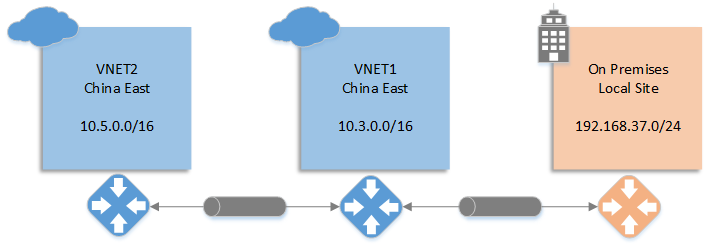
如何在Azure VPN 网关上实现网络透传

**背景介绍**

在一些使用Azure的较复杂的网络架构中，会存在多个虚拟网络和本地网络。鉴于某些特殊的使用场景或需求，需要实现某一个虚拟网络透过跟其相连的虚拟网络网关去跟其后端的虚拟网络或者本地网络进行通讯。

比如在下面的应用场景中，虚拟网络VNET1已经跟本地On Premises Local Site 打通了VPN，客户在Azure又创建了虚拟网络VNET2也需要跟本地进行通信。为了降低成本以及维护方便，客户不希望跟本地打通多个VPN通道，VNET2需要通过VNET1的VPN网关作为跳板来访问本地网络。这是一个比较典型的需要使用VPN网关网络透传功能的场景，本文也将以这个场景为例来描述搭建这样的环境的具体方法。



**实现方法**

目前实现VPN网关的网络透传主要有以下三种方案：

1. 使用VPN网关的BGP功能

BGP作为动态路由协议，可以用来在多个节点之间传递路由。当我们在所有的虚拟网络网关和本地VPN设备上都启用BGP功能并打通VPN连接后，可以轻松的实现各个虚拟网络和本地网络之间的互通而不需要进行额外配置。并且由于BGP动态路由的特性，当网络架构需要调整时我们需要进行的配置修改也相对较少。比如在上图所示的应用场景中，当我们又创建了虚拟网络VNET3需要透过VNET1的VPN网关来访问本地，我们甚至不需要对本地设备进行任何的操作就能实现本地与VNET3的互通。

1. 自定义本地网络（Local Network）地址空间

对于Azure虚拟网络的VPN连接，我们都需要配置一个本地网络来告知VPN 网关对方所使用的地址空间，我们可以利用这个特性用一些“小技巧”来实现网络透传。(这里的**本地网络**是指在Azure上面配置的本地网络【Local Network】，而不是指客户On Premises Local Site的网络)。 比如在上图所示的应用场景中，正常情况下VNET1和VNET2如果使用VPN的方式进行连接，我们只需要配置VNET2连接的本地网络地址空间为VNET1的地址空间，VNET1连接的本地网络地址空间为VNET2的地址空间。如果要实现透传，需要将VNET2连接的本地网络地址空间改为VNET1的地址空间与On Premises Local Site地址空间的合集。同样的，在On Premises Local Site的VPN设备上，也要添加路由将走向VNET2的流量导向跟VNET1建立的VPN隧道上。由于VNET1的VPN 网关已经有路由来传递这些目标地址不是自己虚拟网络内的流量并且Azure VPN 网关本身是支持透传的，所以我们不需要在VNET1上再做额外的配置。由于这个方案需要根据当前的网络架构来修改本地网络的配置，如果用户不能真正了解Azure本地网络的作用往往容易出错，所以配置的时候要多加小心。

1. 使用虚拟网络对等互联（VNET Peering）

虚拟网络对等互联是Azure在2016年年底发布的最新功能，可以利用此功能在不创建VPN 网关的前提下实现两个虚拟网络的互联。默认情况下虚拟网络对等互联就是支持网络透传的，但是目前虚拟网络对等互联只支持同一个数据中心的虚拟网络进行互联，所以按照上图所示的架构如果VNET2创建在中国北部，VNET1创建在中国东部时，目前是没法使用虚拟网络对等互联来实现网络透传的。

