(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110012016 B
(45)授权公告日 2021.04.27

(21)申请号 201910286462.7

(22)申请日 2019.04.10

(65)同一申请的已公布的文献号
申请公布号 CN 110012016 A

(43)申请公布日 2019.07.12

(73)专利权人 山东师创云服务有限公司
地址 250101 山东省济南市高新区新泺大街1166号奥盛大厦1号楼8层

(72)发明人 高寿柏 仲茜

(74)专利代理机构 济南圣达知识产权代理有限公司 37221
代理人 李圣梅

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

(56)对比文件
CN 106790194 A,2017.05.31
CN 106603513 A,2017.04.26
CN 101330495 A,2008.12.24
CN 107818268 A,2018.03.20
CN 102457507 A,2012.05.16
US 2013291121 A1,2013.10.31
US 2017329957 A1,2017.11.16
雷瑶等.一种基于XACML 的混合云跨域资源访问控制方案.《计算机应用与软件》.2014,

审查员 李星星

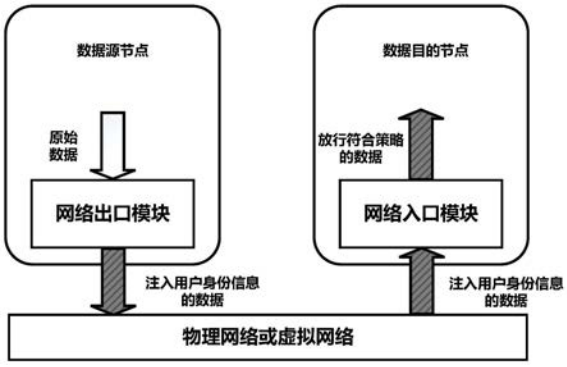
权利要求书2页 说明书8页 附图3页

(54)发明名称

混合云环境中资源访问控制的方法及系统

(57)摘要

本公开提出了混合云环境中资源访问控制的方法及系统，接收用户访问的业务系统的指令，在网络数据包的源端注入用户的有效身份信息；在网络数据包的目的端截获网络数据包并分析用户身份，通过策略列表中已定义的用户与所访问应用的关联关系，判定放行还是拒绝本次网络数据包。本公开技术方案从网络驱动层实现访问控制，加强了对企业业务系统的安全防护。



CN 110012016 B

1.混合云环境中资源访问控制的方法,其特征是,包括:

接收用户访问的业务系统的指令,在网络数据包的源端注入用户的有效身份信息,具体步骤如下:

步骤(1):用户访问业务系统时,在网络数据包的源端的驱动层判断所访问的目的地址以及应用端口是否是第一策略列表中所定义的资源所在的服务器的地址及端口,如果是第一策略列表中所定义的合法的访问并且用户当前处于登录状态,则在驱动层注入用户身份的有效信息;

在网络数据包的目的端截获网络数据包并分析用户身份,通过策略列表中已定义的用户与所访问应用的关联关系,判定放行还是拒绝本次网络数据包,具体步骤如下:

步骤(2):用户访问业务系统时,在网络数据包的目的端的驱动层判断,所访问的业务系统的端口是否在第二策略列表中所定义以及判断用户身份的合法性,根据第二策略列表中记录的用户的访问权限、用户当前的状态信息、业务系统的访问级别,放行或禁止当前网络数据包;

用户的访问权限是指,用户信息与所能访问的业务系统的端口的关联关系,访问权限记录在第一策略列表中;

用户的状态信息是指,用户登录或注销的状态,只有当用户处于登录状态时,网络数据包的源端的驱动层才有可能注入用户身份的有效信息,状态信息记录在第一策略列表中;

业务系统的访问级别是指,细粒度的控制用户的访问权限,以应急特殊事件的发生,业务系统的访问级别记录在第二策略列表中;

第一策略列表与第二策略列表必须保持用户有效信息一致,当步骤(1)中发生在驱动层注入用户身份的有效信息的事件时,相同的用户身份的有效信息必须同步更新到步骤(2)中的策略列表中;

用户身份的有效信息,是指4字节长度的数字,该数字按照一定的时间规律动态的变化。

2.混合云环境中资源访问控制的系统,其特征是,包括:

网络出口模块,被配置为:接收用户访问的业务系统的指令,在网络数据包的源端注入用户的有效身份信息,具体步骤如下:

步骤(1):用户访问业务系统时,在网络数据包的源端的驱动层判断所访问的目的地址以及应用端口是否是第一策略列表中所定义的资源所在的服务器的地址及端口,如果是第一策略列表中所定义的合法的访问并且用户当前处于登录状态,则在驱动层注入用户身份的有效信息;

网络入口模块,被配置为:在网络数据包的目的端截获网络数据包并分析用户身份,通过策略列表中已定义的用户与所访问应用的关联关系,判定放行还是拒绝本次网络数据包,具体步骤如下:

步骤(2):用户访问业务系统时,在网络数据包的目的端的驱动层判断,所访问的业务系统的端口是否在第二策略列表中所定义以及判断用户身份的合法性,根据第二策略列表中记录的用户的访问权限、用户当前的状态信息、业务系统的访问级别,放行或禁止当前网络数据包;

用户的访问权限是指,用户信息与所能访问的业务系统的端口的关联关系,访问权限

记录在第一策略列表中；

用户的状态信息是指，用户登录或注销的状态，只有当用户处于登录状态时，网络数据包的源端的驱动层才有可能注入用户身份的有效信息，状态信息记录在第一策略列表中；

业务系统的访问级别是指，细粒度的控制用户的访问权限，以应急特殊事件的发生，业务系统的访问级别记录在第二策略列表中；

第一策略列表与第二策略列表必须保持用户有效信息一致，当步骤(1)中发生在驱动层注入用户身份的有效信息的事件时，相同的用户身份的有效信息必须同步更新到步骤(2)中的策略列表中；

用户身份的有效信息，是指4字节长度的数字，该数字按照一定的时间规律动态的变化。

3.IAM系统，其特征是，所述系统包括IAM系统服务器、信息输入单元及显示单元，利用信息输入单元用于输入用户访问业务系统的指令，利用显示单元将IAM系统服务器处理后的相关信息进行显示；

其中，所述IAM系统服务器被配置为执行权利要求1中的具体步骤。

4.一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现权利要求1所述的混合云环境中资源访问控制的方法的步骤。

5.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现权利要求1混合云环境中资源访问控制的方法的步骤。

混合云环境中资源访问控制的方法及系统

技术领域

[0001] 本公开涉及信息数据处理技术领域，特别是涉及混合云环境中资源访问控制的方法及系统。

背景技术

[0002] 随着云计算技术的日益成熟和广泛应用，其在费用、性能、可靠性、扩展性等方面的优势日益凸显，事业单位和企业逐渐将其业务系统由传统的数据中心迁移到混合云环境中。混合云通过将公有云和私有云融合运用，克服了公有云、私有云的固有不足，是云计算的主要模式和发展方向。在混合云环境中，信息资源多以硬件设施、软件系统、数据等形式提供给用户，综合考虑安全性、费用、性能等要素，通常将核心系统及数据部署到私有云，其他系统及数据部署于公有云。为确保只有合法用户能够访问授权资源，提高混合云信息资源访问的安全性和可管理性，有必要对私有云和公有云中的身份认证和资源访问进行统一管控，管控对象既包括物理主机等硬件资源，又包括虚拟主机等虚拟资源，还包括应用系统等软件资源。

[0003] 在混合云环境中，云的运营方通常是专业的云服务机构，而事业单位、企业只是云资源的用户，它们通过租用、托管等方式获得混合云中的硬件资源，并将它们的系统和数据部署到云端。混合云的上述特点，使其在资源管理与使用模式上与传统的私有数据中心存在很大的不同，混合云环境中资源的管理者 (云服务机构)和使用者(硬件/虚拟资源的租用者，软件系统和数据的部署者) 通常是不同的实体，而传统数据中心资源的管理者和使用者通常相同。与之相对应，混合云环境中资源访问控制也与传统数据中心有着较大的区别，在传统数据中心模式下，资源的访问控制由资源管理者独立实施，而在混合云环境中资源的访问控制由资源的管理者和使用者共同实施，其中前者负责部署及运维安全认证平台、配置并维护总体安全认证和访问控制策略，后者负责配置并维护本机构相关资源安全认证及访问控制策略。

[0004] 混合云环境中管控资源的多样性和资源模式的复杂性，决定了访问控制方式不仅仅只针对数据包的网络参数(如:IP地址、端口等)，还需针对具体访问的资源及访问该资源的用户，文中称前者为网络级访问控制，后者称为用户级访问控制，显然后者是更高级别的访问控制方式。实现用户级访问的关键问题是识别数据包所属的用户，一个直观的想法是通过用户登陆认证系统时使用的 IP地址，但实际上由于IPV4地址数量的限制，不可能为每一个终端设备在 Internet上都分配一个全球唯一的IPV4地址。解决IP地址不足通常采用网络地址映射(NAT)的方法，它在网络出口处对数据包的局域网内网地址和公网地址(通常是Internet地址)进行转换，这样对于同一局域网的数据包，无论其内网地址是否相同，在公网只有一个地址与其对应，因此只通过IP地址无法对用户进行标识。

[0005] 发明人在实际工作中发现，从技术层面看，实现数据中心的资源访问控制目前主要包括两类技术方案，一类采用网络防火墙和VPN(Virtual Private Network，虚拟专用网)等传统的网络安全技术，另一类称为IAM(Identity and Access Management，身份识别

与访问管理)系统,为专用于身份认证和访问控制的系统。其中,网络防火墙主要工作在网络层,只能处理网络级访问控制,不能满足用户级访问控制;VPN技术具有一定的用户级访问控制能力,但是数据在传输过程中需加密,且所有数据包均需要VPN服务器进行加解密、所属用户识别、拆包重组和访问控制策略的实施,易成为性能瓶颈,影响用户体验;IAM 系统是专门针对用户认证和用户级访问控制开发的系统,具有单点登录、认证管理、用户授权和安全审计等功能。但是现有的IAM系统,通常只针对单一企业的私有数据中心,采用侵入式方式进行部署实施,需对用户现有系统进行修改,将现有系统的用户认证统一交由IAM系统服务器处理,部署维护难度大、成本高、灵活性差,只适用于传统的大型企业的私有数据中心,难以应用于混合云环境。

