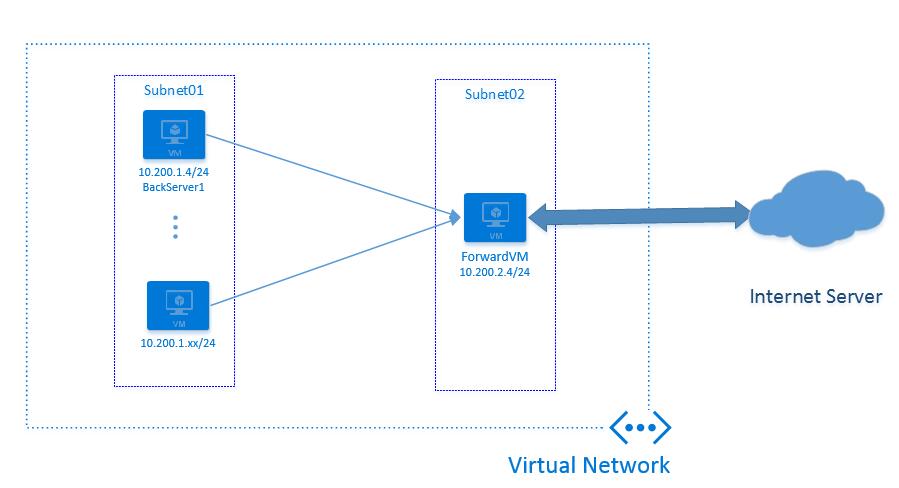
ARM虚拟机使用同一个公共IP访问公网的解决方案

Azure目前有两种部署模型：资源管理器ARM和经典部署模型ASM。ASM的虚拟机默认公用云服务的VIP来访问Internet，ARM的虚拟机默认使用自己的公共IP访问Internet。因为有的服务器有访问白名单的设置，因此有的客户可能想实现的一个需求就是ARM的多个虚拟机也公用一个公共IP来访问公网的某个服务器，这样就不需要在对方的白名单上添加多个虚拟机的公共IP地址。下面介绍如何实现这个方案。

虚拟网络的Subnet01子网中的多台虚拟机将公用Subnet02中的虚拟机ForwardVM访问Internet上的某台服务器。假设Internet上的这台服务器的地址是42.159.4.113，这里是以Azure的经典管理门户（https:// manage.windowsazure.cn）示例。下面介绍操作步骤。

1、首先借助Azure的自定义路由功能，创建一个路由表，将Subnet01这个子网访问Internet服务器的流量定向到虚拟机ForwardVM。下面通过Azure Powershell来操作。其实也可以在门户上创建。

#创建一个路由条目

$route = New-AzureRmRouteConfig -Name subnet01route -AddressPrefix 42.159.4.113/8 -NextHopType VirtualAppliance -NextHopIpAddress 10.200.2.4

#创建一个路由表，关联上面创建的路由条目

$routeTable = New-AzureRmRouteTable -ResourceGroupName TestVnetGroup –Location “China North” -Name tableforsubnet01 -Route $route

#将上面创建的路由条目关联到子网Subnet01

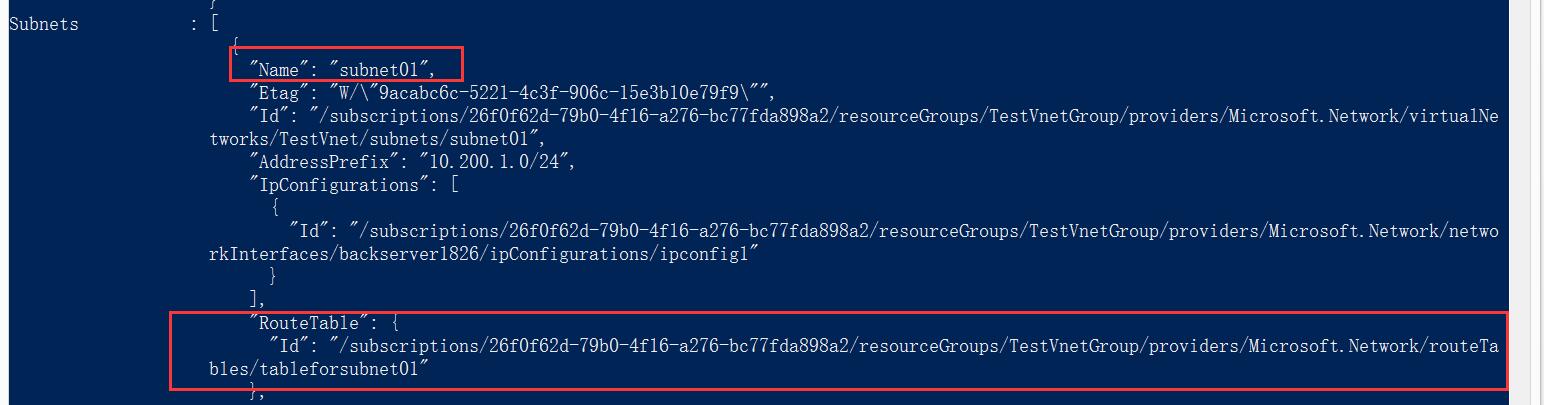
$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName TestVnetGroup -Name TestVnet

Set-AzureRmVirtualNetworkSubnetConfig -Name subnet01 -VirtualNetwork $vnet -AddressPrefix 10.200.1.0/24 –RouteTable $routeTable

