Journal of System Simulation

Volume 27 | Issue 11 Article 21

8-5-2020

Policies Conflict Detection Algorithm Coordinated Defense-oriented of Firewall and IDS/IPS

Qiu Song
1. Department of Engineering, Xiangyuan Hexin Power Co. Ltd. , Taiyuan 030001, China; ;

Jiao Jian
2. Department of Computer, Beijing Information Science & Technology University. Beijing 100192, China; ;

Dongyang Zhang
3. Department of Computer, North China Electric Power University, Baoding 071002, China;

Policies Conflict Detection Algorithm Coordinated Defense-oriented of Firewall and IDS/IPS

Abstract

Abstract: Coping with the distributed and complex threaten of networking attack, the requirement of coordinated defense of Firewall and IDS/IPS are becoming more and more urgent. As the existence of uncertainty of the judgment of Intrusion performed by IDS/IPS, Firewall and IDS/IPS often perform contradict action, that the same package matched the both rules of Firewall and IDS/IPS, and conflict arose, which would lead to illegal access control or deny of legal access control. The policies conflict detection algorithm of coordinated defense of Firewall and IDS/IPS were researched. *The semantic models of firewall policy and IDS/IPS policy were proposed, the classification of the policies conflicts was proposed, and the conflicts detection algorithm of policies were proposed using OBDD (ordered binary decision diagram)*. The experiment demonstrates the correctness and scalability of the algorithm, and the proportion of the conflicts in real network scenario.

Keywords

firewall, coordinated defense, conflict detection, ordered binary decision diagram

第 27 卷第 11 期 系统仿真学报© Vol. 27 No. 11
2015 年 11 月 Journal of System Simulation Nov., 2015

面向防火墙和 IDS/IPS 协同防御的策略冲突检测算法

邱松[1]，焦健[2]，张东阳[3]
(1. 襄垣和信发电有限公司工程部，太原 030001；2. 北京信息科技大学计算机学院，北京 100192；
3. 华北电力大学计算机学院，保定 071002)

摘要：为应对分布式、复杂的网络攻击威胁，防火墙和 IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)协同防御的需求越来越迫切。由于 IDS/IPS 对入侵判断不确定等问题的存在，当防火墙策略和 IDS/IPS 策略中的规则对同样数据包执行的动作矛盾时，会产生冲突。冲突会导致允许非法访问或者阻断合法访问。通过研究面向防火墙和 IDS/IPS 协同防御的策略冲突检测算法。给出了防火墙策略和 IDS/IPS 策略的语义模型，实现了策略冲突的分类，设计基于 OBDD(ordered binary decision diagram，有序决策二叉图)的策略冲突检测算法，在实际场景下验证了算法的正确性和可扩展性，并分析了冲突的分布比例。

关键词：防火墙；协同防御；冲突检测；有序决策二叉图
中图分类号：TP301 文献标识码：A 文章编号：1004-731X (2015) 11-2770-08

Policies Conflict Detection Algorithm Coordinated Defense-oriented of Firewall and IDS/IPS

Qiu Song[1], *Jiao Jian*[2], *Zhang Dongyang*[3]
(1. Department of Engineering, Xiangyuan Hexin Power Co. Ltd., Taiyuan 030001, China; 2. Department of Computer, Beijing Information Science & Technology University. Beijing 100192, China; 3. Department of Computer, North China Electric Power University, Baoding 071002, China)

Abstract: Coping with the distributed and complex threaten of networking attack, the requirement of coordinated defense of Firewall and IDS/IPS are becoming more and more urgent. As the existence of uncertainty of the judgment of Intrusion performed by IDS/IPS, Firewall and IDS/IPS often perform contradict action, that the same package matched the both rules of Firewall and IDS/IPS, and conflict arose, which would lead to illegal access control or deny of legal access control. The policies conflict detection algorithm of coordinated defense of Firewall and IDS/IPS were researched. *The semantic models of firewall policy and IDS/IPS policy were proposed, the classification of the policies conflicts was proposed, and the conflicts detection algorithm of policies were proposed using OBDD (ordered binary decision diagram).* The experiment demonstrates the correctness and scalability of the algorithm, and the proportion of the conflicts in real network scenario.

