(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 103812704 B
(45)授权公告日 2017.12.15

(21)申请号 201410065000.X

(22)申请日 2014.02.25

(65)同一申请的已公布的文献号
申请公布号 CN 103812704 A

(43)申请公布日 2014.05.21

(73)专利权人 国云科技股份有限公司
地址 523808 广东省东莞市松山湖科技产业园区松科苑14号楼

(72)发明人 熊梦 杨松 莫展鹏 季统凯

(74)专利代理机构 北京科亿知识产权代理事务所(普通合伙) 11350
代理人 汤东凤

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 12/46(2006.01)
H04L 29/06(2006.01)
H04L 29/12(2006.01)

(56)对比文件
CN 102664972 A,2012.09.12,
CN 102209124 A,2011.10.05,
US 2009106404 A1,2009.04.23,

审查员 黄欣欣

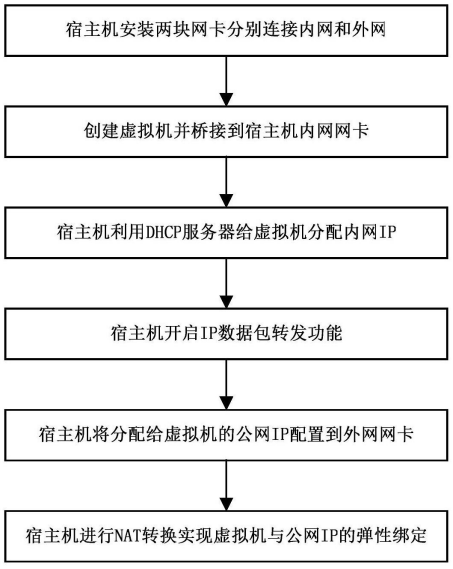
权利要求书1页 说明书6页 附图1页

(54)发明名称

一种面向虚拟机的公网IP动态管理方法

(57)摘要

本发明涉及云计算领域,特别是一种面向虚拟机的公网IP动态管理方法。本发明包括如下步骤:1、在宿主机至少安装两块物理网卡分别用于连接到内网和外网;2、在宿主机上将创建的虚拟机以桥接方式连接到内网网卡;3、宿主机安装配置内网DHCP服务器给虚拟机分配内网IP;4、宿主机开启IP数据包转发功能;5、宿主机将分配给虚拟机的公网IP配置给本身外网网卡子接口;6、最后在宿主机上面通过NAT转换实现虚拟机与公网IP的弹性绑定。本发明解决了虚拟机网络配置复杂且混乱等相关问题;可以用于虚拟机IP管理。



CN 103812704 B

1.一种面向虚拟机的公网IP动态管理方法,其特征在于:

包括如下步骤:

步骤1:在宿主机至少安装两块物理网卡分别用于连接到内网和外网;

步骤2:在宿主机上将创建的虚拟机以桥接方式连接到内网网卡;

步骤3:宿主机安装配置内网DHCP服务器给虚拟机分配内网IP;

步骤4:宿主机开启IP数据包转发功能;

步骤5:宿主机将分配给虚拟机的公网IP配置给本身外网网卡子接口;

步骤6:最后在宿主机上面通过NAT转换实现虚拟机与公网IP的弹性绑定;

所述的弹性绑定是指虚拟机所使用的公网IP可以动态修改,当虚拟机被删除或者无需继续使用此公网时,系统可以自动回收IP重新绑定到其他虚拟机继续使用;

所述的内网DHCP服务器即DNSmasq,可以实现虚拟机内网IP的动态指定;前述内网IP动态指定具体包括如下步骤:

(1)准备虚拟机内网IP规划配置文件;(2)编写IP设置回调函数,并指定操作日志文件;(3)获取宿主机上面虚拟机桥接到的网桥;(4)根据前三步得到的参数启动DNSmasq监听服务进程;(5)修改IP规划配置文件,向DNSmasq监听服务进程发送信号来管理虚拟机IP信息;

所述的IP规划配置文件是一个文本文件,里面存放着各个虚拟机的MAC和对应的IP,DNSmasq会根据此文件来动态修改虚拟机的IP信息;

