙规则的顺序敏感性，消除了匹配数据包集合被重复使用的可能，记录了原规则集任意 2 条规则之间匹配数据包的交叠信息。此外，上述过程结束后产生了一个在过滤效果上与原规则集等效的新规则集，且新规则集中任意 2 条规则都不相关，称之

为不相关规则集，这对分析防火墙实际的过滤效果非常有意义。使用上述方法对表 1 所示的规则集进行处理得到对应的不相关规则集，如表 2 所示。

表 2　经过处理的防火墙访问控制列表

规则号	协议类型	源 IP 地址	源端口	目的 IP 地址	目的端口	动作
1	UDP	224.0.21.0 (255.255.255.0)	any	209.165.202.128 (255.255.255.192)	100~200	*Accept*
2	TCP	139.66.0.0 (255.255.0.0)	any	209.165.202.128 (255.255.255.192)	<100	*Deny*
3	UDP	224.0.21.0 (255.255.255.0)	any	209.165.202.128 (255.255.255.192)	201~300	*Accept*
5	TCP	139.66.0.0 (255.255.0.0)	any	209.165.202.128 (255.255.255.192)	≥100	*Accept*

由表2可看出，原始访问控制列表中第4、第6和第7条规则完全失效，可以将其删除，符合情形(1)；第5条规则部分失效，可以对其进行修改，符合情形(2)；规则1~规则3没有发生变化，完全有效，符合情形(3)。

此外，由于表 2 中各条访问规则所对应的匹配数据包集合不再有交集，因此可以根据协议类型和动作域将相应的访问控制规则进行合并，进一步简化防火墙访问控制列表，如规则 1 和规则 3 可以合并为一条新的规则。

4.2　复杂度分析

本方法主要是顺序遍历规则，对每条规则和其后面的所有规则进行两两比较，同时修改匹配数据包集合并重写与之对应的新规则。若将 2 条规则进行一次比较作为基本操作，规则集中规则的数量为 n，那么总的比较次数为 $n\times(n-1)/2$，总的时间复杂度为 $O(n\times(n-1)/2)=O(n^2)$。

实际应用时还可以先根据规则过滤域中的协议类型将规则进行聚类，然后分类独立进行分析，这样每一类中规则的数量会更小，总的比较次数会大幅减少。

5　结束语

本文分析了防火墙规则的组成特点，然后使用一个七元组对规则进行形式化描述，对 2 条规则间可能存在的异常进行分类描述，提出基于集合之间包含关系的异常判定方法，分析了将其应用于规则集时存在的不足，最后提出一个基于规则顺序敏感性的异常分析方法。本方法中根据差集写出的新规则的算法只考虑了 2 个过滤域的简单情况，针对多个过滤域的情形还有待进一步改进。目前大多数规则异常分析方法都只能分析 2 条规则间的异常，多条规则间异常分析方法也是今后的研究方向。

参考文献

[1] Wool A. A Quantitative Study of Firewall Configuration Errors[C]// Proceedings of IEEE Computer. [S. l.]: IEEE Press, 2004.

[2] Gouda M, Liu Xiangyang. Firewall Design: Consistency, Completeness, and Compactness[C]//Proceedings of the 24th IEEE International Conference on Distributed Computing Systems. [S. l.]: IEEE Press, 2004-03.

[3] Al-Shaer E, Hamed H. Management and Translation of Filtering Security Policies[C]//Proceedings of IEEE International Conference on Communications. [S. l.]: IEEE Press, 2003-05: 256-260.

[4] Al-Shaer E, Hamed H. Firewall Policy Advisor for Anomaly Detection and Rule Editing[C]//Proceedings of IEEE/IFIP Integrated Management. [S. l.]: IEEE Press, 2003: 17-30.

[5] Al-Shaer E, Hamed H. Design and Implementation of Firewall Policy Advisor Tools[R]. School of Computer Science Telecommunications and Information Systems, DePaul University, Technical Rept.: CTI-techrep0801, 2002-08.

(上接第 163 页)

4　安全性分析

(1)重放攻击。由于 *SEQ* 是不断更新的，当服务器进行重放攻击时，客户端能够根据 *SEQ* 的值判断出服务器方发来的挑战消息是旧值，并予以拒绝。用 $AK\oplus SEQ$ 传送有效避免了 *SEQ* 的值在网络中被窃取。因此，本机制可以防止重放攻击。

(2)服务器伪装攻击。在步骤(3)中，通过验证 *SEQ* 及 *AM* 的正确性，2 次验证了服务器的身份。显然，攻击者无法伪装成服务器欺骗用户。

(3)离线猜测密钥攻击。如果 *RES* 值被截获，攻击者猜测密钥 *K*。而 *RES* 产生函数的复杂性和 *nonce* 的随机性使其几乎不可能实现。因此，这种方式可以避免密钥猜测的攻击。

(4)伪装用户攻击。由于加密密钥 *CK* 和完整性密钥 *IK* 在服务器和客户端之间从不传送，因此攻击者无法通过截获消息窃取密钥。即使伪装用户的攻击者可以假冒合法用户入网，也因为不知道密钥而对以后窃取的信令和数据无从下手。

(5)消息篡改攻击。在认证过程完成后，完整性保护保证消息不被非法篡改。但有时，如在第 1 次建立连接时还没有完成认证的情况下，某些敏感消息可能被篡改。当客户端希望与服务器建立连接时，客户端向网络发送的请求消息中包含自己支持的加密算法 *UEA* 和完整性算法 *UIA*。该消息本身应该是受完整性保护的，但由于还未生成完整性密钥，该消息无法受到完整性保护，因此可能被篡改加密算法 *UEA* 信息，使服务器端和客户端的加密算法不匹配，造成连接不加密的情况，出现安全漏洞。此时，服务器先将该信息存储起来。在随后的认证过程中，服务器向客户端发送的 *challenge* 消息中又包含该信息，这时整条消息是受完整性保护的，客户端比较前后 2 条消息中的 *UEA* 和 *UIA* 信息，即可知该信息有没有被篡改，从而弥补开始没有完整性保护带来的漏洞。

这样在一次连接上，连接开始时系统使用对实体的认证，并在连接的存活期使用完整性保护，就能联合起来为在此连接上传递的所有数据单元的来源和完整性提供确认。

5　结束语

在相关研究成果的基础上，本文对 SIP 的 HTTP 摘要协议加以改进，改进方案在保留客户端和服务器之间相互认证的基础上，用加密机制和完整性机制进一步保证了消息传输的安全性。认证消息传递次数并未增加，只增加了加解密的运算量，对系统的效率不会产生太大的影响，同时有效地防止了各种攻击。

参考文献

[1] 姬　宁, 林　晓, 普杰信. 一种基于 SIP 安全认证机制的研究[J]. 计算机应用, 2007, 27(3): 616-618.

[2] 3G TS 33.102 V7.1.0. 3G Security: Security Architecture[S]. 2006.

[3] 俞志春, 方滨兴, 张兆心. SIP 协议的安全性研究[J]. 计算机应用, 2006, 26(9): 2124-2126.

[4] 刘伟明, 鲜继清, 陈伟凌. VoIP 安全——基于 SIP 协议的深入剖析和解决策略[J]. 计算机应用, 2006, 26(6): 167-170.