Keywords: firewall**;** coordinated defense; conflict detection; ordered binary decision diagram

引言

网络攻击从早期的“红色代码”、“冲击波”等传统病毒，发展为复杂的间谍软件、DDOS(Distributed Denial of Service)攻击等新型分布式、复杂的网络威胁。这些威胁的存在，可能会导致网络敏感信息的泄漏，或面临巨大的财产损失等严重后果。因对分布式、复杂的攻击，需要多个安全组件协同防御。防火墙和 IDS/IPS 是普遍采用的安全组件。入侵监测系统(IDS)是对网络系统的运行状态进行监视、

收稿日期：2014-04-19 修回日期：2014-07-27；
基金项目：国家自然科学基金项目(61370065)；
作者简介：邱松(1982-)，男，河北大城县，学士，工程师，研究方向为网络及信息管理；焦健(1978-)，男，博士，副教授，研究方向为网络安全；张东阳(1981-)，男，硕士，研究方向为计算机测控技术。

以识别入侵者、入侵行为并记录入侵信息的系统[1]。IDS 是防火墙的有效补充。但随着攻击不断复杂化，对攻击的响应需求不断增加，在 IDS 基础上，提出了 IPS(Intrusion Prevention System)，IPS 能够检测并阻止入侵事件的系统，对流量进行监测，对可能的入侵采取告警、记录、响应的动作。

防火墙侧重于访问控制，属于静态被动防御，IDS/IPS 侧重于主动发现入侵，属于动态主动防御。在面临复杂的攻击威胁的网络中，防火墙和 IDS/IPS 的有效协同，既可以防御静态的攻击，又可以主动地防御动态出现的攻击。

防火墙和 IDS/IPS 的协同分为 2 种方式，一种是 2 种组件动作上的协同，即防火墙和 IDS 的联动[2]，另一种两种组件任务上的协同，即防火墙和 IPS 的协同。前者的协同，由 IDS 产生动态的阻断规则，并将其添加到防火墙的策略中，由防火墙执行阻断动作完成。后者的协同，由防火墙和 IPS 按照各自的防御任务配置各自的策略完成。

防火墙和 IDS/IPS 组成的防护体系，理想的前提假设是：防火墙对流量进行初始筛选，IDS/IPS 对流量进行细粒度检查，将检测出的入侵阻止。这是最优的协同防御效果。其前提假设是：

(1) IDS/IPS 对入侵的检测是正确的。

(2) 防火墙对数据报做第一道检查关口，IDS/IPS 分析的流量仅是防火墙允许的流量。

但这样理想的前提假设，在分布式、复杂攻击威胁的场景中通常是不满足的，原因在于：

(1) IDS/IPS 对入侵的检测不一定是完全正确的。IDS/IPS 对于流量是否是入侵的判断，存在一定的误报率。

(2) 在面临分布式、复杂攻击威胁的场景中，IDS/IPS 需要分析更广泛的流量，因此 IDS/IPS 要监控更完整的流量，有时 IDS/IPS 配置规则中监控的流量范围，会超过防火墙允许的流量。甚至有时 IDS 部署在防火墙的外侧以监控更多的流量。

因此对于同样的数据报，防火墙策略和 IDS/IPS 策略会有矛盾的判断，从而导致不能达成最优的防御效果。例如：防火墙禁止了 IDS/IPS 监控的流量，或者 IDS/IPS 阻止了防火墙允许的正常流量。策略冲突，会导致对于同样的流量，存在不同的动作决策。而策略在由设备执行时，设备如果没有检测冲突的算法，会按照既定的确定顺序执行策略，导致允许非法的流量，或者阻断合法的流量的后果。