所述的回调函数是指DNSmasq执行修改虚拟机IP信息时调用执行的一个程序,可产生相关日志并记录到日志文件,管理员可通过日志文件查看IP更新是否成功。

2.根据权利要求1所述的面向虚拟机的公网IP动态管理方法,其特征在于:所述的动态管理是指对虚拟机公网IP的增加、删除和修改。

3.根据权利要求1所述的面向虚拟机的公网IP动态管理方法,其特征在于:所述的桥接方式即“Bridge方式”,是虚拟机连接宿主机的一种网络连接方式,使虚拟机与宿主机处于同一个网段,虚拟机相当于网络内一台独立的机器。

4.根据权利要求2所述的面向虚拟机的公网IP动态管理方法,其特征在于:所述的桥接方式即“Bridge方式”,是虚拟机连接宿主机的一种网络连接方式,使虚拟机与宿主机处于同一个网段,虚拟机相当于网络内一台独立的机器。

一种面向虚拟机的公网IP动态管理方法

技术领域

[0001] 本发明涉及云计算领域，特别是一种面向虚拟机的公网IP动态管理方法。

背景技术

[0002] 在云计算时代，虚拟机通过服务的形式向用户提供，公网的用户需要通过公网IP才能访问到虚拟机。同时，由于云计算服务商提供的虚拟机都需要经过防火墙的隔离；因此，传统的的公网IP管理方法中虚拟机实际上配置的IP都是个内网IP，通过防火墙配置公网IP与内网IP的映射关系，当公网用户通过公网IP访问虚拟机时，防火墙把连接转发到对应的虚拟机上。这种管理方法存在以下的缺点：

[0003] 1、公网IP的管理较混乱，在防火墙中配置的内网IP与公网IP的映射关系是一个静态的对应关系，公网IP与虚拟机并没有联系在一起，公网IP的管理与虚拟机的管理是脱离的，公网IP的映射与回收必须依靠人工的方式进行，容易产生管理混乱的情况，公网IP映射出错、存在无效的映射关系都是有可能的。

[0004] 2、内网攻击不容易隔离，虚拟机对公网用户公开以后，容易发生病毒感染、被劫持的情况，进而影响内网其他主机的安全，由于防火墙只能防御来自外部的攻击，因此，这种情况下不容易单独隔离感染了病毒和被隔离的虚拟机，受影响的范围会进一步扩大，影响整个内网的安全。

发明内容

[0005] 本发明解决的技术问题在于提供一种面向虚拟机的公网IP动态管理方法，解决了云计算领域里虚拟机网络配置复杂且混乱等相关问题。

[0006] 本发明解决上述技术问题的技术方案是：

[0007] 包括如下步骤：

[0008] 步骤1：在宿主机至少安装两块物理网卡分别用于连接到内网和外网；

[0009] 步骤2：在宿主机上将创建的虚拟机以桥接方式连接到内网网卡；

[0010] 步骤3：宿主机安装配置内网DHCP服务器给虚拟机分配内网IP；

[0011] 步骤4：宿主机开启IP数据包转发功能；

[0012] 步骤5：宿主机将分配给虚拟机的公网IP配置给本身外网网卡子接口；

[0013] 步骤6：最后在宿主机上面通过NAT转换实现虚拟机与公网IP的弹性绑定。

[0014] 所述的动态管理是指对虚拟机公网IP的增加、删除和修改。

[0015] 所述的桥接方式即“Bridge方式”，是虚拟机连接宿主机的一种网络连接方式，使虚拟机与宿主机处于同一个网段，虚拟机相当于网络内一台独立的机器。

[0016] 所述的内网DHCP服务器即DNSmasq，可以实现虚拟机内网IP的动态指定；前述内网IP动态指定具体包括如下步骤：

[0017] (1)准备虚拟机内网IP规划配置文件；(2)编写IP设置回调函数，并指定操作日志文件；(3)获取宿主机上面虚拟机桥接到的网桥；(4)根据前三步得到的参数启动DNSmasq监

听服务进程；(5)修改IP规划配置文件，向DNSmasq监听服务进程发送信号来管理虚拟机IP信息；

[0018] 所述的IP规划配置文件是一个文本文件，里面存放着各个虚拟机的MAC和对应的IP，DNSmasq会根据此文件来动态修改虚拟机的IP信息；

[0019] 所述的回调函数是指DNSmasq执行修改虚拟机IP信息时调用执行的一个程序，可产生相关日志并记录到日志文件，管理员可通过日志文件查看IP更新是否成功。

[0020] 所述的弹性绑定是指虚拟机所使用的公网IP可以动态修改，当虚拟机被删除或者无需继续使用此公网时，系统可以自动回收IP重新绑定到其他虚拟机继续使用。

[0021] 本发明方案的有益效果如下：

[0022] 1、本发明的方法能自动进行公网IP的管理，避免混乱；公网IP的生命周期与虚拟机的生命周期联系在一起。

[0023] 2、本发明的方法能对虚拟机的内网攻击进行隔离，一旦发现某个虚拟机被病毒感染或受到劫持，只需要进行在宿主机中进行iptable规则的修改即可隔离其对内网其他主机的攻击，保证内网的安全。

附图说明

[0024] 下面结合附图对本发明进一步说明：

[0025] 图1为本发明的流程图；

[0026] 图2为本发明的模型架构图。

具体实施方式

[0027] 如图1、2所示，配置宿主机网络信息：宿主机安装两张网卡分别为eth0、eth1，假设eth0连接到外网，eth1连接到内网；启动两张网卡，并创建内网网卡eth1的网桥br0，进行如下配置：

[0028] 内网eth1配置文件/etc/sysconfig/network-script/ifcfg-eth0如下：

[0029] DEVICE="eth1"

[0030] ONBOOT="yes"

[0031] BRIDGE=br0

[0032] 网桥br0配置文件/etc/sysconfig/network-scripts/ifcfg-br0如下：

[0033] DEVICE=br0

[0034] TYPE=Bridge

[0035] ONBOOT=yes

[0036] BOOTPROTO=static

[0037] IPADDR=192.168.6.22

[0038] NETMASK=255.255.255.0

[0039] GATEWAY=192.168.6.254

[0040] 宿主机上面创建虚拟机，并使其以桥接方式连接到宿主机内网网卡，即保证虚拟机配置文件网络接口部分如下(mac address可自定义)：

```
<interface type="bridge">
    <mac address="d0:0d:8e:9f:42:88"/>
    <source bridge="br0"/>
    <script path="/etc/xen/scripts/vif-bridge"/>
</interface>
```

[0042] 上述配置文件中mac address可根据需要自定义配置，其余部分保持不变，另外虚拟机启动之后确保其网络配置为自动获取IP方式，配置虚拟机内部系统时间与宿主机系统时间一致。

[0043] 配置宿主机内网DHCP服务器：

[0044] (1)首先在宿主机上面安装DNSmasq内网DHCP服务器程序dnsmasq-2.48-13.e16.x86_64。

[0045] (2)准备虚拟机IP配置文件/etc/network.conf，格式及内容如下：

[0046] d0:0d:8e:9f:42:88,vm-001,192.168.6.243

[0047] (3)准备callback脚本(即回调脚本)，将以下python脚本保存到宿主机/mnt/damon/update2db.py，内容如下：

[0048]

```
#!/usr/bin/env python

import gettext

import os

import sys

def log(command,mac,ip):

        fd=open('/home/zyk/db.info','a')      #这里将 IP 信息保存在 db.info 文件里

        mess="%s %s %s \n"    %(command,mac,ip)

        fd.write(mess)

        fd.close()

def add_lease(mac, ip):

    log('add',mac,ip)

def del_lease(mac,ip):

    log('del',mac,ip)

def main():

    argv = sys.argv

    command = argv[1]

    if command in ['add', 'del', 'old']:

        mac = argv[2]

        ip = argv[3]
```

```
                mac = argv[2]
            if command=='add':
                add_lease(mac,ip)
[0049]      if command=='del':
                del_lease(mac,ip)
    if __name__ == "__main__":
        main()
```

[0050] (4)执行如下命令为br0网桥启动DNSmasq监听服务进程,DNSmasq服务进程根据IP配置文件管理虚拟机IP:

[0051] #/usr/sbin/dnsmasq --strict-order --bind-interfaces --conf-file= --domain=local--pid-file=/var/run/test.pid --listen-address=192.168.6.22 --interface br0--except-interface=lo --dhcp-range=192.168.6.1,static,120s --dhcp-lease-max=256--dhcp-hostsfile=/etc/network.conf --dhcp-script=/mnt/damon/update2db.py--leasefile-ro

[0052] 执行以上操作以正确配置虚拟机vm-001,并给其设定而来内网IP为192.168.6.243;如果需要修改虚拟机内网IP只需要在DNSmasq内网IP配置文件中进行相应修改,发送信号使dnsmasq守护进程及时更新即可。

[0053] 以下进行给虚拟机vm001分配公网操作,现在假设需要将公网IP:20.251.48.99分配给虚拟机vm-001使用,执行执行如下操作:

[0054] (1)开启宿主机IP数据包转发功能,具体操作为修改/etc/sysctl.conf文件里面net.ipv4.ip_forward配置项为1即可:

[0055] #controls IP packet forwarding

[0056] net.ipv4.ip_forward=1//开启宿主机IP数据包转发功能

[0057] (2)开启宿主机防火墙功能:

[0058] #/etc/init.d/iptables start

[0059] (3)给宿主机防火墙nat表设定内网路由转发规则实现对虚拟机公网IP的动态管理:

[0060] 1)分配虚拟机公网IP

[0061] #ifconfig eth0:120.251.48.99/24&&ifconfig eth0:1up

[0062] 给宿主机外网网卡eth0创建一个子接口eth0:1,并将分配给虚拟机vm-001的公网IP:20.251.48.99首先配置给该子接口,启动eth0:1。

[0063] #iptables-A PREROUTING-t nat-d20.251.48.99-j DNAT--to192.168.6.243

[0064] 设定规则,使从公网发来的目的地为20.251.48.99的IP数据包重定向到内网192.168.6.243,即虚拟机vm-001。

[0065] #iptables -A POSTROUTING-t nat -j SNAT -s 192.168.6.243 --to20.251.48.99

[0066] 同样设定反向映射,即将从私有网络192.168.6.243发送出去的IP数据包源地址改为公网IP:20.251.48.99。

[0067] 2)回收虚拟机公网IP

[0068] #ifconfig eth0:1down

[0069] 关掉虚拟机vm-001所对应的外网子接口eth0:1;

[0070] #iptables-D PREROUTING -t nat -d 20.251.48.99 -j DNAT --to192.168.6.243

[0071] #iptables -D POSTROUTING -t nat -j SNAT -s 192.168.6.243 --to20.251.48.99

[0072] 执行上面两个操作从iptables中的nat表中去掉虚拟机vm-001私有IP192.168.6.243与公网IP20.251.48.99的映射。回收后的虚拟机公网IP可以被重新分配给其他虚拟机使用,分配方法同上。

