(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 104168200 A
(43)申请公布日 2014.11.26

(21)申请号 201410328769.6

(22)申请日 2014.07.10

(71)申请人 汉柏科技有限公司
地址 300384 天津市华苑产业区海泰西 18 号西 3 楼 104 室

(72)发明人 张群轼

(74)专利代理机构 北京路浩知识产权代理有限公司 11002
代理人 李相雨

(51)Int.Cl.
H04L 12/741(2013.01)

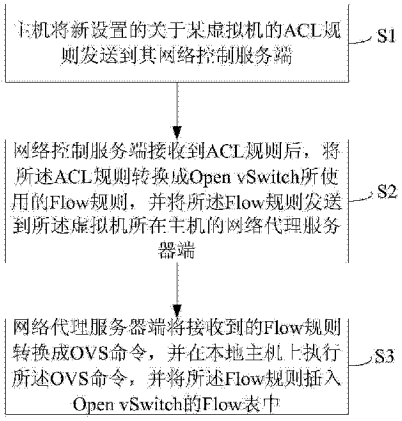
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于Open vSwitch实现ACL功能的方法及系统

(57)摘要

本发明提供了一种基于Open vSwitch实现ACL功能的方法，该方法包括：主机将新的关于某虚拟机的ACL规则发送到其网络控制服务端；网络控制服务端接收到ACL规则后，将所述ACL规则转换成Open vSwitch所使用的Flow规则，并将所述Flow规则发送到所述虚拟机所在主机的网络代理服务端；网络代理服务端将接收到的Flow规则转换成OVS命令，并在本地主机上执行所述OVS命令，将所述Flow规则插入Open vSwitch的Flow表中。该方法采用Open vSwitch解决虚拟机流量的ACL功能，从而达到控制虚拟机数据流量的目的。



CN 104168200 A

1. 一种基于 Open vSwitch 实现 ACL 功能的方法，其特征在于，该方法包括：

S1：第一主机将设置的关于某虚拟机的访问控制列表 ACL 规则发送到第一主机的网络控制服务端；

S2：网络控制服务端接收到ACL规则后，将所述ACL规则转换成开放虚拟交换标准Open vSwitch所使用的流Flow规则，并将所述Flow规则发送到所述虚拟机所在第二主机的网络代理服务端；

S3：网络代理服务端将接收到的 Flow 规则转换成 OVS 命令，并在第二主机上执行所述 OVS 命令，以将所述 Flow 规则插入 Open vSwitch 的流 Flow 表中。

2. 根据权利要求 1 所述的方法，其特征在于，该方法步骤 S3 后还包括：

当虚拟机内有流量进入到 Open vSwitch 中，Open vSwitch 会在 Flow 表中进行对比，并执行相应 Flow 规则所定义的动作。

3. 根据权利要求 1 所述的方法，其特征在于，该方法步骤 S2 还包括：

网络控制服务端将接收到的 ACL 规则保存到分布式数据库中。

4. 根据权利要求 1 所述的方法，其特征在于，所述 ACL 规则适用于网络或虚拟网卡。

5. 根据权利要求 4 所述的方法，其特征在于，所述 ACL 规则之间的优先级从高到低依次为：不可覆盖的网络级别、虚拟网卡级别以及可覆盖的网络级别。

6. 一种基于 Open vSwitch 实现 ACL 功能的系统，其特征在于，该系统包括虚拟机、Open vSwitch、网络代理服务端及网络控制服务端；

网络控制服务端，用于将接收到的 ACL 规则转换成 Open vSwitch 所使用的 Flow 规则，将所述 Flow 规则发送到所述虚拟机所在主机的网络代理服务端；

网络代理服务端，用于将将接收到的 Flow 规则转换成 OVS 命令，并在本地主机上执行所述 OVS 命令，以并将所述 Flow 规则插入所述 Open vSwitch 中的 Flow 表中；

Open vSwitch，用于根据进入到 Open vSwitch 中虚拟机的流量，在其 Flow 表中进行对比，并执行相应 Flow 规则所定义的动作。

7. 根据权利要求 6 所述的系统，其特征在于，所述网络控制服务端的功能还包括：将接收到的 ACL 规则保存到分布式数据库中。

8. 根据权利要求 6 所述的系统，其特征在于，所述虚拟机、所述 Open vSwitch 和所述网络代理服务位于同一主机，所述网络控制服务端位于另一主机。

9. 根据权利要求 6 所述的系统，其特征在于，该系统还包括物理交换机，用于通过物理网卡连接不同主机。

一种基于 Open vSwitch 实现 ACL 功能的方法及系统

技术领域

[0001] 本发明涉及计算机网络技术领域，具体涉及一种基于 Open vSwitch 实现 ACL 功能的方法及系统。

背景技术

[0002] 由于一个虚拟机上可能存在多个虚拟后的系统，系统之间通讯就需要通过网络，但和普通的物理系统间通过实体网络设备互联不同，虚拟系统的网络接口也是虚拟的，因此不能直接通过实体网络设备互联，目前流行的一种解决方案是：虚拟交换 (Virtual Switching，简称 vSwitch) 技术。所谓的 vSwitch，是指将虚拟网桥完全在服务器 (终端) 硬件上实现，不涉及外部交换机的协作。

[0003] 跟普通服务器设备一样，每个虚拟机有着自己的虚拟网卡 (virtual NIC)，每个 virtual NIC 有着自己的 MAC 地址和 IP 地址。vSwitch 相当于一个虚拟的二层交换机，该交换机连接虚拟网卡和物理网卡，将虚拟机上的数据报文从物理网口转发出去。根据需要，vSwitch 还可以支持二层转发、安全控制、端口镜像等功能。

[0004] 但现有技术中，利用传统的 vSwitch 实现访问控制列表 (Access Control list，简称 ACL) 功能需要消耗 CPU 资源，对服务器的性能有影响。

发明内容

[0005] 针对现有技术的缺陷，本发明提供的实现 ACL 功能的方法，采用 Open vSwitch 解决虚拟机流量的 ACL 功能，从而达到控制虚拟机数据流量的目的。

[0006] 第一方面，本发明提供了一种基于 Open vSwitch 实现 ACL 功能的方法，该方法包括：

[0007] S1：第一主机将设置的关于某虚拟机的访问控制列表 ACL 规则发送到第一主机的网络控制服务端；

[0008] S2：网络控制服务端接收到 ACL 规则后，将所述 ACL 规则转换成开放虚拟交换标准 Open vSwitch 所使用的流 Flow 规则，并将所述 Flow 规则发送到所述虚拟机所在第二主机的网络代理服务端；

[0009] S3：网络代理服务端将接收到的 Flow 规则转换成 OVS 命令，并在第二主机上执行所述 OVS 命令，以将所述 Flow 规则插入 Open vSwitch 的流 Flow 表中。

[0010] 优选地，该方法步骤 S3 后还包括：

[0011] 当虚拟机内有流量进入到 Open vSwitch 中，Open vSwitch 会在 Flow 表中进行对比，并执行相应 Flow 规则所定义的动作。

[0012] 优选地，该方法步骤 S2 还包括：

[0013] 网络控制服务端将接收到的 ACL 规则保存到分布式数据库中。

[0014] 优选地，所述 ACL 规则适用于网络 Network 或虚拟网卡。

[0015] 优选地，所述 ACL 规则之间的优先级从高到低依次为：不可覆盖的网络 Network 级

别、虚拟网卡级别以及可覆盖的 Network 级别。

[0016] 第二方面，本发明提供了一种基于 Open vSwitch 实现 ACL 功能的系统，该系统包括虚拟机、Open vSwitch、网络代理服务端及网络控制服务端；

[0017] 网络控制服务端，用于将接收到的 ACL 规则转换成 Open vSwitch 所使用的 Flow 规则，将所述 Flow 规则发送到所述虚拟机所在主机的网络代理服务端；

[0018] 网络代理服务端，用于将将接收到的 Flow 规则转换成 OVS 命令，并在本地主机上执行所述 OVS 命令，并将所述 Flow 规则插入所述 Open vSwitch 中的 Flow 表中；

[0019] Open vSwitch，用于根据进入到 Open vSwitch 中虚拟机的流量，在其 Flow 表中进行对比，并执行相应 Flow 规则所定义的动作。