[0006] 通过上面描述可见,混合云环境中资源访问控制所面临的主要问题有:

[0007] (1)如何在内网环境或在公网环境中有效识别数据包所属用户。

[0008] (2)如何跟踪用户访问资源时的权限。

[0009] (3)如何以非侵入方式对资源进行安全适配。

发明内容

[0010] 本说明书实施方式的目的之一是提供混合云环境中资源访问控制的方法,可以在宏观上控制用户对业务系统的访问,加强了对企业业务系统的安全防护。

[0011] 本说明书实施方式提供混合云环境中资源访问控制的方法,通过以下技术方案实现:

[0012] 包括:

[0013] 接收用户访问的业务系统的指令,在网络数据包的源端注入用户的有效身份信息;

[0014] 在网络数据包的目的端截获网络数据包并分析用户身份,通过策略列表中已定义的用户与所访问应用的关联关系,判定放行还是拒绝本次网络数据包。

[0015] 作为进一步的实施例子,接收用户访问的业务系统的指令,并在网络数据包的源端的驱动层对用户访问的业务系统进行判断:所访问的信息是否是第一策略列表中所定义的所述业务系统的应用所在的服务器的信息,如果是第一策略列表中所定义的合法的访问并且用户当前处于登录状态,则在源端的驱动层注入用户身份的有效信息。

[0016] 进一步的,在源端的驱动层注入用户身份的有效信息后,相同的用户身份的有效信息同步更新到第二策略列表中;

[0017] 进一步的,在网络数据包的目的端的驱动层判断所访问的业务系统的信息是否在第二策略列表中所定义以及判断用户身份的合法性,根据第二策略列表中记录的控制信息放行或禁止当前网络数据包。

[0018] 本说明书实施方式的目的之二是提供混合云环境中资源访问控制的系统,可以在宏观上控制用户对业务系统的访问,加强了对企业业务系统的安全防护。

[0019] 本说明书另一实施方式提供混合云环境中资源访问控制的系统,通过以下技术方案实现:

[0020] 包括:

[0021] 网络出口模块,被配置为:接收用户访问的业务系统的指令,在网络数据包的源端

注入用户的有效身份信息；

[0022] 网络入口模块，被配置为：在网络数据包的目的端截获网络数据包并分析用户身份，通过策略列表中已定义的用户与所访问应用的关联关系，判定放行还是拒绝本次网络数据包。

[0023] 作为本公开进一步的技术方案，所述网络出口模块，接收用户访问的业务系统的指令，并在网络数据包的源端的驱动层对用户访问的业务系统进行判断：所访问的信息是否是第一策略列表中所定义的所述业务系统的应用所在的服务器的信息，如果是第一策略列表中所定义的合法的访问并且用户当前处于登录状态，则在源端的驱动层注入用户身份的有效信息；

[0024] 进一步的，还包括：用户身份的有效信息同步模块，被配置为：在源端的驱动层注入用户身份的有效信息后，相同的用户身份的有效信息同步更新到第二策略列表中；

[0025] 进一步的，网络入口模块，被配置为：在网络数据包的目的端的驱动层判断所访问的业务系统的信息是否在第二策略列表中所定义以及判断用户身份的合法性，根据第二策略列表中记录的控制信息放行或禁止当前网络数据包。

[0026] 本说明书实施方式的目的之三是提供IAM系统，利用可以在宏观上控制用户对业务系统的访问，加强了对企业业务系统的安全防护。

[0027] 本说明书又一实施方式提供IAM系统，通过以下技术方案实现：

[0028] 所述系统包括IAM系统服务器、信息输入单元及显示单元，利用信息输入单元用于输入用户访问业务系统的指令，利用显示单元将IAM系统服务器处理后的相关信息进行显示；

[0029] 其中，所述IAM系统服务器被配置为执行以下过程：

[0030] 接收用户访问的业务系统的指令，并在网络数据包的源端的驱动层对用户访问的业务系统进行判断：所访问的信息是否是第一策略列表中所定义的所述业务系统的应用所在的服务器的信息，如果是第一策略列表中所定义的合法的访问并且用户当前处于登录状态，则在源端的驱动层注入用户身份的有效信息；

[0031] 在源端的驱动层注入用户身份的有效信息后，相同的用户身份的有效信息同步更新到第二策略列表中；

[0032] 在网络数据包的目的端的驱动层判断所访问的业务系统的信息是否在第二策略列表中所定义以及判断用户身份的合法性，根据第二策略列表中记录的控制信息放行或禁止当前网络数据包。与传统的IAM系统不同，上述过程对用户系统是非侵入式的，无需对用户系统进行任何修改。

[0033] 本说明书实施方式的目的之四是提供一种计算机设备，利用可以在宏观上控制用户对业务系统的访问，加强了对企业业务系统的安全防护。

[0034] 本说明书实施方式提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现混合云环境中资源访问控制的方法的步骤。