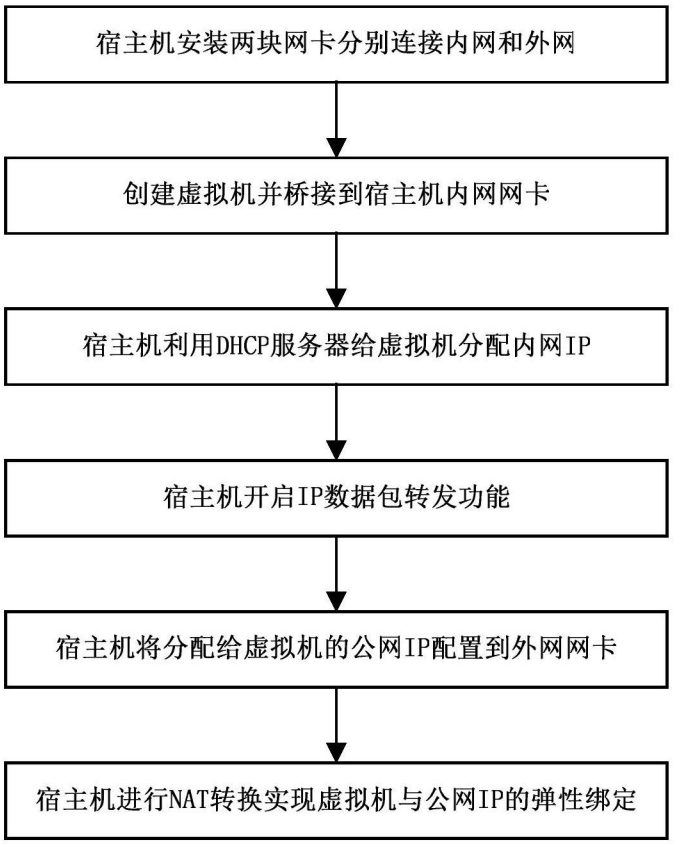

宿主机安装两块网卡分别连接内网和外网
创建虚拟机并桥接到宿主机内网网卡
宿主机利用DHCP服务器给虚拟机分配内网IP
宿主机开启IP数据包转发功能
宿主机将分配给虚拟机的公网IP配置到外网网卡
宿主机进行NAT转换实现虚拟机与公网IP的弹性绑定

图1

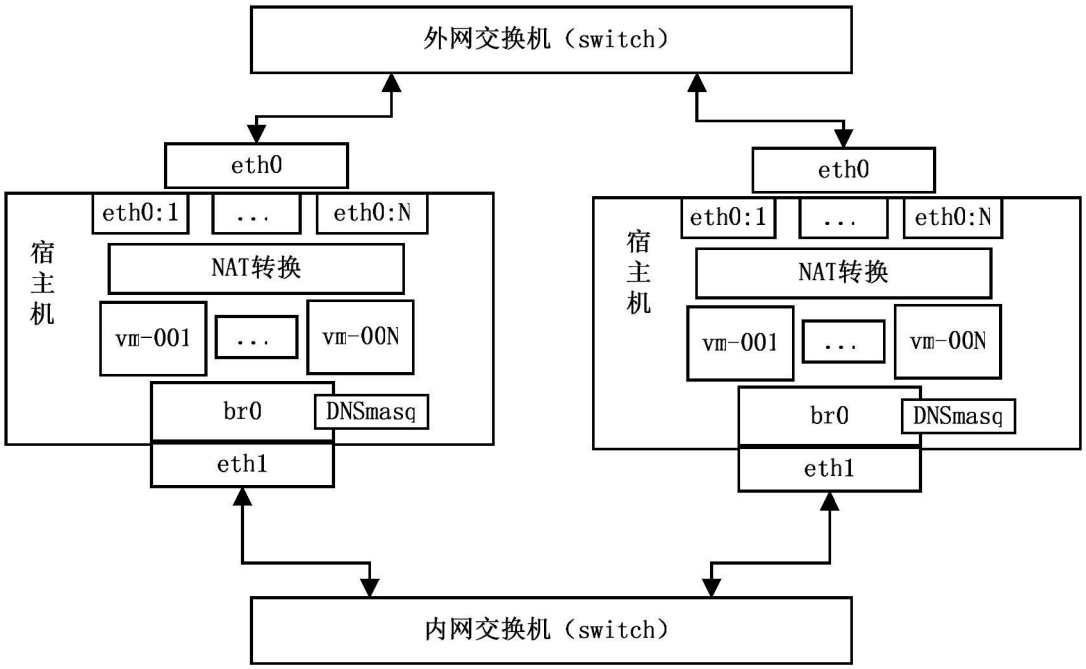

外网交换机（switch）
eth0
eth0:1
...
eth0:N
宿主机
NAT转换
vm-001
...
vm-00N
br0
DNSmasq
eth1
eth0
eth0:1
...
eth0:N
宿主机
NAT转换
vm-001
...
vm-00N
br0
DNSmasq
eth1
内网交换机（switch）

图2