[0020] 优选地，所述网络控制服务端的功能还包括：将接收到的 ACL 规则保存到分布式数据库中。

[0021] 优选地，所述虚拟机、所述 Open vSwitch 和所述网络代理服务位于同一主机，所述网络控制服务端位于另一主机。

[0022] 优选地，所述系统还包括物理交换机，用于通过物理网卡连接不同主机。

[0023] 由上述技术方案可知，本发明提供的一种实现 ACL 功能的方法和系统，采用 Open vSwitch 及分布式的结构解决了虚拟机流量的 ACL 功能，从而达到控制虚拟机数据流量的目的，由于整个系统分布于不同的主机，使得服务器性能明显提高。

附图说明

[0024] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些图获得其他的附图。

[0025] 图 1 是本发明实施例提供的基于 Open vSwitch 实现 ACL 功能的方法的流程图；

[0026] 图 2 是本发明实施例提供的基于 Open vSwitch 实现 ACL 功能的系统的结构示意图；

[0027] 图 3 是本发明另一实施例提供的 Open vSwitch 在 Flow 表中进行对比的流程示意图。

具体实施方式

[0028] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0029] Open vSwitch 是一种软件，Open vSwitch 即开放虚拟交换标准。如图 1 所示，图 1 示出了本发明提供的基于 Open vSwitch 实现 ACL 功能的方法的流程图，该方法包括：

[0030] S1：第一主机将设置的关于某虚拟机的访问控制列表 ACL 规则发送到第一主机的网络控制服务端；

[0031] S2：网络控制服务端接收到 ACL 规则后，将所述 ACL 规则转换成开放虚拟交换标准

Open vSwitch 所使用的流 Flow 规则，并将所述 Flow 规则发送到所述虚拟机所在第二主机的网络代理服务端；

[0032] S3：网络代理服务端将接收到的 Flow 规则转换成 OVS 命令，并在第二主机上执行所述 OVS 命令，以将所述 Flow 规则插入 Open vSwitch 的流 Flow 表中。

[0033] 其中，该方法步骤 S3 后还包括：

[0034] 当虚拟机内有流量进入到 Open vSwitch 中，Open vSwitch 会在 Flow 表中进行对比，并执行相应 Flow 规则所定义的动作。

[0035] 因此若新设定的 ACL 规则为不允许 TCP 协议的 8080 端口的流量通过，则当虚拟机流量是 TCP 协议，且端口是 8080 时，就会执行 DROP 动作。

[0036] 如图 3 所示，图 3 示出了 Open vSwitch 中 Flow 表，共包括 3 个 Flow 表 Table0、Table1 和 Table2，由图可知，当有流量进入 Open vSwitch 中时，Open vSwitch 在 Flow 表中进行对比的过程为：

[0037] (1) 当有流量进入 Open vSwitch 时，Table0 判断该流量是都为虚拟机网卡中出来的流量，若是，则加上 VLAN Tag，并跳转到 Table1；

[0038] (2)Table1 根据优先级依次判断该流量是否与不可覆的 Network 级别的 Flows、虚拟网卡级别的 Flows 及可覆盖的 Network 级别 Flows 中的 Flow 规则匹配，若与其中某个 Flow 规则匹配，则执行该 Flow 规则所定义的动作 (action)，而若需执行的动作为允许 (normal) 动作，跳转到 Table2；

[0039] (3)Table2 判断该流量是否为虚拟机网卡出来的流量，若是，则去掉 VLAN Tag。

[0040] 上述方法中的步骤 S2 还包括：

[0041] 网络控制服务端将接收到的 ACL 规则保存到分布式数据库中。

[0042] 可选地，所述 ACL 规则适用于网络 Network 或虚拟网卡。具体来说，它们分别针对的是某一个网络和某一个虚拟机上的虚拟网卡。当用户给一个虚拟机的虚拟网卡设置 ACL 后，那么 Flow 只下发到虚拟机所在的主机上。当用户给一个虚拟网络设置 ACL 后，那么首先会查找出所有属于这个虚拟网络的虚拟网卡，之后再找出这个虚拟网卡对应的虚拟机在那些主机上，最后把这个 Flow 下发到这些主机上。

