防火墙安全策略配置与分析方法研究

李沛婷，陈　飞，鲁知朋
（中国电子科技集团公司第三十研究所，四川　成都　610041）

摘　要：提出了一种基于流量数据的防火墙安全策略配置与分析方法，首先进行流程数据采集，然后基于攻击和恶意代码特征库以及规则特征库展开流量检测，对流量数据进行特征行为匹配，标记异常流量数据，接着基于异常流量报警信息生成防火墙安全策略并进行阻断以实现策略自动生成。最后提出安全策略分析的规则及流程，实现防火墙安全策略优化建议的生成，以辅助管理员完成安全策略配置及优化，提升运行维护效能，满足系统快速开通、策略动态调整等场景下的快速响应需求。

关键词：流量数据；特征库；策略自动生成；防火墙策略；安全策略优化建议
中图分类号：TP393. 09　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 06. 004
引用格式：李沛婷，陈飞，鲁知朋. 防火墙安全策略配置与分析方法研究［J］. 网络安全与数据治理，2025，44(6)：28 - 35.

Research on firewall security policy configuration and analysis methods

Li Peiting，Chen Fei，Lu Zhipeng
（The 30th Research Institute of China Electronics Technology Group Corporation，Chengdu 610041，China）

Abstract：This paper proposes a firewall security policy configuration and analysis method based on traffic data. Firstly，process data is collected，followed by traffic detection based on attack and malicious code feature libraries as well as rule feature libraries. The traffic data is analyzed by matching characteristic behaviors，and abnormal traffic data is marked to obtain the traffic analysis results. Based on the abnormal traffic alarm information，firewall security policies are generated to detect and block abnormal traffic，achieving automatic policy generation. Finally，rules and processes for security policy analysis are proposed to implement a security policy analysis method. This enables the generation of firewall security policy optimization recommendations to assist administrators in completing security policy configuration and optimization，improving operation and maintenance efficiency，and meeting the needs of rapid system deployment and dynamic policy adjustments.

Key words：traffic data；feature library；security policy auto-generation；firewall policy；security policy optimization recommendations

www.pcachina.com

0　引言

随着企业的关键业务活动越来越依赖于网络，各种安全事件的发生率不断攀升，造成的不良影响越来越大，防火墙的重要性也越来越高[1]。防火墙作为网络安全的第一道防线，一直作为内部网络和外部网络之间的屏障。其用途是通过允许、拒绝、重定向通过防火墙的数据流量，提供不同网络之间服务访问的控制和审计，包括基于用户和协议的策略定义、URL 过滤、协议识别等。典型的防火墙策略由源地址、目的地址、传输层协议、源端口、目的端口、应用协议决定，并以数据包到达或者离开接口为基准。防火墙策略的部署依赖于业务需求的正确解析、防火墙策略配置方案的正确生成、策略内容的正确下发，是一个复杂且容易出错的过程[2]。正确提升防火墙策略配置效率，对防护网络和设备的安全至关重要[3]。

已有很多学者展开了安全策略相关研究，陈浩宇[4]提出网络安全策略的自动化管理方案，使网络管理员能够采用可编程的方式对网络安全事件进行响应，提高了策略管理效率与事件响应速度，但是缺少对安全策略的分析，没有给管理员提供配置建议。吴蓓[5]研究了安全策略转换和冲突检测技术，详细剖析了安全策略的概念及策略分类准则，提出了安全策略冲突模型和安全策略转换模型，但是这些模型的普适性、正确性还有待验证。周佳等[6]进行了安全配置策略自动生成与验证技术研究，分别从安全配置策略形式化描述、安全配置意图与策略

映射模型构建及验证、安全配置策略自动转译、安全配置策略冲突检测及优化等进行详细介绍，以实现网络安全配置意图准确、快速转化为安全设备可识别执行的网络安全策略，但是没有将研究方法应用在具体安全设备上进行验证。综上所述，已经有很多学者研究如何高效智能地配置安全策略，以期降低人工成本以及减少人为配置安全策略的主观性和复杂性，但是将方法应用到实际安全设备中的较少。本文以防火墙安全设备为切入点，研究防火墙安全策略，以及进行安全策略分析。

本文首先介绍防火墙安全策略，并基于结构化语言对防火墙安全策略进行描述。然后采用一种流量数据分析技术，通过特征匹配获得异常流量数据，为安全策略的生成提供数据支撑。接着提出安全策略分析方法，通过分析防火墙安全策略配置情况，如空闲、冗余、被覆盖、冲突、可合并等，给出策略配置建议。安全策略配置与分析方法体系模型如图 1 所示。

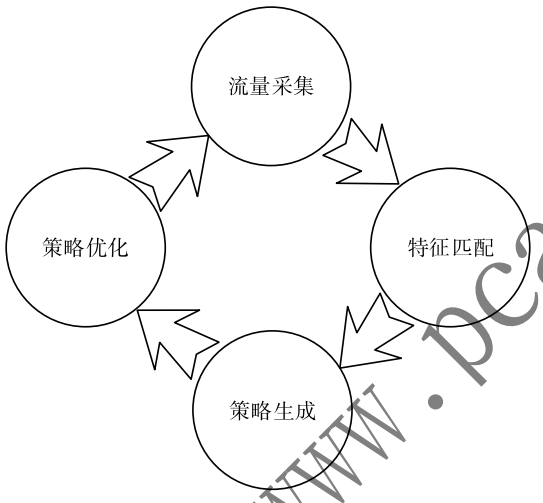

图 1　安全策略配置与分析方法体系模型

1　安全策略结构化语言描述

1.1　双协议栈

双协议栈是指支持 IPv4 和 IPv6 两种协议，使得安全设备在两种协议下均能正常工作，确保网络的兼容性和灵活性。其中 IPv6 是互联网协议第 6 版（Internet Protocol Version 6），是互联网工程任务组设计的用于替代 IPv4 的下一代 IP 协议[7]。随着 IPv6 的推进部署，IPv6 网络威胁数据急剧增加[8]，IPv6 协议下的防火墙安全策略引发关注。本文提出的方法也适用于 IPv6 协议。

1.2　防火墙安全策略描述

防火墙是网络边界安全防护的基础，其连接着内网与外网的不同系统，配置合理的防火墙安全策略可以有效阻止来自外部网络的攻击[9]。防火墙安全策略往往包含了大量规则，如果人为配置规则有时候会导致规则冲突，严重时会影响安全策略的执行效率，大大增加防火墙出现问题的概率。同时，目前网络安全厂商推出多种防火墙产品，如何将多种防火墙产品的安全策略进行统一描述，且转换存储到数据库是安全策略统一配置的前提。所以本文提出了基于结构化语言的安全策略描述，提高了策略的可管理性和可维护性，使得安全策略易于解析和执行，也为不同系统和平台之间的互操作性提供了有力支持。

结构化语言是用来描述定义安全策略的语法结构，可以实现异构系统间的统一解析。本文选用可扩展标记语言（eXtensible Markup Language，XML）对防火墙安全策略进行结构化语言描述。防火墙安全策略主要由地址对象策略、地址对象组策略、服务对象策略、服务对象组策略等进行组合得到，其中相关定义如下：

（1）地址对象策略：定义网络中的具体地址，地址可以是具体 IP 地址、IP 地址范围、子网。

（2）地址对象组策略：由多个地址对象策略组合得到的策略。

（3）服务对象策略：定义网络中的服务，通常由协议和端口号定义。

（4）服务对象组策略：由多个服务对象策略组合得到的策略。

安全策略的 XML 参数及参数说明如表 1 ~ 表 5 所示。

表 1　地址对象配置策略参数说明

序号	参数名	示例/允许取值	说明
1	Name	—	地址对象的名称
2	Desc	—	描述信息
3	IPv	IPv4/IPv6	网络协议版本，IPv4/IPv6
4	Type	=	IN	ENUM	类型，“=”表示地址和子网，“IN”表示范围，“ENUM”表示枚举
5	IP	—	若 Type 为“=”，填写 IP 地址；若 Type 为“IN”，填写起始地址 IP；若 Type 为“ENUM”，填写单个或者多个 IP（最多 64 个），若有多个，用半角逗号分隔
6	Mask	—	若 Type 为“=”，填写子网掩码；若 Type 为“IN”，填写结束地址 IP；若 Type 为“ENUM”，为空
7	Except	—	若无，填写空串；若有，则可以填写单个或多个排除地址。若为多个（最多 64 个），多个地址之间用半角逗号分隔；若存在地址为范围，以“-”分隔

www.pcachina.com

表 2　地址对象组配置策略参数说明

序号	参数名	示例/允许取值	说明
1	Name	—	地址对象组的名称
2	Desc	—	描述
3	AddrObjs	地址对象必须是地址对象配置文件中已有的地址对象名称	地址对象名称列表，填写单个或者多个地址对象，若有多个，用半角逗号分隔
4	IPv	IPv4/IPv6	网络协议版本

