(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109391590 A
(43)申请公布日 2019.02.26

(21)申请号 201710665613.0

(22)申请日 2017.08.07

(71)申请人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 刘庆云 郑超

(74)专利代理机构 北京君尚知识产权代理事务所(普通合伙) 11200
代理人 司立彬

(51)Int.Cl.
H04L 29/06(2006.01)

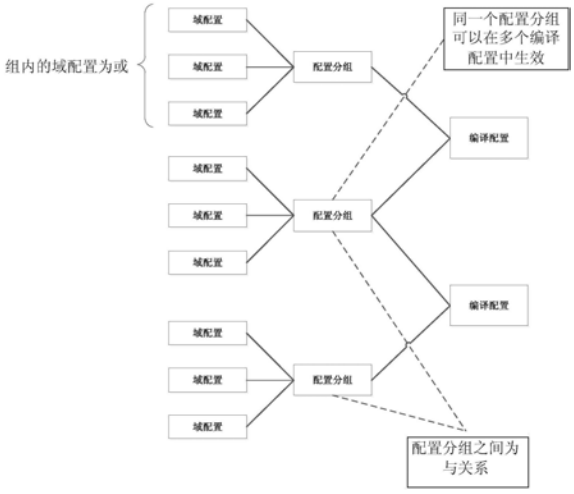
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种面向网络访问控制的规则描述方法及构建方法、介质

(57)摘要

本发明公开了一种面向网络访问控制的规则描述方法及构建方法、介质。本发明的规则描述方法,其特征在于,每一规则包括域配置、分组配置和编译配置三个层次;其中,域配置用来描述所要匹配的网络行为;分组配置包括若干个域配置,即描述所要匹配的网络行为的集合;编译配置用来描述流量符合所述分组配置所描述的网络行为时所采取的策略。基于本发明描述的规则,可以实现高效、精确、灵活的访问控制。



CN 109391590 A

1.一种面向网络访问控制的规则描述方法,其特征在于,每一规则包括域配置、分组配置和编译配置三个层次;其中,域配置用来描述所要匹配的网络行为;分组配置包括若干域配置,即描述所要匹配的网络行为的集合;编译配置用来描述流量符合所述分组配置所描述的网络行为时所采取的策略。

2.如权利要求1所述的规则描述方法,其特征在于,同一规则包括若干所述域配置,同一所述域配置只属于一个所述分组配置;同一所述分组配置允许在多个不同所述编译配置中复用。

3.如权利要求1或2所述的规则描述方法,其特征在于,所述分组配置中的多个域配置为“或”关系,所述编译配置中的域配置分组之间是“与”或者是“非”关系。

4.如权利要求1所述的规则描述方法,其特征在于,所述域配置为网络传输协议或网络传输数据的设定字段。

5.如权利要求1所述的规则描述方法,其特征在于,所述域配置r的描述信息包括:匹配位置、域类型和匹配内容。

6.如权利要求5所述的规则描述方法,其特征在于,所述域类型为字符串、IP地址、数值区间或哈希值。

7.如权利要求1所述的规则描述方法,其特征在于,每一所述域配置、所述分组配置和所述编译配置分别设有一生效标志。

8.一种面向网络访问控制的规则构建方法,其步骤包括:

1)新建一分组配置,并分配唯一性分组配置ID;然后在该分组配置内添加域配置并对每一域配置分配一域配置ID,存储域配置ID与该分组配置ID的对应关系;确定该域配置的匹配位置和匹配内容;

2)建立一编译配置并分配编译配置ID,建立该编译配置ID与该分组配置ID之间的从属关系,以及该编译配置中的域配置分组之间是“与”或者是“非”关系。

9.如权利要求8所述的方法,其特征在于,所述匹配位置是解析网络传输协议或其载荷后得到的字段。

10.一种存储计算机程序的计算机可读存储介质,其特征在于,存储计算机程序和如权利要求1～7任一所述的规则描述方法所描述的规则,所述计算机程序包括指令,所述指令包括如权利要求8至9中任一方法中的各个步骤。

一种面向网络访问控制的规则描述方法及构建方法、介质

技术领域

[0001] 本发明属于网络安全领域，涉及一种面向网络访问控制的规则描述方法及构建方法、介质。

背景技术

[0002] 近年来，随着各类技术的发展，网络安全形势的日益严峻，企业、组织对于内部网络访问控制的需求十分强烈。

[0003] 在入侵检测场景，为了避免内部用户访问有风险的网站，如钓鱼网站、挂马网站，会通过建立黑名单等方式，禁止对该类网站的访问。在数据防泄漏场景，为了避免企业重要数据被内部人员或攻击者窃取，也会采用访问控制技术防止该问题。