针对此类问题，需要设计检测防火墙策略和 IDS/IPS 策略的冲突算法，在实际策略执行前，检测出其中存在的冲突，将其作为一种警告，预先告知管理员，由管理员判断消除这种不确定性，从而辅助达到最优的协同防御效果。而目前的冲突检测算法主要集中在防火墙策略内部冲突检测及防火墙策略之间的冲突检测[3-7]、和防火墙策略类似的包过滤策略冲突检测[8-11]，IDS 策略内的冲突检测[12]，文献[3]给出了一系列防火墙策略内冲突检测的技术和算法来。作者用集合论表示防火墙规则之间的关系，来提供自动的防火墙异常发现来给出规则冲突。文献[11]从提高算法响应时间的角度，给出了快速的防火墙冲突检测算法，提高了检测算法的响应时间，以应对大规模的策略冲突检测。文献[6-7]给出了策略内多个规则之间的冲突检测的可视化的算法。文献[8]给出了策略内基于有序决策二叉图的冲突检测算法，有序决策二叉图，是可以表示每个规则字段的取值范围(语义)的数据结构，并且可以提供布尔函数的有效表述和操作运算。基于 OBDD(ordered binary decision diagram)的过滤包策略的条件部分语义的表示方法被后来研究普遍接受，之后作者将其扩展到更广泛的范围[9]。文献[10]从“安全严重程度”的角度，对防火墙策略冲突给出了新的划分和检测算法，并给出了冲突消解算法。文献[12]给出了 IDS 策略内冲突检测的算法。但文中没有给出 IDS 策略的语义表示模型，算法是基于语法的检测。文献[4-5]将冲突扩展到分布式防火墙的场景，给出了分布式防火墙策略内和策略间的冲突分类和冲突检测算法。作者给出的算法仅限于检测防火墙策略之间的冲突。文献[11]从多网络安全

第 27 卷第 11 期 系统仿真学报 Vol. 27 No. 11
2015 年 11 月 Journal of System Simulation Nov., 2015

组件策略冲突的角度，给出了策略间冲突检测算法，此算法可以用来检测防火墙策略和 IDS 策略间的冲突，但由于考虑场景于本文不同，文中给出的冲突分类，相对于防火墙和 IDS 协同防御中的策略冲突检测来说不够完整。文献[13]给出了防火墙和 IDS/IPS 的策略冲突检测算法，但文中仅给出的两类防火墙和 IDS/IPS 策略冲突的检测算法，没有考虑面向防火墙和 IDS/IPS 的协同防御场景中的策略冲突检测。本文在以上研究的基础之上，从语义分析入手，研究了面向防火墙和 IDS/IPS 协同的策略冲突分类及相应检测算法。

1 防火墙策略和 IDS 策略的语义模型

防火墙和 IDS/IPS 都采用基于策略的管理方式。RFC3198[14]对策略的定义为：策略是管理、控制网络资源访问的一组规则。其中，规则由条件和动作两部分组成。防火墙策略和 IDS 策略中的规则，由数据报的条件，和针对数据报所采取的动作两部分组成。

以 CISCO 防火墙和 snort IDS/IPS 为例，说明防火墙规则和 IDS/IPS 规则的语法和语义，如下：

(1) CISCO 防火墙规则实例为：

access-list 101 permit tcp 1.1.1.1 0.0.0.255 any eq 80

表示的含义为：允许源 IP 为 1.1.1.*、发往任意 IP 地址的、tcp 协议的、端口号为 80 的流量。

(2) snort IDS 规则的实例为：

0 alert TCP $EXTERNAL_NET any -> $HOME_NET 80 (content:"OBJ");

表示的含义为：对于从外网发往内网的 80 端口的、内容包含"OBJ"字段的流量，采取告警的动作。

规则的语义，表示对数据报采取的动作。条件部分表示数据报的条件，动作表示采取的动作。因此：用(数据报，动作)的二元组，来表示规则的语义。

1.1 防火墙策略的语义模型

防火墙策略是规则的集合，本小节首先给出防火墙规则的语义模型，然后在此基础上给出防火墙策略的语义模型。

防火墙规则的抽象文法表示如下：

rule:=sourceip,sourceport,derection,destip,
destport,action

文法中前 5 个字段，表示规则的条件，即数据报所满足的条件。后一个字段，表示对数据报采取的动作。数据报所满足的条件用 condition(packet) 谓词来表示。

我们用指称语义来表示防火墙规则的语义，语义模型如下：

$$\text{semantic}_i^{\text{rule}} = (\text{PACKET}, \text{action})$$

$$\text{PACKET} = \{\text{packet} \mid \text{paket} \in \text{S}, \text{condition}_i^{fw}(\text{packet})\}$$

$$\text{action} \in \text{ACTION}$$

$$\text{ACTION} = \text{PERMIT} \cup \text{DENY}$$

$$\text{PERMIT} = \{\text{permit}\}$$

$$\text{DENY} = \{\text{deny}\}$$

其中，$\text{semantic}_i^{\text{rule}}$ 表示规则的语义，由二元组 $(\text{PACKET}, \text{action})$ 表示。PACKET 为所有满足 $\text{condition}_i^{fw}(\text{packet})$ 谓词的数据报($\text{condition}_i^{fw}(i)$ 为第 i 条规则条件部分对数据报源 IP、源端口、目的 IP、目的端口取值的限定)，action 属于动作集合 ACTION，ACTION 由 PERMIT 和 DENY 两类分别含有"允许"和"拒绝"动作的集合组成，在防火墙规则中，PERMIT 和 DENY 都分别仅包含一个动作——" permit "和" deny "。