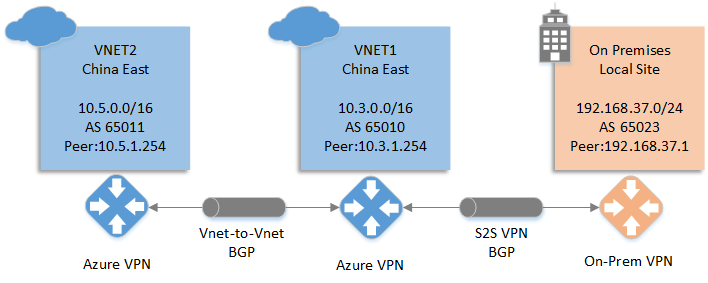
下表将三种方案进行了对比，用户可以根据具体的需求进行选择

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **方案** | **灵活性** | **本地设备要求\*** | **是否支持跨区域** | **操作复杂度** |
| BGP | 高 | 高 | 是 | 高 |
| 自定义本地地址空间 | 低 | 一般 | 是 | 中 |
| VNET Peering | 中 | 一般 | 否 | 低 |

\*启用BGP的方案需要设备支持BGP功能，有些防火墙支持VPN功能但是并不支持BGP功能，在使用前需要了解设备是否支持BGP功能。而其他两种方案不需要设备支持BGP功能而只需要支持VPN功能。所以这里启用BGP的方案相对来说对设备的要求高一些。

下面介绍三种方案的具体配置方法。

**使用VPN网关的BGP功能**



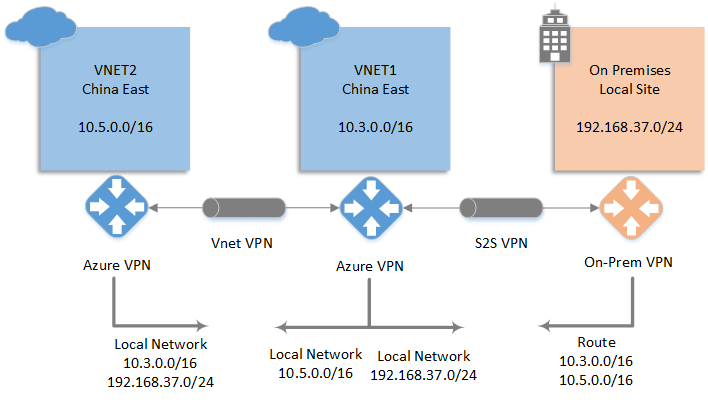
如上图所示，VNET2与VNET1的VPN 网关需要开启BGP功能，并且在VNET2和VNET1之间建立支持BGP的连接。同样VNET1和On Premises Local Site 也建立支持BGP的VPN连接。建立好这些支持BGP的连接之后不需要再进行额外的配置可以使得VNET2透过VNET1的VPN 网关来访问On Premises Local Site。

由于已经有文章来详细讲述如何配置这样的环境，本文不再赘述。读者可以参考下面的两篇文章进行配置：

<https://www.azure.cn/documentation/articles/vpn-gateway-bgp-resource-manager-ps>

<https://www.azure.cn/documentation/articles/aog-virtual-machines-howto-windows-server-2016-bgp-vpn/>

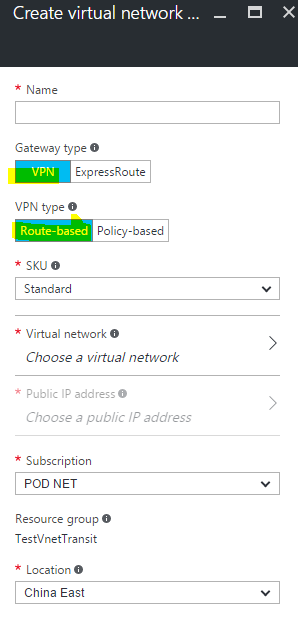
**自定义本地网络（Local Network）地址空间**



如上图所示，VNET2与VNET1使用VPN进行连接，VNET1和On Premises Local Site也通过站点到站点VPN进行连接。该配置的关键地方是要将VNET2连接VNET1所对应的本地网络地址空间设置为10.3.0.0/16和192.168.37.0/24的合集。这样VNET2的 VPN 网关也会将目标地址为192.168.37.0/24的流量转发给VNET1的VPN 网关，由于VNET1的VPN 网关有去往本地On Premises Local Site的路由，所以会将192.168.37.0/24的流量转发到跟本地连接的VPN隧道，同时本地VPN设备也需要添加路由将去往10.5.0.0/16的流量指向VPN隧道。通过这样的配置就实现了VNET2和On Premises Local Site之间的流量通过VNET1的VPN 网关进行透传。

下面详细介绍在ARM模式下如何进行配置：

1. 建立虚拟网络VNET1，地址空间为10.3.0.0/16，添加网关子网为10.3.1.0/224。
2. 建立虚拟网络VNET2，地址空间为10.5.0.0/16，添加网关子网为10.5.1.0/224。
3. 建立VNET1 对应的VPN 网关，Gateway类型为VPN， VPN类型必须为Route-based**。**

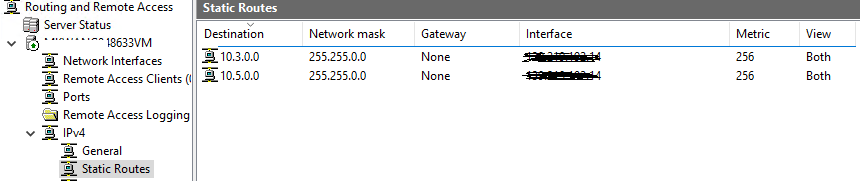


1. 建立VNET2对应的VPN 网关，Gateway类型为VPN， VPN类型为Route-based。
2. 建立本地网关LocalGW, IP地址为本地VPN设备地址，地址空间为192.168.37.0/24。
3. 建立连接，用于连接VNET1 VPN 网关和LocalGW （密钥自行指定，后续建立的连接都使用这个密钥）。
4. 按照下面的文档配置本地VPN设备。

<https://www.azure.cn/documentation/articles/vpn-gateway-about-vpn-devices/>

注意：不仅需要把VNET1的地址空间指向VPN tunnel 还需要把VNET2的地址空间指向VPN tunnel。

比如我这边使用的Windows Server 2016 搭建的VPN，需要建立静态路由把10.3.0.0/16和10.5.0.0/16两个地址空间的流量指向VPN tunnel。



1. 建立VNET1 和VNET2所对应的本地网络网关。

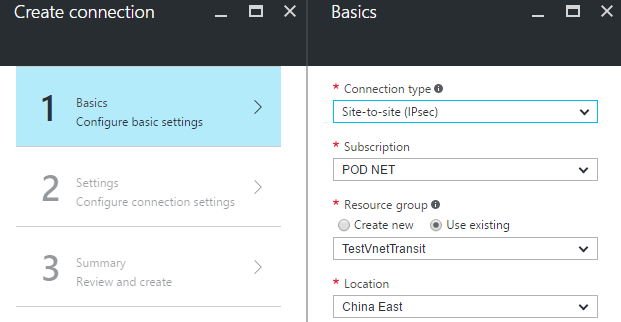
假设VPN 网关建立成功后VNET1对应的Gateway IP为VIP1，VNET2对应的Gateway IP为VIP2。

|  |  |  |
| --- | --- | --- |
| VNET1 | 10.3.0.0/16 | VIP1 |
| VNET2 | 10.5.0.0/16 | VIP2 |

需要建立VNET1对应的本地网络网关LocalVnet1，VPN地址为VIP1，地址空间为10.3.0.0/16，192.168.37.0/24 （这里一定要把On premises Local Site的地址空间加上）。

还需要建立VNET2对应的本地网络网关LocalVnet2，VPN地址为VIP2，地址空间为10.5.0.0/16。

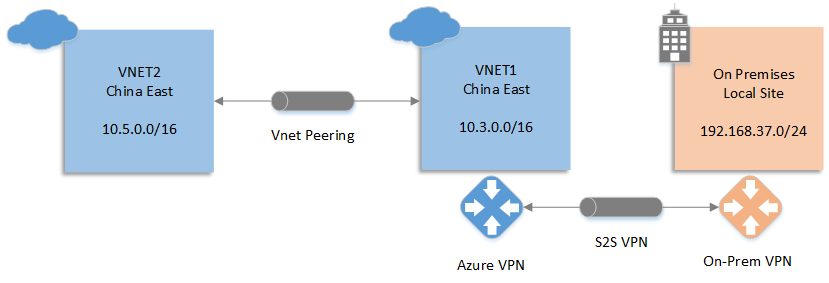
1. 建立VNET1 VPN 网关到LocalVnet2的连接，同时建立VNET2 VPN 网关到LocalVnet1的连接。建立连接的时候选择类型为Site-to-Site (IPsec) 而不要选择VNET to VNET。



