Partner Readiness

**Azure Fundamental PART Ⅱ**

* **Network**



2019.12

目录

[写在前面： 3](#_Toc26224078)

[快速查看Azure常见问题： 3](#_Toc26224079)

[快速开始： 3](#_Toc26224080)

[Core Networking 4](#_Toc26224081)

[TCP/IP（100） 4](#_Toc26224082)

[HTTP / HTTPS, SSL / TLS（100） 4](#_Toc26224083)

[DNS（100） 4](#_Toc26224084)

[VNET / VM 5](#_Toc26224085)

[VNET / Subnet（100） 5](#_Toc26224086)

[Lab18: Deploy a VNET through Portal(ARM & ASM) and learn address management and Segmentation & Deploy a VNET through PowerShell（100） 6](#_Toc26224087)

[Lab19: Deploy two VNETs and establish VNET Peering（100） 6](#_Toc26224088)

[Lab20: Deploy two VNETs and establish VNET to VNET（100） 7](#_Toc26224089)

[VM 9](#_Toc26224090)

[Lab21：Use PowerShell to reserve VIP for ASM VM and set ARM VM PIP static（100） 9](#_Toc26224091)

[Lab22: Set VM's private IP as static IP (Portal and PowerShell) （200） 9](#_Toc26224092)

[NSG / Endpoints 10](#_Toc26224093)

[What is NSG / Endpoints（100） 10](#_Toc26224094)

[Lab23：Create a NSG and associate it with VM and Subnet （100） 12](#_Toc26224095)

[UDR 12](#_Toc26224096)

[What is UDR 12](#_Toc26224097)

[Lab24：Create a UDR and associate it with VM or Subnet, and verify. （100） 13](#_Toc26224098)

[Azure VPN 14](#_Toc26224099)

[IPsec and IKE Fundamental（100） 14](#_Toc26224100)

[Azure VPN Gateway（100） 15](#_Toc26224101)

[Lab25：Deploy two VNETs and establish VNET to VNET（100） 17](#_Toc26224102)

[Lab26：Configure P2S VPN and test connectivity between your client and Azure VNET（200） 17](#_Toc26224103)

[Lab27：Establish VPN between On-premise policy-based device and Azure Route-Based VPN Gateway（200） 18](#_Toc26224104)

[High-Available VPN Connection（100） 18](#_Toc26224105)

[ExpressRoute 21](#_Toc26224106)

[SLB/ILB Application Gateway 21](#_Toc26224107)

[SLB/ILB（100） 21](#_Toc26224108)

[Lab28: SLB deployment & ILB deployment（200） 21](#_Toc26224109)

[Application Gateway（100） 21](#_Toc26224110)

[Lab29: Create and configure non-ssl AppGW（200） 22](#_Toc26224111)

[Application Gateway (WAF) Network Watcher AOG Docs 22](#_Toc26224112)

[Lab30: Create and configure SSL-offload AppGW（200） 22](#_Toc26224113)

[Lab31: Create and configure end to end SSL AppGW（200） 22](#_Toc26224114)

[Lab32: Create and configure URL-based routing AppGW（200） 22](#_Toc26224115)

[Lab33: Create and configure URL-based routing AppGW（200） 22](#_Toc26224116)

[Network Watcher（100） 22](#_Toc26224117)

[AGO（100） 23](#_Toc26224118)

[Checkpoint 24](#_Toc26224119)

[Tips 25](#_Toc26224120)

[Reference 25](#_Toc26224121)

# 写在前面：

本篇readiness主要Azure level100-200为主要的内容，涵盖了Network相关知识点，包括VNet, VPN, ER, LB, APPGW等。旨在帮助Partner做Azure基础培训。

本文主要内容会以链接的形式出现，但是除此之外，重点的部分也会以文字的形式呈现，在链接后出现以示强调，其中最重要的部分会画下划线进行标注，方便读者快速浏览。

*本文包含多个Labs，编号承接****Part Ⅰ****。请按照链接完成Lab。*

在文章最后有本Part相关的Checkpoint，帮助检查知识点掌握情况。

# 快速查看Azure常见问题：

* **Azure 订阅和服务限制、配额和约束：**

<https://docs.microsoft.com/zh-cn/azure/azure-subscription-service-limits?toc=%2fazure%2fvirtual-network%2ftoc.json#azure-resource-manager-virtual-networking-limits>

*此链接包含了几乎所有Azure当中的产品的限制性的策略。*

* **Azure产品定价：**

<https://www.azure.cn/zh-cn/pricing/>

*在这里可以找到每个产品的具体价格。*

* **价格计算器：**

<https://www.azure.cn/zh-cn/pricing/calculator/>

*这里可以让用户在购买前进行一个价格的估算。*

# 快速开始：

* Partner 三周Learning Path：

<https://mspartner123.github.io/ms.github.io/>

# Core Networking

这部分知识很多，但是都是基础知识，看完之后对于更加深刻的掌握Azure Network方面的内容十分有帮助，其中物理地址解析部分跟后面的内容相关性更加密切。

## TCP/IP（100）

在这个部分学习完成之后，需要掌握以下内容：

1. 了解TCP / UDP ARP ICMP MTU TTL
2. TCP SYN三向握手和TCP FIN四向握手，TCP重传
3. 熟悉WireShark /网络监控器/消息分析器 (选学)

* TCP / IP工作原理

<https://docs.microsoft.com/zh-cn/previous-versions/windows/it-pro/windows-server-2003/cc786128(v=ws.10)?redirectedfrom=MSDN>

* WireShark学习资料（*电子书请自行搜索*）
  + Wireshark网络分析就这么简单.pdf
  + Wireshark网络分析的艺术.pdf

## HTTP / HTTPS, SSL / TLS（100）

在这个部分学习完成之后，需要掌握以下内容：

1. 了解HTTP如何工作
2. 了解公钥和私钥，HTTPS握手
3. SSL和TLS如何提供标识，身份验证，机密性和完整性

* TLS / SSL工作原理

<https://docs.microsoft.com/zh-cn/previous-versions/windows/it-pro/windows-server-2003/cc783349(v=ws.10)>

## DNS（100）

在这个部分学习完成之后，需要掌握以下内容：

1. DNS 记录
2. DNS请求/ DNS响应格式”

* DNS工作原理

<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772774(v=ws.10)?redirectedfrom=MSDN>