[0035] 本说明书实施方式的目的之五是提供一种计算机可读存储介质，利用可以在宏观上控制用户对业务系统的访问，加强了对企业业务系统的安全防护。

[0036] 本说明书实施方式提供一种计算机可读存储介质，其上存储有计算机程序，其特

征在于，该程序被处理器执行时实现混合云环境中资源访问控制的方法的步骤。

[0037] 本公开技术方案不需要复杂的网络环境建设，并且对于企业的业务系统是透明的，不需要在企业的业务系统中增加安全接口。本公开技术方案适用于混合云环境中的运营管理，可以在宏观上控制用户对业务系统的访问。以本公开技术方案描述的实现方法为基础，可以为业务系统遭受攻击的调查取证、用户对业务系统访问的操作审计、用户对业务系统的偏好喜爱等数据的分析挖掘提供技术支撑。

[0038] 与现有技术相比，本公开的有益效果是：

[0039] 本公开技术方案通过在网络数据包中注入身份识别信息的方式来追踪用户的有效身份，通过在网络驱动层分析策略列表的方式来追踪用户访问应用的有效权限，通过端口保护的方式为资源进行安全适配。

[0040] 本公开技术方案对应的方法不需要复杂网络环境的建设，并且不需要侵入式的变更企业的业务接口。

[0041] 本公开技术方案从网络驱动层实现访问控制，加强了对企业业务系统的安全防护，入侵者必须先攻陷网络驱动层能够访问到业务系统，才能进一步的对业务系统自身的安全机制进行入侵。该方法相当于在原业务系统的安全锁的基础上又增加了一把锁。

[0042] 本公开技术方案可以为业务系统遭受攻击的调查取证、用户对业务系统访问的操作审计、用户对业务系统的偏好喜爱等数据的分析挖掘提供技术支撑。

附图说明

[0043] 构成本公开的一部分的说明书附图用来提供对本公开的进一步理解，本公开的示意性实施例及其说明用于解释本公开，并不构成对本公开的不当限定。

[0044] 图1为本公开一个或多个实施例子的结构流程示意图；

[0045] 图2为本公开一个或多个实施例子的网络出口模块工作流程示意图；

[0046] 图3为本公开一个或多个实施例子的网络入口模块工作流程示意图。

具体实施方式

[0047] 应该指出，以下详细说明都是例示性的，旨在对本公开提供进一步的说明。除非另有指明，本文使用的所有技术和科学术语具有与本公开所属技术领域的普通技术人员通常理解的相同含义。

[0048] 需要注意的是，这里所使用的术语仅是为了描述具体实施方式，而非意图限制根据本公开的示例性实施方式。如在这里所使用的，除非上下文另外明确指出，否则单数形式也意图包括复数形式，此外，还应当理解的是，当在本说明书中使用术语“包含”和/或“包括”时，其指明存在特征、步骤、操作、器件、组件和/或它们的组合。

[0049] 实施例子一

[0050] 本公开技术方案采用分布式方式部署，包括管理端系统、代理端系统和用户端系统三部分，其中管理端系统部署于专用服务器中，用于实现用户管理、安全认证策略管理、代理端管理等；代理端系统部署于拥有受保护资源的服务器中，用于对数据包所属用户进行识别，根据安全认证策略实施访问控制；用户端系统用于实现用户登陆，访问受保护资源时注入用户身份识别信息。上述分布式部署方式对企业的应用来讲是透明的，本公开技术

方案通过在网络数据包中注入身份识别信息的方式来追踪用户的有效身份，本公开技术方案通过在网络驱动层分析策略列表的方式来追踪用户访问应用的有效权限，本公开技术方案通过端口保护的方式为资源进行安全适配。

[0051] 该实施例子公开了混合云环境中资源访问控制的方法其整体技术构思是：用户访问业务系统时，在网络数据包的源端(用户端系统)注入用户的有效身份信息，在网络数据包的目的端截获网络包并分析用户身份，通过第二策略列表中已定义的用户与所访问应用的关联关系，判定放行还是拒绝本次网络数据包。

[0052] 在具体的一实施例子中，公开了混合云环境中资源访问控制的方法，包括：

[0053] 步骤(1)：用户访问业务系统时，在网络数据包的源端的驱动层判断所访问的目的地址以及应用端口是否是第一策略列表中所定义的资源所在的服务器的地址及端口，如果是第一策略列表中所定义的合法的访问并且用户当前处于登录状态，则在驱动层注入用户身份的有效信息。

[0054] 步骤(2)：用户访问业务系统时，在网络数据包的目的端的驱动层判断，所访问的业务系统的端口是否在第二策略列表中所定义以及判断用户身份的合法性，根据第二策略列表中记录的用户的访问权限、用户当前的状态信息、业务系统的访问级别，放行或禁止当前网络数据包。

[0055] 具体实施例子中，网络数据包是指，用户访问业务系统时所产生的基于 TCP/IP协议的数据包。

[0056] 具体实施例子中，用户的访问权限是指，用户信息与所能访问的业务系统的端口的关联关系，访问权限记录在第一策略列表中。

[0057] 具体实施例子中，用户的状态信息是指，用户登录或注销的状态，数字0代表注销状态、数字1代表登录状态，只有当用户处于登录状态时，网络数据包的源端的驱动层才有可能注入用户身份的有效信息。状态信息记录在第一策略列表中。