[0043] 优选地，所述 ACL 规则之间的优先级从高到低依次为：不可覆盖的网络 Network 级别、虚拟网卡级别以及可覆盖的 Network 级别。

[0044] 如图 2 所示，图 2 示出了本发明提供的基于 Open vSwitch 实现 ACL 功能的系统的结构示意图，该系统包括虚拟机、Open vSwitch、网络代理服务端及网络控制服务端。

[0045] 具体来说，网络控制服务端，用于将接收到的 ACL 规则转换成 Open vSwitch 所使用的 Flow 规则，并将所述 Flow 规则发送到所述虚拟机所在主机的网络代理服务端；网络代理服务端，用于将将接收到的 Flow 规则转换成 OVS 命令，并在本地主机上执行所述 OVS 命令，并将所述 Flow 规则插入所述 Open vSwitch 中的 Flow 表中；Open vSwitch，用于根据进入到 Open vSwitch 中虚拟机的流量，在其 Flow 表中进行对比，并执行相应 Flow 规则所定义的动作。

[0046] 而且，所述系统还包括物理交换机，用于通过物理网卡连接不同主机。

[0047] 其中，所述虚拟机、所述 Open vSwitch 和所述网络代理服务位于同一主机 B，所述网络控制服务端位于另一主机 A。

[0048] 优选地，所述网络控制服务端的功能还包括：将接收到的 ACL 规则保存到分布式数据库中。

[0049] 由上述技术方案可知，本发明提供的一种实现 ACL 功能的方法和系统，采用 Open vSwitch 及分布式的结构解决了虚拟机流量的 ACL 功能，从而达到控制虚拟机数据流量的目的，由于整个系统分布于不同的主机，使得服务器性能明显提高。

[0050] 以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

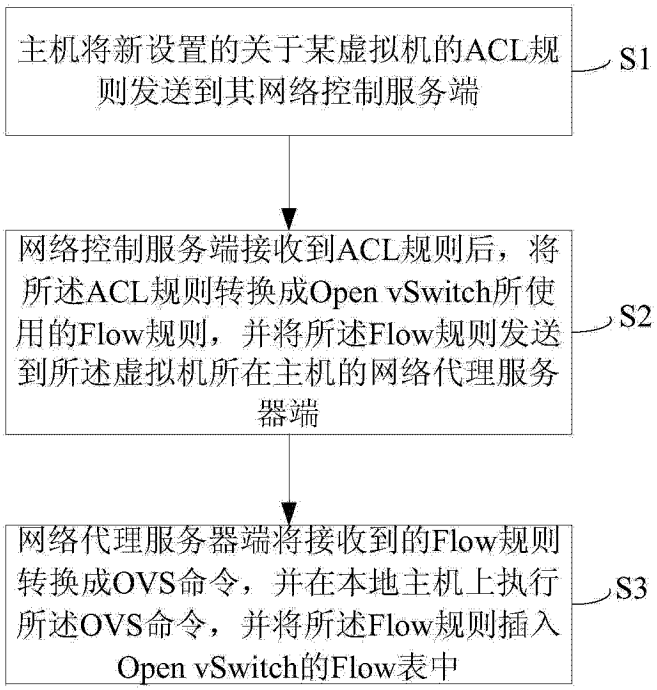

主机将新设置的关于某虚拟机的ACL规则发送到其网络控制服务端
S1
网络控制服务端接收到ACL规则后，将所述ACL规则转换成Open vSwitch所使用的Flow规则，并将所述Flow规则发送到所述虚拟机所在主机的网络代理服务器端
S2
网络代理服务器端将接收到的Flow规则转换成OVS命令，并在本地主机上执行所述OVS命令，并将所述Flow规则插入Open vSwitch的Flow表中
S3