# VNET / VM

## VNET / Subnet（100）

在这个部分学习完成之后，需要掌握以下内容：

1. Azure VNET的基本知识
2. 了解如何创建VNET /子网/网关子网
3. 公共/私有IP
4. 静态/动态IP

* Azure 虚拟网络

VNet的基本概念：

**地址空间：** 创建VNet时，必须使用公共和专用 (RFC 1918) 地址指定自定义的专用IP地址空间。Azure从分配的地址空间中向虚拟网络中的资源分配一个专用IP地址。

**子网：**使用子网可将虚拟网络划分为一个或多个子网络，并向每个子网分配一部分虚拟网络地址空间。 然后，可以在特定的子网中部署 Azure 资源。

**区域：**VNet 局限于一个区域/位置；

**订阅：**VNet 的范围限定为订阅。

VNet的最佳实践的通用设计原则：

确保地址空间不重叠。 确保VNet地址空间（CIDR 块）不与组织的其他网络范围重叠。

子网不应涵盖VNet的整个地址空间。 提前规划，为将来留出一些地址空间。

建议使用少量的大型VNet，而不要使用多个小型VNet。这可以防止出现管理开销。

使用网络完全组 (NSG) 保护 VNet。

Azure 资源采用安全地相互通信的方式：

**通过虚拟网络：**可以将VM和多个其他类型的 Azure 资源部署到虚拟网络。

**通过虚拟网络服务终结点：**通过直接连接将虚拟网络专用地址空间和虚拟网络的标识扩展到 Azure 服务资源。使用服务终结点可以保护关键的 Azure 服务资源，只允许在客户自己的虚拟网络中对其进行访问。

**通过 VNet 对等互连：**可以互相连接虚拟网络，使虚拟网络中的资源能够通过虚拟网络对等互连相互进行通信。连接的虚拟网络可以在相同或不同的 Azure 区域中。

VNet和本地资源之间的通信：

**点到站点虚拟专用网络 (VPN)：** 在网络中的虚拟网络和单台计算机之间建立连接。 要与虚拟网络建立连接的每台计算机必须配置其连接。 这种连接类型适用于刚开始使用 Azure 的人员或开发人员，因为该连接类型仅需对现有网络做极少更改或不做任何更改。 计算机与虚拟网络之间的通信经 Internet 通过加密的通道来发送。

**站点到站点 VPN：** 在本地 VPN 设备和虚拟网络中部署的 Azure VPN 网关之间建立连接。 此连接类型可使授权的任何本地资源访问虚拟网络。 本地 VPN 设备和 Azure VPN 网关之间的通信经 Internet 通过加密的通道来发送。

**Azure ExpressRoute：** 通过 ExpressRoute 合作伙伴在网络和 Azure 之间建立连接。 此连接是专用连接。流量不经过 Internet。

筛选网络流量：

**安全组：**网络安全组和应用程序安全组可包含多个入站和出站安全规则，通过这些规则可按源和目标 IP 地址、端口和协议筛选出入资源的流量。

**网络虚拟设备：** 虚拟网络设备是可执行网络功能（例如防火墙、WAN 优化等）的 VM。若要查看可在虚拟网络中部署的网络虚拟设备，请参阅 Azure 市场。

路由网络流量：

**路由表：**可创建自定义路由表，其中包含可对每个子网控制流量路由到位置的路由。

**边界网关协议 (BGP) 路由：**如果使用 Azure VPN 网关或 ExpressRoute 连接将虚拟网络连接到本地网络，则可将本地 BGP 路由传播到虚拟网络。

## Lab18: Deploy a VNET through Portal(ARM & ASM) and learn address management and Segmentation & Deploy a VNET through PowerShell（100）

在这个部分学习完成之后，需要掌握以下内容：

1. 通过Portal（ARM＆ASM）部署VNET，并学习地址管理和分段
2. 通过PowerShell部署VNET

* 快速入门：使用 Azure 门户创建虚拟网络

<https://docs.azure.cn/zh-cn/virtual-network/virtual-networks-create-vnet-arm-pportal>

* 快速入门：使用 PowerShell 创建虚拟网络

<https://docs.azure.cn/zh-cn/virtual-network/virtual-networks-create-vnet-arm-ps>

* 快速入门：使用 Azure CLI 创建虚拟网络

<https://docs.azure.cn/zh-cn/virtual-network/quick-create-cli>

## Lab19: Deploy two VNETs and establish VNET Peering（100）

* 虚拟网络对等互连的种类

VNet 对等互连 - 连接同一 Azure 区域中的 VNet

全局 VNet 对等互连 - 跨 Azure 区域连接 VNet

* 虚拟网络对等互连的优点

对等虚拟网络之间的网络流量是专用的。 虚拟网络之间的流量仅限于 Azure 主干网络。 在虚拟网络之间通信不需公共 Internet、网关或加密。

不同虚拟网络中资源之间的连接延迟低且带宽高。

在虚拟网络对等互连之后，一个虚拟网络中的资源与另一虚拟网络中的资源通信的功能。

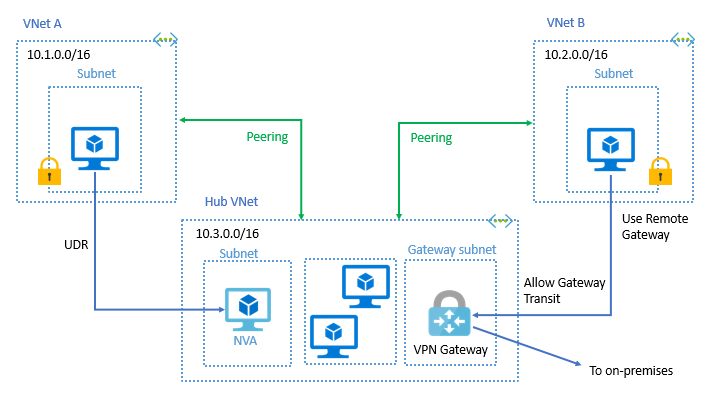
跨 Azure 订阅、部署模型和 Azure 区域传输数据的功能。

可将通过 Azure 资源管理器创建的虚拟网络对等互连，或者将一个通过资源管理器创建的虚拟网络对等互连到通过经典部署模型创建的虚拟网络。

在创建对等互连之时或之后，虚拟网络中的资源不会出现停机的现象。

* 网关和本地连接

将虚拟网络对等互连后，还可以将对等虚拟网络中的网关配置为本地网络的传输点。 在这种情况下，使用远程网关的虚拟网络没有自己的网关。 一个虚拟网络只能有一个网关。 网关可以是本地网关或远程网关（对等虚拟网络中），如下图所示：



* 教程：通过 Azure 门户使用虚拟网络对等互连连接虚拟网络

<https://docs.azure.cn/zh-cn/virtual-network/tutorial-connect-virtual-networks-portal>

## Lab20: Deploy two VNETs and establish VNET to VNET（100）

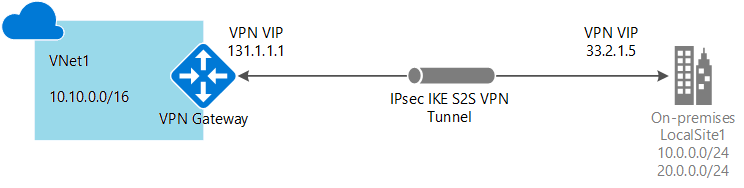
* 使用 Azure 门户配置 VNet 到 VNet VPN 网关连接

<https://docs.azure.cn/zh-cn/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal>

* VPN 网关

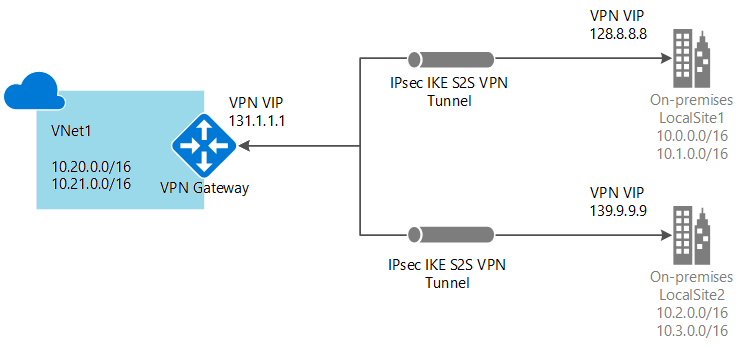
**站点到站点和多站点（IPsec/IKE VPN 隧道）**

站点到站点 (S2S) VPN 网关连接是通过 IPsec/IKE（IKEv1 或 IKEv2）VPN 隧道建立的连接。 S2S 连接可用于跨界和混合配置。 S2S 连接要求位于本地的 VPN 设备分配有一个公共 IP 地址，并且不位于 NAT 后面。



**多站点**

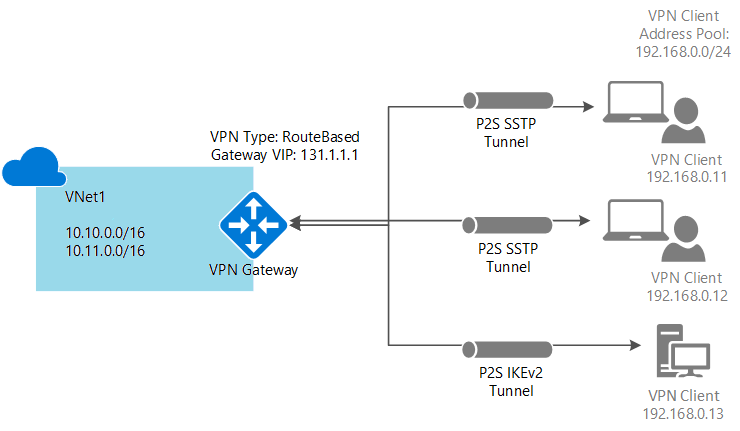
此类型的连接是站点到站点连接的变体。 从虚拟网络网关创建多个 VPN 连接，通常情况下连接到多个本地站点。 使用多个连接时，必须使用 RouteBased VPN 类型（使用经典 VNet 时称为动态网关）。 由于每个虚拟网络只能有一个 VPN 网关，因此通过该网关的所有连接都共享可用带宽。 此类连接通常称为“多站点”连接。



**点到站点 VPN**

点到站点 (P2S) VPN 网关连接用于创建从单个客户端计算机到虚拟网络的安全连接。 可通过从客户端计算机启动连接来建立 P2S 连接。 对于要从远程位置（例如从家里或会议室）连接到 Azure VNet 的远程工作者，此解决方案很有用。 如果只有一些客户端需要连接到 VNet，则还可以使用 P2S VPN 这一解决方案来代替 S2S VPN。

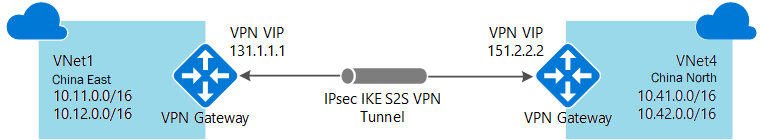
与 S2S 连接不同，P2S 连接不需要本地面向公众的 IP 地址或 VPN 设备。 可以通过同一 VPN 网关将 P2S 连接与 S2S 连接结合使用，前提是这两种连接的所有配置要求都兼容。



**VNet 到 VNet 连接（IPsec/IKE VPN 隧道）**

将一个虚拟网络连接到另一个虚拟网络（VNet 到 VNet）类似于将 VNet 连接到本地站点位置。 这两种连接类型都使用 VPN 网关来提供使用 IPsec/IKE 的安全隧道。 甚至可以将 VNet 到 VNet 通信与多站点连接配置结合使用。 这样，便可以建立将跨界连接与虚拟网络间连接相结合的网络拓扑。

但是这种方法基本上已经可以用Peering进行替代，不过需要注意每个虚拟网络可以创建的对等互联数目上限为**500**。



# VM

## Lab21：Use PowerShell to reserve VIP for ASM VM and set ARM VM PIP static（100）

* 保留 IP 地址（经典部署）

<https://docs.azure.cn/zh-cn/virtual-network/virtual-networks-reserved-public-ip>

* 使用 Azure 门户创建具有静态公共 IP 地址的虚拟机

<https://docs.azure.cn/zh-cn/virtual-network/virtual-network-deploy-static-pip-arm-portal>

## Lab22: Set VM's private IP as static IP (Portal and PowerShell) （200）

在实验之前先看一下几个基本的概念：

* Azure 中的 IP 地址类型和分配方法

<https://docs.azure.cn/zh-cn/virtual-network/virtual-network-ip-addresses-overview-arm>

可以将 IP 地址分配到与其他 Azure 资源通信的 Azure 资源，也可以将其分配到本地网络和 Internet。 Azure 中可使用两种类型的 IP 地址：