防火墙策略由多条规则按照有限匹配顺序组成。防火墙策略的语义，表示这些规则组合在一起，对数据报的动作，因此，策略的语义模型如下所示。

$$\text{semantic}_i^{\text{policy}} = (\text{PACKET}, \text{action})$$

$$\text{PACKET} = \bigcup_{k \in \text{index}'} \left(\text{PACKET}_k - \bigcup_{l \in \text{prior}} \text{PACKET}_l \right)$$

计算策略语义中，计算某个动作 action 所作用的数据报的方法如后一个公式所示——由所有此动作的规则的数据报，按照顺序优先匹配的原则，所限定的数据报的并集。其中，index′ 表示与策略的动作(或)为相同动作的所有的规则的 ID 号，prior 表示所有比规则 *l* 优先的规则的 ID 号。

1.2 IDS/IPS 策略的语义模型

IDS/IPS 策略中规则的抽象文法如下所示：

rules:=rule[,…,rule]

rule:= ruleheadr,ruleoption

ruleheader:=action, sourceip, sourceport, derection, destip, destport

action:=alert|log|pass|activate|dynamic

ruleoption:=(optionname:optionvalue;[…;optionname:optionvalue;],)

optionname:=msg|logto|ttl|tos|id|ipotion|fragbits|dsize|flags|seq|ack|window|itype|icode|icmp_id|icmp_seq|content|content-list|offset|depth|nocase|session|rpc|resp|react|reference|sid|rev|classtype|priority|uricontent|tag|ip_proto|sameip|stateless|regex|distance|within|byte_test|byte_jump

根据以上的文法，IDS/IPS 策略的规则由规则头(ruleheader)和规则选项(ruleoption)2 部分组成，其中规则选项(ruleoption)限定数据报内容的特征的值(如 ttl 字段，限定 ttl 特征的取值)和参数(如 msg，限定告警的信息)，规则选项是入侵检测引擎的核心。

IDS 规则的语义，与防火墙规则的语义类似，都表示对数据报采取的动作。条件部分表示数据报的条件，动作表示采取的动作。因此：我们仍用(数据报，动作)的二元组，来表示 IDS/IPS 规则的语义。

IDS/IPS 策略的语义与防火墙策略不同之处在于：

1) IDS/IPS 的动作分为 3 种：允许通过、拒绝通过、发送响应报文，前 2 个动作，我们称为控制动作(controlaction)，后一个动作我们称为响应动作(respaction)。

2) IDS/IPS 策略中的规则，对于同样的数据报，如果有多条规则匹配，不是优先匹配的顺序单一规则匹配，而所有这些规则全部匹配。

因此，IDS 规则的语义元素表示如下：

controlaction={permit,deny}

$PACKET_{response}$ ={packet|response(packet)}

respaction = action, action ∈ RESPONSE

PERMIT = {alert,log}

DENY = {drop,sdrop,reject,resp,react}

RESPONSE = {reject,resp,react}

规则的语义有两种，一种是对数据报的控制动作，记做$(PACKET, controlaction)$；另一种除了控制动作，还有产生响应报文的动作(respaction)，产生的新报文为 $PACKET_{response}$，其中 response (packet) 是响应报文所满足的谓词，表示从 IDS/IPS 的 IP 地址发往源地址的报文。IDS 策略的语义，即是这些规则语义的集合。

2 防火墙和 IDS 策略冲突定义及分类

RFC3198 对“策略冲突”的定义为：当两条规则的条件部分都满足，但动作相矛盾时，称为策略冲突[14]。

因此，当防火墙策略中的规则，和 IDS/IPS 策略中的规则的条件部分同时满足，而动作部分相矛盾时，称为防火墙策略和 IDS/IPS 策略冲突。

防火墙和 IDS/IPS 的协同防御，是串联在某一网络路径上的，防火墙策略靠近外网的位置，IDS/IPS 在防火墙之后，靠近内网的位置。我们给出 3 类冲突的定义：

