随着Azure平台用户越来越多，同时需求也越来越广泛，其中之一就是网络架构上的需求，比如需要强大的应用层防火墙，网络访问控制管理，网络安全认证，出口网关统一等，而用户为了满足架构需求，希望借助第三方网络设备厂商来兼容Azure的网络服务来实现。虽然看起来是一个很好的方式，但是其中存在着很多兼容问题以及需要通过实践来测试架构上的可信性。

很幸运，有机会需要实现Azure和Palo Alto Network之间的结合来满足客户的需求，从而借此机会把经验分享给大家，希望对大家以后的工作和项目有所帮助

内容说明：

1. 以下内容不涉及太多技术分析，以结果为主
2. 如今Cloud产业更新快速，因此不排除Azure与厂商之间兼容性会存在变化
3. 不涉及太多的Palo Alto的产品介绍，如果你选择的厂商技术特点与之类似，本人认为可以借鉴
4. 以下内容涉及到部分Azure基本知识，如果对某些服务不了解请查询官方文档
5. 以下内容针对的都是新门户服务和环境，无法保证经典门户都能够实现

环境介绍：

1. 由厂商Palo Alto提供如下资源
   * Azure的VHD镜像文件：软件版本号为7.1.10
   * 提供在Azure上部署的Template配置文件：多网卡并属于不同的子网
   * 产品License用于激活
2. 用提供的VHD创建Azure的VM
   * 使用azcopy将VHD镜像上传到Storage Account
   * 通过Powershell/Portal/CLI使用Template配置文件部署VM
   * 保证内网地址可以ICMP可达
   * 保证从外网通过Azure VM的VIP地址访问到Palos Alto的Web管理界面
3. 注意点
   * Palo Alto提供的配置文件并不一定是一站式部署，很多资源可能需要自己去创建，比如存储账号，虚拟网络，子网，资源组等
   * 注意配置文件中的一些资源的参数可能会和你创建的资源有冲突，请仔细核对，比如存储账号里面的SKU

建立IPsec隧道场景介绍

1. 不同VNet的NVA之间建立IPsec隧道



部署步骤

* + pavm1：通过Palo Alto的VHD镜像创建出来的Azure VM1，并属于VNet1
  + pavm2：通过Palo Alto的VHD镜像创建出来的Azure VM2，并属于VNet2
  + VNet Gateway之间建立VNetToVNet连接
  + 基于VNetToVNet连接，pavm1 与pavm2建立IPsec隧道
  + 在IPsec隧道的基础上实现路由传递

1. Azure NVA与本地Palo Alto设备建立IPsec隧道



部署步骤

* + pavm1：通过Palo Alto的VHD镜像创建出来的Azure VM1，并属于VNet1
  + Local-PA：拥有独立公网地址的Palo Alto硬件设备，目前没有发现版本兼容性问题
  + pavm1的网卡绑定PIP地址
  + Local-PA通过Internet与pavm1的PIP建立IPsec隧道
  + 在IPsec隧道的基础上实现路由传递：BGP或者静态

1. 通过VPN Gateway来实现本地Palo Alto设备与Azure NVA之间建立IPsec隧道



部署步骤

* + pavm1：通过Palo Alto的VHD镜像创建出来的Azure VM1，并属于VNet1
  + Local-PA：拥有独立公网地址的Palo Alto硬件设备，目前没有发现版本兼容性问题
  + Local-PA通过Internet与VPN Gateway建立基于路由的IPsec隧道并传递内网路由
  + 基于此IPsec隧道，Local-PA的私有地址与pavm1的私有地址建立IPsec隧道
  + 在IPsec隧道的基础上实现路由传递

从以上介绍可以看出，基于NVA来建立IPsec隧道方式有多种，需要根据自身的网络架构需求来选择最适合的方式，以下介绍一个较复杂的需求供各位参考：让本地网络去往Internet的流量通过Azure出口进行转发



部署步骤：

* pavm2：通过Palo Alto的VHD镜像创建出来的Azure VM2，并属于VNet2
* Local-PA：拥有独立公网地址的Palo Alto硬件设备，目前没有发现版本兼容性问题
* Local-PA通过Internet与VNet1中的VPN Gateway建立基于路由的IPsec隧道并建立EBGP邻居
* VNet1中的VPN Gateway与pavm2的PIP建立IPsec隧道并建立EBGP邻居
* pavm2在BGP路由协议中通告默认路由
* pavm2配置NIC的默认路由
* pavm2配置NAT条目，封装来自本地网段的源地址为NIC的地址

本地网络Internet流量走向（绿色箭头）：

1. 本地网络通过内部路由转发到Local-PA
2. Local-PA根据从BGP学到的默认路由转发到VPN Gateway
3. VPN Gateway根据从BGP学到的默认路由转发到pavm2
4. pavm2根据配置的NIC的默认路由丢给PIP，并将源地址封装成NIC地址
5. 将源地址转化成PIP地址丢到公网

分析：

* 为了网络的扩展性，让其中一个VNet中的VPN Gateway作为网络Hub是一个比较可行的方式
* BGP路由协议是目前VPN Gateway唯一支持的动态路由协议
* 由于Azure VM的公网地址并不是直接绑定到VM上，而是对VM的NIC地址进行NAT的地址转化，因此如果将VM作为路由器，还需要对转发的流量进行NAT转化
* 实现的方式有多种，各自都有利弊

目前以下方式无法实现

1. 由于Azure VM网络禁用GRE协议，因此任何基于GRE的隧道技术都无法实现

2. 避免在VNet中的VPN Gateway与同一个VNet中的pavm建立BGP邻居并传递路由，可能会造成环路

小结：

如果你的网络架构会参考到部分文章内容，请进行测试评估后再考虑部署，在部署过程中可能会遇到一些小问题，这里不会进行扩展讨论，请咨询相关厂商和Azure技术支持。