发明名称
一种虚拟机流量重定向的方法及装置

摘要
本发明公开了一种虚拟机流量重定向的方法及装置。通过修改虚拟交换机功能模块，动态监测同 VLAN 不同虚拟机之间的二层流量交互，当监测到同 VLAN 不同虚拟机之间的二层流量时，根据预先配置的策略修改虚拟机发送的报文 VLAN，实现报文被重定向到外部的网络安全设备，从而实现服务器内部同 VLAN 不同虚拟机之间的二层流量的安全防护。
1. 一种虚拟机流量重定向的装置，该装置应用于物理服务器上，其中该物理服务器上已创建一个或者多个虚拟机，并且为虚拟机已分配相应的硬件资源，其特征在于，所述装置包括：

策略配置模块，用于根据预定的策略配置同 VLAN 不同虚拟机之间发送的二层流量报文的 VLAN 标签转换规则；

报文监测模块，用于动态监测同 VLAN 不同虚拟机之间的二层流量报文交互；

虚拟交换模块，用于当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的二层流量报文时，根据预先配置的 VLAN 标签转换规则，将虚拟机发送的二层流量报文中携带的第一 VLAN 替换为第二 VLAN，并将该替换为第二 VLAN 的二层流量报文发送到外部网络安全设备进行安全处理。

2. 如权利要求 1 所述的装置，其特征在于，所述外部网络安全设备接收来自虚拟交换模块发送的二层流量报文，按照预定的安全规则对该二层流量报文进行安全处理，并根据预设的 VLAN 标签转换规则，将该经过安全处理的二层流量报文携带的第二 VLAN 替换为第三 VLAN，并将该替换为第三 VLAN 的二层流量报文发送给虚拟交换模块。

3. 如权利要求 1 或 2 所述的装置，其特征在于，所述虚拟交换模块接收来自外部网络安全设备的经过安全处理的二层流量报文，并将该二层流量报文内携带的第三 VLAN 替换为原始的第一 VLAN 后，根据目的 MAC 地址对该二层报文进行转发。

4. 如权利要求 1 所述的装置，其特征在于，当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的反向二层流量报文时，所述虚拟交换模块根据预先配置的 VLAN 标签转换规则，将该反向二层流量报文中携带的第一 VLAN 替换为第三 VLAN，确保反向报文同样经过外部网络安全设备处理。

5. 一种虚拟机流量重定向的方法，所述方法应用于物理服务器上，其中该物理服务器已创建一个或者多个虚拟机，并且为虚拟机已分配相应的硬件资源，其特征在于，所述方法包括：

步骤 31，根据预定的策略，通过策略配置模块为同 VLAN 不同虚拟机之间发送的二层流量报文配置 VLAN 标签转换规则；

步骤 32，通过报文监测模块监测是否存在同 VLAN 内不同虚拟机之间发送的二层流量报文，如果是，则进行步骤 33；

步骤 33，根据预设 VLAN 标签转换规则，通过虚拟交换模块将该二层流量报文中携带的第一 VLAN 替换为第二 VLAN，且对该替换为第二 VLAN 的二层流量报文发送到外部网络安全设备进行安全处理。

6. 如权利要求 4 所述的方法，其特征在于，在所述步骤 33 之后，还包括：

所述外部网络安全设备接收来自虚拟交换模块发送的二层流量报文，并按照预定的安全规则，对该二层流量报文进行安全处理，并根据预设的 VLAN 标签转换规则，并将该经过安全处理的二层流量报文携带的第二 VLAN 替换为第三 VLAN，然后将该替换为第三 VLAN 的二层流量报文发送给虚拟交换模块。

7. 如权利要求 4 或 5 所述的方法，其特征在于，所述虚拟交换模块接收来自外部网络安全设备发送的经过安全处理的二层流量报文，并将该二层流量报文内携带的第三 VLAN 替换为原始的第一 VLAN 后，根据目的 MAC 地址对该二层报文进行转发。
8. 如权利要求5所述的方法，其特征在于，当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的反向二层流量报文时，所述虚拟交换模块根据预先配置的 VLAN 标签转换规则，将该反向报文中携带的第一 VLAN 替换为第三 VLAN，确保反向报文同样经过外部网络安全设备处理。
一种虚拟机流量重定向的方法及装置