定义 1(遮盖冲突)。防火墙策略允许的数据报，被 IDS/IPS 策略拒绝，这种冲突称为遮盖冲突。

定义 2(异常冲突)。 在从源 IP 到目的 IP 的网络路径上，靠近目的 IP 端的策略允许的数据报，被靠近源 IP 端的策略拒绝，这种冲突称为异常冲突。

定义 3(响应阻断冲突)。IDS 策略的响应报文，

第 27 卷第 11 期 系统仿真学报 Vol. 27 No. 11
2015 年 11 月 Journal of System Simulation Nov., 2015

被防火墙策略阻断，这种冲突称为响应阻断冲突。

定理 1 防火墙策略和 IDS 策略的冲突，包含且仅包含遮盖冲突和异常冲突和响应阻断冲突这 3 类冲突。

证明：(1)证明当防火墙策略和 IDS 策略发生冲突时，一定属于遮盖冲突、异常冲突和响应冲突这 3 类。

由上节的分析可知，防火墙策略的动作分为两类：PERMIT 和 DENY，IDS/IPS 策略的动作分为 3 类：PERMIT，DENY 和 RESPONSE。

所以防火墙和 IDS/IPS 动作的可能组合如下：

ACTIONFW×ACTIONIDS=

(PERMIT∪DENY)×(PERMIT∪DENY∪RESPONSE)=(PERMIT×PERMIT)∪(PERMIT×DENY)∪(PERMIT×RESPONSE)∪(DENY×PERMIT)∪(DENY×DENY)∪(DENY×RESPONSE)

其中可能的组合一共有 6 种。其中矛盾的组合有：$(\text{PERMIT}\times\text{DENY})$，$(\text{DENY}\times\text{PERMIT})$，$(\text{DENY}\times\text{RESPONSE})$ 3 种。

这 3 种类型的冲突，依据定义 1、定义 2 和定义 3，分别记为：遮盖冲突、异常冲突和响应阻断冲突。

(2) 证明防火墙策略和 IDS 策略属于遮盖冲突、异常冲突和响应冲突这 3 类时，一定是冲突。

当防火墙策略和 IDS 策略属于这 3 类时，对于同样的数据包，有矛盾的动作，根据策略冲突的定义可知是冲突。

由(1)和(2)得：定理得证。

3 防火墙和 IDS 策略冲突检测算法

3.1 防火墙策略语义与 IDS 策略语义表示

数据报的条件部分，用布尔函数表示。防火墙的规则的条件部分包括：协议、源 IP 和源掩码、源端口、目的 IP 和目的掩码、目的端口五项，每部分用一个 n 元布尔表达式形式表示，结合每部分的取值范围，协议用 2 元布尔表达式表示，源 IP 和源掩码用 32 元布尔表达式表示，源端口用 16 元布尔表达式表示，目的 IP 和目的掩码用 32 元布尔表达式表示，目的端口用 16 元布尔表达式表示。防火墙的条件是这几部分布尔表达式的“并”操作。

因此防火墙规则的条件部分表示的数据报，用 98 元布尔变量的“并”操作的布尔表达式来形式表示。防火墙策略中每个规则的表达式基础上，运用公式(4)可得防火墙策略的数据报。同理，用 445 元布尔表达式表示 IDS/IPS 策略的条件限定的数据报，并用公式(6)表示 IDS/IPS 策略的数据报。

我们用 buddy 软件包[15]提供的能够表达布尔表达式的数据结构——有序决策二叉图(Ordered Binary Decision Diagram，OBDD)[16]，来表示的防火墙策略和 IDS/IPS 策略的语义。

3.2 检测算法

本节给出防火墙策略与 IDS 策略的冲突检测算法，算法中的数据结构及其含义如下：

ruleaction[i]：表示第 i 条 IPS 规则的动作；bdd_and()：2 个表示数据报的 OBDD 求交集；fwruleaction[i]：表示第 i 条防火墙规则的动作；rules[i][0]：表示第 i 条 IPS 规则的数据报；rules[i][1]：表示第 i 条 IPS 规则的响应报文；fwPermit：表示防火墙策略允许的数据报；fwDeny：表示防火墙策略拒绝的数据报。算法代码如下：

```
int IDSfwconflict()
{   int i,j;
    for (i=0;i<number;i++)
    {
```

/*IDS 允许类规则与防火墙拒绝规则的语义有交叉，产生冲突，说明 IDS 允许的规则防火墙拒绝，产生冲突*/

```
if((strcmp(ruleaction[i],"alert")==0)||(strcmp(ruleaction[i],"log")==0)
||(strcmp(ruleaction[i],"activate")==0)||(strcmp(ruleaction[i],"dynamic")==0)
```



```
||(strcmp(ruleaction[i],"pass")==0))

    {if(bdd_and(rules[i][0],fwDeny)!=bddfalse)
            {for(j=0;j<number2;j++)

    { if((strcmp(fwruleaction[j],"deny")==0)

    &&(bdd_and(rules[i][0],fwrule[j])!=bddfalse))

{fprintf(output_fd,"rule101-%d and rule%d conflict;
                    conflict type:shield
conflict\n",j,i);
                                    }} } }
    /*IDS 拒绝类规则与防火墙允许规则的语义有交叉，产生冲突，说明 IDS 拒绝的规则防火墙允许*/
    if((strcmp(ruleaction[i],"drop")==0)||(strcmp(rul
eaction[i],"reject")==0)
    ||(strcmp(ruleaction[i],"sdrop")==0)||(strcmp(rule
action[i],"react")==0))

{ if(bdd_and(rules[i][0],fwPermit)!=bddfalse)
                    { for(j=0;j<number2;j++)
                {
    if((strcmp(fwruleaction[j],"permit")==0)

    &&(bdd_and(rules[i][0],fwrule[j])!=bddfalse))
                                    {
    fprintf(output_fd,"rule101-%d and rule%d
conflict;
            conflict type:abnormal conflict\n",j,i);
                                    }} } }
    /*IDS 响应动作的语义与防火墙拒绝规则的语义有交叉，IDS 的响应被防火墙阻断*/
    for (i=0;i<number+1;i++)
            {
    if(bdd_and(rules[i][1],fwDeny)!=bddfalse)
        { for(j=0;j<number2;j++)
        {
    if((strcmp(fwruleaction[j],"deny")==0)&&(j!=0)
)
    fprintf(output_fd,"rule101-%d and rule%d
conflict; conflict type:react block\n",j,i);
            } } } }
```

算法的时间复杂度为 $o(mn)$，其中 m 是防火墙策略的规则条数，n 是 IDS/IPS 策略的规则条数。

4 实验验证

实验验证分别从算法的正确性，算法的性能和对实际安全策略分析 3 方面进行。

4.1 正确性验证

为验证算法的正确性，本文以山西某大型电厂网络系统安全配置为分析对象，部分输入的防火墙策略(policy1)和 IDS/IPS 策略(policy2)如表 1 所示。

表 1 输入的防火墙策略和 IDS/IPS 策略的规则内容

Policy	Rules
Firewall Policy	access-list 101 deny tcp 1.1.1.1 2.2.2.1 access-list 101 deny tcp 1.1.1.4 1.1.1.2 access-list 101 deny tcp 1.1.1.3 2.2.2.3
IDS/IPS Policy	0 alert tcp 1.1.1.1/24 any -> 2.2.2.1/24 any (content:ac;); 1 drop tcp 1.1.1.3 any -> 2.2.2.3 any (content:bd;);2 reject tcp 1.1.1.2 any -> 2.2.2.2 any (id:1;);

表 1 给出了防火墙策略(Firewall Policy)和 IDS/IPS 策略(IDS/IPS Policy)，防火墙策略采用的是 CISCO 设备的格式，IDS/IPS 策略采用的是符合 snort 格式。用我们实现的 3.2 所示防火墙策略和 IDS/IPS 策略冲突检测的算法检测对表 1 所示的策略进行冲突检测，输出结果的截图如图 1 所示。

```
Result Save to file:./fwlDSconflict 12.txt
Here is the Result:
rule101-0 and rule0 conflict; conflict type:shield conflict
rule101-2 and rule1 conflict; conflict type:abnormal conflict
rule101-1 and rule2 conflict; conflict type:react blocked
```

图 1 表 1 所示的两种策略的冲突检测结果

第 27 卷第 11 期 系统仿真学报 Vol. 27 No. 11
2015 年 11 月 Journal of System Simulation Nov., 2015