1. 以上配置成功后，就可以在VNET2和On Premises Local Site之间进行访问了。

**使用虚拟网络对等互联（VNET Peering）**

使用虚拟网络对等互联从架构上来讲是最简单的，操作也相对比较容易，但是必须得注意的是目前VNET1和VNET2必须创建在同一个数据中心。

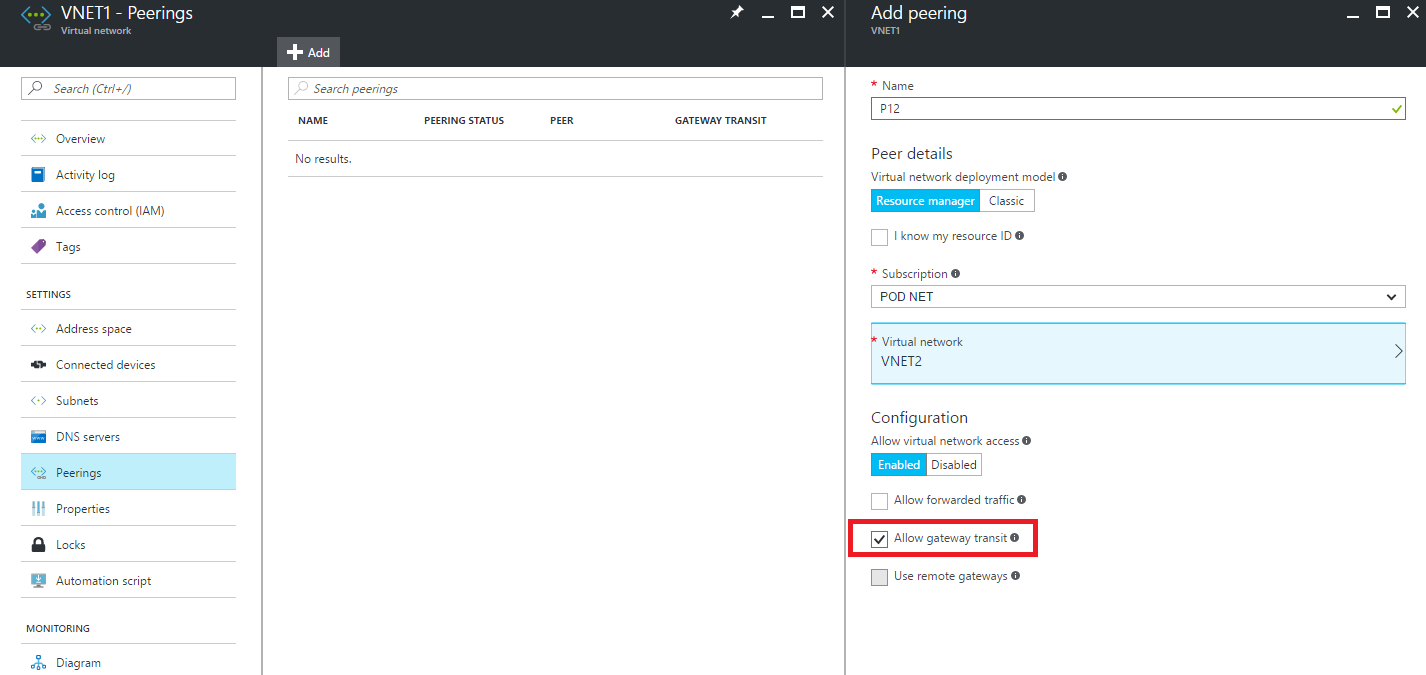


如上图所示，在这个架构中对于虚拟网络VNET2不再需要建立VPN 网关，而利用VNET Peering所自带的网络透传功能进行配置。具体的操作步骤如下：

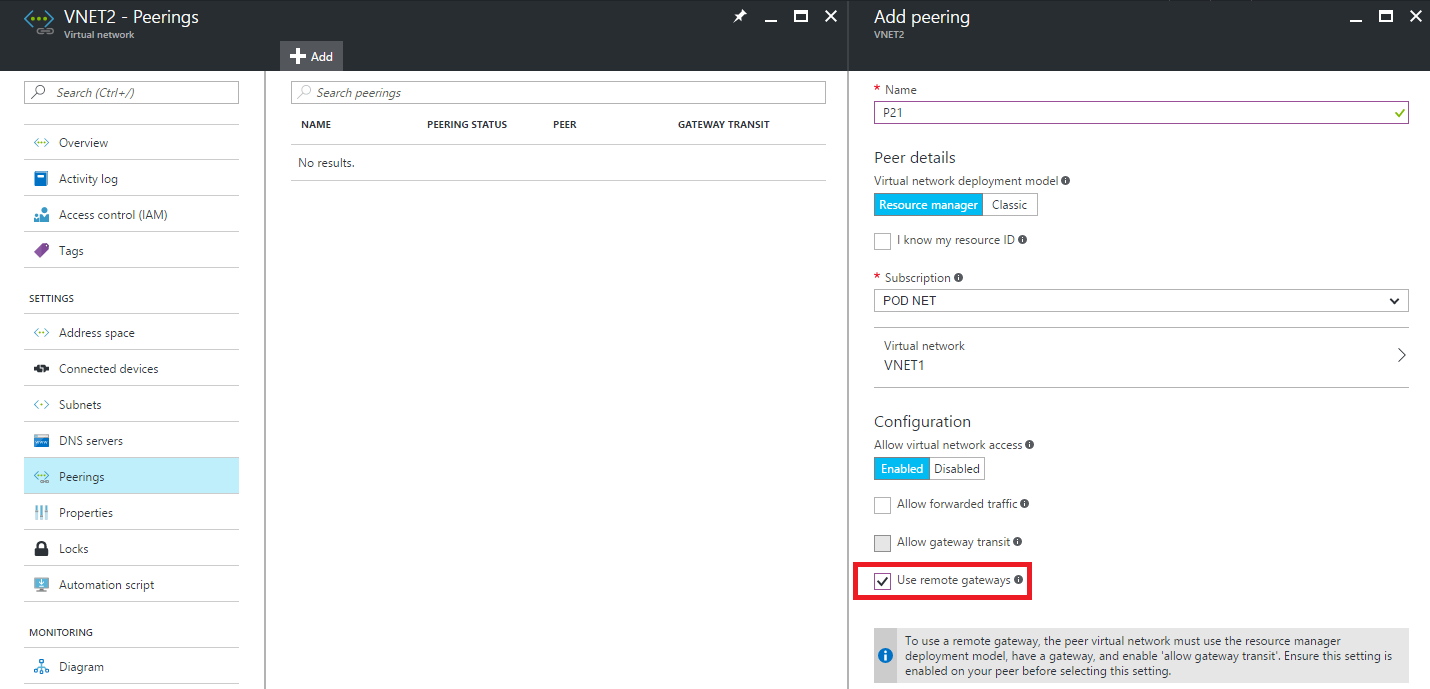
1. 参考下面的文章建立VNET1和On Premises Local Site之间的站点到站点VPN连接。

<https://www.azure.cn/documentation/articles/vpn-gateway-howto-site-to-site-resource-manager-portal/>