技术领域
[0001] 本发明涉及数据通信领域，尤其涉及一种同 VLAN 不同虚拟机之间的二层流量重定向的方法及装置。

背景技术
[0002] 数据中心通常包括三个主要的组成部分：计算、网络和存储，这三家部分在向虚拟化方向发展。其中作为计算资源的服务器的虚拟化是云计算中的核心技术之一，也是目前发展最为成熟的虚拟化技术。传统服务器由于服务器性能和网络通信带宽的不匹配等问题导致服务器计算性能可能被闲置。而服务器的虚拟化技术，则可以将单一物理服务器虚拟成多台虚拟机并独立安装各自的操作系统和应用程序，从而有效提升服务器本身硬件资源的利用率。
[0003] 然而，虚拟化技术的应用使得传统的网络和服务器的管理边界变得模糊，传统的网络和服务器的管理分别属于不同的运维组织。服务器管理人员仅负责业务、数据安装，而网络管理员负责网络连通性和服务器安全防护。但是，虚拟机引入后由于服务器内置了虚拟交换机 VSwitch, 处于同一 VLAN 的不同虚拟机之间的二层流量转发将直接通过虚拟交换机 VSwitch 交换转发，导致目前成熟的安全防护技术无法实施。

发明内容
[0004] 有鉴于此，本发明提供一种虚拟机流量重定向的方法和装置，以解决上述现有技术中存在的不足。
[0005] 本发明是通过如下技术方案实现的：
[0006] 一种虚拟机流量重定向的装置，该装置应用于物理服务器上，其中物理服务器上已创建一个或者多个虚拟机，并且为虚拟机分配相应的硬件资源，其中所述装置包括：
[0007] 策略配置模块，用于根据预定的策略配置同 VLAN 不同虚拟机之间发送的二层流量报文的 VLAN 标签转换规则；
[0008] 报文监测模块，用于动态监测同 VLAN 不同虚拟机之间的二层流量报文交互；
[0009] 虚拟交换模块，用于当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的二层流量报文时，根据预先配置的 VLAN 标签转换规则，将虚拟机发送的二层流量报文中携带的第一 VLAN 替换为第二 VLAN，并将该替换为第二 VLAN 的二层流量报文发送到外部网络服务设备进行安全处理。
[0010] 进一步地，所述外部网络安全设备接收来自虚拟交换模块发送的二层流量报文，按照预定的安全规则对该二层流量报文进行安全处理，并根据预设的 VLAN 标签转换规则，将该经过安全处理的二层流量报文携带的第二 VLAN 替换为第三 VLAN，并将该替换为第三 VLAN 的二层流量报文发送给虚拟交换模块。
[0012] 进一步地，所述虚拟交换模块接收来自外部网络安全设备的经过安全处理的二层流量报文，并将该二层流量报文内携带的第三 VLAN 替换为原始的第一 VLAN 后，根据目的 MAC 地址对该二层报文进行转发。

[0013] 进一步地，当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的反向二层流量报文时，所述虚拟交换模块根据预先配置的 VLAN 标签转换规则，将该反向二层流量报文中携带的第一 VLAN 替换为第三 VLAN，确保反向报文同样经过外部网络安全设备处理。

[0014] 本发明同时还提供一种虚拟机流量重定向的方法，所述方法应用于物理服务器上，其中该物理服务器已创建一个或者多个虚拟机，并且为虚拟机分配相应的硬件资源，其中所述方法包括：

[0015] 步骤 31，根据预定的策略，通过策略配置模块为同 VLAN 不同虚拟机之间发送的二层流量报文配置 VLAN 标签转换规则；

[0016] 步骤 32，通过报文监测模块监测是否存在同 VLAN 内不同虚拟机之间发送的二层流量报文，如果是，则进行步骤 33；

[0017] 步骤 33，根据预设 VLAN 标签转换规则，通过虚拟交换模块将该二层流量报文中携带的第一 VLAN 替换为第二 VLAN，且对该替换为第二 VLAN 的二层流量报文发送到外部网络安全设备进行安全处理。

[0018] 进一步地，在所述步骤 33 之后，还包括：

[0019] 所述外部网络安全设备接收来自虚拟交换模块发送的二层流量报文，并按照预定的安全策略，对该二层流量报文进行安全处理，并根据预设的 VLAN 标签转换规则，并将该经过安全处理的二层流量报文携带的第二 VLAN 替换为第三 VLAN，然后将该替换为第三 VLAN 的二层流量报文发送给虚拟交换模块。

[0020] 进一步地，所述虚拟交换模块接收来自外部网络安全设备发送的经过安全处理的二层流量报文，并将该二层流量报文内携带的第三 VLAN 替换为原始的第一 VLAN 后，根据目的 MAC 地址对该二层报文进行转发。

[0021] 进一步地，当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的反向二层流量报文时，所述虚拟交换模块根据预先配置的 VLAN 标签转换规则，将该反向报文中携带的第一 VLAN 替换为第三 VLAN，确保反向报文同样经过外部网络安全设备处理。

[0022] 与现有的技术相比，本发明通过修改虚拟交换机的功能模块，动态监测同 VLAN 不同虚拟机之间的二层流量交互，当监测到同 VLAN 不同虚拟机之间的二层流量时，根据预先配置的 VLAN 标签转换规则修改虚拟机发送的报文 VLAN，实现该报文被重定向到外部网络安全设备，从而实现服务器同 VLAN 不同虚拟机之间的二层流量的安全防护处理。

附图说明

[0023] 图 1 为典型的物理服务器虚拟化之后的架构示意图。

[0024] 图 2 为本发明虚拟机流量重定向的方法流程示意图。

[0025] 图 3 为本发明虚拟机流量重定向的装置结构示意图。

具体实施方式
[0026] 请参考图1，服务器的虚拟化架构是在物理服务器上引入虚拟化层，其中是中亚层虚拟化软件，主要用于创建虚拟机（Virtual Machine, VM），并与虚拟机分配合理的硬件资源，比如 CPU 中的一个或者多个内核（即 CPU 中集成的一个或多个完整的计算引擎）分配给虚拟机 1 等。虚拟机从逻辑功能上看，与传统的物理服务器并无区别，拥有自己的操作系统，并可以在操作系统之上安装各种应用。在数据中心的物理服务器被广泛虚拟化后，安全问题也就相应产生了。在计算机网络及软件技术中，任何新增的功能都可能存在安全问题而需要加以考虑。虚拟化软件相当于在已知传统安全威胁（如针对操作系统和应用程序的攻击）基础上引入了新的安全威胁。例如，针对虚拟化软件及对应管理平台的漏洞攻击。

[0027] 在虚拟化环境下，单台物理服务器上的各虚拟机之间可能存在直接的二层流量交换。例如，当管理员将多个虚拟机规划在同一 VLAN 中时，若在应用环境下，如果虚拟机 1 和虚拟机 2 属于同一 VLAN，而在一个广播域，此时虚拟机 1 和虚拟机 2 之间的通信显然是不需要经过网关设备的。虚拟机 1 和虚拟机 2 可以通过 ARP 协议知晓对方的 MAC 地址，于是在发送二层报文时，直接使用对方的 MAC 地址作为其目的 MAC 地址，虚拟机 1 和虚拟机 2 通信时发送的报文到达虚拟交换机时，虚拟交换机就可以通过查找 MAC 地址表执行二层转发。通常这种二层交换并不需要经过外置的二层交换机。管理员对于该部分流量既不可控也不可见。

[0028] 因此，管理员面临的挑战是确保虚拟机之间的互相访问符合预定的安全策略。如果该虚拟机之间的访问服务被允许，如何判断这些访问是否存在攻击行为。目前针对上述问题有一些解决方案，比如 Cisco 公司提供的 Cisco802.1BR 技术，该技术方案的设计思路是将虚拟机互访报文流量重定向到外部接入交换机或其他网络设备上的外置安全模块进行安全控制。在该方案中，将流量重新定向到接入交换机的方式需要同时在 Hypervisor 层面、服务器网卡层面和接入交换机层面做出修改，具体来说，802.1BR 技术需要在 hypervisor 层面进行重定向，每个每一个虚拟机需要有相应的虚拟通道和位于接入交换机上的虚拟端口，需要接入交换机做较大的修改来支持，技术实现难度大。

[0029] 为此，为实现本发明目的，本发明采用的核心思想为；通过修改虚拟交换机的功能模块，动态监测同 VLAN 内的不同虚拟机之间的二层流量交互，当监测到同 VLAN 不同虚拟机之间的二层流量，根据预先配置的策略修改虚拟机发送的报文 VLAN，实现报文被自然重定向到外部网络安全设备，从而实现服务器内部同 VLAN 不同虚拟机之间的二层流量的安全防护。

[0030] 为使本领域技术人员更加清楚和明白，以下结合附图及实施例详细说明本发明的具体实现方式。

[0031] 请参考图 2，为本发明的一个实施方式中提供的一种实现虚拟机流量重定向的装置示意图。该装置应用于物理服务器上，其中该物理服务器可采用当前各种流行的硬件架构，包括 CPU、内存、存储器以及网卡等基本硬件。另外，该物理服务器上已创建一个或者多个虚拟机，并且为虚拟机已分配相应的硬件资源。所述装置包括：

[0032] 策略配置模块，用于根据预定的策略配置同 VLAN 不同虚拟机之间传送的二层流量报文的 VLAN 标签名转规则。

[0033] 为实现本发明目的，在本发明中，所述 VLAN 标签名转换规则需要管理员根据预定的策略事先在策略配置模块上配置好。其中所述 VLAN 标签名转换规则具体表现为定义了哪些
特征的数据流需要转换为哪种标签，定义示例如下表 1 所示：

<table>
<thead>
<tr>
<th>策略应用端口</th>
<th>策略应用 VLAN</th>
<th>源目的 IP 地址关系</th>
<th>策略应用元组</th>
<th>VLAN 标签转换</th>
</tr>
</thead>
<tbody>
<tr>
<td>连接 VM 上行端口</td>
<td>100</td>
<td>源 IP 地址&lt;-&gt;目的 IP 地址</td>
<td>Src:192.168.1.0/24;dst:192.168.1.0/24</td>
<td>10</td>
</tr>
<tr>
<td>连接 VM 上行端口</td>
<td>100</td>
<td>源 IP 地址-&gt;目的 IP 地址</td>
<td>Src:192.168.1.0/24;dst:192.168.1.0/24</td>
<td>20</td>
</tr>
<tr>
<td>连接物理网卡下行端口</td>
<td>20</td>
<td>源 IP 地址&lt;-&gt;目的 IP 地址</td>
<td>Src:192.168.1.0/24;dst:192.168.1.0/24</td>
<td>100</td>
</tr>
<tr>
<td>连接物理网卡下行端口</td>
<td>10</td>
<td>源 IP 地址-&gt;目的 IP 地址</td>
<td>Src:192.168.1.0/24;dst:192.168.1.0/24</td>
<td>100</td>
</tr>
</tbody>
</table>

表 1

报文监测模块，用于动态监测同 VLAN 内不同虚拟机之间的二层流量报文交互。

虚拟交换模块，用于当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的二层流量报文时，则根据预先配置的 VLAN 标签转换规则，将虚拟机发送的二层流量报文携带的第一 VLAN 替换为第二 VLAN，并将该替换为第二 VLAN 的报文发送到外部网络安全设备进行安全处理。

具体地，当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的二层流量时，所述虚拟交换模块根据预设的 VLAN 标签转换规则对虚拟机发送的二层流量报文 VLAN（第一 VLAN）进行替换，使得该二层流量报文中携带转换后的 VLAN（第二 VLAN）。经过这样的处理后，原先同 VLAN 不同虚拟机之间发送的二层流量就变成跨 VLAN 转发，那么，虚拟交换模块会认为原先同 VLAN 不同虚拟机之间的通信是三层间的 IP 通信，需要通过外部的网关设备才能实现。为此，虚拟交换模块会自然地将该二层流量报文发送到外部的网关设备，通过该网关设备将二层流量报文进一步发送到外置的网络安全设备，从而实现服务器内部不同虚拟机之间同 VLAN 的二层流量的安全防护。

所述外部网络安全设备接收到来自虚拟交换模块发送的二层流量报文后，按照预设的安全规则对该二层流量报文进行安全处理。进一步地，为了避免同 VLAN 不同虚拟机之间发送的反向二层流量报文不经过网络安全设备的处理直接发送到虚拟机上（因为此时外置的接入交换机可能已学习到正向二层流量报文的 MAC 地址等信息），在本发明实现方式中，优选地，还需要进一步根据预设的 VLAN 标签转换规则，对该经过安全处理的二层流量报文 VLAN 再次进行替换，其中该替换后的 VLAN（第三 VLAN）与经安全处理前的 VLAN（第二 VLAN）以及原始的 VLAN（第一 VLAN）不一样，并将该经过 VLAN（第三 VLAN）替换的报文发送给虚拟交换模块。

当所述虚拟交换模块接收到来自网络安全设备的经过安全处理的报文时，将该经过安全处理的报文中携带的 VLAN（第三 VLAN）替换为原始的 VLAN（第一 VLAN），然后，通过虚拟交换模块根据该二层报文的目的 MAC 地址对该二层报文进行转发。

当所述虚拟交换机收到反向报文时，根据标签转换规则将 VLAN 标签从第一 VLAN 替换为第三 VLAN，确保反向报文同样经过外部网络安全设备处理，由于反向报文的转发流程同正向报文的一致，在此不赘述。

下面以上述表 1 所示的 VLAN 标签转换规则为例进行说明。假设在某一应用场景
下，所述报文监测模块监测到 VLAN100 内不同虚拟机（VM1 发送到 VM2）之间的二层流量到达时，此时需要根据预设的 VLAN 标签转换规则，将该二层流量的 VLAN 标签由 100 修改为 10，然后通过虚拟交换模块经由外置接入交换机发送到网络安全设备进行安全处理。

【0043】进一步地，为了避免同 VLAN 不同虚拟机之间发送的反向二层流量报文（即 VM2 发送给 VM1 的 VLAN 为 100 的二层流量报文）不经过网络安全设备的处理直接发送到虚拟机上，所述外部网络安全设备需要根据预设的 VLAN 标签转换规则，将该经过安全处理的二层流量的 VLAN 标签由 10 替换为 20，所述虚拟交换模块接收到携带 VLAN20 的报文后，进一步将该 VLAN20 修改为 100，然后，根据该二层报文的目的 MAC 地址对该二层报文进行转发。

【0044】当所述虚拟交换机收到反向报文时，根据标签转换规则将 VLAN 标签从第一 VLAN100 替换为第三 VLAN20，确保反向报文同样经过外部网络安全设备处理，由于反向报文的转发流程同正向报文一致，在此不赘述。进一步请参考图 3 所示，为本发明同 VLAN 不同虚拟机之间二层流量交互流程交互示意。在一种实施方式中，该物理服务器上已创建一个或者多个虚拟机，并且为虚拟机已分配相应的硬件资源。本发明装置可以理解为对服务器内部的虚拟交换机功能模块的改进，该装置运行在服务器上执行如下的处理过程。

【0045】步骤 31，根据预定的策略，通过策略配置模块为同 VLAN 不同虚拟机之间发送的二层流量报文配置 VLAN 标签转换规则。

【0046】步骤 32，通过报文监测模块监测是否存在同 VLAN 内不同虚拟机之间发送的二层流量报文，如果存在，则进行步骤 33，否则，依照现有的技术对该报文丢弃或者由虚拟交换模块进行其他转发处理。

【0047】步骤 33，根据预设 VLAN 标签转换规则，通过虚拟交换模块将该二层流量报文中携带的第一 VLAN 替换为第二 VLAN，且将该替换为第二 VLAN 的二层流量报文发送到外部网络安全设备进行安全处理。

【0048】具体地，当所述报文监测模块监测到存在同 VLAN 不同虚拟机之间发送的二层流量时，所述虚拟交换模块将根据预设的 VLAN 标签转换规则对虚拟机发送的二层流量报文 VLAN（第一 VLAN）进行替换，使得该二层流量报文中携带替换后的 VLAN（第二 VLAN）。经过这样的处理后，原先同 VLAN 不同虚拟机之间发送的二层流量就变成跨 VLAN 转发，那么，虚拟交换模块会认为原先同 VLAN 不同虚拟机之间的通信是三层的 IP 通信，需要通过外部的网关设备才能实现的。为此，虚拟交换模块会自然地将该二层流量报文发送到外部的有关设备。通过该网关设备，我们就可以将二层流量报文发送至外部网络安全设备进行安全处理，从而实现服务器内部不同虚拟机之间同 VLAN 的二层流量的安全防护。

【0049】进一步地，为了避免同 VLAN 不同虚拟机之间发送的反向二层流量报文不经过网络安全设备的处理直接发送到虚拟机上（因为此时外置的接入交换机可能已学习到正向二层流量报文的 MAC 地址等信息），所述外部网络安全设备按照预定的安全规则对该二层流量报文进行安全处理后，还需要根据预设的 VLAN 标签转换规则，对该经过安全处理的二层流量报文 VLAN 再次进行替换，其中该替换后的 VLAN（第三 VLAN）与经过安全处理前的 VLAN（第二 VLAN）以及原始的 VLAN（第一 VLAN）不一样，并将该经过 VLAN（第三 VLAN）替换的报文发送给虚拟交换模块。

【0050】当所述虚拟交换模块接收到来自网络安全设备的经过安全处理的报文时，将该经过安全处理的报文中携带的 VLAN（第三 VLAN）替换为原始的 VLAN（第一 VLAN），然后，通过
虚拟交换模块根据该二层报文的目的 MAC 地址对该二层报文进行转发。

[0051] 当所述虚拟交换机收到反向报文时，根据标签转换规则将 VLAN 标签从第一 VLAN 替换为第三 VLAN，确保反向报文同样经过外部网络安全设备处理。由于反向报文的转发流程同正向报文的一致，在此不赘述。

[0052] 在本发明中，通过修改虚拟交换机的功能模块，动态监测同 VLAN 内的不同虚拟机之间的二层流量交互，对不同 VLAN 之间虚拟机之间的二层流量，根据预先配置的策略改变虚拟机发送的报文 VLAN，实现报文被自然重定向到外部接入交换机，进而通过现有普通二层转发技术将虚拟机发送的二层流量转发到外置的安全设备，从而实现服务器内部同 VLAN 不同虚拟机之间的二层流量的安全防护。总体来说是充分利用已有资源，开发工作量非常少，成本得以极大程度的降低。

[0053] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。
<table>
<thead>
<tr>
<th>应用1</th>
<th>应用2</th>
<th>应用3</th>
<th>应用4</th>
<th>应用5</th>
<th>应用6</th>
</tr>
</thead>
<tbody>
<tr>
<td>操作系统</td>
<td>操作系统</td>
<td>操作系统</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>虚拟机1硬件资源</td>
<td>虚拟机2硬件资源</td>
<td>虚拟机3硬件资源</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

虚拟化层

包括CPU、内存、硬盘以及网卡等在内的硬件资源

图 1

- 策略配置模块
- 动态监测模块
- 虚拟交换模块

图 2

- 监测来自虚拟机的二层报文
- 接收来自经过安全设备处理的二层报文
- 来自虚拟机的二层报文发送至外部网络安全设备
- 经过安全处理的二层报文转发
根据预定的策略，通过策略配置模块为同 VLAN 不同虚拟机之间发送的二层流量配置 VLAN 标签转换规则

否

通过报文监测模块监测是否存在同 VLAN 内不同虚拟机之间发送的二层流量

是

虚拟交换模块根据预设 VLAN 标签转换规则，对该二层报文进行 VLAN 替换，并将 VLAN 经过替换的二层报文发送到外部网络安全设备进行安全处理

外部网络安全设备按照预定的安全规则对该二层报文进行安全处理，并根据预设的 VLAN 标签转换规则将经过安全处理的二层报文 VLAN 再次替换，然后将该经过 VLAN 替换的二层报文发送给虚拟交换模块

虚拟交换模块接收到来自经过安全处理的二层报文后，根据预设的 VLAN 标签转换规则将该二层报文 VLAN 替换为原始的 VLAN 后转发给对应的应用

丢弃该报文或者转由虚拟交换模块进行其他处理

图 3