图 1 显示了 Firewall Policy 和 IDS/IPS Policy 中的三种类型的冲突，并能够检测出冲突所涉及的规则。经人工验证，算法检测出的冲突全部正确。

4.2 算法性能测试

在主机 CPU 2.5G 双核，内存：4G 的环境下，分别对 IDS/IPS 策略的不同规模(50 条，100 条，150 条，200 条)、防火墙策略的不同规模(50 条，100 条，300 条，500 条)的响应时间进行了验证。结果如图 2 所示。

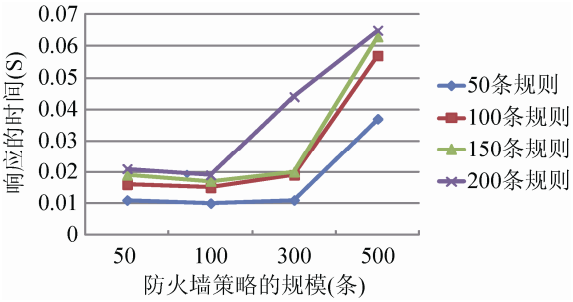

图 2 冲突检测算法的响应时间

图 2 显示了防火墙策略和 IDS/IPS 策略冲突检测算法，在不同规模下的的响应时间。从图中可以看出：在防火墙规则的规模为 500 条，IDS/IPS 规则的规模为 200 条的情况下，响应时间为：0.065 s。

实验结果验证了算法可以适应大规模的防火墙策略和 IDS/IPS 策略的冲突检测。

4.3 冲突在策略中所占的比例

该电厂网络中安全规则的总条数为 820 条，对其中隐含冲突实现全面检测，其结果如图 3 所示。

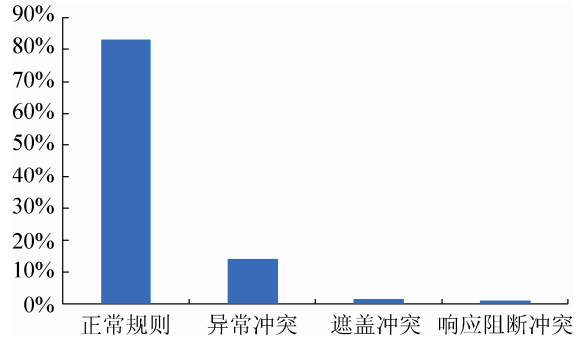

图 3 冲突在总规则中所占的比例

检测结果显示，其中正常的规则数为 682 条，异常冲突的规则数为 120 条，遮盖冲突的规则数为 13 条，响应阻断冲突的规则数为 5 条。3 类冲突在总规则中所占的比例：正常规则占 83%，异常冲突的规则占 14%，遮盖冲突的规则占 2%，响应阻断冲突的规则占 1%。从数据中，可以看出异常冲突是 3 类冲突里最多的一类冲突，这类冲突中，IPS 丢弃防火墙允许的报文。规则中存在少量的遮盖冲突和响应阻断冲突。

5 结论

本文研究防火墙和 IDS/IPS 协同防御场景中，防火墙策略和 IDS 策略冲突检测算法。首先给出了防火墙策略的语义模型、IDS/IPS 策略的语义模型。然后给出了防火墙策略和 IDS/IPS 策略冲突的划分，并证明了划分的完整性，接着，基于 buddy 软件包，给出了防火墙策略和 IDS/IPS 策略的冲突检测算法；最后验证了算法的正确性和可扩展性，并统计了三种冲突的分布比例。实验表明：算法在较大规模的网络环境中，响应时间也较小；算法检测出的三种类型的分布比例显示：在实际网络冲突的数目高达 14%。将来的工作主要集中在防火墙策略和 IDS/IPS 策略的自动冲突消解算法的研究。

参考文献：

[1] Karen Scarfone, Peter Mell. Guide to Intrusion Detection and Prevention Systems (IDPS) [EB/OL]. (2007-02) [2014-06].http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[2] Andy Cuff Intrusion Detection Terminology [EB/OL]. (2010-02) [2014-06] www.securityfocus.com/infocus/1728

[3] Al-Shae E S, Hamed H H. Firewall Policy Advisor for anomaly discovery and rule editing [C]// IFIP/IEEE Eighth International Symposium on Integrated Network Management. USA: IEEE, 2003 (5): 17- 30.