**公共IP地址：**用来与 Internet 通信，包括与面向公众的Azure服务通信。

公共 IP 地址允许 Internet 资源与 Azure 资源进行入站通信。 在 IP 地址已分配给 Azure 资源的情况下，公共 IP 地址还允许这些资源与 Internet 和面向公众的 Azure 服务进行出站通信。 此地址专门用于该资源，直到你对其取消分配。 如果公共 IP 地址未分配给资源，该资源仍可与 Internet 进行出站通信，但 Azure 会动态分配不专用于该资源的可用 IP 地址。 这里需要千万注意一旦动态IP地址被取消分配，是没有办法通过后台帮忙找回的，因此如果，程序当中已经写死了IP地址，那么请务必将IP地址设置为静态IP。

**公有IP地址的SKU：**

必须为负载均衡器和公用 IP 资源使用匹配的 SKU。 不能混合使用基本 SKU 资源和标准 SKU 资源。 无法将独立的虚拟机、可用性集资源中的虚拟机或虚拟机规模集资源同时附加到两个 SKU。 新的设计应当考虑使用标准 SKU 资源。

**公有IP地址的分配方法：**

基本 SKU 公用 IP 地址支持“动态” 分配方法，这是未指定分配方法时将采用的默认方法。 为基本的公用 IP 地址资源选择“动态” 分配方法意味着在创建资源时“不”分配 IP 地址。 将公用 IP 地址与虚拟机进行关联时或者将第一个虚拟机实例放置到基本负载均衡器的后端池中时，将分配公用 IP 地址。 停止（或删除）该资源时，就会释放该 IP 地址。 例如，从资源 A 中释放后，可将该 IP 地址分配到不同的资源。 如果在停止资源 A 的情况下将 IP 地址分配到不同的资源，则重启资源 A 时，会分配一个不同的 IP 地址。 如果将基本的公用 IP 地址资源的分配方法从“静态”更改为“动态”，则会释放地址。 要确保所关联资源的 IP 地址保持不变，可将分配方法显式设置为静态。 静态 IP 地址是立即分配的。

**专用IP地址：**使用 VPN 网关或 ExpressRoute线路将网络扩展到Azure时，用于在Azure 虚拟网络 (VNet)和本地网络中通信。

* 使用 Azure 门户为虚拟机配置专用 IP 地址

<https://docs.azure.cn/zh-cn/virtual-network/virtual-networks-static-private-ip-arm-pportal>

* 使用 PowerShell 创建具有静态专用 IP 地址的虚拟机

<https://docs.azure.cn/zh-cn/virtual-network/virtual-networks-static-private-ip-arm-ps>

* 使用 Azure CLI 为虚拟机配置专用 IP 地址

<https://docs.azure.cn/zh-cn/virtual-network/virtual-networks-static-private-ip-arm-cli>

# NSG / Endpoints

## What is NSG / Endpoints（100）

* 计划虚拟网络

<https://docs.azure.cn/zh-cn/virtual-network/virtual-network-vnet-plan-design-arm>

这里基本上涵盖了虚拟网络在创建阶段的所有知识点，其中需要着重看的部分是：

**分段：**

可为每个订阅和每个区域创建多个虚拟网络。 可在每个虚拟网络中创建多个子网。 以下注意事项可帮助确定需要多少个虚拟网络和子网：

**虚拟网络：**

虚拟网络是 Azure 公共网络的虚拟隔离部分。 每个虚拟网络专用于你的订阅。 决定在订阅中创建一个虚拟网络还是多个虚拟网络时需要考虑的事项：

* 是否存在将流量隔离到单独的虚拟网络中的组织安全需求？ 可选择连接或不连接虚拟网络。 如果连接虚拟网络，则可实施网络虚拟设备（如防火墙）来控制虚拟网络之间的流量流。
* 是否存在将虚拟网络隔离到单独的订阅或区域的组织需求？
* 网络接口使 VM 能够与其他资源进行通信。 可为每个网络接口分配一个或多个专用 IP 地址。 虚拟网络中需要多少个网络接口和专用 IP 地址？ 在虚拟网络中可以拥有的网络接口和专用 IP 地址数有上限。
* 是否要将虚拟网络连接到其他虚拟网络或本地网络？ 可选择将某些虚拟网络互相连接或连接到本地网络，而不是其他网络。连接到另一个虚拟网络或本地网络的每个虚拟网络必须具有唯一的地址空间。 每个虚拟网络都向其地址空间分配了一个或多个公共和专用地址范围。 地址范围以无类别的 Internet 域路由 (CIDR) 格式指定，例如 10.0.0.0/16。
* 是否对不同虚拟网络中的资源有任何组织管理需求？如果有，可将资源分隔到单独的虚拟网络中，以简化组织中个体的权限分配，或将不同的策略分配给不同的虚拟网络。
* 将某些 Azure 服务资源部署到虚拟网络时，他们将创建自己的虚拟网络。 若要确定 Azure 服务是否创建自己的虚拟网络，请参阅每个可部署到虚拟网络中的 Azure 服务的信息。

**子网：**

* 可将虚拟网络分段为一个或多个子网，直至达到上限。 决定在订阅中创建一个子网还是多个虚拟网络时需要考虑的事项：
* 在虚拟网络的地址空间内，每个子网必须具有唯一的地址范围，且以 CIDR 格式指定。 其地址范围不能与虚拟网络中其他子网重叠。
* 如果计划将某些 Azure 服务资源部署到虚拟网络中，则他们可能需要或创建自己的子网，因此必须有足够的未分配空间才能进行此操作。 例如，如果使用 Azure VPN 网关将虚拟网络连接到本地网络，虚拟网络必须具有该网关的专用子网。
* 默认情况下，Azure 在虚拟网络中的所有子网之间路由流量。 例如，可替代 Azure 的默认路由以防止在子网之间进行 Azure 路由，或通过网络虚拟设备在子网之间路由流量。 如果要求相同虚拟网络中资源之间的流量流经网络虚拟设备 (NVA)，请将资源部署到不同的子网。
* 可将对 Azure 资源（例如 Azure 存储账户或 Azure SQL 数据库）的访问权限限制为具有虚拟网络服务终结点的特定子网。 此外，可拒绝通过 Internet 访问资源。 可创建多个子网，并为某些子网启用服务终结点，但不启用其他项。
* 可将零个或一个网络安全组与虚拟网络中的每个子网相关联。 可将相同或不同的网络安全组关联到每个子网。 每个网络安全组都包含规则，允许或拒绝到达和来自源和目标的流量。

**安全性：**

可使用网络安全组和网络虚拟设备来筛选虚拟网络中到达或来自资源的流量。 可控制 Azure 如何路由来自子网的流量。 还可限制组织中的人员使用虚拟网络中的资源。

**流量筛选：**

* 可使用网络安全组和/或筛选流量的 NVA 来筛选虚拟网络中资源之间的流量。 若要部署 NVA（如防火墙）来筛选流量，使用 NVA 时，还可以创建自定义路由将流量从子网路由到 NVA。
* 网络安全组包含多个默认安全规则，允许或拒绝到达或来自资源的流量。 可将网络安全组关联到网络接口和/或网络接口所在的子网。 若要简化安全规则的管理，建议尽可能将网络安全组与单独的子网相关联，而不是与子网内单独的网络接口相关联。
* 如果子网中不同 VM 需要应用不同的安全规则，则可将 VM 中的网络接口与一个或多个应用程序安全组相关联。 安全规则可以在其源和/或目标中指定应用程序安全组。 该规则仅适用于属于应用程序安全组成员的网络接口。
* Azure 在每个网络安全组中创建了多个默认安全规则。 其中一个默认规则允许所有流量在虚拟网络中的所有资源之间流动。 若要替代此行为，可使用网络安全组和/或自定义路由将流量路由到 NVA。 建议熟悉 Azure 的所有默认安全规则，并了解网络安全组规则如何应用于资源。

**流量路由：**

Azure 为子网中的出站流量创建多个默认路由。 可通过创建路由表并将其关联到子网来替代 Azure 的默认路由。 替代 Azure 的默认路由的常见原因是：

* 想要子网之间的流量流经 NVA。
* 想要通过 Azure VPN 网关强制所有 Internet 绑定流量通过 NVA 或本地。 强制 Internet 流量本地进行检查和记录通常被称为强制隧道。

**连接**

可使用虚拟网络对等将虚拟网络连接到其他虚拟网络，或使用 Azure VPN 网关将其连接到本地网络。

**对等互连**

使用虚拟网络对等时，虚拟网络可位于相同的或不同的受支持 Azure 区域中。 虚拟网络可位于相同或不同的 Azure 订阅中（即使订阅属于不同的 Azure Active Directory 租户）。 建立对等之前，建议熟悉所有对等需求和约束。 同一区域的对等互连虚拟网络中的资源之间的带宽与资源在同一虚拟网络中的带宽相同。

**VPN 网关**

可通过站点到站点 VPN 或与 Azure ExpressRoute 的专用连接，使用 Azure VPN 网关将虚拟网络连接到本地网络。

**名称解析**

一个虚拟网络中的资源无法使用 Azure 的内置 DNS 来解析对等互连虚拟网络中的资源名称。 若要在对等互连虚拟网络中解析名称，请部署自己的 DNS 服务器或使用 Azure DNS 专用域。在虚拟网络和本地网络的资源之间解析名称也需要部署自己的 DNS 服务器。

## Lab23：Create a NSG and associate it with VM and Subnet （100）

* 创建、更改或删除网络安全组

<https://docs.azure.cn/zh-cn/virtual-network/manage-network-security-group>

* 使用 Azure CLI 创建网络安全组

<https://docs.azure.cn/zh-cn/cli/network/nsg?view=azure-cli-latest#az-network-nsg-create>

* 使用 PowerShell 创建网络安全组

<https://docs.microsoft.com/zh-cn/powershell/module/az.network/new-aznetworksecuritygroup?view=azps-3.0.0>

# UDR

### What is UDR

* 虚拟网络流量路由

<https://docs.azure.cn/zh-cn/virtual-network/virtual-networks-udr-overview>

## Lab24：Create a UDR and associate it with VM or Subnet, and verify. （100）

* 教程：使用 Azure 门户通过路由表路由网络流量

<https://docs.azure.cn/zh-cn/virtual-network/tutorial-create-route-table-portal>

这个实验的要点是明白UDR的原理，并且理清楚这些地址段之间的关系，哪个路由跳到哪个路由。

# Azure VPN

## IPsec and IKE Fundamental（100）

在这个部分学习完成之后，需要掌握以下内容：

1. 了解IKEv1主模式和快速模式
2. 能够在MM模式下详细解释这6条消息
3. 作为主模式SA的一部分，协商了四个强制性参数
4. 比较IKEv1和IKEv2

* 浅谈IPSec

<http://noops.me/?p=176>

* IKEv2数据包交换和协议级别调试

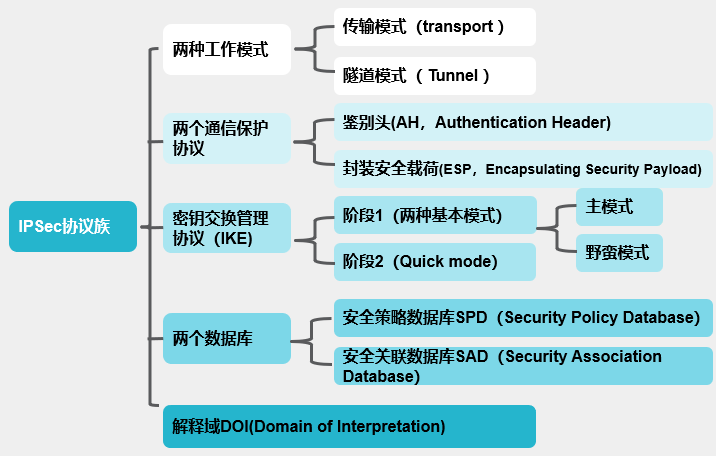
<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/115936-understanding-ikev2-packet-exch-debug.html>

* 电子书：CISCO IPSEC VPN实战指南.pdf (请自行搜索)

**IPSec：**

汉语译为互联网安全协议是一个协议包，通过对IP协议的分组进行加密和认证来保护IP协议的网络传输协议族（一些相互关联的协议的集合）。

通过加密保证数据的私密性，通过Hush保证数据的完整性，通过身份认证保证数据的真实性。



* IPSec安全协议：

- AH (Authentication Header) 网络认证协议,只能进行数据摘要不能实现数据加密

- ESP (Encapsulating Security Payload) 封装安全载荷协议,能够进行数据加密和数据摘要(hash)

* IPsec的封装模式：

- 传输模式：不改变原有的IP包头，通常用于主机与主机之间。

- 隧道模式：增加新的IP包头，通常用于私网与私网之间，通过公网进行通信。

* IPSec 安全通道协商过程：

- 需要保护的流量流经路由器，触发路由器启动相关的协商过程。

- 启动IKE (Internet key exchange,密钥管理协议)阶段1，对通信双方进行身份认证，并在两端之间建立一条安全的通道。

- 启动IKE阶段2，在上述安全通道上协商IPSec参数。

- 按协商好的IPSec参数对数据流进行加密、hash等保护。

* IPSec的两个数据库：

安全策略数据库SPD，安全关联数据库SAD。

* IPSec解释域

DOI将所有的IPSec小组的文献捆绑在一起。它可以被认为是所有IPSec安全参数的主数据库。

有关这部分知识的具体介绍，请参加下面这个blog链接，讲的十分清楚。

* IPSec介绍

<https://blog.csdn.net/NEUChords/article/details/92968314>

## Azure VPN Gateway（100）

在这个部分学习完成之后，需要掌握以下内容：

1. 熟悉网关配置
2. 了解静态/动态（基于策略/基于路由）VPN网关之间的区别
3. 了解Azure网关体系结构

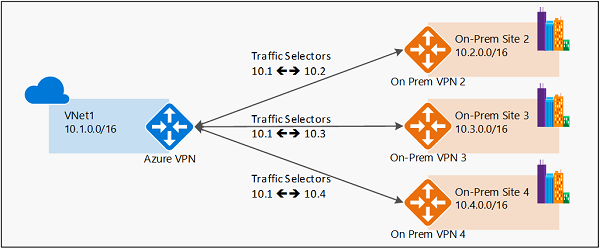
* VPN 网关文档

<https://docs.azure.cn/zh-cn/vpn-gateway/>

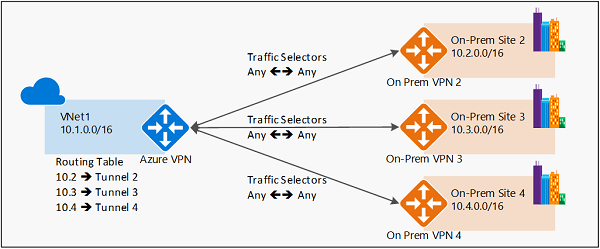
* 虚拟网络网关

基于策略与基于路由的 VPN 设备的差异体现在如何在连接上设置 IPsec 流量选择器：

* 基于策略的 VPN 设备使用两个网络的前缀组合来定义如何通过 IPsec 隧道加密/解密流量。 它通常构建在执行数据包筛选的防火墙设备的基础之上。 IPsec 隧道加密和解密将添加到数据包筛选及处理引擎。



* 基于路由的 VPN 设备使用任意到任意（通配）流量选择器，允许路由/转发表将流量定向到不同的 IPsec 隧道。 它通常构建在其中每个 IPsec 隧道建模为网络接口或 VTI（虚拟隧道接口）的路由器平台的基础之上。



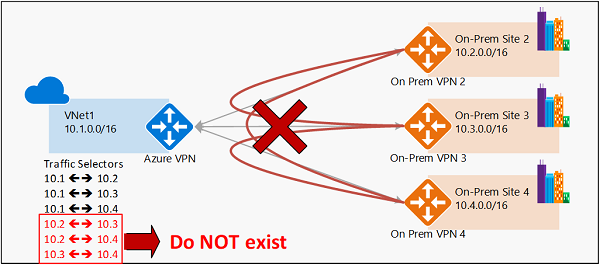
* Azure 对基于策略的 VPN 的支持

目前，Azure 支持两种 VPN 网关模式：基于路由的 VPN 网关和基于策略的 VPN 网关。 两者基于不同的内部平台，因而规格也不同：

|  |  |  |
| --- | --- | --- |
|  | **基于策略的 VPN 网关** | **RouteBased VPN 网关** |
| **Azure 网关 SKU** | 基本 | 基本、标准、高性能、VpnGw1、VpnGw2、VpnGw3 |
| **IKE 版本** | IKEv1BG | IKEv2 |
| **最大S2S 连接** | **1** | 基本/标准：10 个  高性能：30 |

* 重要：
* 若要启用此连接，基于策略的本地 VPN 设备必须支持 IKEv2，才能连接到基于路由的 Azure VPN 网关。 请查看 VPN 设备规格。
* 通过基于策略的 VPN 设备采用此机制进行连接的本地网络只能连接到 Azure 虚拟网络；不能经由相同的 Azure VPN 网关传输到其他本地网络或虚拟网络。
* 配置选项是自定义 IPsec/IKE 连接策略的一部分。 如果启用基于策略的流量选择器选项，则必须指定完整的策略（IPsec/IKE 加密和完整性算法、密钥强度和 SA 生存期）。

图显示了在选择基于策略的 VPN 时，经由 Azure VPN 网关的传输路由为何无法工作：



## Lab25：Deploy two VNETs and establish VNET to VNET（100）

* 使用 Azure 门户配置 VNet 到 VNet VPN 网关连接

<https://docs.azure.cn/zh-cn/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal>

## Lab26：Configure P2S VPN and test connectivity between your client and Azure VNET（200）

* 使用本机 Azure 证书身份验证配置与 VNet 的点到站点 VPN 连接：Azure 门户

<https://docs.azure.cn/zh-cn/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

使用

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `

-Subject "CN=P2SChildCert" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" `

-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")

命令创建证书的时候，使用该命令创建的证书是在个人的证书管理器当中的，因此在查找证书的时候一定要到个人证书管理器当中起查看。

## Lab27：Establish VPN between On-premise policy-based device and Azure Route-Based VPN Gateway（200）

* 使用 PowerShell 将 Azure VPN 网关连接到多个基于策略的本地 VPN 设备

<https://docs.azure.cn/zh-cn/vpn-gateway/vpn-gateway-connect-multiple-policybased-rm-ps>

* 使用 Azure 门户创建基于路由的 VPN 网关

<https://docs.microsoft.com/zh-cn/azure/vpn-gateway/create-routebased-vpn-gateway-portal>

## High-Available VPN Connection（100）

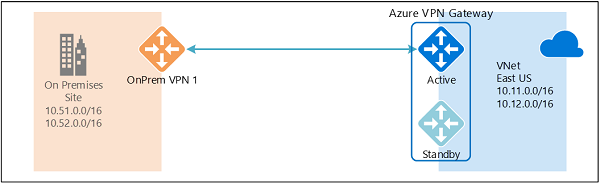
在这个部分学习完成之后，需要掌握以下内容：

了解高可用VPN连接的不同模式

* 高可用性跨界连接与 VNet 到 VNet 连接

<https://docs.azure.cn/zh-cn/vpn-gateway/vpn-gateway-highlyavailable>

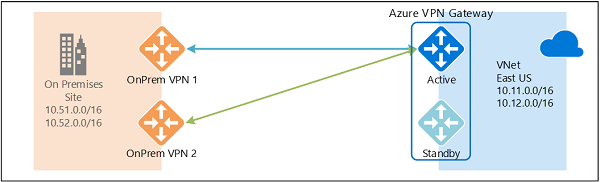
* 关于 Azure VPN 网关冗余

每个 Azure VPN 网关由两个采用主动-待机配置的实例组成。 当主动实例发生任何计划内维护或计划外中断时，待机实例将自动接管负载（故障转移），恢复 S2S VPN 连接或 VNet 到 VNet 连接。 这种交接会造成短暂的中断。 发生计划内维护时，10 到 15 秒内应可恢复连接。 发生计划外的问题时，恢复连接所需的时间更长，在最糟的情况下大约需要 1 到 1.5 分钟。 为使 P2S VPN 客户端与网关建立连接，需要先断开 P2S 连接，然后，用户必须从客户端计算机重新连接。

* 高可用性跨界连接

若要为跨界连接提供更高的可用性，可以使用多种选项：

- 多个本地 VPN 设备

可以使用本地网络中的多个 VPN 设备连接到 Azure VPN 网关，如下图所示： 

此配置提供多个活动隧道用于从同一个 Azure VPN 网关连接到同一位置中的本地设备。 此配置有一些要求和限制：

需要创建从 VPN 设备到 Azure 的多个 S2S VPN 连接。 将多个 VPN 设备从同一本地网络连接到 Azure 时，需要为每个 VPN 设备创建一个本地网络网关，以及一个从 Azure VPN 网关到每个本地网络网关的连接。

对应于 VPN 设备的本地网络网关在“GatewayIpAddress”属性中必须有唯一的公共 IP 地址。

此配置需要 BGP。 必须在“BgpPeerIpAddress”属性中为代表 VPN 设备的每个本地网络网关指定唯一的 BGP 对等 IP 地址。

每个本地网络网关中的 AddressPrefix 属性字段不能重叠。 应在 AddressPrefix 字段中指定 /32 CIDR 格式的“BgpPeerIpAddress”，例如 10.200.200.254/32。

应使用 BGP 向 Azure VPN 网关播发同一本地网络的相同前缀，流量将同时通过这些隧道转发。

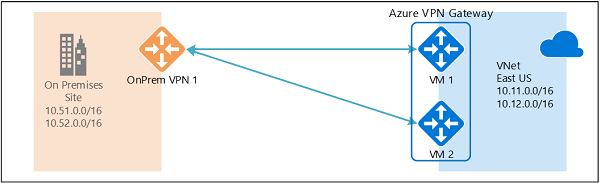
必须使用等价多路径路由 (ECMP)。

每个连接将计入 Azure VPN 网关的隧道数目上限，基本和标准 SKU 的上限为 10，高性能 SKU 的上限为 30。

在此配置中，Azure VPN 网关仍处于主动-待机模式，因此，仍会发生 上述故障转移行为和短暂中断。 但是，这种设置可针对本地网络和 VPN 设备故障或中断提供保护。

- 主动-主动 Azure VPN 网关

现在，可以在主动-主动配置中创建一个 Azure VPN 网关，其中的两个网关 VM 实例与本地 VPN 设备建立 S2S VPN 隧道，如下图所示：



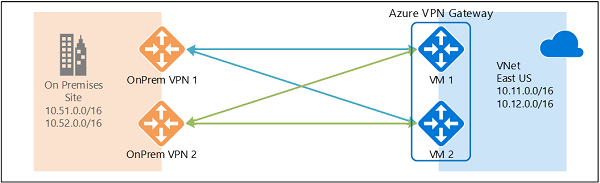
在此配置中，每个 Azure 网关实例都有唯一的公共 IP 地址，每个实例将与本地网络网关和连接中指定的本地 VPN 设备建立 IPsec/IKE S2S VPN 隧道。 请注意，这两个 VPN 隧道实际上属于同一个连接。 仍然需要配置本地 VPN 设备，以便与这两个 Azure VPN 网关公共 IP 地址建立两条 S2S VPN 隧道，或者接受这种通道。

由于 Azure 网关实例采用主动-主动配置，因此，从 Azure 虚拟网络到本地网络的流量同时通过这两条隧道路由，即使本地 VPN 设备优先选择其中一个隧道，也是如此。 请注意，除非其中一个实例发生维护事件，否则相同的 TCP 或 UDP 流量始终会遍历相同的隧道或路径。

当一个网关实例发生计划内维护或计划外事件时，从该实例到本地 VPN 设备的 IPsec 隧道会断开。 VPN 设备上的对应路由应会自动删除或撤消，以便将流量切换到其他活动 IPsec 隧道。 在 Azure 端，自动从受影响的实例切换到活动实例。

- 双重冗余：Azure 和本地网络的主动-主动 VPN 网关

最可靠的选项是结合网络和 Azure 上的主动-主动网关，如下图所示。



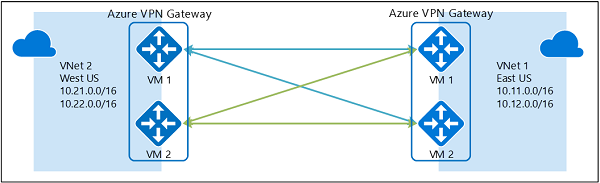
此处创建并设置了采用主动-主动配置的 Azure VPN 网关，并针对上述两个本地 VPN 设备创建了两个本地网络网关和两个连接。 结果是在 Azure 虚拟网络与本地网络之间建立了包含 4 个 IPsec 隧道的全面网格连接。

所有网关和隧道从 Azure 端激活，因此流量同时分散在 4 个隧道之间，每个 TCP 或 UDP 流量再次沿着源自 Azure 端的相同隧道或路径传送。 尽管分散了流量，但你可能会发现，IPsec 隧道上的吞吐量稍有提高，而此配置的主要目标就是实现高可用性。 由于分散的统计特征，难以通过某种测量方式来确定不同的应用程序流量状况对聚合吞吐量造成的影响。

此拓扑需要使用两个本地网络网关和两个连接来支持本地 VPN 设备对，需要使用 BGP 来与同一个本地网络建立两个连接。 上述配置同样需要满足这些要求。

* 通过 Azure VPN 网关实现高可用性 VNet 到 VNet 连接

上述主动-主动配置同样适用于 Azure VNet 到 VNet 连接。 可为两个虚拟网络创建主动-主动 VPN 网关并将它们连接到一起，同样在两个 VNet 之间构成包含 4 个隧道的全面网格连接，如下图所示：



这可以确保用于任何计划内维护事件的两个虚拟网络之间始终有一对隧道，进一步提高可用性。 尽管用于跨界连接的相同拓扑需要两个连接，但如上所示的 VNet 到 VNet 拓扑只需要为每个网关建立一个连接。 此外，除非基于 VNet 到 VNet 连接的传输路由是必需的，否则 BGP 是可选的。

# ExpressRoute

在这个部分学习完成之后，需要掌握以下内容：

1. BGP的基础知识
2. Understand ExpressRoute

* BGP for Beginners

<https://gns3vault.com/blog/bgp-for-beginners>

* ExpressRoute 文档

<https://docs.azure.cn/zh-cn/expressroute/>

# SLB/ILB Application Gateway

## SLB/ILB（100）

在这个部分学习完成之后，需要掌握以下内容：

1. 了解SLB / ILB，分发模式，运行状况探针
2. SLB：SLB MUX，SLB管理器，VFP，SNAT，端口重用，DSR（浮动IP）

* Azure 中的出站连接

<https://docs.microsoft.com/zh-cn/azure/load-balancer/load-balancer-outbound-connections>

* 负载均衡器文档

<https://docs.azure.cn/zh-cn/load-balancer/>

## Lab28: SLB deployment & ILB deployment（200）

* 快速入门：使用 Azure 门户创建基本负载均衡器

<https://docs.azure.cn/zh-cn/load-balancer/quickstart-create-basic-load-balancer-portal>

* 教程：在 Azure 门户中通过基本负载均衡器对内部流量负载进行均衡

<https://docs.azure.cn/zh-cn/load-balancer/tutorial-load-balancer-basic-internal-portal>

## Application Gateway（100）

在这个部分学习完成之后，需要掌握以下内容：

了解应用程序网关，比较Azure 负载均衡器和应用程序网关

* 什么是 Azure 应用程序网关？

<https://docs.azure.cn/zh-cn/application-gateway/overview>

## Lab29: Create and configure non-ssl AppGW（200）

* 快速入门：使用 Azure 应用程序网关定向 Web 流量 - Azure 门户

<https://docs.azure.cn/zh-cn/application-gateway/quick-create-portal>

# Application Gateway (WAF) Network Watcher AOG Docs

## Lab30: Create and configure SSL-offload AppGW（200）

* 教程：通过 Azure 门户使用 SSL 终端配置应用程序网关

<https://docs.azure.cn/zh-cn/application-gateway/create-ssl-portal>

## Lab31: Create and configure end to end SSL AppGW（200）

* 使用 PowerShell 通过应用程序网关配置端到端 SSL

<https://docs.azure.cn/zh-cn/application-gateway/application-gateway-end-to-end-ssl-powershell>

## Lab32: Create and configure URL-based routing AppGW（200）

* 教程：通过 Azure 门户使用基于路径的路由规则创建应用程序网关

<https://docs.azure.cn/zh-cn/application-gateway/create-url-route-portal>

## Lab33: Create and configure URL-based routing AppGW（200）

* 教程：使用 Azure 门户创建和配置托管多个网站的应用程序网关

<https://docs.azure.cn/zh-cn/application-gateway/create-multiple-sites-portal>

## Network Watcher（100）

在这个部分学习完成之后，需要掌握以下内容：

1. 了解Network Watcher中的每个功能
2. 在以前的实验室中构建的环境中测试每个功能

* Azure 网络观察程序是什么？

<https://docs.azure.cn/zh-cn/network-watcher/network-watcher-monitoring-overview>

## AGO（100）

在这个部分学习完成之后，需要掌握以下内容：

Catch up with AOG articles

* Azure Operations Guide

<https://docs.azure.cn/zh-cn/articles/azure-operations-guide/networking/>

# Checkpoint

***Core Networking***

|  |
| --- |
| 1. The process of TCP SYN three-way handshake and TCP FIN four-way handshake. |
| 2. TCP Retransmission? |
| 3. Another flag to terminate TCP session? |
| 4. How to capture package in Linux and in Windows without Wireshark or NetMon? |
| 5. What is the main difference between http and https? |
| 6. SSL/Certificate knowledge |
| 7. DNS Recursion and Iteration query principle and process? |
| 8. DNS protocol & port |
| 9. The difference between ping and tcpping? |
| 10. Whether resources could be accessed by others in different subnets of the same VNET by default? |
| 11. What is the default rule in NSG for Azure VNET subnet? |
| 12. Key points in configuration UDR |
| 13. How to create SSH key in windows client? |

***VPN/ER***

|  |
| --- |
| 1. IKEV1: main mode & quick mode. |
| 2. IKEV2: explain negotiation process with parameters in details. |
| 3. The difference between IKEV1 and IKEV2. |
| 4. Explain the difference between policy-based and route-based VPN gateway. |
| 5. Talk about key steps of creating ER and linking ER gateway to ER circuit. |
| 6. For ER and VPN co-exist environment, what's the request prefix of Gateway subnet ? What's the steps of creating VPN Gateway and ER Gateway? |

***SLB/APPGW***

|  |
| --- |
| 1. Can you SSH or RDP to a VM through SLB? |
| 2. Talk about the Idle time of outbound and inbound for SLB. |
| 3. Describe the distribution mode of SLB/ILB. |
| 4. How to confirm if there is high SNAT which may cause packet loss? |
| 5. Tell the difference of load balance between APPGW and SLB? |
| 6. Describe basic configuration for a APPGW briefly. |
| 7. Can you disable certain rule in WAF APPGW? Can you change rule? |
| 8. How to check WAF rule hitting log and how to give advices? |
| 9. Describe the usage of each function in Network Watcher. |

# Tips

* 给客户deliver之前，一定要自己先做lab验证一遍
* 整理好Azure CLI/Powershell使用的template/cheet sheets
* 做方案时一定要参考[Azure limitation](https://docs.microsoft.com/zh-cn/azure/azure-subscription-service-limits?toc=%2fazure%2fvirtual-network%2ftoc.json#azure-resource-manager-virtual-networking-limits)

# Reference

* 非常全面的博客：

<https://blog.51cto.com/rdsrv>