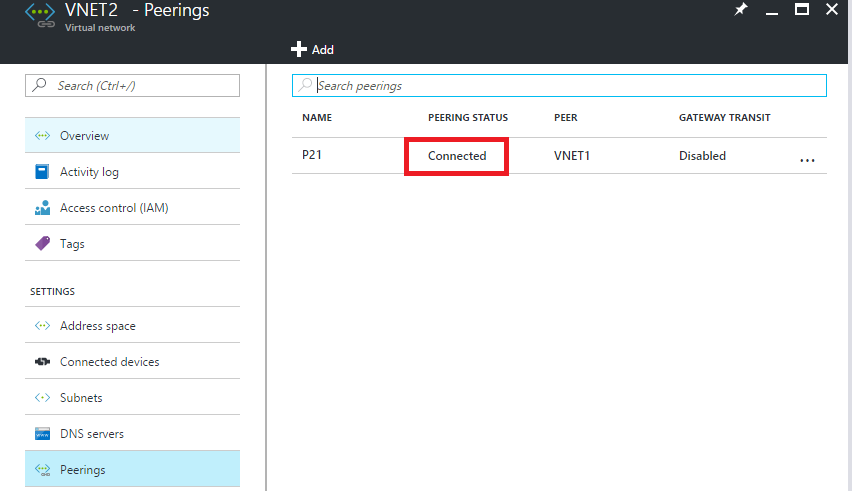
1. 点击创建好的VNET1并找到Peering，再次点击添加（Add）按钮。配置所连接的虚拟网络为VNET2并且在配置部分选择允许网络透传（allow gateway transit）。



1. 点击VNET2并找到Peering, 再次点击添加（Add）按钮。配置所连接的虚拟网络为VNET1并且在配置部分选择使用远程网关（use remote gateway）。



1. 当Peering状态显示为已连接时（connected）表示虚拟网络对等互联建立成功。



1. 本地的VPN设备需要添加路由将去往VNET2 10.5.0.0/16的流量指向VPN tunnel。
2. 以上配置成功后，就可以在VNET2和On Premises Local Site之间进行访问。