表 3　服务对象配置策略参数说明

序号	参数名	示例/允许取值	说明
1	Name	—	服务对象的名称
2	Type	TCP丨UDP丨LDG丨SDG丨RTITP	协议格式检查类型，TCP丨UDP丨长报文丨短报文丨实时报文
3	Desc	—	描述信息
4	Protocol	TCP丨UDP丨IP	协议类型，全部大写
5	ProtocolNum	1～255	若 Protocol 为 IP 时该字段有效，后续字段全填空；若 Protocol 为 TCP、UDP 时该字段为空，后续字段有效
6	SrcPortOpr	> = 丨IN丨ENUM丨Any	大于等于丨范围丨枚举丨任意
7	SrcPortEnum	—	若 SrcPortOpr 为“ENUM”，可以填写一个或者多个端口值。若为多个，用半角逗号分隔，且端口值范围为（1～65535）
8	SrcPortS	—	若 SrcPortOpr 为“IN”，表示源端口范围的起始值；若 SrcPortOpr 为“ > = ”，为 > = 端口值
9	SrcPortE	—	若 SrcPortOpr 为“IN”，表示源端口范围的结束值
10	DstPortOpr	> = 丨IN丨ENUM丨Any	大于等于丨范围丨枚举丨任意
11	DstPortEnum	—	若 DstPortOpr 为“ENUM”，可以填写一个或者多个端口值。若为多个，用半角逗号分隔，且端口值范围为（1～65535）
12	DstPortS	—	若 DstPortOpr 为“IN”，表示目的端口范围的起始值；若 SrcPortOpr 为“ > = ”，为 > = 端口值
13	DstPortE	—	若 DstPortOpr 为“IN”，表示目的端口范围的结束值

表 4　服务对象组配置策略参数说明

序号	参数名	示例/允许取值	说明
1	Name	—	服务对象组的名称
2	Desc	—	描述
3	SvcObjs	服务对象必须是服务对象配置文件中已有的服务对象名称	服务对象名称列表，填写单个或者多个服务对象，若有多个，用半角逗号分隔

表 5　访问控制策略参数说明

序号	参数名	示例/允许取值	说明
1	Name	—	访问控制策略名称
2	Action	Pass丨Drop	操作动作，放行或阻断
3	Enable	Yes丨No	是否启用策略
4	SrcType	Grp丨Object丨Addr丨Any	源 IP 地址，可以选择地址对象组、地址对象、IP 地址、任意
5	SrcGrp	—	如果 SrcType 源 IP 地址选择地址对象组，填写此字段，若有多个，用半角逗号分隔
6	SrcObj	—	如果 SrcType 源 IP 地址选择地址对象，填写此字段，若有多个，用半角逗号分隔

www.pcachina.com

（续表）

序号	参数名	示例/允许取值	说明
7	SrcAddr	0. 0. 0. 0	255. 255. 255. 255	如果 SrcType 源 IP 地址选择 IP 地址，填写此字段，取值为地址	掩码
8	DstType	Grp	Object	Addr	Any	目的 IP 地址，可以选择地址对象组、地址对象、IP 地址、任意
9	DstGrp	—	如果 DstType 目的 IP 地址选择地址对象组，填写此字段，若有多个，用半角逗号分隔
10	DstObj	—	如果 DstType 目的 IP 地址选择地址对象，填写此字段，若有多个，用半角逗号分隔
11	DstAddr	0. 0. 0. 0	255. 255. 255. 255	如果 DstType 目的 IP 地址选择 IP 地址，填写此字段，取值为地址	掩码
12	SvcType	Grp	Object	Any	服务对象，其中包括端口号和协议类型，服务对象组	服务对象	任意
13	SvcGrp	—	SvcType 值为 Grp 有效，取值为服务对象组名称，填写单个或者多个对象，若有多个，用半角逗号分隔
14	SvcObj	—	SvcType 值为 Object 有效，取值为服务对象名称，填写单个或者多个对象，若有多个，用半角逗号分隔
15	Desc	—	详细描述
16	IPv	IPv4	IPv6	网络协议版本

2 流量数据分析

流量数据采集是流量数据分析的基础，常用的流量采集方式有 Sniffer 嗅探、Wireshark 软件采集、简单网络管理协议 SNMP 采集、NetFlow 或 sFlow 流量监控协议采集、网络接口镜像采集等[10]。本文使用基于镜像端口进行网络流量采集，其主要在网络设备（如交换机、路由器）上配置镜像端口，将指定端口的流量复制到另一个端口进行采集，接着按照地址五元组抽样采集流量，即按源地址、源端口、目的地址、目的端口、协议组合对流量进行抽样采集。流量数据分析主要由数据采集和数据处理两部分组成，如图 2 所示。

2.1 流量数据采集

传统的数据采集流程过多地采用硬件中断、多次数据拷贝等方式来完成数据采集，不可避免地造成过多的硬件资源和性能消耗。提升数据采集效率的方法一方面通过增加硬件资源，另一方面可通过绕过内核的方式来进行。一味增加硬件资源存在成本过高、性能瓶颈等问题，因此，本文引入高性能数据采集引擎，通过基于用户空间输入输出（Userspace I/O，UIO）的旁路数据处理，实现从网卡到最终用户层业务的高效数据传输。整个过程采用轮询模式和高性能数据采集技术，绕过传统内核拷贝和 CPU 硬中断等效率瓶颈，显著节省了 CPU 中断时间和内存拷贝时间，从而大幅度提升流量数据采集效率，节约了大量成本，为后续的处理分析提供良好基础。高性能数据采集流程如图 3 所示，其中：

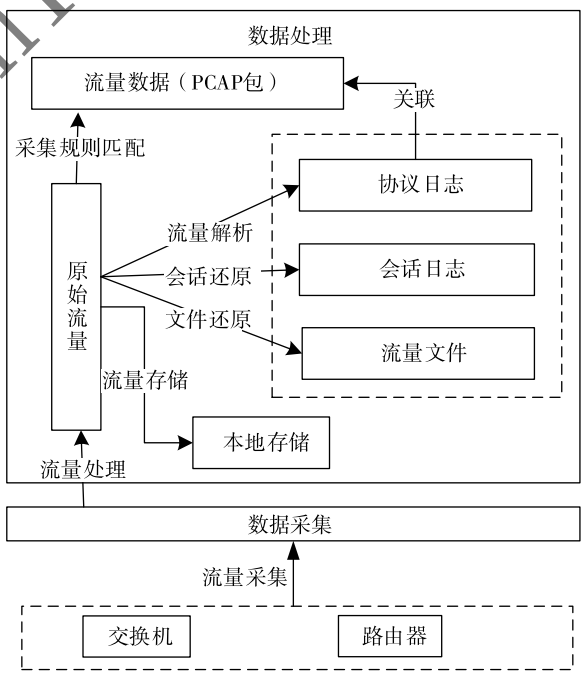

图 2 流量数据分析流程图

（1）旁路部署模式监听经过网卡的镜像网络流量。

（2）高性能数据采集引擎采用轮询模式，调用 UIO 模块直接对网卡进行流量数据读取，绕过内核层。

（3）高性能数据采集引擎对流量中的数据进行规范化处理，并向流量数据处理模块传输处理后的流量数据。

www.pcachina.com

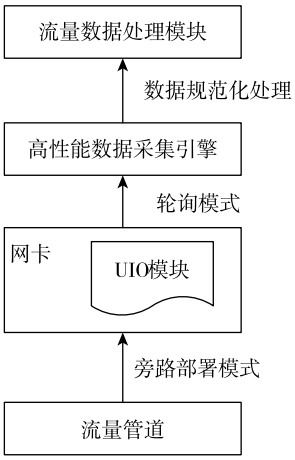

图 3　高性能数据采集流程图

2.2　流量数据处理

流量数据处理指对网络流量进行流量过滤和预处理，提取出 IP 地址、端口、传输协议、应用协议等信息并输出会话日志与协议日志。流量数据处理包括会话还原、流量解析、文件还原和流量存储等处理过程。

（1）会话还原过程提取出五元组数据，识别协议类型及某些特定报文信息。

（2）流量解析过程分析五元组数据、协议类型等报文数据。

（3）文件还原是从网络流量数据中恢复出原始文件的过程。

（4）流量存储是将捕获的网络流量数据进行存储，以便后续的分析和检索。

2.3　特征匹配

通过流量数据处理可以获取网络流量的特征信息，包括 IP 五元组、流量阈值、上下行总流量、持续时间、访问频次、会话数量、会话报文数量、协议和敏感行为识别等。然后基于攻击和恶意代码特征库以及规则特征库进行检测，对流量数据进行特征行为匹配，发现威胁隐患，标记异常流量数据，并生成异常流量报警信息，特征匹配流程如图 4 所示。

（1）协议参数特征匹配：对 IP、ICMP、TCP、UDP、HTTP、DNS、FTP、SMTP 等协议的参数进行特征匹配。

（2）固定位置特征码匹配：在报文的特定位置（如 header、User-Agent 等）进行特征码匹配。

（3）范围特征码匹配：对起始位置和结束位置之间的数据进行特征码匹配。

（4）复合特征码匹配：将上述特征匹配方式组合使用，发现可疑流量。

（5）自定义规则匹配：自定义设置特征规则库。

3　安全策略生成

安全策略生成的核心是将流量中的访问关系按规则或策略库模板生成安全策略，主要生成匹配特征库的异常可疑流量阻断策略。

根据规则生成的策略需要进行聚合，以减少策略条目实现相同的防护效果，同时可以根据业务变化进行策略的适当增删操作，结合策略的优化分析结果，逐步对安全策略进行优化调整使之达到最优状态。基于异常流量生成安全策略的流程如图 5 所示。

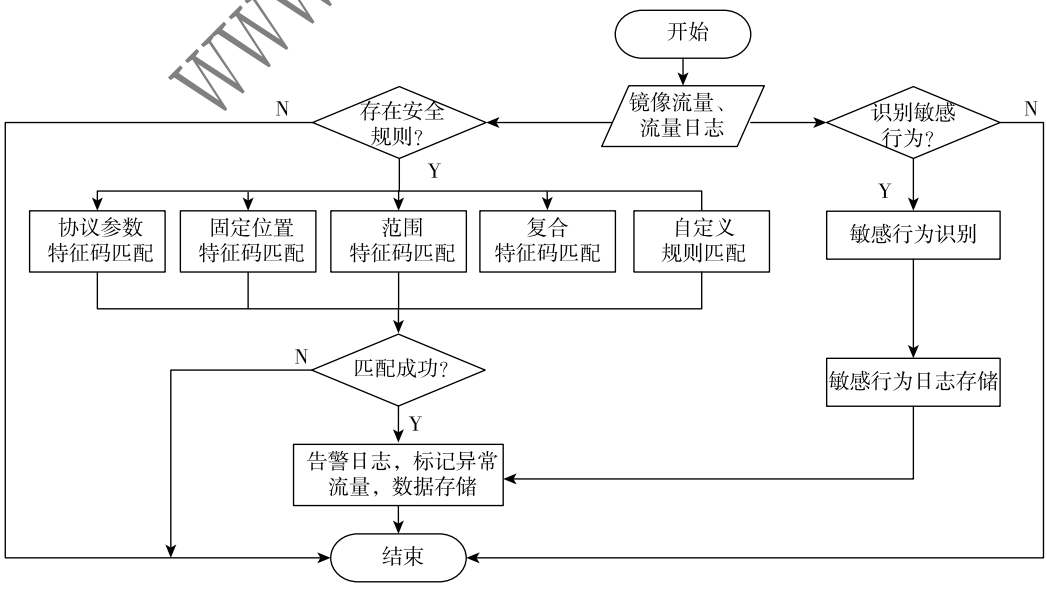

图 4　特征匹配流程图

www.pcachina.com

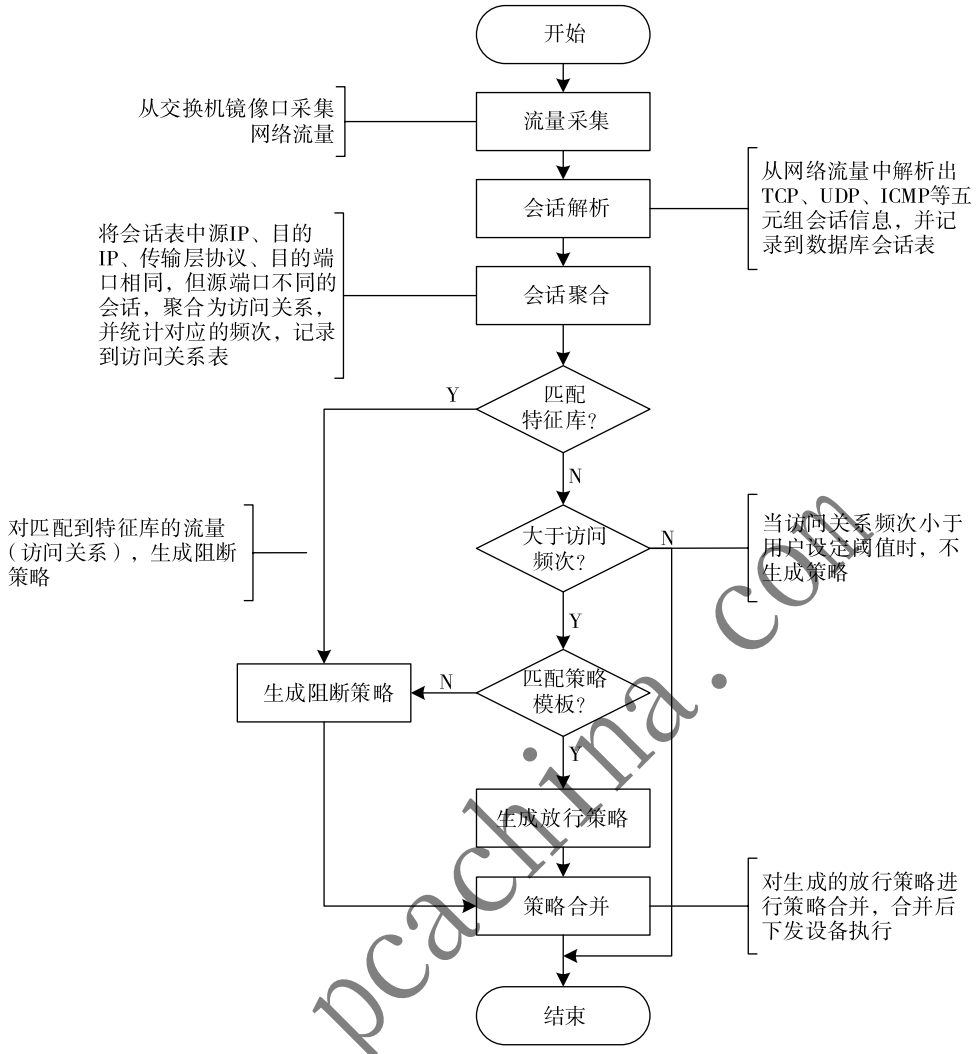

图5　基于异常流量生成安全策略流程图

4　安全策略分析

4.1　策略规则定义

针对不同的网络环境，防火墙策略的配置不仅越来越复杂，而且多域间各策略之间的冲突时有发生，严重影响安全策略的执行效率[11]。因此策略分析主要结合采集的流量数据，检查防火墙配置的安全策略是否空闲、冗余、被覆盖、冲突、可合并等，根据策略分析结果给出策略配置建议，其中空闲、冗余、被覆盖、冲突、可合并的策略规则定义如下：

（1）空闲策略：配置但从未被实际使用的策略，此类策略需要进行删除。

（2）冗余策略：与现有策略重复或覆盖相同流量的策略为冗余策略，通过比较策略的源地址、目的地址、服务对象端口等条件找出冗余策略，此类策略可以删除或者进行合并。

（3）被覆盖策略：其效果被其他策略覆盖，此类策略需要调整策略顺序或进行修改以确保预期的行为。

（4）冲突策略：两条或多条策略之间存在矛盾的情况，此类策略可以进行修改或删除。

（5）可合并策略：两条或多条策略具有相似的策略条件，此类策略可以合并成一条。

4.2　策略分析流程

策略分析主要包含规则管理和优化分析管理，其中规则管理用来配置源地址黑名单、服务黑名单、源地址数量上限、目的地址数量上限、目的端口数量上限等分析规则。优化分析管理主要基于配置的各种分析规则，实现对策略的优化分析并形成优化建议。策略分析流程如图6所示。

4.3　策略优化分析

策略优化分析首先筛选可删除策略，再筛选可拆分策略，最后筛选可合并策略，遵循冗余、被覆盖、冲突、可合并的先后顺序进行分析。当判断出策略冗余，后续

www.pcachina.com

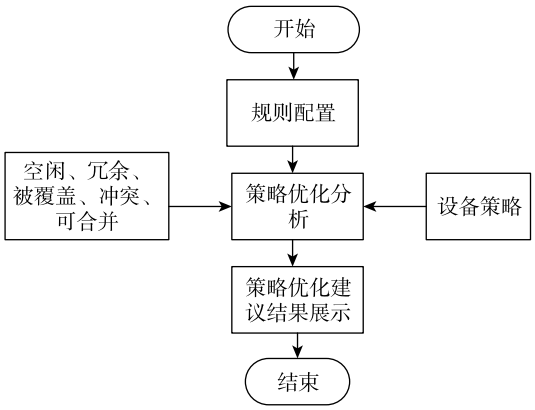

图 6　策略分析流程图

被覆盖、冲突、可合并将不再分析，有问题的策略只会归属于一类问题，这样方便快速定位需要优化的安全策略。其中，空闲策略根据策略配置的五元组与采集到的流量数据进行命中数的判断，分析其是否被命中，未命中的策略标识为空闲策略，当识别出空闲策略时，建议直接删除该策略。策略优化建议生成流程如图 7 所示。

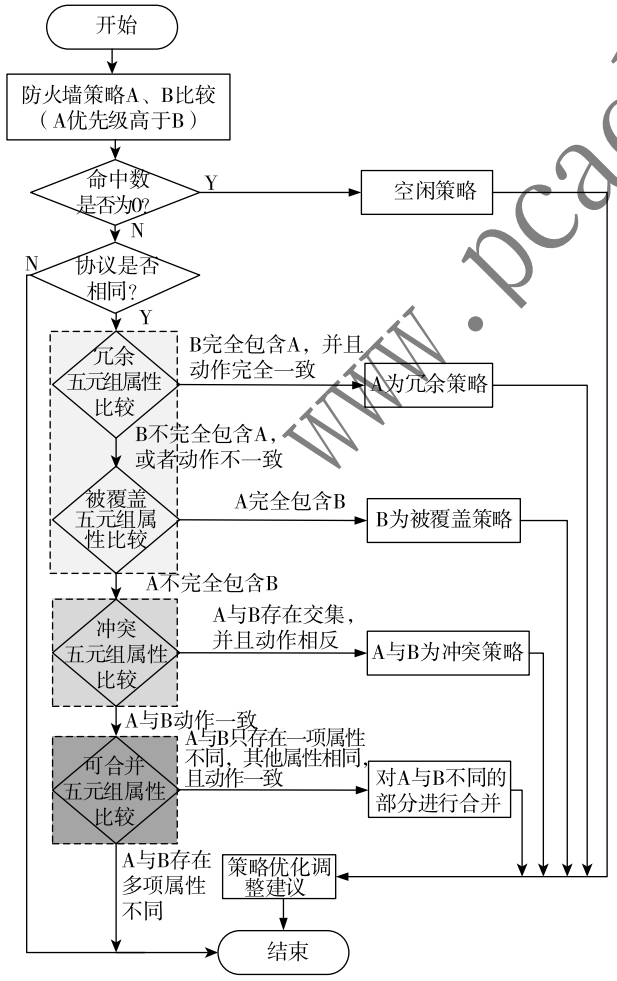

图 7　策略优化建议生成流程图

5　系统设计

5.1　系统架构

根据提及的方法进行了系统设计，设计了一种基于流量数据的策略分析优化系统，旨在验证本文方法的可行性和准确性，系统架构如图 8 所示。

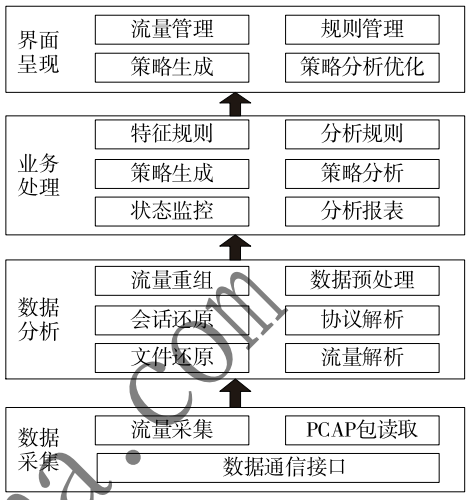

图 8　系统架构图

（1）数据采集层，基于镜像端口的网络流量采集，将符合采集规则配置的网络原始流量保存至本地和外置存储平台。

（2）数据分析层，对流量数据包进行特征解析获取特征信息，包括 IP 五元组、流量阈值、上下行总流量、持续时间、访问频次、会话数量、会话报文数量、协议、敏感行为识别（认证登录行为和文件传输行为日志）。特征解析包括流量重组、数据预处理、会话还原、协议解析和文件还原。

（3）业务处理层，实现业务相关功能，提供自身管理和外部交互的功能，包括特征规则库、策略分析规则、策略生成、策略分析、状态监控和分析报表。

（4）界面呈现层，提供可视化操作界面，基于业务处理层提供的安全服务能力，为网络安全监测、自动防御等使用场景提供支撑。可视化操作界面展示的内容包括流量管理、规则管理、策略生成、策略分析。