[4] E Al-Shaer, H Hamed. Discovery of policy anomalies in distributed firewalls [C]// IEEE INFOCOM. USA: IEEE, 2004(4): 2605-2616.

[5] Al-Shaer E, Hamed H, Boutaba R, *et al*. Conflict classification and analysis of distributed firewall policies

[J]. IEEE Journal on Selected Areas in Communications (S0733-8716), 2005, 23(10): 2069-2084.

[6] Hu H, Ahn G J, Kulkarni K. FAME: a firewall anomaly management environment [C]// Proceedings of the 3rd ACM workshop on Assurable and usable security configuration. USA: ACM, 2010: 17-26.

[7] Hu H, Ahn G J, Kulkarni K. Detecting and resolving firewall policy anomalies [J]. IEEE Transactions on Dependable and Secure Computing (S1545-5971), 2012, 9(3): 318-331.

[8] Hamed H, Al-Shaer E, Marrero W. Modeling and verification of IPSec and VPN security policies [C]// 13th IEEE International Conference on Network Protocols. USA: IEEE, 2005 (11).

[9] Hamed H, Al-Shaer E. Taxonomy of conflicts in network security policies [J]. Communications Magazine (S0163-6804), 2006, 44(3): 134-141.

[10] S Ferraresi, S Pesic, L Trazza, *et al*. Automatic Conflict Analysis and Resolution of Traffic Filtering Policy for Firewall and Security Gateway [C]// IEEE International Conference on Communications. USA: IEEE, 2007: 1304-1310.

[11] Gobjuka H, Ahmat K A. Fast and scalable method for resolving anomalies in firewall policies [C]// 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). USA: IEEE. 2011: 828-833.

[12] Stakhanova N, L Yao, A A Ghorbani. Classification and Discovery of Rule Misconfigurations in Intrusion Detection and Response Devices [C]// Privacy, Security, Trust and the Management of e-Business, 2009. USA: IEEE. 2009: 29-37.

[13] J Alfaro, N Boulahia-Cuppens, F Cuppens. Complete analysis of configuration rules to guarantee reliable network security policies [J]. International Journal of Information Security (S1615-5262), 2008, 7(2): 103-122.

[14] A Westerinen, J Schnizlein, J Strassner, *et al*. Terminology for Policy-Based Management [EB/OL]. (2001-11) [2014-07] http://www.rfc-editor.org/rfc/rfc3198.txt

[15] J Lind-Nielsen. The buddy obdd package [Z/OL]. http://www.bddportal.org/buddy.html.2005.

[16] 古天龙, 徐周波. 有序二叉决策图及应用 [M]. 北京: 科学出版社, 2000: 30-45.

(上接第 2769 页)

[13] 甘敏, 丁明, 董学平. 基于改进 Mycielski 方法的风速预测 [J]. 系统工程理论与实践 (S1000-6788), 2013, 33(4): 1084-1088.

[14] 陈妮亚, 钱政, 孟晓风, 等. 基于空间相关法的风电场风速多步预测模型 [J]. 电工技术学报, 2013, 28(5): 15-21.

[15] 王扬, 张金江, 温柏坚, 等. 风电场超短期风速预测的相空间优化邻域局域法 [J]. 电力系统自动化 (S1000-1026), 2011, 35(24): 39-43.

[16] Liu H, Tian H Q, Li Y F, *et al*. Comparison of Four Adaboost Algorithm based Artificial Neural Networks in Wind Speed Predictions [J]. Energy Conversion and Management (S0196-8904), 2015, 92: 67-81.

[17] Shi J, Ding Z H, Lee W J, *et al*. Hybrid Forecasting Model for Very-short Term Wind Power Forecasting based on Grey Relational Analysis and Wind Speed Distribution Features [J]. IEEE Transactions on Smart Grid (S1949-3053), 2014, 5(1): 521-526.

[18] 李俊芳, 张步涵, 谢光龙, 等. 基于灰色模型的风速-风电功率预测研究 [J]. 电力系统保护与控制 (S1674-3415), 2010, 38(19): 151-159.

[19] 王子赟, 纪志成. 基于灰色-辨识模型的风电功率短期预测 [J]. 电力系统保护与控制 (S1674-3415), 2013, 41(12): 79-85.

