Notes on Site-to-Site VPN connections

**Notes on Site-to-Site VPN Connection**

A Site-to-Site VPN connection is used to establish a secure connection between an on-premise network and an Azure network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario

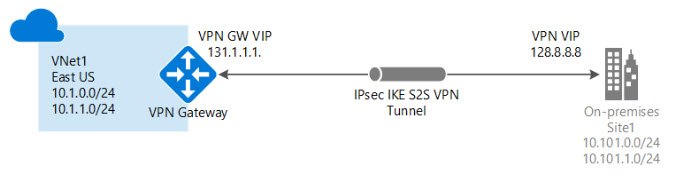


Image reference - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

* On the on-premise side, you need to have a VPN device that can route traffic via the Internet onto the VPN gateway in Azure. The VPN device can be a hardware device like a Cisco router or a software device ( e.g Windows Server 2016 running Routing and Remote services). The VPN device needs to have a publically routable IP address.
* The subnets in your on-premise network must not overlap with the subnets in your Azure virtual network
* The Site-to-Site VPN connection uses an IPSec tunnel to encrypt the traffic.
* The VPN gateway resource you create in Azure is used to route encrypted traffic between your on-premise data center and your Azure virtual network.
* There are different SKU's for the Azure VPN gateway service. Each SKU has a different pricing and attributes associated with it - Reference - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings>