基于动态模板的策略翻译及配置方法

郭云川[1]，李凌[1,2]，李勇俊[1,2]，成林[3]，杜君[4]，张玲翠[1]

（1. 中国科学院信息工程研究所，北京 100093；2. 中国科学院大学网络空间安全学院，北京 100049；
3. 中国信息安全测评中心，北京 100085；4. 北京网御星云信息技术有限公司，北京 100085）

摘 要：为解决大型系统中大量设备配置方式多样性导致人工安全设备配置复杂烦琐、容易出错、效率低下的问题，设计了一种基于动态模板的策略翻译及配置方法。通过构建基于编码的策略翻译模板，利用编码简单、通用、易计算的特点，指导归一化策略向设备个性化配置命令行转换，同时通过关键词对比法，保证策略配置的准确性。实验分析结果证明，所提策略翻译及配置方法具有强扩展性和高准确度。

关键词：设备配置；安全策略；策略翻译；动态模板

中图分类号：TP311

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019236

Policy translation and configuration using dynamic template

GUO Yunchuan[1], LI Ling[1,2], LI Yongjun[1,2], CHENG Lin[3], DU Jun[4], ZHANG Lingcui[1]

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. China Information Technology Security Evaluation Center, Beijing 100085, China
4. Beijing Leadsec Technology Co. ,Ltd, Beijing 100191, China

Abstract: To solve the problem of complex, cumbersome and error-prone configuration of security devices caused by the heterogeneous configuration modes in complex networks, a dynamic template-based scheme for translating and configuring policy was proposed. In detail, considering the code's features, the code-based template for translating policies was constructed to configure the command line conversion, and the keyword comparison method was used to ensure the accuracy of policy configuration. Experiments show that the scalability and the accuracy of the proposed scheme.

Key words: device configuration, security policy, policy translation, dynamic template

1 引言

目前，网络威胁呈现多样化、复杂化和频繁化的特征。为保证网络与系统的安全，需要部署异构安全设备，配置有效安全策略，以确保及时处理网络威胁、保障网络稳定运行。

安全设备的策略具有明显的个性化特征，即对于相同语义的配置命令，不同安全设备的配置命令不同。为异构设备进行统一配置，需要兼容不同安全设备的配置命令。当前普遍采用的策略配置方式是逐一配置，这要求管理员学习不同安全设备的配置命令语法和语义，并通过设备提供的命令行接口（CLI, command-line interface）等方式逐一配置设备策略。该方法需要管理员学习大量配置语法，工作

收稿日期：2019−07−10；**修回日期**：2019−10−23

通信作者：张玲翠，zhanglingcui@iie.ac.cn

基金项目：国家重点研发计划基金资助项目（No.2017YFB0801802, No.2016QY06X1203）；国家自然科学基金资助项目（No.U1836203）；中国科学院战略性先导科技专项基金资助项目（No.XDC02040400）

Foundation Items: The National Key Research and Development Program of China (No.2017YFB0801802, No.2016QY06X1203), The National Natural Science Foundation of China (No.U1836203), The Strategic Priority Research Program of the Chinese Academy of Sciences (No.XDC02040400)

成本较高，且当需要对多台设备配置相同的策略时，管理员需要重复大量相同的操作，效率较低、容易出错。

针对异构设备网络环境下安全设备配置命令语法各异的特点所带来的安全策略配置过程烦琐、容易出错、效率低下的问题，现已有多位学者从不同角度展开了研究[1]。首先，在异构设备网络策略和配置命令描述方面，目前的研究工作主要集中在高级抽象策略描述语言的构建上[2-12]。如 Damianou 等[3]设计了声明性、强类型和面向对象的策略描述语言 Ponder，并在文献[10]中拓展了 Ponder，使其满足分布式的异构环境的策略描述需求。但是，在本文异构设备网络的背景下，这些高级抽象语言并不能高效地从底层对策略进行准确描述。其次，在策略翻译[13]方法的研究方面，早期工程中主要采用了基于特定设备的策略翻译方法，即为每种设备的配置开发一种特定的翻译方法，但该方法通用性差，复杂度高。作为此方法的改进，学者们提出了基于历史推理[14-16]和基于翻译规则的策略翻译方法[17-19]。其中，文献[18]提出了一种自动化生成翻译模板的方法，该方法在满足特定安全性需求的基础上，实现了自动化的翻译模板派生。但在异构设备网络中存在对复杂策略进行高精度翻译的需求，目前的策略翻译方法大多仅适用于简单的访问控制策略，翻译过程复杂，且精度不能满足本文中设备异构网络的需求。最后，在策略配置方面，目前的研究工作主要集中在自动化策略配置方法上[20-23]。其中，文献[20]在自动化策略配置方法的基础上，定义了 5 种配置错误，同时基于归纳法和树结构设计了 2 种错误检测算法，实现了对配置错误的有效检测，保证了自动化策略配置的有效执行。但在本文的异构设备网络的背景下，策略配置过程的可控性较差，准确度较低，现有方法不能保证策略配置的有效性。

由于以上 3 个方面的研究工作无法有效解决本文异构设备网络背景下的产生的问题，因此本文设计了一种基于动态模板的策略翻译及配置方法，主要贡献如下。

1) 为提高配置效率，提出了基于编码的统一策略描述和翻译方法，支持异构设备的配置策略的归一化描述，将归一化的配置策略向个性化策略转换。

2) 为将个性化策略有效地配置到设备上，提出了基于关键词的策略配置方案，通过对比关键词，判定下一步配置动作，以控制配置过程，获取准确的配置结果，保障策略配置的有效性。

3) 为兼容异构安全设备的策略配置方式，提出了基于动态模板的策略翻译及配置方法，通过构建动态模板库，保障以上方案的可扩展性，实现可扩展的策略翻译及配置。

2　相关工作

策略翻译及配置[1]是将统一描述的策略转化为设备个性化的策略并配置到相应设备上的过程，包括策略描述语言（PDL, policy description language）、策略翻译方法和策略配置方法，其相关工作讨论如下。

2.1　策略描述语言

异构网络设备环境下，信息异构性和自治性等特征导致各类设备安全策略兼容性低和可扩展性低等问题[2]。因此，需要一种具有高兼容性、细粒度和可扩展性的策略描述语言，来统一管理和配置设备策略。针对上述需求，很多学者从不同角度对策略描述语言展开了研究。

首先，策略描述语言研究初期的重点主要集中在策略静态描述。Damianou 等[3]设计了 Ponder 语言，通过采用强类型、声明性和面向对象的方法，满足了大规模策略管理及配置的需求，同时使 Ponder 语言保持了良好的灵活性和自适应性。为了满足复杂计算机系统存在的策略表述需求，研究者提出了 SANTA 语言[4-7]，该语言遵循基于规则的方法，采用积极授权、消极授权、冲突裁决 3 种策略规则来定义访问控制策略语言。上述工作主要侧重于静态地对安全策略描述，并未考虑如何对系统的行为情况进行表示。

针对上述问题，研究者提出了动态策略描述语言，该类语言的研究重点是对系统行为进行建模。Lobo 等[8]设计了策略描述语言，基于自动机理论采用“事件−条件−行为”形式将一系列事件映射为特定行为功能函数，从而实现对策略的精确描述。Ribeiro 等[9]提出的安全策略语言（SPL, security policy language）是一种事件驱动（event-driven）的策略语言，其支持基于历史（history-based）的和基于义务（obligation-based）的访问控制策略。SPL 采用类形式的定义，可以使用不同的参数实例化。

尽管上述策略描述语言能够简洁地对策略进行准确描述，但它们并没有充分考虑对异构环境的兼容程度。针对该问题，Damianou 等[10]将 Ponder 语言进行了进一步改进，规范了 Ponder 语言在分布式环境下的主体、目标、生命周期以及部署模型等性质，提高了 Ponder 语言的在分布式环境下的兼容性。Abwnawar 等[11]则将 SANTA 语言拓展到了异构云环境的数据隐私保护场景中，实现了对复合属性的支持。代向东等[12]提出了一种简单策略规范描述语言，实现对底层设备策略的描述。

上述策略描述语言实现了对异构策略的精确描述，但这类策略描述语言大多都存在抽象程度高，且执行性和扩展性较差的缺点，因此无法对异构设备网络环境下底层安全设备策略进行统一描述。

2.2 策略翻译方法

策略翻译是将统一的策略转换成设备个性化策略的过程[13]，是兼容异构配置方式的核心，包括以下 3 种方式：基于特定设备的策略翻译、基于历史推理的策略翻译和基于规则的策略翻译。

基于特定设备的策略翻译的核心思想是为每一种配置开发一种翻译方法。这类方法简单且翻译精准，但是无法随着设备种类增加进行灵活扩充，需要针对新设备进行重新开发，通用性和扩展性弱。

基于历史推理的策略翻译的核心思想主要是借鉴历史案例进行翻译。Beigi 等[14]采用案例推理的方法进行策略翻译，通过将案例存储于历史案例库中，对其进行推理翻译。为了保证此类方法的翻译效果，需要大量的历史案例。随着案例增多，此类方法搜索和推理速度下降。针对这一问题，Han 等[15]提出了一种协同策略管理机制（CPA, collaborative policy administration）来减小历史策略的搜索和推理负担，通过计算相似性来获取相似的历史策略，提高了策略翻译速度。Wang 等[16]采用大规模半监督学习分类历史数据，基于分类结果实现了安全策略的自动分析及精化，进而实现了策略翻译。

基于规则的策略翻译[9]通过自定义策略描述语言，设计了一套基于固定翻译方法的解析重构器，对统一策略进行解析、拆分、重构、组装等操作，将统一的策略转换为个性化策略。Leighton 等[17]通过构建转换规则，将统一描述的策略翻译为新格式的策略，达到策略翻译的可扩展性。这种方法虽然较传统的策略翻译方法更灵活，但需要通过人工添加新的脚本和转换规则。针对此问题，Rudolph 等[18]设计了翻译模板自动生成方法，实现了满足特定域的安全性需求的模板派生，并将该类方法应用于工业案例中。Yang 等[19]提出了基于自动机的安全策略翻译方法，该方法实现了在用户只具有有限知识的情况下进行策略翻译。当前基于规则的策略翻译仅适用于高级访问控制策略，存在翻译过程复杂和翻译结果不够精准等问题。

2.3 策略配置方法

陈文惠等[20]定义了 5 种配置错误，给出了基于归纳法和树结构的 2 种错误检测算法。但该方法主要从策略本身逻辑出发，检测当前策略与历史策略之间冲突导致的配置错误，并没有考虑当前策略语法语义与设备需求不符导致配置失败。Lobo 等[21]通过拓展 PDL 语言，在私有域中实现了防火墙策略的描述、翻译和配置。Jillepalli 等[22]将其提出的 HERMES 语言动态地集成到 HiFiPol 策略管理系统中，实现了策略自动配置。李福亮等[23]将对配置结果的验证作为独立模块，以确保策略自动配置的有效性，但该方案不能调整不满足预期的配置。

3 策略归一化描述

本文中的策略是用于描述异构设备网络环境中安全设备行为规则的集合。设备配置命令格式依赖于设备类型，不同类型设备具有不同的配置命令格式。本节提出一种统一的策略描述格式，并将之实例化为不同模板，以兼容不同类型设备的配置。

本节定义基于编码的统一策略，如式(1)所示。策略 C 是由 Sub 、 Obj 、 Type 和 Param 构成的四元组，其中， Sub 表示策略的生成与发送者， Obj 表示策略的接收与执行者， Type 表示策略类型（如包过滤、连接关闭等）， Param 表示策略参数。

$$C=\{<\text{Sub},\text{Obj},\text{Type},\text{Param}>,\cdots\} \tag{1}$$

其中， Sub 、 Obj 、 Param 可统一用式(2)来描述。

$$\begin{aligned} F&=N:V;F\\ F&=N:[V];F\\ F&=\varnothing \end{aligned} \tag{2}$$

其中， F 为策略元素，表示 Sub 、 Obj 或 Param ； N 为元素编码， V 为元素值。

如式(3)所示，参数类型包括 3 种类型，用 n、e、s 表示，分别为数值、枚举值、字符串值。

$$V = n \cup e \cup s \tag{3}$$

如式(4)所示，若参数值类型为枚举型，其具体值用符号“|”分隔，表示该值为 $e_1 \sim e_n$ 中的一个，且需要被符号“[ ]”包括起来。一条策略包括多个参数编码和参数值组成的键值对，参数编码与参数值之间通过符号“:”分隔，键值对之间由符号“;”分隔。

$$e = e_1 \,|\, e_2 \,|\, \cdots \,|\, e_n \tag{4}$$

策略类型 Type 的语义定义如式(5)所示。

$$\begin{aligned} &\text{Type} = N : T; \\ &\text{Type} = \varnothing; \end{aligned} \tag{5}$$

其中，$T = n \cup s$。

基于上述定义的统一策略格式，归一化的策略描述格式示例如下。

PolicyType_SerialNum : *PolicyType*;

PolicyObject_SerialNum : *PolicyObject*;

PolicySubject_SerialNum : *PolicySubject*;

Parameter1_SerialNum: [*Parameter1-1*| *Parameter*1-2|…];

Parameter2_SerialNum :”*Parameter2*”;

Parameter3_SerialNum : *Parameter3*;

…

其中，正体字为元素编码（即式(2)和式(5)中的 N），斜体字为参数值（即式(2)和式(5)中的 V 或 T）。该策略采用编码表示策略元素，采用键值对的方式表示元素及其对应值。

基于该描述方式，可对差异化的命令求并集，得到归一化策略模板，以此兼容各种设备，且可定义新的策略或对参数进行扩展，动态获得新的模板，以此支持未来的新命令。

4　归一化策略翻译

策略翻译是将归一化成统一格式的策略转换为设备个性化策略。为了保障策略翻译的可扩展性和精准有效性，本文在动态模板的基础上通过策略校验和策略映射这 2 个步骤，实现向个性化策略的翻译，确保策略翻译的可扩展性。

4.1　归一化策略校验

为使归一化策略能适配多种类的安全设备，保障安全设备的个性化配置能力，本文采用求并集的方式对所有设备策略参数进行归一化编码。由此导致在配置异构设备时，存在某些设备无法支持归一化策略中的部分参数配置的现象。此外，某些参数间存在依赖关系。为此，本文基于统一描述的策略格式，设计了基于编码的策略检验算法。该算法提取设备各异的配置需求，构建为策略校验模板，在策略映射前对策略进行校验，筛选设备能识别的参数，并计算这些参数能否满足设备需求。

图 1 给出了 2 种防火墙的数据分组过滤命令组（分别称这 2 种防火墙为防火墙 A 和防火墙 B）。从图 1 可以看出，这 2 种防火墙具有如下特征。1) 数据分组过滤能力差异。如图 1 所示，防火墙 A 可以根据网络数据分组协议、IP 地址等参数进行判断处理，而防火墙 B 的配置参数更加丰富，如可以对 LSAP 等参数进行设置。2) 参数/命令间存在依赖关系。如在为防火墙 A 配置 IP 数据分组过滤之前，必须先通过命令行定义该 IP 对象，而后引用该对象进行配置过滤规则。3) 具有不同的必选和可选参数。如防火墙 A 的配置命令中，网络二层协议号是必选项，目的 MAC 地址是可选参数。

在策略翻译中若不考虑上述 3 个特征，将导致翻译不准确，翻译后的命令组无法识别等问题。针对该问题，本文设计了统一策略校验算法，如算法 1 所示。其核心思想是：首先删除统一策略中设备不能识别的参数；然后校验策略中是否包含设备所必须参数及其依赖参数，若校验不通过，则校验失败；最后删除策略中目标设备的可选参数及其不完整的依赖参数，形成校验后的统一策略，从而减轻管理员的策略配置难度，防止管理员错误配置导致的不可控问题。

算法 1　统一策略校验算法

输入　统一策略的参数编码集合 S，策略校验模板 TP

输出　校验通过或失败

1)for $i \in S$

2)　if $i \notin$ TP

3)　　del $S(i)$

4)for $j \in$ TP

5)　if j 为必选项，且 $j \notin S$

6)　　return false

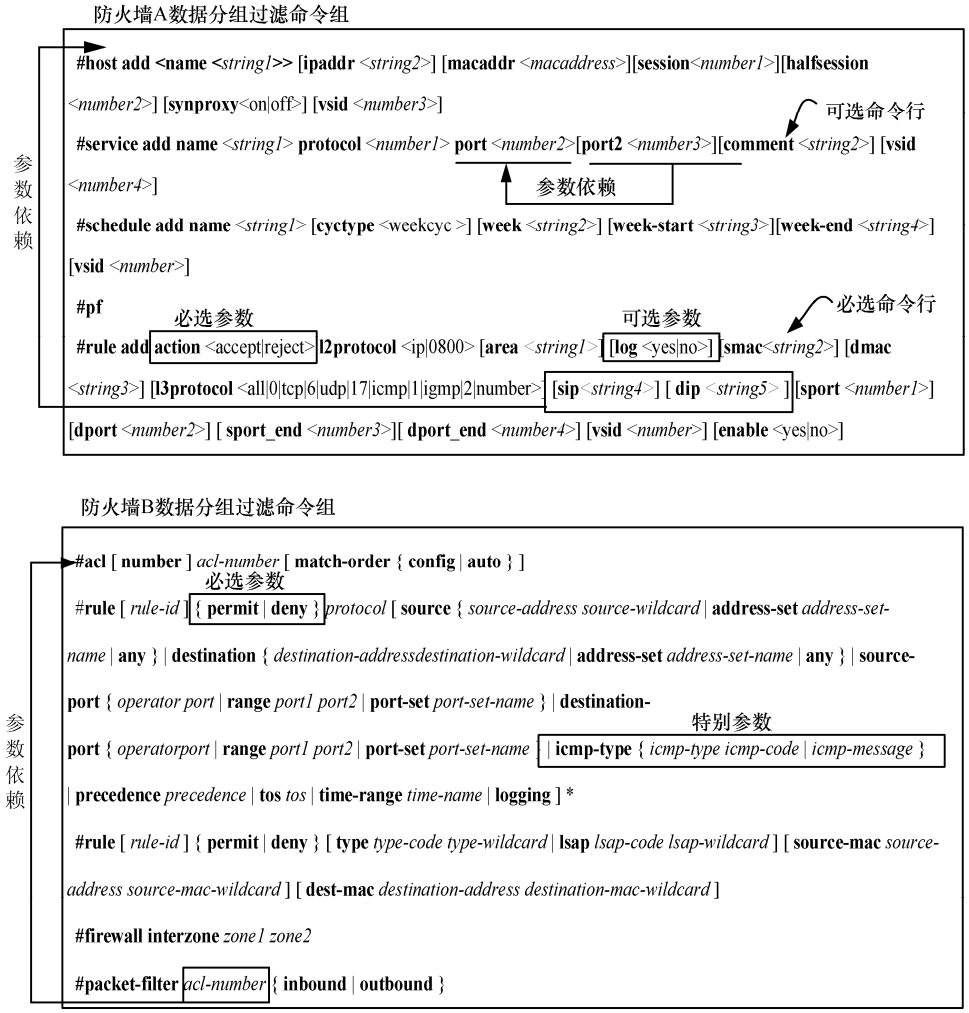


图 1　策略参数关系示例

7)　if j 是必选项 and j 依赖的参数$\notin S$

8)　　return false

9)　if $j\in S$ and j 依赖的参数$\notin S$

10)　　del $S(j)$ and del S(j 依赖的参数)

11) return true

为了保证策略翻译的准确性和可扩展性，需依据设备配置命令需求，构建策略校验模板，并动态添加至策略模板库中。

4.2　归一化策略映射

虽然不同类型的安全设备个性化配置策略存在差异，但均由一条或若干条命令行组成，命令行由命令标识符、提示词和提示符组成。为了保证有效的策略翻译，本节定义一种统一的策略翻译模板，基于个性化的策略构建为策略翻译模板。

策略翻译模板由组成该策略的所有命令行的翻译模板组成，命令行翻译模板语法如式(6)所示，其中，S 表示单条命令行翻译模板；A 为每行命令行的开始标志符，如式(7)所示，由符号@或者符号#组成，@表示当条命令行为当前策略的可选命令行，#表示当条命令行为当前策略的必选命令行；B 为每行命令行的实际内容，如式(8)所示，可以为 $[KNP]B$ 、$KNPB$ 或者 ∅ 的形式。K 表示命令标识符，N 为参数编码，P 表示目标设备的参数格式，如式(9)所示，其中 pattern 为目标设备能识别的格式信息。KNP 组成命令行参数模板的基本信息，若某参数不是必选参数，则用[ ]表示。

$$S = AB \tag{6}$$

$$A = @\,|\,\# \tag{7}$$

$$B = [KNP]B;|\,KNPB;|\,\varnothing \tag{8}$$

$$P = <\text{pattern}> \tag{9}$$

从个性化策略向策略翻译模板的映射思路为，通

过统一提示字符串，填充目标设备识别格式模板，构建策略翻译模板。图 2 给出了一个模板构建示例，第一条命令行中，命令标识符“host add”用于提示设备该条命令行的功能，因此翻译模板中保留该命令标识符；而用于提示用户需要填充具体 IP 地址提示字符串“string2”不需要被设备识别，基于归一化策略中的 IP 参数的编码，修改其为对应的编码值，并在其后续连接“<>”并填充“%d.%d.%d.%d”表示该设备需要识别点分十进制的 IP 地址格式。

将个性化的策略命令组重构为翻译模板后，即可指导将统一的策略转换为个性化的策略。如图 3 示例所示，具体过程如下。

1) 参数映射。由于策略归一化中将参数进行统一的编码，因此基于编码解析归一化策略中每个参数编码，在翻译模板找到每个编码中出现的所有位置，并获取该位置后紧接着的目标格式。

2) 格式转换。根据翻译模板中参数后的目标格式，对归一化格式的参数进行转换，形成设备能识别的参数格式。如将归一化 IP 地址数值型参数 0x0ca85a10 根据目标设备需要的点分十进制正则表达式翻译为设备需要的格式“192.168.90.10”。

3) 命令生成。根据步骤 1) 找到的参数位置，将步骤 2)中转换好的参数填充入对应位置，并且删

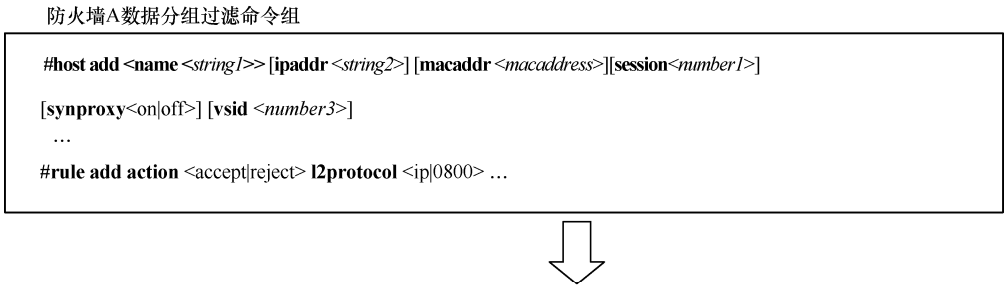


图 2　模板构建示例

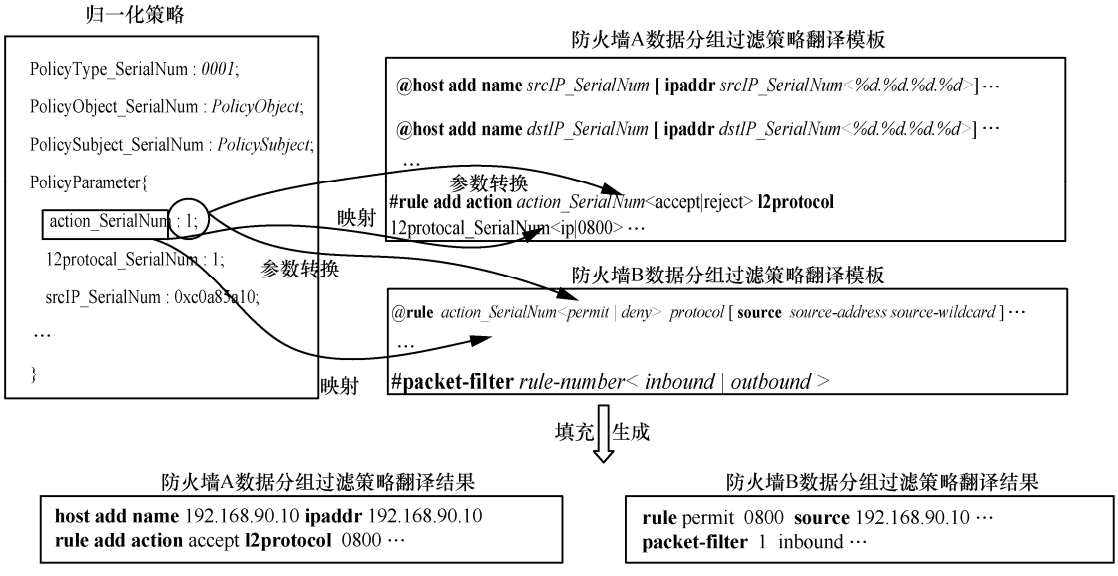


图 3　翻译过程示例

除设备不能识别的字符串和符号，包括自定义的编码和符号，如#和[ ]，最终生成目标设备配置命令组。

通过以上步骤，将归一化描述的策略进行解析、映射、转换、填充，形成目标设备可识别的配置命令，并将归一化的策略翻译为不同设备的配置命令，完成策略翻译。由于采用翻译模板指导翻译的方式，因此可基于设计的翻译模板动态构建规则，通过增改翻译模板的方式实现策略翻译的可扩展性。

5 个性化策略配置

在生成个性化的策略后，根据配置策略对目标设备进行配置，具体配置过程如下。

1) 命令配置。通过设备提供的 CLI 接口，将翻译后的命令行配置到设备上。

2) 结果匹配。在命令行配置过程中，获取每条命令行的配置反馈信息，根据待对比的关键词，判定该反馈信息所体现的配置结果。

循环以上 2 个步骤，在将配置命令下发并配置到目标设备的过程中，目标设备存在 4 种状态，即 $Status_0$~ $Status_3$。$Status_0$ 状态表示目标设备处于监听数据，$Status_1$ 状态表示目标设备接收到连接，$Status_2$ 状态表示目标设备收到命令行集合后准备配置，$Status_3$ 状态表示目标设备配置命令行后获取配置结果。

如图 4 所示，首先目标设备处于 $Status_0$ 状态，当收到连接请求时进入 $Status_1$ 状态；在 $Status_1$ 状态时收到非空命令行集合后进入 $Status_2$ 状态，而在连接超时或收到断开连接信号时，断开连接进入 $Status_0$ 状态；在 $Status_2$ 状态时，当命令行集合非空时配置命令行后进入 $Status_3$ 状态，而当命令行集合为空时进入 $Status_1$ 状态继续等待接收命令行；在 $Status_3$ 状态时，返回配置成功结果进入 $Status_2$ 状态，继续配置，而返回配置失败结果时进入 $Status_1$ 状态，重新接收命令行。

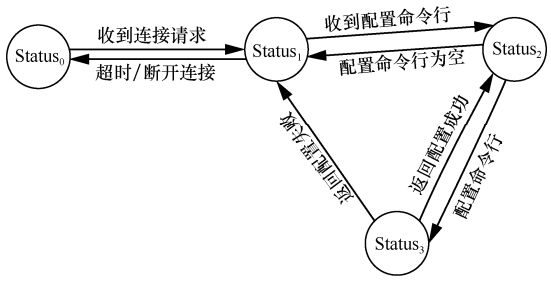


图 4 策略配置目标设备状态转移

通过以上步骤，可以将配置命令逐一配置到设备上，并通过动态增改关键词库，配置新类型的设备，保证策略配置的可扩展性。

6 实验分析

6.1 实验环境

实验环境包括 3 台异构的安全设备、一台服务器和一台交换机，具体信息如表 1 所示。其中，3 台安全设备分别为天融信 NGFW 防火墙、华为 USG6000V 模拟防火墙和 Linux 系统的 IPtables 防火墙，作为待配置安全设备；交换机型号为 CiscoSG200，用于连接服务器与安全设备；服务器的操作系统为 CentOS，用于运行策略翻译及配置系统，使用本文所提出的方法对 3 台异构安全设备进行策略翻译及配置。

表 1 实验拓扑设备信息

设备类别	设备类型	操作系统
服务器	物理机	CentOS
安全设备	天融信 NGFW 防火墙	NGTOS
	华为 USG6000V 模拟防火墙	eNSP 模拟
	IPtables 防火墙	Linux
交换机	CiscoSG200	—

6.2 模板库构建

基于策略归一化方案，对异构安全设备策略进行归一化描述。以网络数据分组过滤策略为例，该策略的归一化过程可描述如下。首先，为网络数据分组过滤策略的序列号 PolicyType_SerialNum 赋值，此处将其定义为“0001”号策略。然后，从“01”号开始依次对策略参数进行编码，编码格式为“SerialNum_0X: Param_Name”，其中“0X”表示第 X 个参数，“Param_Name”为参数名。基于上述策略归一化过程，采用统一的策略编码形式，对异构的策略形式进行归一化描述，从而构建出兼容性强、描述准确的策略形式。结合上述的例子，网络数据分组过滤策略的归一化描述如下。

PolicyType_SerialNum : 0001;
PolicyObject_SerialNum : PolicyObject;
PolicySubject_SerialNum : PolicySubject;
SerialNum_01 : Action;
SerialNum_02 : SrcStartIP;
SerialNum_03 : SrcEndIP;

SerialNum_04 : SrcStartPort;
SerialNum_05 : SrcEndPort;
SerialNum_07 : DstStartIP;
SerialNum_08 : DstEndIP;
SerialNum_09 : DstStartPort;
SerialNum_10 : DstEndPort;
SerialNum_11 : Protocol;
…

基于上述策略形式，构建基于位图的配置命令校验模板。由于归一化的策略采用编码的方式描述策略参数，因此可根据编码将其转换为位图，即将参数编码作为图中的位置向量，并采用二进制值 0 和 1 来表示对应位置的该参数是否存在。位图的构建过程简单，通过“按位与”运算，能实现较快的位图校验。

根据以上校验方法和位图构建方法，构建配置命令的校验模板，方式如下。首先获取配置命令组所有参数编码，将编码作为位图位置向量，将位图对应的比特位赋值为 1，其他位置赋值为 0，生成第一个校验模板位图，用于过滤不能配置的参数；然后获取配置命令组中必选命令行中必选参数对应的归一化编码，构建为位图，用于初步判断是否包含必选参数；最后依次获取所有参数与命令行依赖的必选参数编码，构建为位图，生成若干个模板位图（若是没有依赖关系，则不需要构建）。将构建完成的位图组放入校验模板库中，当进行策略翻译时，先提取校验模板进行校验，校验不通过则通知管理员。

根据翻译模板构建方案。对实验环境中的防火墙设备进行翻译模板构建。图 5 为对天融信防火墙翻译模板构建的示例，将设备原配置命令格式经过符号转换、关键词替代和目标格式信息填充等步骤，生成策略翻译模板。

天融信防火墙数据分组过滤命令模板

@host add name *srcIP_SerialNum* **[ipaddr** *srcIP_SerialNum*<%d.%d.%d.%d>] [**macaddr** srcMAC_SerialNum<%2x.%2x.%2x.%2x.%2x.%2x>][**session** *session_SerialNum*]
@host add name *dstIP_SerialNum* **[ipaddr** *dstIP_SerialNum*<%d.%d.%d.%d>] [**macaddr** dstMAC_SerialNum<%2x.%2x.%2x.%2x.%2x.%2x>] [**session** *session_SerialNum*]
…
#rule add action *action_SerialNum*<accept|reject> **l2protocol** <ip|0800> …

图 5　策略翻译模板示例

同时，构建策略配置命令标识符模板，将 3 台设备的回复命令标识符存储于模板库中，方便后续提取匹配。

6.3　策略翻译

当策略发送到设备直属的配置系统时，会进行策略翻译，生成目标设备可识别的配置命令，并将其作为策略配置的指导。

进行策略翻译前，首先根据目标设备当前策略的校验模板进行策略校验，如图 6 所示，具体过程如下。

1) 生成配置策略位图。提取当前待配置策略的参数部分，读取其参数关键词编码，将所读编码转化为相应位图，例如若当前策略包含编码为 1、6、7、8、10、14、24 的参数，则将位图中的第 1、6、7、8、10、14、24 位置的比特位赋值为 1，其他位置赋值 0。

2) 获取目标设备校验规则位图集合。获取模板库中对应设备的校验模板。

3) 过滤无关参数。通过 “按位与”操作进行位图校验，过滤当前不能配置的参数。

4) 校验当前策略能否配置。首先，校验策略是

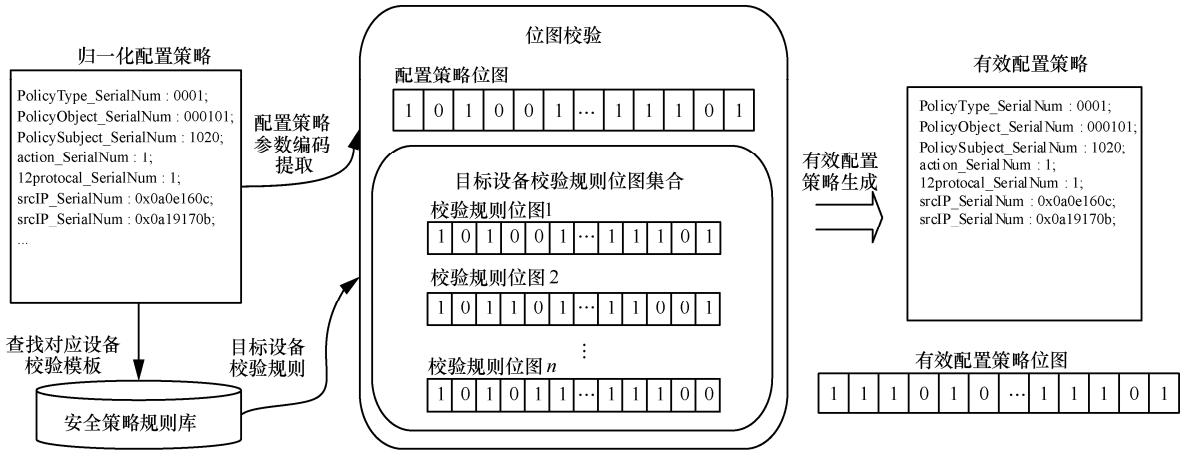


图 6　参数校验示例

否含有必选参数与命令行；然后，依次迭代校验确保策略中包含每个必选参数与命令行所依赖的参数；最后，校验判断是否包含可选参数以及其依赖的参数，确定策略中能配置的可选参数。

校验后，将可配置的策略进行翻译，即基于设备的翻译模板，将归一化编码策略转换为该设备能识别的配置命令，如图 7 所示，具体过程如下。

1) 翻译模板获取。根据当前策略类型和目标设备类型，从模板库中提取该设备配置策略的翻译模板。

2) 参数映射。将待配置策略中的源参数映射到翻译模板上具有相同语义的目标参数。由于采用归一化的编码，因此通过简单的编码数字解析，即可将源参数与翻译模板中的目标参数进行一一映射。

3) 参数格式转换。相同的参数在不同的设备上可能存在不同的表示格式，因此需要将源参数格式转换为目标设备可识别的参数格式。通过提取翻译模板中的参数格式，不需要人工介入，即可实现简单的参数格式转换。

4) 个性化命令生成。根据目标设备翻译模板，按照策略参数编码所映射的位置，填入转换后的策略参数，最终形成目标设备可识别的个性化配置命令集合。

6.4 策略配置

在实验环境中，一共涉及 3 种防火墙，这 3 种防火墙的配置命令各不相同，通过构建这 3 种防火墙配置命令的翻译模板，实现策略到配置命令行的翻译，同时获取每条命令行的配置结果。通过关键词对比判定配置结果，即提取关键词模板中的字符串，比对不同情况的关键词确定配置结果，如天融信防火墙配置命令失败时会返回“error”关键词和具体的错误代码，因此提取“error”关键词与当前配置结果匹配，若匹配成功，则表示该命令行配置失败，反之则配置成功。通过配置结果判定，可以避免连环失败配置，通过重新配置或对失败进行反馈，避免了无效的策略配置。

如图 8 所示，通过人工查看此次实验配置结果

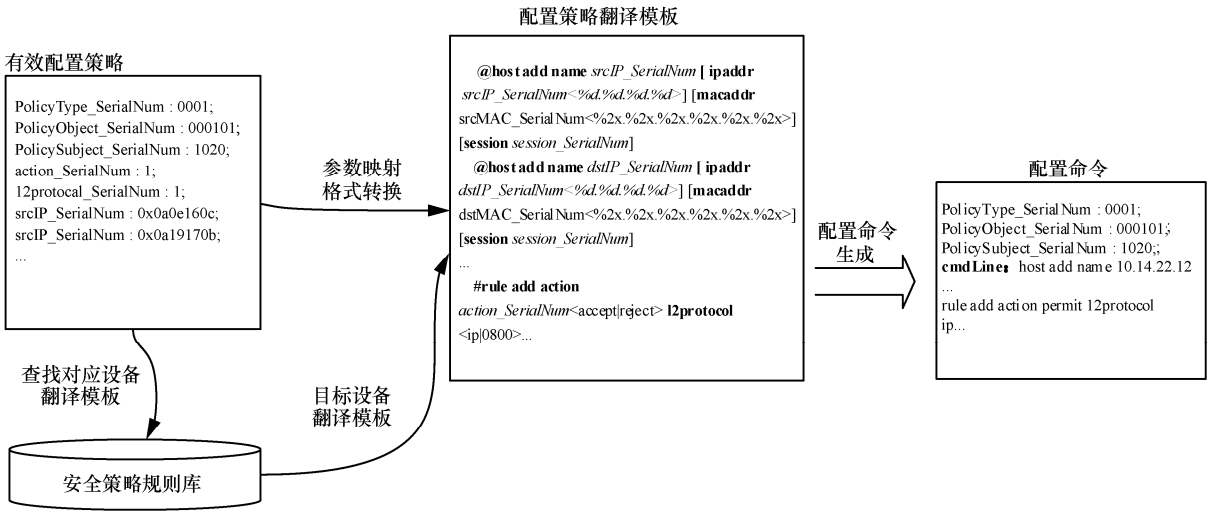


图 7 个性化配置命令生成示例

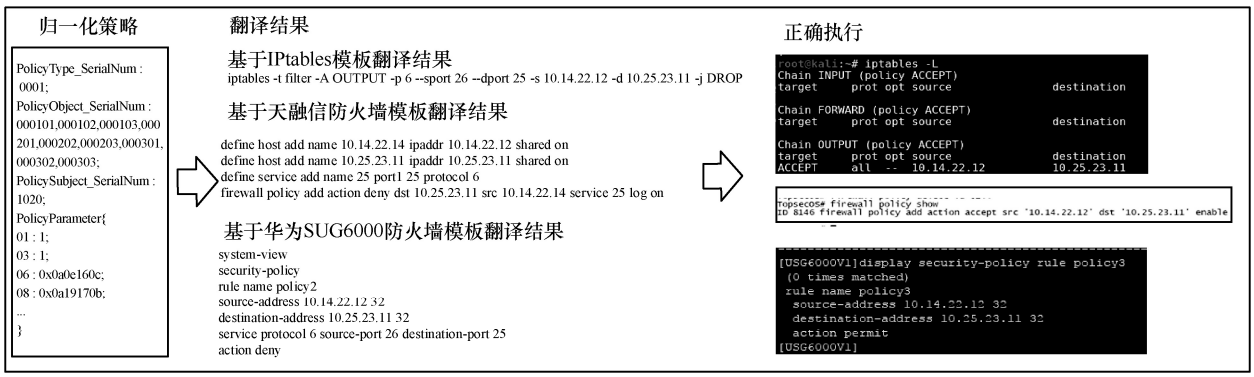


图 8 策略翻译实验

与配置反馈结果一致，证明策略翻译的准确性。由实验结果可知，通过构建新的翻译模板，将归一化的策略翻译为异构设备格式的配置命令，证明了本文所提出的策略翻译方法的可扩展性；图 8 中策略配置成功表明设备正确识别该翻译结果，证明本文中策略翻译的准确性；同时，尝试构建具有参数不全的策略配置设备，获得配置失败的反馈，证明本文中策略校验功能的有效性。

7　结束语

针对异构设备网络中安全设备配置语法不一所带来的配置烦琐、效率低下的问题，设计了一种可扩展、准确性高的策略翻译及配置方法。利用编码简单、易计算的特点降低了策略翻译的复杂度；利用策略校验保证了策略翻译的准确度；通过构建翻译模板，指导归一化策略向个性化策略转换；并采用关键词对比法控制策略配置流程，防止出现无效的、与预期不符的策略配置结果；通过构建动态模板库的方式，保证以上各个步骤的可扩展性。未来的工作可以对翻译模板构建进行优化，采用自动构建方法，减少人工构建的成本。

参考文献：

[1] JOHNSON M, BRADSHAW J M, JUNG H, et al. Policy management across multiple platforms and application domains[C]//IEEE Workshop on Policies for Distributed Systems and Networks. IEEE, 2008: 199-202.

[2] HOLMES B L. Heterogeneous systems: can they ever work together?[C]//Symposium Record Policy Issues in Information and Communication Technologies in Medical Applications. IEEE, 1988: 169-174.

[3] DAMIANOU N, DULAY N, LUPU E, et. al. The ponder policy specification language[J]. Proc of policy, 2001, 55(8):18-38.

[4] JANICKE H, CAU A, SIEWE F, et al. Deriving enforcement mechanisms from policies[C]//IEEE International Workshop on Policies for Distributed Systems and Networks. IEEE, 2007: 161-172.

[5] JANICKE H, CAU A, SIEWE F, et al. A compositional event & time-based policy model[C]//IEEE International Workshop on Policies for Distributed Systems and Networks. IEEE, 2006: 173-182.

[6] SIEWE F, CAU A, ZEDAN H. A compositional framework for access control policies enforcement[C]//The 2003 ACM workshop on Formal Methods in Security Engineering. ACM, 2003: 32-42.

[7] JANICKE H, CAU A, SIEWE F, et al. Dynamic access control policies: specification and verification[J]. The Computer Journal, 2012, 56(4): 440-463.

[8] LOBO J, BHATIA R, NAQVI S. A policy description language[C]//The 16th National Conference on Artificial Intelligence and the 11th Innovative Applications of Artificial Intelligence Conference. 1999:291-298.

[9] RIBEIRO C, ZUQUETE A, FERREIRA P, et al. SPL: an access control language for security policies and complex constraints[C]// The Network and Distributed System Security Symposium. 2001, 1.

[10] DAMIANOU N, DULAY N, LUPU E, et al. Tools for domain-based policy management of distributed systems[C]// IEEE/IFIP Network Operations and Management Symposium. IEEE, 2002: 203-217.

[11] ABWNAWAR N, JANICKE H, SMITH R, et al. Towards data privacy in heterogeneous cloud environments: an extension to the SANTA policy language[C]//2017 Second International Conference on Fog and Mobile Edge Computing. IEEE, 2017: 14-19.

[12] 代向东. 安全策略管理系统中策略描述及策略翻译关键技术研究[D]. 郑州: 信息工程大学, 2007.
DAI X D. Research on key technologies of policy description and policy translation in security policy management system[D]. Zhengzhou: Information Engineering University, 2007.

[13] HALE J, GALIASSO P, PAPA M, et al. Security policy coordination for heterogeneous information systems[C]//The 15th Annual Computer Security Applications Conference. IEEE, 1999: 219-228.

[14] BEIGI M S, CALO S, VERMA D. Policy transformation techniques in policy-based systems management[C]//The 15th IEEE International Workshop on Policies for Distributed Systems and Networks. 2004:13-22.

[15] HAN W, FANG Z, YANG L T, et. al. Collaborative policy administration[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 25(2):498-507.

[16] WANG R, ENCK W, REEVES D, et al. EASEAndroid: automatic policy analysis and refinement for security enhanced android via large-scale semi-supervised learning[C]// 24th USENIX Security Symposium. 2015: 351-366.

[17] LEIGHTON G, BARBOSA D. Access control policy translation, verification, and minimization within heterogeneous data federations[J]. ACM Transactions on Information and System Security, 2011, 14(3):1-28.

[18] RUDOLPH M, FETH D, DOERR J, et. al. Requirements elicitation and derivation of security policy templates—an industrial case study[C]//The 24th International Requirements Engineering Conference. 2016.

[19] YANG J, JEONG J P. An automata-based security policy translation for network security functions[C]//2018 International Conference on Information and Communication Technology Convergence. IEEE, 2018: 268-272.

[20] 陈文惠. 防火墙系统策略配置研究[D]. 合肥: 中国科学技术大学, 2007.
CHEN W H. Research on policy configuration of firewall system[D].

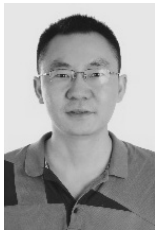
Hefei: University of Science and Technology of China, 2007.

[21] LOBO J, MARCHI M, PROVETTI A. Firewall configuration policies for the specification and implementation of private zones[C]//2012 IEEE International Symposium on Policies for Distributed Systems and Networks. IEEE, 2012: 78-85.

[22] JILLEPALLI A, DE LEON D C, STEINER S, et al. Hermes: a high-level policy language for high-granularity enterprise-wide secure browser configuration management[C]//2016 IEEE Symposium Series on Computational Intelligence. IEEE, 2016: 1-9.

[23] 李福亮, 杨家海, 吴建平, 等. 互联网自动配置研究[J]. 软件学报, 2014, 25(1):118-134.
LI F L, YANG J H, WU J P, et al. Research on Internet auto configuration[J]. Journal of Software, 2014, 25(1):118-134.

[作者简介]



郭云川（1977− ），男，四川营山人，博士，中国科学院副研究员、博士生导师，主要研究方向为访问控制、形式化方法。

李凌（1993− ），女，湖南浏阳人，中国科学院硕士生，主要研究方向为安全策略管理。

李勇俊（1992− ），男，浙江丽水人，中国科学院博士生，主要研究方向为入侵响应、安全评估、访问控制。

成林（1983− ），男，河北邢台人，博士，中国信息安全测评中心助理研究员，主要研究方向为云计算安全、大数据安全。

杜君（1982− ），男，陕西宁强人，北京网御星云信息技术有限公司助理总裁，主要研究方向为网络安全、云计算、工控安全。

张玲翠（1986− ），女，河北故城人，中国科学院博士生，主要研究方向为网络安全、信息保护。