图 1

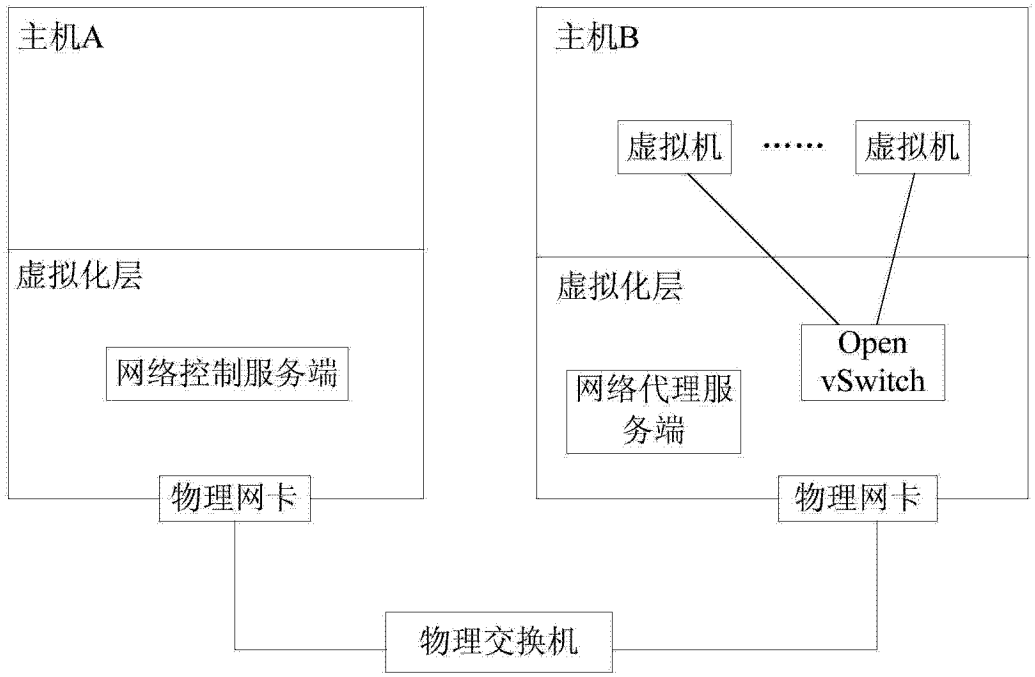

主机A
虚拟化层
网络控制服务端
物理网卡
主机B
虚拟机
……
虚拟机
虚拟化层
Open vSwitch
网络代理服务端
物理网卡
物理交换机

图 2

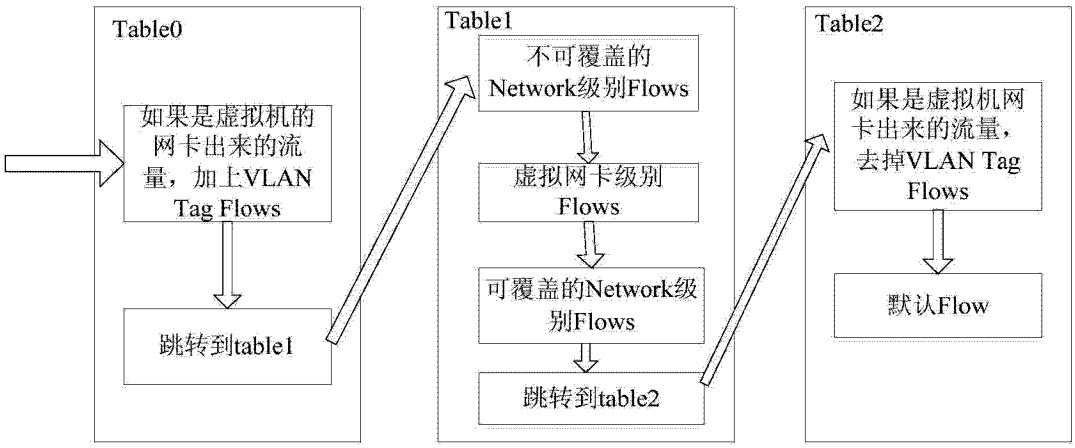


Table0
如果是虚拟机的网卡出来的流量，加上VLAN Tag Flows
跳转到table1
Table1
不可覆盖的Network级别Flows
虚拟网卡级别Flows
可覆盖的Network级别Flows
跳转到table2
Table2
如果是虚拟机网卡出来的流量，去掉VLAN Tag Flows
默认Flow

图 3