[0058] 具体实施例子中，业务系统的访问级别是指，细粒度的控制用户的访问权限，以应急特殊事件的发生，比如临时切断所有用户对某业务系统的访问。访问级别分为三级：0级表示策略列表失效，所有用户都可以访问业务系统；1级表示策略列表生效，用户按照策略中配置的权限访问业务系统；2级表示策略列表失效，所有用户都不能访问业务系统。这里再次强调，访问业务系统与登录业务系统是两个不同的访问控制，前者是本公开实施例子的内容，后者是业务系统自身的权限设定。业务系统的访问级别记录在第二策略列表中。

[0059] 具体实施例子中，第一策略列表通常以数据结构列表的方式，保存用户信息与所能访问的业务系统的端口的关联关系、保存用户登录或注销的状态。

[0060] 具体实施例子中，第二策略列表通常以数据结构列表的方式，保存用户信息与所能访问的业务系统的端口的关联关系、保存用户登录或注销的状态、保存业务系统的访问级别。

[0061] 第一策略列表与第二策略列表必须保持用户有效信息一致，当步骤(1)中发生在驱动层注入用户身份的有效信息的事件时，相同的用户身份的有效信息必须同步更新到步骤(2)中的策略列表中。

[0062] 具体实施例子中，用户身份的有效信息，是指4字节长度的数字，该数字按照一定的时间规律动态的变化。

[0063] 具体实施例子中，驱动层，是指能够截获原始网络数据包的驱动层，针对 Windows系统一般采用NDIS网络过滤驱动的方式拦截网络数据包，针对Linux系统一般采用网络驱动扩展模块的方式拦截网络数据包。

[0064] 具体实施例子中，驱动层注入用户身份的有效信息，是指在驱动层对基于 TCP/IP协议的数据包，在TCP协议的option选项中按照标准的数据结构格式注入 8字节长度的信息，该数据结构中第一个字节是数字253代表类型是实验数据，后一个字节代表数据结构总长度，采用固定的数字8，后两个字节代表魔术数据，通常采用自定义的用于识别数据有效性的数字，比如0xEFEF，最后四个字节的数据代表用户身份的有效信息。当在网络数据包的目的端的驱动层解析TCP数据包时，如果TCP包有option的类型是253的数据，并且魔术数据是0xEFEF，则代表此网络数据包中包含用户身份有效信息。

[0065] 参见附图2所示，具体实施例子中，步骤(1)中驱动层对网络数据包的处理，包括以下步骤：

[0066] (1-1)判断当前的网络数据包是否是基于IPV4的TCP包，如果是转向步骤 (1-2)，否则转向步骤(1-8)。

[0067] (1-2)解析TCP包的目的IP、目的端口。

[0068] (1-3)判断当前的目的IP和目的端口是否在第一策略列表中，如果是转向步骤(1-4)，否则转向步骤(1-8)。

[0069] (1-4)判断第一策略列表中记录的当前用户的状态，如果是登录状态转向步骤(1-5)，否则转向步骤(1-8)。

[0070] (1-5)在TCP的option中注入用户身份的有效信息。

[0071] (1-6)重新计算TCP和IP的校验值。

[0072] (1-7)发送注入用户身份有效信息后的网络包，然后返回到(1-1)继续执行。

[0073] (1-8)发送原始网络包，然后返回到(1-1)继续执行。

[0074] 参见附图3所示，具体实施例子中，步骤(2)中驱动层对网络数据包的处理，包括以下步骤：

[0075] (2-1)判断当前的网络数据包是否是基于IPV4的TCP包，如果是转向步骤 (2-2)，否则转向步骤(2-10)。

[0076] (2-2)解析TCP包的目的端口。

[0077] (2-3)判断当前的目的端口是否在第二策略列表中，如果是转向步骤(2-4)，否则转向步骤(2-10)。

[0078] (2-4)判断第二策略列表中记录的业务系统的访问级别，如果是0转向步骤 (2-10)，如果是1转向步骤(2-5)，如果是2转向步骤(2-11)。

[0079] (2-5)判断策略列表中记录的当前用户的状态，如果是登录状态转向步骤 (2-6)，否则转向步骤(2-11)。

[0080] (2-6)判断在TCP的option中是否包含用户身份的有效信息，例如option数据结构中是否包含魔术数字0xEFEF，如果是转向步骤(2-7)，否则转向步骤 (2-11)。

[0081] (2-7)解析出用户身份的有效信息。

[0082] (2-8)判断解析出的用户身份的有效信息与步骤(1)注入的用户身份的有效信息是否一致，如果是转向步骤(2-9)，否则转向步骤(2-11)。

[0083] (2-9)根据第二策略列表判断当前用户是否有权限访问目的端口,如果是转向步骤(2-10),否则转向步骤(2-11)。

[0084] (2-10)放行该数据包,然后返回到(2-1)继续执行。

[0085] (2-11)阻止该数据包,然后返回到(2-1)继续执行。

[0086] 本公开技术方案涉及在TCP协议的option选项中进行信息的注入,所以要求用户所访问的业务系统是基于TCP协议的。

[0087] 实施例子二

[0088] 本说明书实施方式是提供混合云环境中资源访问控制的系统,可以在宏观上控制用户对业务系统的访问,加强了对企业业务系统的安全防护。

[0089] 本说明书另一实施方式提供混合云环境中资源访问控制的系统,通过以下技术方案实现:

[0090] 包括:

[0091] 网络出口模块,被配置为:接收用户访问的业务系统的指令,在网络数据包的源端注入用户的有效身份信息;

[0092] 网络入口模块,被配置为:在网络数据包的目的端截获网络数据包并分析用户身份,通过策略列表中已定义的用户与所访问应用的关联关系,判定放行还是拒绝本次网络数据包。

[0093] 作为本公开进一步的技术方案,所述网络出口模块,接收用户访问的业务系统的指令,并在网络数据包的源端的驱动层对用户访问的业务系统进行判断:所访问的信息是否是第一策略列表中所定义的所述业务系统的应用所在的服务器的信息,如果是第一策略列表中所定义的合法的访问并且用户当前处于登录状态,则在源端的驱动层注入用户身份的有效信息;

[0094] 还包括:用户身份的有效信息同步模块,被配置为:在源端的驱动层注入用户身份的有效信息后,相同的用户身份的有效信息同步更新到第二策略列表中;

[0095] 网络入口模块,被配置为:在网络数据包的目的端的驱动层判断所访问的业务系统的信息是否在第二策略列表中所定义以及判断用户身份的合法性,根据第二策略列表中记录的控制信息放行或禁止当前网络数据包。

[0096] 应当注意,尽管在上文的详细描述中提及了设备的若干模块或子模块,但是这种划分仅仅是示例性而非强制性的。实际上,根据本公开的实施例,上文描述的两个或更多模块的特征和功能可以在一个模块中具体化。反之,上文描述的一个模块的特征和功能可以进一步划分为由多个模块来具体化。

[0097] 在该实施例子中,混合云环境中资源访问控制的系统的模块的具体实现参见实施例子一,此处不再详细描述。

[0098] 实施例子三

[0099] 本说明书实施方式提供IAM系统,利用可以在宏观上控制用户对业务系统的访问,加强了对企业业务系统的安全防护。

[0100] 本说明书又一实施方式提供IAM系统,通过以下技术方案实现:

[0101] 所述系统包括IAM系统服务器、信息输入单元及显示单元,利用信息输入单元用于输入用户访问业务系统的指令,利用显示单元将IAM系统服务器处理后的相关信息进行显

示；

[0102] 其中，所述IAM系统服务器被配置为执行以下过程：

[0103] 接收用户访问的业务系统的指令，并在网络数据包的源端的驱动层对用户访问的业务系统进行判断：所访问的信息是否是第一策略列表中所定义的所述业务系统的应用所在的服务器的信息，如果是第一策略列表中所定义的合法的访问并且用户当前处于登录状态，则在源端的驱动层注入用户身份的有效信息；

[0104] 在源端的驱动层注入用户身份的有效信息后，相同的用户身份的有效信息同步更新到第二策略列表中；

[0105] 在网络数据包的目的端的驱动层判断所访问的业务系统的信息是否在第二策略列表中所定义以及判断用户身份的合法性，根据第二策略列表中记录的控制信息放行或禁止当前网络数据包。

[0106] 实施例子四

[0107] 本说明书实施方式的目的之四是提供一种计算机设备，利用可以在宏观上控制用户对业务系统的访问，加强了对企业业务系统的安全防护。

[0108] 本说明书实施方式提供一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现混合云环境中资源访问控制的方法的步骤。

[0109] 在该实施例子中，混合云环境中资源访问控制的方法的步骤参见实施例子一，此处不再详细描述。

[0110] 实施例子五

[0111] 本说明书实施方式的目的之五是提供一种计算机可读存储介质，利用可以在宏观上控制用户对业务系统的访问，加强了对企业业务系统的安全防护。

[0112] 本说明书实施方式提供一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现混合云环境中资源访问控制的方法的步骤。

[0113] 在该实施例子中，混合云环境中资源访问控制的方法的步骤参见实施例子一，此处不再详细描述。

[0114] 在本实施例中，计算机程序产品可以包括计算机可读存储介质，其上载有用于执行本公开的各个方面的计算机可读程序指令。计算机可读存储介质可以是可以保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以是－－但不限于－－电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。

[0115] 可以理解的是，在本说明书的描述中，参考术语“一实施例”、“另一实施例”、“其他实施例”、或“第一实施例～第N实施例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[0116] 以上所述仅为本公开的优选实施例而已，并不用于限制本公开，对于本领域的技术人员来说，本公开可以有各种更改和变化。凡在本公开的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本公开的保护范围之内。

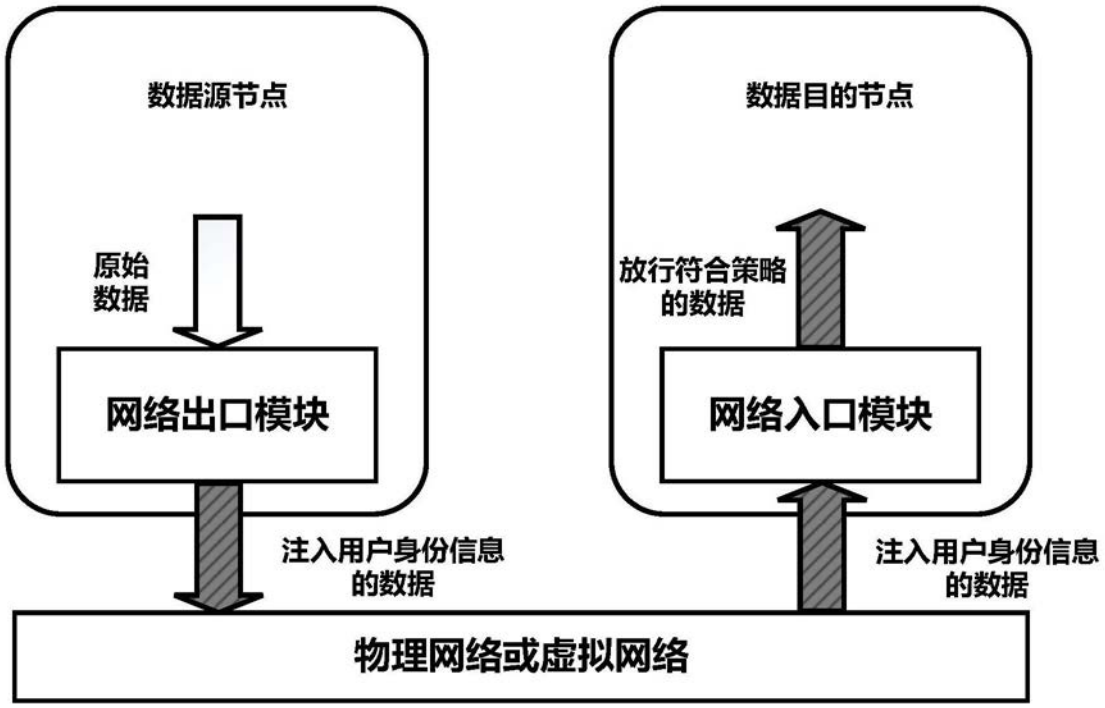

数据源节点
原始
数据
网络出口模块
注入用户身份信息
的数据
数据目的节点
放行符合策略
的数据
网络入口模块
注入用户身份信息
的数据
物理网络或虚拟网络

图1

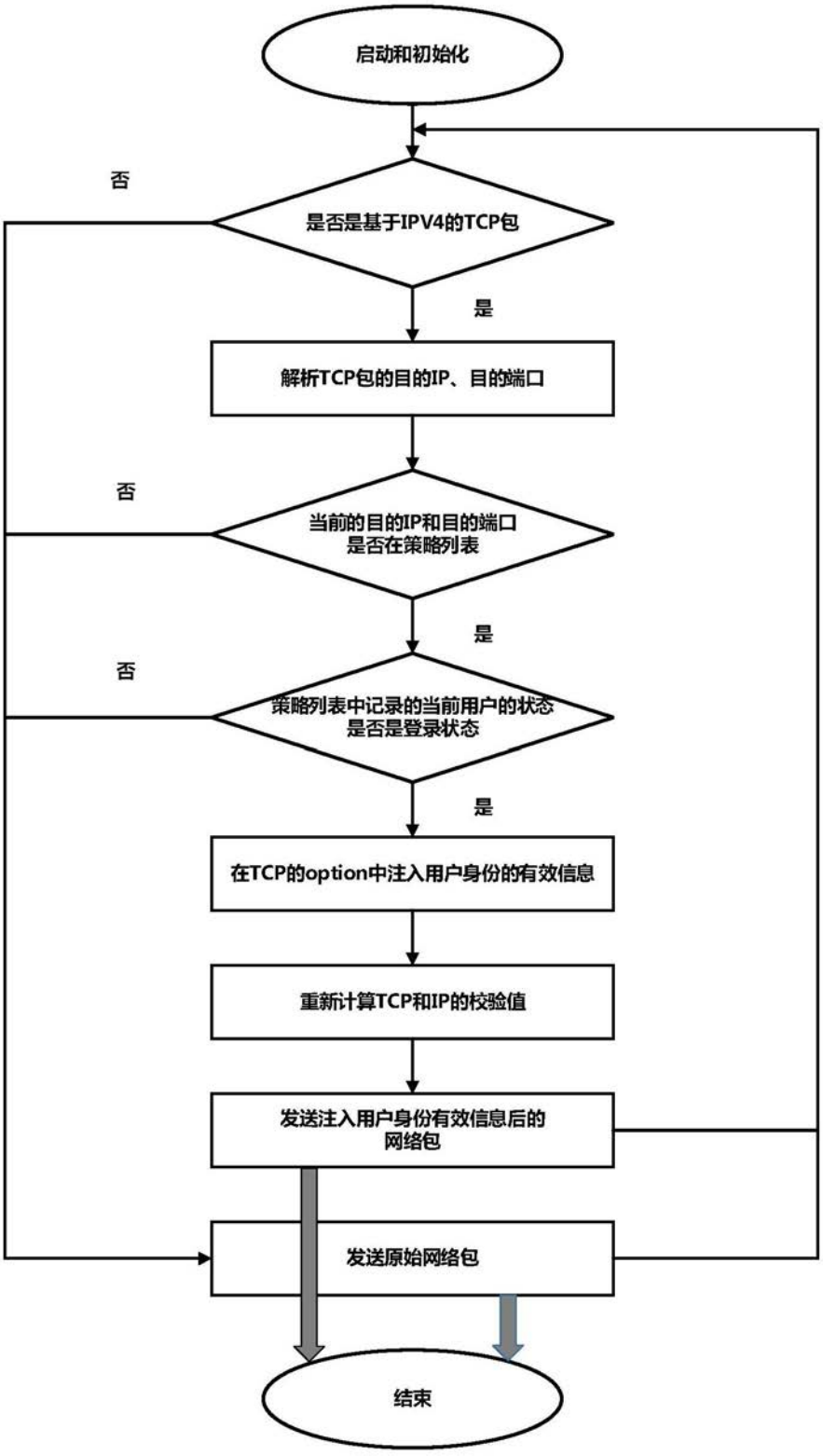

启动和初始化
否
是否是基于IPV4的TCP包
是
解析TCP包的目的IP、目的端口
否
当前的目的IP和目的端口
是否在策略列表
是
否
策略列表中记录的当前用户的状态
是否是登录状态
是
在TCP的option中注入用户身份的有效信息
重新计算TCP和IP的校验值