#保存虚拟网络的配置

Set-AzureRmVirtualNetwork -VirtualNetwork $vnet

保存成功后，我们看到Subnet01上已经关联了上面创建的路由表。



2、在虚拟机ForwardVM上开启IP转发并对Subnet01子网中访问Azure经典管理门户的流量做SNAT

（1）在平台层面，开启虚拟机的IP转发功能

在门户上看到，虚拟机ForwardVM的网卡名称为forwardvm350



#获取网卡对象

$nicfwvm=Get-AzureRMNetworkInterface -ResourceGroupName TestVnetGroup -Name forwardvm350

#开启IP转发

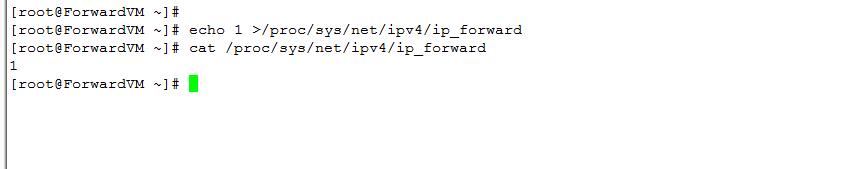
$nicfwvm.EnableIPForwarding = 1

#保存配置

Set-AzureRmNetworkInterface -NetworkInterface $nicfwvm

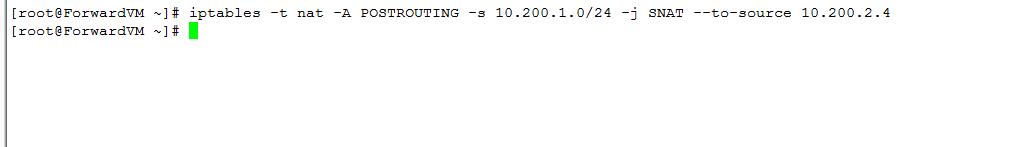
（2）在虚拟机ForwardVM内部开启IP转发功能

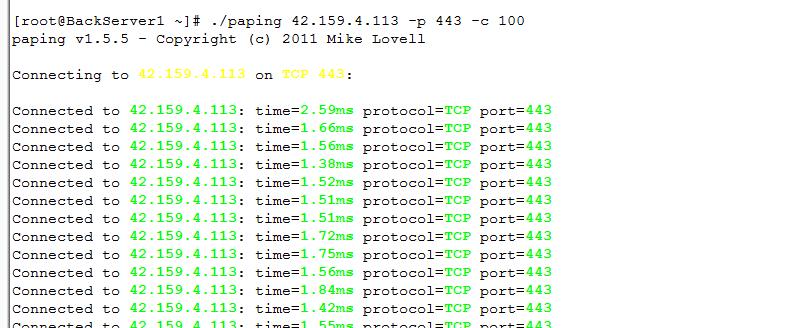
echo 1 >/proc/sys/net/ipv4/ip\_forward



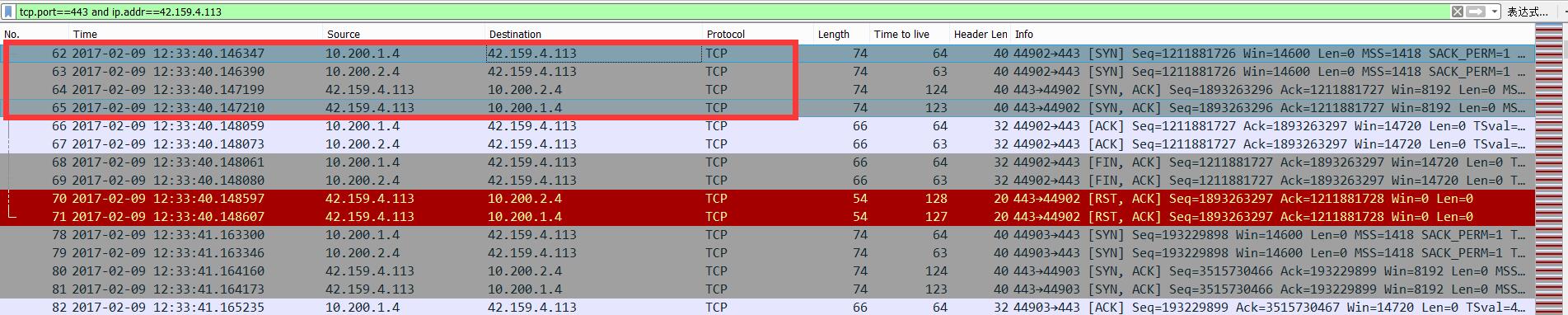
（3）在虚拟机ForwardVM内做一个SNAT，将Subnet01中虚拟机访问Azure管理门户（Internet）的数据包的源地址改为虚拟机ForwardVM的地址

iptables -t nat -A POSTROUTING -s 10.200.1.0/24 -j SNAT --to-source 10.200.2.4



3、在Subnet01内的一台虚拟机BackServer1上进行测试。一直用Paping测试Azure经典管理门户地址42.159.4.113的443端口，一直可以访问

同时在ForwardVM上进行抓包，发现BackServer1访问42.159.4.113的数据包确实发往了ForwardVM。

从上面的数据包可以看出，ForwardVM对这个数据包确实做了地址转换。将访问数据包的源地址转换为了ForwardVM自己的IP 10.200.2.4.

因此上面的操作，实现了多个VM公用一台VM的公有IP访问Internet服务器的操作。