6- VPNs

- A virtual private network (VPN) used an *encrypted tunnel* within another network.
- VPNs are typically deployed to connect two or more trusted *private networks* to one another oven an untrusted network (*public network*)
- Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks.
- VPNs can enable networks to safely and securely share sensitive information.

VPN gateways

What if you want to connect your VNet to an on-premises network?

There are two ways to do that: either use a VPN or use Azure ExpressRoute. The main difference between the two is that a VPN (or Virtual Private Network) traverses the internet, while ExpressRoute is a direct connection between your on-premises network and Azure.

Since traffic on a VPN goes over the internet, it's encrypted to prevent other parties from viewing it. To implement a VPN, you can deploy an Azure VPN Gateway in your virtual network. This'll take care of the Azure side of the connection, but you'll need something on the other side of the connection, too. *What you put on the other end depends on the type of connection you're setting up.*

If you want to connect to an on-premises location, then you can set up a site-to-site connection. To make this work, you need to *install a VPN device* in your on-premises location and give it a public IP address. You need to let Azure know about this VPN device by *defining it as a local network gateway*. A site-to-site connection is a good solution if you have many devices in the same location that need to have access to your Azure virtual network.

If you want to connect individual devices, such as mobile phones, to your virtual network, then you can set up point-to-site connections. This method works differently from the site-to-site method because there's no VPN device on the user's side. Instead, *you have to install a certificate* on each mobile device. The certificate is used to authenticate with the Azure VPN Gateway. In most cases, you can use the same VPN Gateway for both site-to-site and point-to-site connections. In fact, you can only have one VPN Gateway in each VNet, so you have to use the same one. The only situation where you can't support both site-to-site and point-to-site connections from the same gateway is when you need to configure a different type of routing for each.

There are two types of routing:

policy-based and *route-based*. In almost every case, route-based is the right option. Not only is it more robust, but it's the only supported option for point-to-site connections. If, for some reason, you need to configure policy-based routing for a site-to-site connection, then you won't be able to support point-to-site connections from the same VPN Gateway. And since

you can only have one VPN Gateway per virtual network, you'd have to create a second virtual network to support the other VPN Gateway. This isn't a common scenario, though, so you probably won't have to deal with it.

If you don't want your connection to go over the internet or you need more bandwidth, then you can set up a direct connection using Azure ExpressRoute. Be aware that this is a much more expensive solution, though.

There are four ways to connect to Azure using ExpressRoute. It all comes down to where you have your IT infrastructure. Many organizations put at least some of their IT systems in a colocation facility, which is a datacenter that rents space to multiple customers.

If you're fortunate enough to have some of your IT infrastructure in a colocation facility that Microsoft has designated as an ExpressRoute location, then you can connect to Microsoft's network directly. You do this by connecting to a Microsoft Enterprise Edge device in the facility. This option is called ExpressRoute Direct, and it has the highest bandwidth of the four options. It can support connections of 10 gigabits or 100 gigabits per second.

Alternatively, if you're in an ExpressRoute location (otherwise known as a peering location or a "cloud exchange"), but you need less than 10 gigabits per second of bandwidth, then you can connect to Microsoft's network through a service provider. They can provide options between 50 megabits and 10 gigabits per second. The service provider can also take care of some of the management tasks involved with having this sort of connection.

If you're not in that sort of facility, then you have a couple of other options. Some organizations use an IPVPN provider to connect their branch offices and datacenters to their core network. This is called any-to-any connectivity. If your organization uses an IPVPN provider, then you can make the Microsoft network look like one of your branch offices and connect to it that way. The final option is to rent a leased line from a point-to-point Ethernet provider to connect your datacenter to an ExpressRoute location.

Regardless of which option you choose, there are a couple of other interesting things you can do with ExpressRoute. First, you can also use it to connect to Microsoft 365, although having a direct connection to Microsoft 365 isn't typically needed as much as it is for Azure.

Second, if you have ExpressRoute connections from branch offices in different parts of the world, you can use ExpressRoute Global Reach to connect those branch offices to each other through the Microsoft network rather than through the internet. You have to pay extra to do this, though.

And that's it for connecting to other networks.