[0004] 目前对网络访问行为进行描述有两类方法，一类是基于属性标注的，如基于角色(RBAC)或任务授权(TBAC)。另一类是基于网络行为特征的，其中SNORT规则得到的应用最为广泛。但是随着规则的日趋复杂，规则中存在大量的重复规则，比如一组恶意的IP地址重复出现在多个SNORT规则中，会影响规则的执行效率，也不利于维护。

发明内容

[0005] 针对现有技术中存在的技术问题，本发明的目的在于提供一种面向网络访问控制的规则描述方法及构建方法、介质。基于本发明描述的规则，可以实现高效、精确、灵活的访问控制，本发明的规则描述模型简称MAAT。

[0006] 本发明主要包含两个方面：(1)根据网络访问控制场景的特点，将规则分为编译配置、分组配置、域配置三个层次。其中域配置用来描述访问行为，分组配置用来描述访问行为的集合，编译配置用来描述流量符合访问行为时所采取的策略。(2)从优化执行效率和方便配置管理的角度，对各类配置的形式和组合关系进行定义。

[0007] 本发明规则描述方法如图1，其包括以下内容：

[0008] 1)为了便于规则的规格化描述，将规则分为域配置、分组配置、编译配置三个层次。为了便于结构化存储和独立增删，每个配置都有各自独立的生效标志。三个层次的配置共同描述了一个访问控制规则，其中域配置和分组配置描述了所要匹配的网络行为，编译配置描述了符合该行为后所采取的策略。

[0009] 2)域配置，访问控制规则中对网络访问行为最细粒度的描述。针对网络传输协议或数据的设定字段的配置，域配置类型依据访问控制的粒度决定，这些域配置的类型包括：字符串、IP地址、数值区间、哈希值等。例如：

[0010] a)例1，指定HTTP协议中UserAgent包含子串“Chrome”和“11.8.1”。

[0011] b)例2，指定HTTP协议中域名以“.emodao.com”结尾。

[0012] c)例3，指定客户端IP地址属于202.118.101.*这个C段。

[0013] 3)分组配置，描述访问控制规则中若干条域配置的组合关系。它是一个域配置的集合，所包含的域配置数量无上限，一条域配置记录只属于一个分组配置。

[0014] 4)编译配置,描述当网络访问行为匹配访问控制规则时,所采取的策略。

[0015] 5)一条访问控制规则是由若干条三类配置组合而成的,其组合关系如下:

[0016] a)分组配置中的多个域配置是“或”关系;

[0017] b)编译配置中的多个域配置分组是“与”或者是“非”关系;

[0018] c)一个分组配置允许在多个编译配置中复用,以方便访问策略的制定,提高规则的使用效率。例如某个分组配置,是若干IP地址的集合,可禁止该分组内的IP访问数个不同的网址。

[0019] 形式化描述为:

[0020] ●域配置r可以描述为(匹配位置:域类型:匹配内容)。

[0021] ●分组配置g可以描述为(r1|r2|…|rrn),布尔运算符只能是‘或’运算符。比如,分组g1中有两个域配置r1和r2,r1=HTTP协议的URL中包含www.abc.com,r2=HTTP协议的URL中包含1.html。在匹配时,以下三个输入的URL都会命中分组配置g1:ww.abc.com/1.html,www.abc.com/2.html,www.efg.com/1.html。

[0022] ●编译配置c可以描述为c=(g1&g2&(!g3)&…&gn,strategy),布尔运算符只能是‘与’运算符或‘非’运算符,strategy表示规则命中后执行的策略。

[0023] 与现有技术相比,本发明的积极效果:

[0024] 本发明采用编译、分组、域的三层模型描述访问控制规则,实现了网络访问特征的与、或、非的布尔运算。利用分组复用机制,在有限的规则容量下,提高了规则表达能力。每个层次的规则有独立的生效标志,方便进行对访问控制规则进行修改。在形式上保证了,在任何子规则的加载顺序下,都不会出现误命中。

[0025] 本发明的规则描述模型的存储,可以采用结构化数据库表、行列式文本文件或json格式文本文件。

附图说明

[0026] 图1为访问控制规则描述结构图。

具体实施方式

[0027] 下面结合实例对本发明的规则描述方法进行详细介绍。

[0028] 本发明的访问控制规则的构建包括以下三个步骤:

[0029] (一)构造对网络访问行为的特征,即执行访问控制规则所要满足的条件。

[0030] a)如复用已存在分组配置,则记录该分组配置ID。否则,新建一条分组配置,分配唯一性分组配置ID。

[0031] b)在该分组配置内添加域配置。对于其包含的每一条域配置,分配域配置ID,存储域配置ID与被所属分组配置ID的关系。之后,确定该域配置的匹配位置和匹配内容

[0032] c)记录该分组配置ID。

[0033] d)如果还有其它条件,则回到步骤a),否则结束。

[0034] (二)分配编译配置ID,与上一步骤记录的分组配置ID建立从属关系,并确认域配置分组之间采用g或是!g(非g)。

[0035] (三)确定符合网络行为特征后所执行的策略(strategy),具体包括:

[0036] a)业务分类,用于对规则进行管理。

[0037] b)处置方式,包括禁止、监视、放行等,可以灵活扩展;

[0038] c)处置参数,包括是否是记录日志、黑名单等,可以灵活扩展;

[0039] 以及配置中包含分组数,用以克服在结构化数据存储中多个表中域配置或分组配置不能原子下发,避免导致误命中。

[0040] 需要说明的是,匹配位置是解析网络传输协议和其载荷后得到的某一个字段,匹配位置的数量由访问控制粒度决定,例如需要控制对某钓鱼网站phishing-site.com的访问,可以定义生效位置为HTTP协议的HOST字段,具体规则为字符串“phishing-site.com”。

[0041] 具体内容从形式上可以分为以下几类:

[0042] 1)字符串类规则,用以描述针对字符串的匹配规则,例如可以用来匹配HTTP流量的URL、Cookie,DNS协议中的域名。从匹配方式上可以分为单串匹配方式(可细分为子串匹配;右匹配;左匹配;完全匹配)、与表达式、正则表达式、带偏移量的子串匹配(即规定某个字符串出现在某个位置的规则);

[0043] 2)IP地址类规则,用以匹配网络数据的传输地址,例如发现有害主机的TCP连接。包括IPv4地址和IPv6地址,具体来说通过地址类型、源IP地址、源IP掩码、源端口、源端口掩码、目的IP、目的IP掩码、目的端口、目的端口掩码、协议(如tcp、udp)、方向等信息描述。

[0044] 3)数值类规则,用以判断数值是否位于某个区间,如文件长度。由数值下界、数值上界两个字段描述。

[0045] 4)哈希类规则,用以匹配传输中的文件是否为匹配目标,如匹配木马、病毒或内部文档。根据哈希值判断传输数据是否符合规则。哈希值可以是密码学哈希,如MD5、SHA1等,进行精确匹配的哈希,也可以是模糊哈希等,进行相似性匹配哈希。

[0046] 5)其它根据需要添加的规则。

[0047] 举例,有如下访问控制规则:

[0048] 对于IP地址192.168.0.1和192.168.0.2,访问www.phishing-site.com和www.virus-site.com的行为,予以禁止,并且产生告警日志。

[0049] 其构造过程如下:

[0050] (一)构造网络访问行为特征。

[0051] a)创建分组配置ID=g1。

[0052] i.在g1内添加域配置,分配域配置ID=r1,设置r1是一个IP类规则,匹配位置是客户端IP,值为192.168.0.1;

[0053] ii.继续在g1中添加域配置r1,同样设置r2是一个IP类规则,匹配位置是客户端IP,值为192.168.0.2;

[0054] b)创建分组配置ID=g2。

[0055] i.在g2内添加域配置,分配域配置ID=r3,设置r3是一个字符串类规则,匹配位置是HTTP协议的URL,其值为www.phishing-site.com,单串匹配,匹配方式为子串匹配。

[0056] ii.在g2内添加域配置,分配域配置ID=r4,设置r4是一个字符串类规则,匹配位置是HTTP协议的URL,其值为www.virus-site.com,单串匹配,匹配方式为子串匹配。

[0057] (二)分配编译配置ID=c1,其包含g1和g2两个分组,两个分组间为与关系,即g1&g2。

[0058] (三)设定c1匹配后执行的策略为:禁止,产生告警日志。

[0059] 配置执行过程:当一个网络流量到达后,首先,经过报文捕获、流还原和协议解析后,得到协议的字段信息,例如对于HTTP协议可以得到IP地址、URL、Referer、Cookies等信息。每解析出一个字段(域),就可以使用域配置进行匹配,如果某组域配置的匹配结果命中了某个编译配置的策略组合,则返回该编译配置,并根据该编译配置的策略的定义执行动作。

[0060] 本发明还提供一种存储计算机程序的计算机可读存储介质,其特征在于,存储计算机程序和上述规则描述方法所描述的规则,所述计算机程序包括指令,所述指令包括上述规则构建方法中的各个步骤。

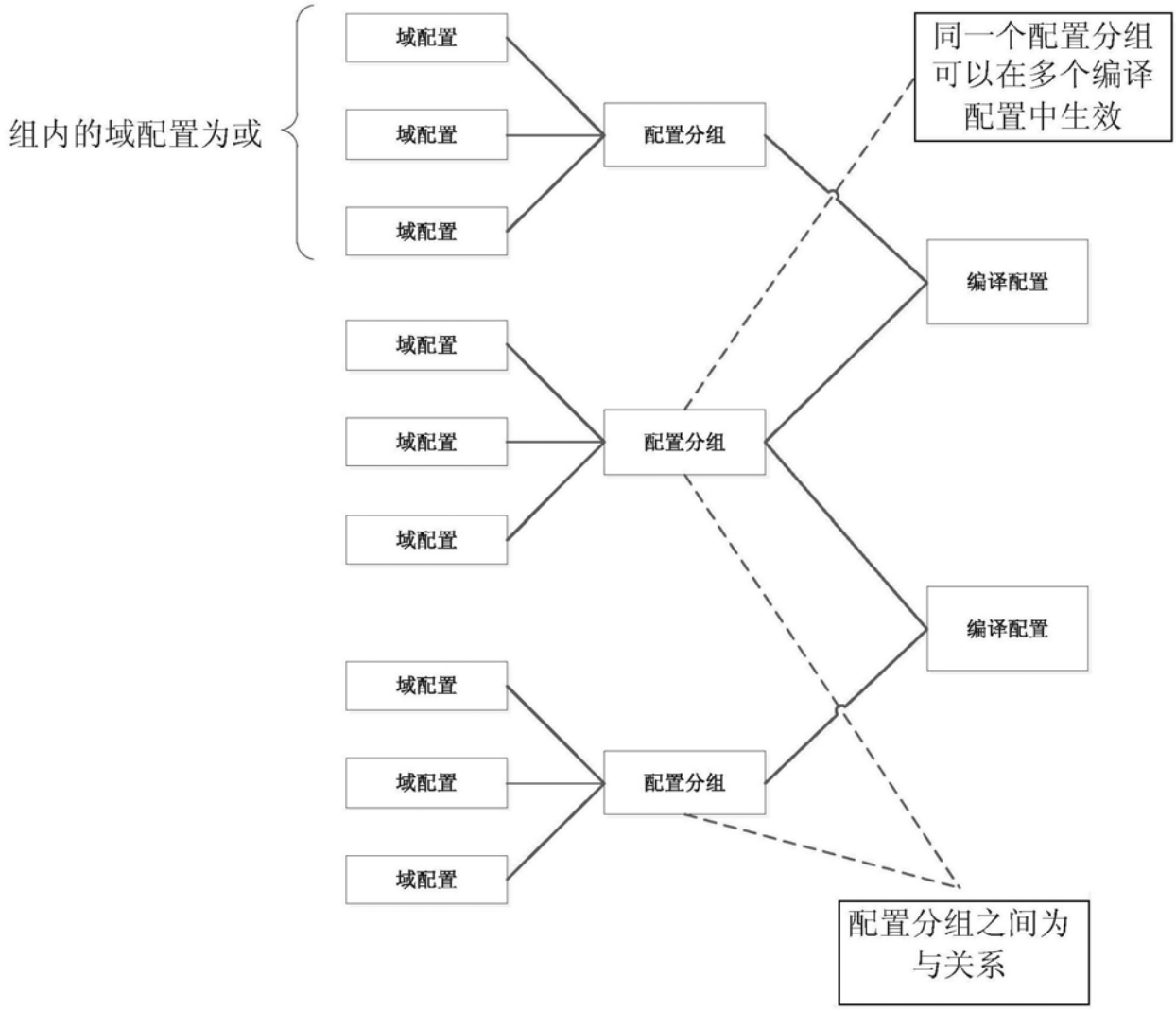

组内的域配置为或
域配置
域配置
域配置
域配置
域配置
域配置
域配置
域配置
域配置
域配置
配置分组
配置分组
配置分组
同一个配置分组
可以在多个编译
配置中生效
编译配置
编译配置
配置分组之间为
与关系

图1