5.2　系统实现

根据系统架构研发一种基于流量数据的策略分析优化系统，其中对防火墙安全策略优化分析，结果如图 9 所示。

6　结束语

在安全策略配置时，防火墙的安全策略需逐条手动配置，不仅花费大量时间，而且策略问题定位慢，配置管理效率低下。此外，策略人工配置方式一方面对安全

www.pcachina.com

设备IP	问题名称	建议内容	分析依据
192.168.5.244	可合并策略检查	经过策略分析,设备[华为防火墙1-192.168.5.244],策略[rule13]优先级高于策略[rule17],策略[rule13]和策略[rule17]可进行合并,建议根	两条策略只存在一项不同,其他项都相同,动
192.168.5.244	冲突策略检查	经过策略分析,设备[华为防火墙1 192.168.5.244],策略[rule13]优先级高于策略[rule14],策略[rule13]与策略[rule14]为冲突策略,建议根...	高优先级的策略与低优先级策略存在交集,...
192.168.5.244	冗余策略检查	经过策略分析,设备[华为防火墙1-192.168.5.244],策略[rule1]优先级高于策略[rule2],策略[rule1]为冗余策略,建议删除	高优先级的策略完全被低优先级策略所包...
192.168.5.244	被覆盖策略检查	经过策略分析,设备[华为防火墙1 192.168.5.244],策略[rule14]优先级高于策略[rule15],且策略[rule14]覆盖策略[rule15],建议删除策略[r...	高优先级的策略完全包含低优先级策略,低...
192.168.5.244	被覆盖策略检查	经过策略分析,设备[华为防火墙1 192.168.5.244],策略[rule1]优先级高于策略[rule4],且策略[rule1]覆盖策略[rule4],建议删除策略[rule4]	高优先级的策略完全包含低优先级策略,低...
192.168.5.244	被覆盖策略检查	经过策略分析,设备[华为防火墙1 192.168.5.244],策略[rule1]优先级高于策略[rule3],且策略[rule1]覆盖策略[rule3],建议删除策略[rule3]	高优先级的策略完全包含低优先级策略,低...
192.168.1.1	可合并策略检查	经过策略分析,设备[PC11 192.168.1.1],策略[可合并01]优先级高于策略[可合并02],策略[可合并01]和策略[可合并02]可进行合并,建议...	两条策略只存在一项不同,其他项都相同,动...

图 9　策略优化分析结果图

防护人员的技术要求较高，另一方面使安全防护人员疲于应对庞杂的设备配置任务，一定程度上限制了网络防御效能的发挥。为满足实际应用需求，本文研究了防火墙安全策略配置与分析方法，结合流量数据进行策略分析，实现自动给出防火墙安全策略优化建议，以减少人力工作量，提升安全策略配置的高效性和准确率。

参考文献

[1] 高智强，张亚加，邱啟蒙，等. 改进蜉蝣算法及其在防火墙策略配置中的应用［J］. 陕西理工大学学报（自然科学版），2022，38（2）：41－48.

[2] 吕新辉. 一种数据中心网络防火墙策略自动部署的方法［J］. 江苏通信，2024，40（3）：115－120.

[3] 嵇海丽周. 防火墙安全管理策略及风险评估路径研究［J］. 自动化博览，2024，41（5）：38－43.

[4] 陈浩宇. 网络安全策略的自动化管理与验证研究［D］. 武汉：华中科技大学，2022.

[5] 吴蓓. 网络安全策略的自动化管理与验证研究［D］. 郑州：解放军信息工程大学，2010.

[6] 周佳，邓永晖，贾悠，等. 安全配置策略自动生成与验证技术研究［J］. 通信技术，2020，53（9）：2257－2263.

[7] 罗全珍，张义平，段小焕. 基于双协议栈校园网的防火墙安全策略配置研究［J］. 电子技术与软件工程，2022（23）：5－8.

[8] 王吉昌，张连成，杨剑波，等. 基于多类型威胁的 IPv6 安全防护有效性检测方法［J］. 郑州大学学报（理学版），2024，56（6）63－69.

[9] 王旭东，陈清萍，李文，等. 基于时间的多层防火墙访问控制列表策略审计方案［J］. 计算机应用，2017，37（1）：212－216.

[10] 郝唯杰. 工业网络流量异常智能分析与动态安全策略［D］. 杭州：浙江大学，2022.

[11] 李镭，余兴华，罗淑丹. 一种防火墙安全策略冲突检测方法［J］. 通信技术，2018，51（6）：1425－1429.

（收稿日期：2025－04－15）

作者简介：

李沛婷（1993－），通信作者，女，硕士，工程师，主要研究方向：网络安全。E-mail：2353659484@qq.com。

陈飞（1987－），男，本科，工程师，主要研究方向：网络安全。

鲁知朋（1996－），男，硕士，工程师，主要研究方向：网络安全。

www.pcachina.com

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com