发送注入用户身份有效信息后的
网络包
发送原始网络包
结束

图2

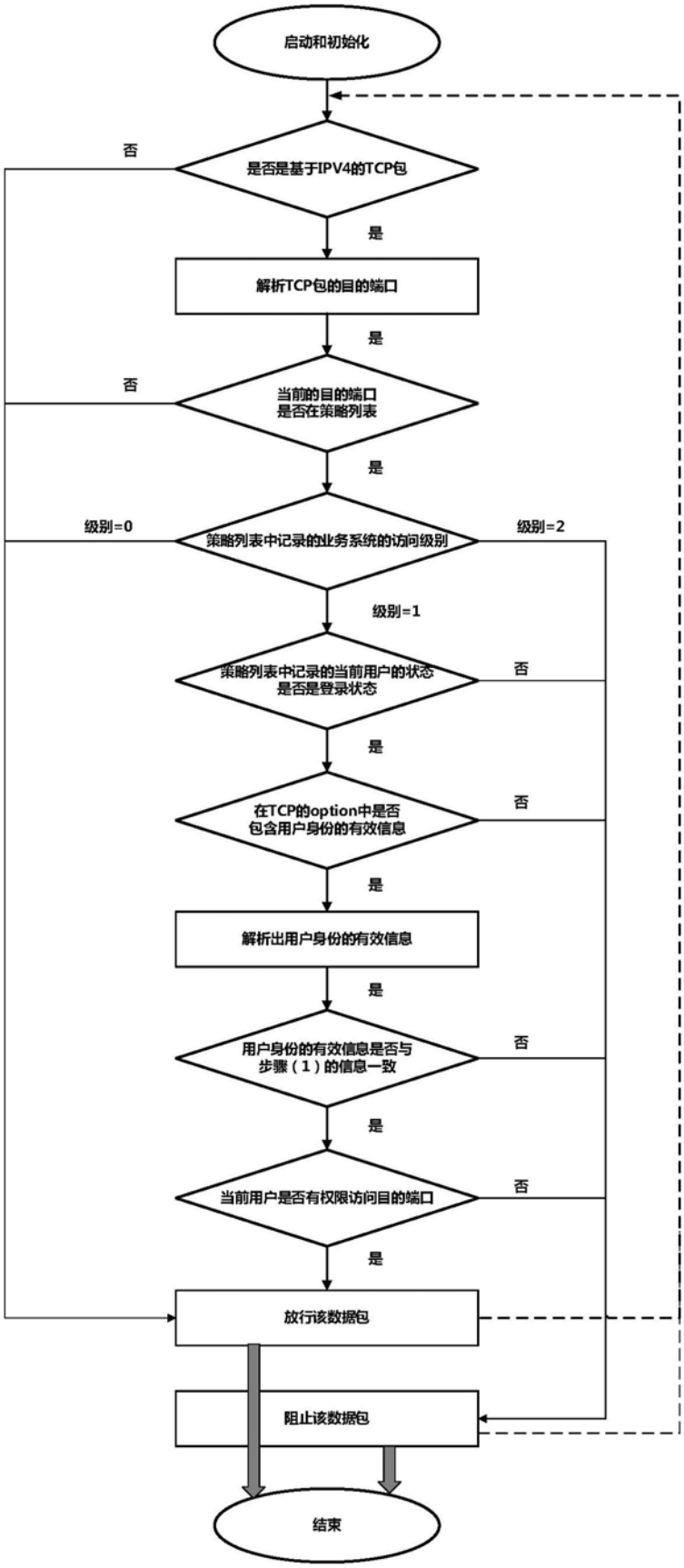

启动和初始化
是否是基于IPV4的TCP包
否
是
解析TCP包的目的端口
是
当前的目的端口
是否在策略列表
否
是
策略列表中记录的业务系统的访问级别
级别=0
级别=2
级别=1
策略列表中记录的当前用户的状态
是否是登录状态
否
是
在TCP的option中是否
包含用户身份的有效信息
否
是
解析出用户身份的有效信息
是
用户身份的有效信息是否与
步骤（1）的信息一致
否
是
当前用户是否有权限访问目的端口
否
是
放行该数据包
阻止该数据包
结束

图3