Module 8: Networking Azure Application Components

Contents:

Module overview

This module describes the various networking and connectivity options available for solutions deployed on Azure. The module explores connectivity options ranging from ad-hoc connections to long-term hybrid connectivity scenarios. The module also discusses some of the performance and security concerns related to balancing workloads across multiple compute instances, connecting on-premise infrastructure to the cloud and creating gateways for on-premise data.

Objectives

After completing this module, students will be able to:

- Describe DNS and IP strategies for VNETs in Azure.
- Compare connectivity options for ad-hoc and hybrid connectivity.
- Distribute network traffic across multiple loads using load balancers.
- Design a hybrid connectivity scenario between cloud and on-premise.

Lesson 1: Virtual Networks

Azure Virtual Networking is the baseline for all Azure networking resources and features. Starting from a high-level topology view and detailed walkthrough of what an Azure VNET is, we drill down into all aspects of Subnet designing, how to integrate networks across Azure regions, as well as between on-premises corporate networks

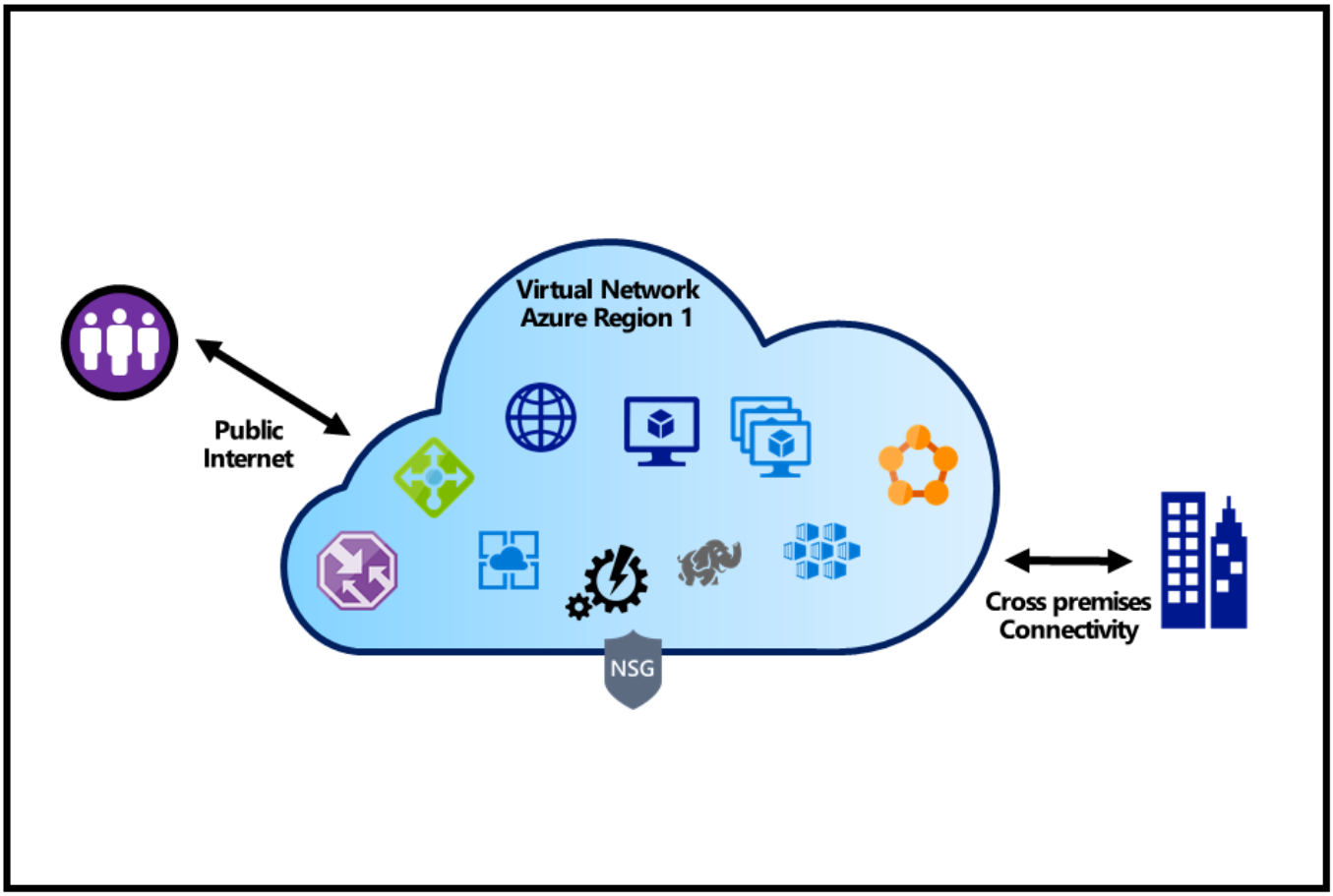
and Azure regions. Next, we describe the different configuration settings within a VNET, like what DNS options are available and how IP-addressing is working for both Public and Private IP's.

Lesson objectives

After completing this lesson, you will be able to:

- Understand Azure Virtual Networks.
- Architect multi-region networking across Azure regions as well as between Azure and on-premises networks.
- Understand several Azure VNET configuration options like DNS, IP addressing and alike.

Azure Virtual Network (VNET) Architecture



An Azure Virtual Network (or VNET), is the logical unit of multiple or all network resources in an Azure region.

On the highest level of the network topology in an Azure Region, you define a Virtual Network. An Azure Region can have one or multiple Virtual Networks defined. Within a Virtual Network, you create one or more subnets. Like in a typical on-premises network, all traffic within a subnet is allowed, but communication across different subnets is blocked by default. Separating your workloads in multiple subnets within a VNET is a best practice and highly recommended.

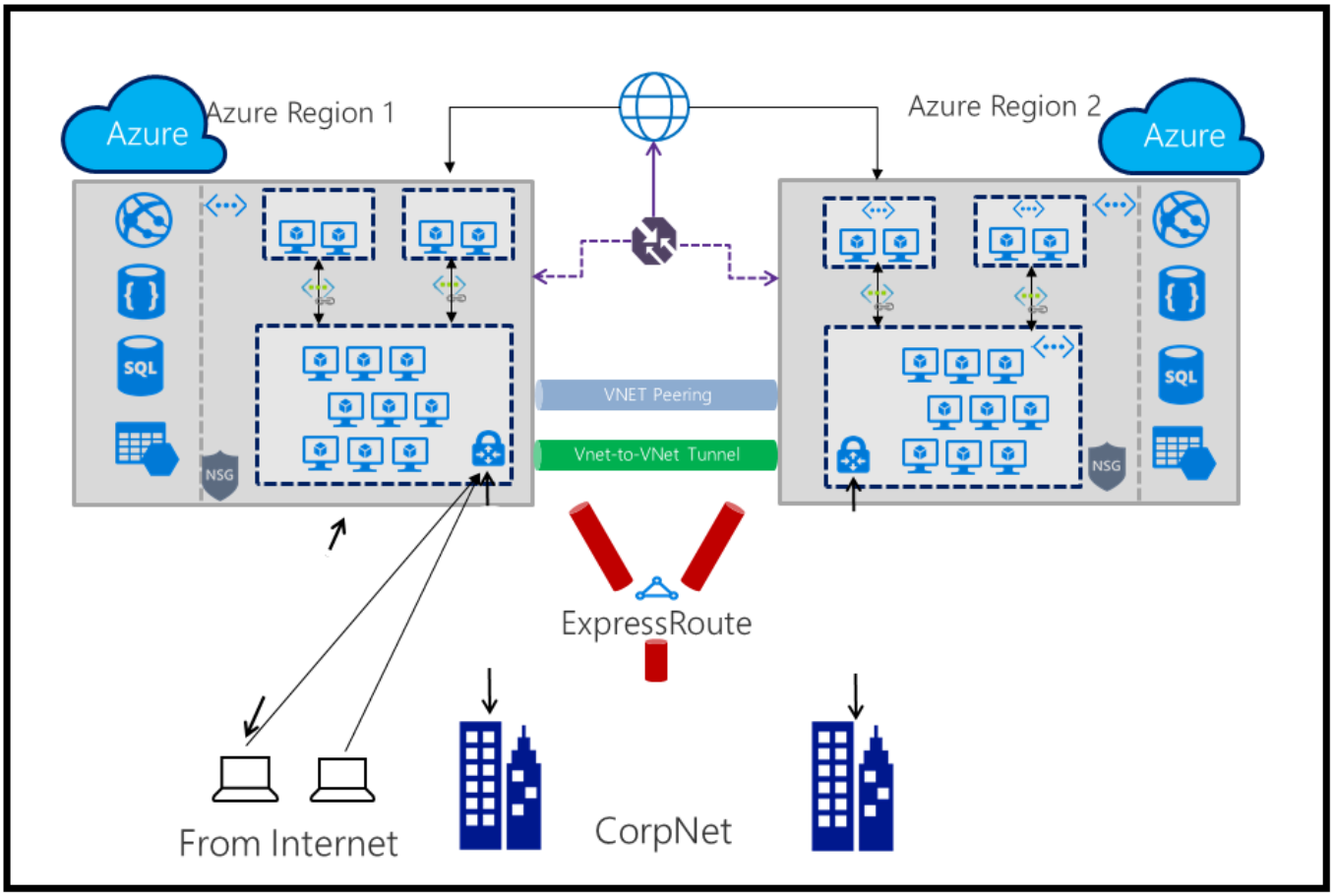
From a high-level perspective, Azure Virtual Networks allow for the following communication flows:

- From the Public Internet, incoming traffic is routed to Public IP addresses of Azure

Resources, secured by Network Security Groups. (think of these as software-defined firewalling for now).

- Several Azure Resources are making use of VNETs and subnets for IP addressing. These Azure Resources can be IAAS related (Virtual Machines, VM Scale Sets, Load Balancers, Azure Traffic Manager,…) as well as PAAS related (Service Fabric, Azure Container Services, Hadoop, Azure Application Services,…).
- From a back-end perspective, Azure allows for a hybrid network integration between multiple Azure Regions, or with on-premises datacenters. In a next module, we will detail the different capabilities and configuration options.

Multi-Region Virtual Network Architecture



Naturally, we can assume an organization wants to leverage the capabilities of the Azure Public Cloud, by deploying workloads across multiple Azure Regions, or across Azure Regions and on-premises data centers. This scenario is entirely achievable in Azure:

- From the Public Internet, Azure allows for load balancing across multiple Azure Regions by deploying Azure Traffic Manager.
- Interconnecting Azure Regions with each other is possible in 3 different ways:
  - Configuring Azure Site-to-Site VPN between both regions
  - Configuring Azure ExpressRoute communication tunnels

- A newer capability that allows for interconnecting multiple Azure regions is called Azure VNET Peering
- (Note: VNET Peering provides typical network communication, where VPN provides tunnel encryption – so it is up to the business requirements to make your decision)

- Interconnecting Azure Regions with on-premises datacenters is possible in 2 different ways:
  - Configuring Azure Site-to-Site VPN between Azure and on-premises
  - Configuring Azure ExpressRoute communication tunnels between Azure and on-premises
- Network Security Groups are active on Azure VNET layer or on individual NIC layer; however, NSGs cannot span Azure Regions. This means that you need to define the configuration within each VNET in each Azure Region.

VNETs & Subnets

- Networking Topology:
  - Define 1 or more VNets within an Azure Region, and configure an address space for each
  - Define 1 or more SubNets within a VNet, and configure address space within the VNet range
  - VNets and SubNets are using CIDR notation (x.x.x.x/24, x.x.x.x/16,...)
  - Configure Network Security Group settings on VNet level
  - Attach a NIC to a SubNet
- SubNet IP Addressing:
  - IP-address gets allocated to a NIC during provisioning of the NIC
  - First available IP-address in a SubNet range is x.x.x.4
  - Azure SubNets support dynamic (=default) and static IP addressing

- **Networking Topology:**
  - Define 1 or more VNETs within an Azure Region, and configure an address space for each
  - Define 1 or more SubNets within a VNET, and configure address space within the VNET range

- VNETs and SubNets are using CIDR notation (x.x.x.x/24, x.x.x.x/16,…)
- Configure Network Security Group settings on VNET level
- Attach a NIC to a SubNet

- **SubNet IP Addressing:**
  - IP-address gets allocated to a NIC during provisioning of the NIC
  - First available IP-address in a SubNet range is x.x.x.**4**
  - Azure SubNets support dynamic (=default) and static IP addressing

Subnets can be configured directly in the Azure Portal

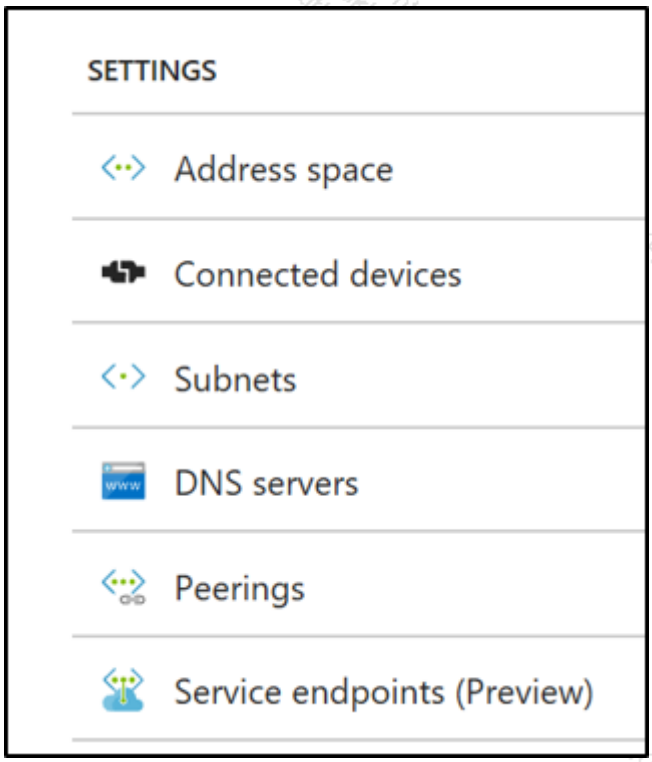


FIGURE 8.1: SUBNET CONFIGURATION

Public & Private IP-Addressing

- **Public IP-addressing**
  - Used for all public internet-facing communication
  - Required parameter when creating a VM from the portal
- **Private IP-addressing**
  - Used for all inter-VNET communication
  - Used for all communication between an Azure VNET and an on-premises VNET

Azure DNS Resolving

- DNS Server settings are configured on VNET level
- Using Azure DNS is de default configuration setting, but this can be modified
- **Or** use your custom DNS configuration
  - Azure DNS Appliance (from Azure MarketPlace)
  - Azure VM (e.g. Windows ADDS with DNS)
  - On-premises DNS solution (requires connectivity)
- Public DNS names (available for VMs and App Services) must be **unique** across Azure regions
- An example of such Public DNS name is **<host.region.cloudapp.azure.com>**

Lesson 2: Load Balancing

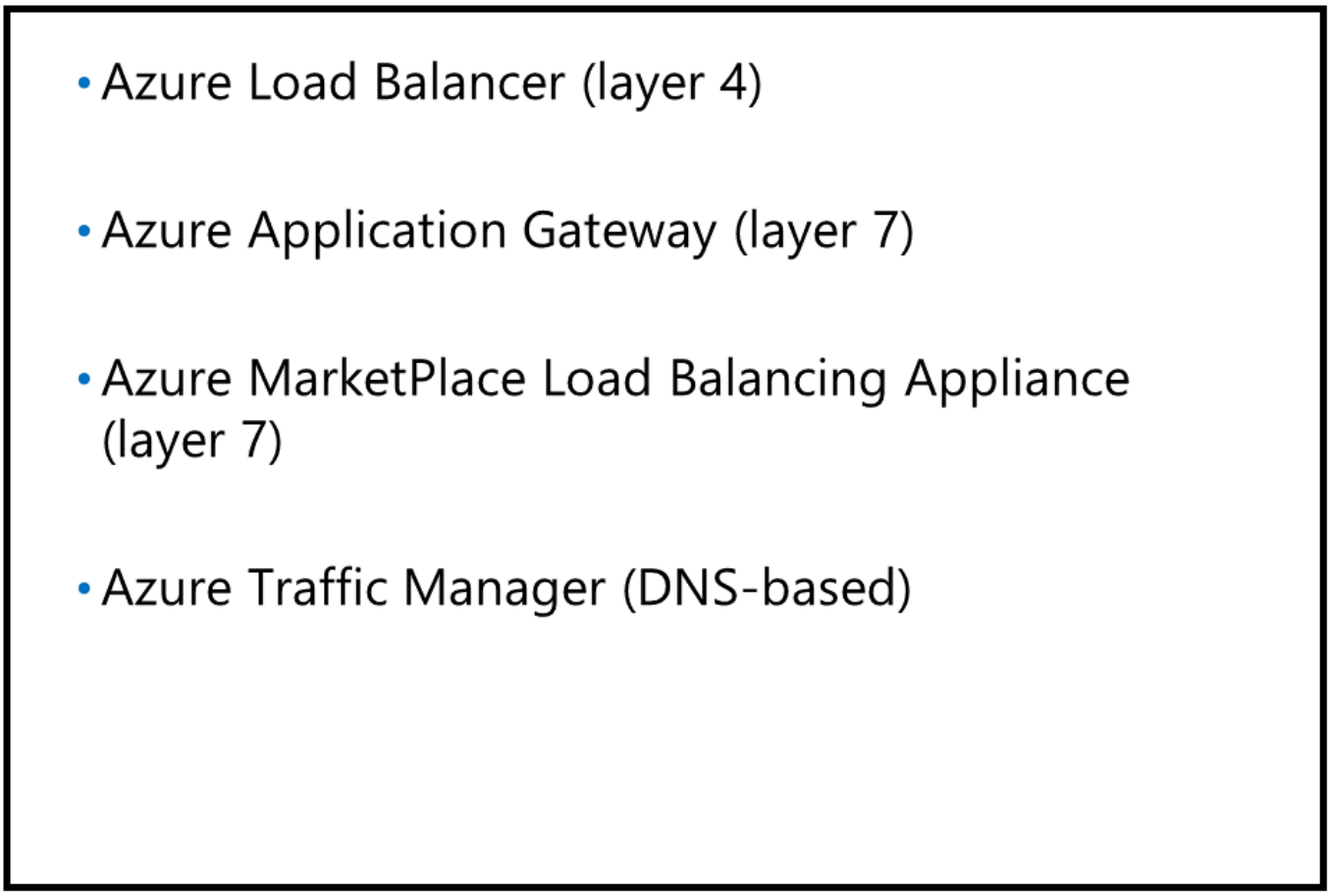
Azure Load Balancing refers to several different Azure Resources that are available on the Azure Platform , offering application workload load balancing capabilities, much similar to traditional on-premises load balancing solutions. This lesson starts with describing the different flavors, zooming in on the characteristics of each of the available flavors.

Lesson objectives

After completing this lesson, you will be able to:

- Understand Azure Load Balancing.
- Recognizing the use case for each of the in-Azure provided Load Balancing solutions.
- Deciding between the different Azure Load Balancing options.

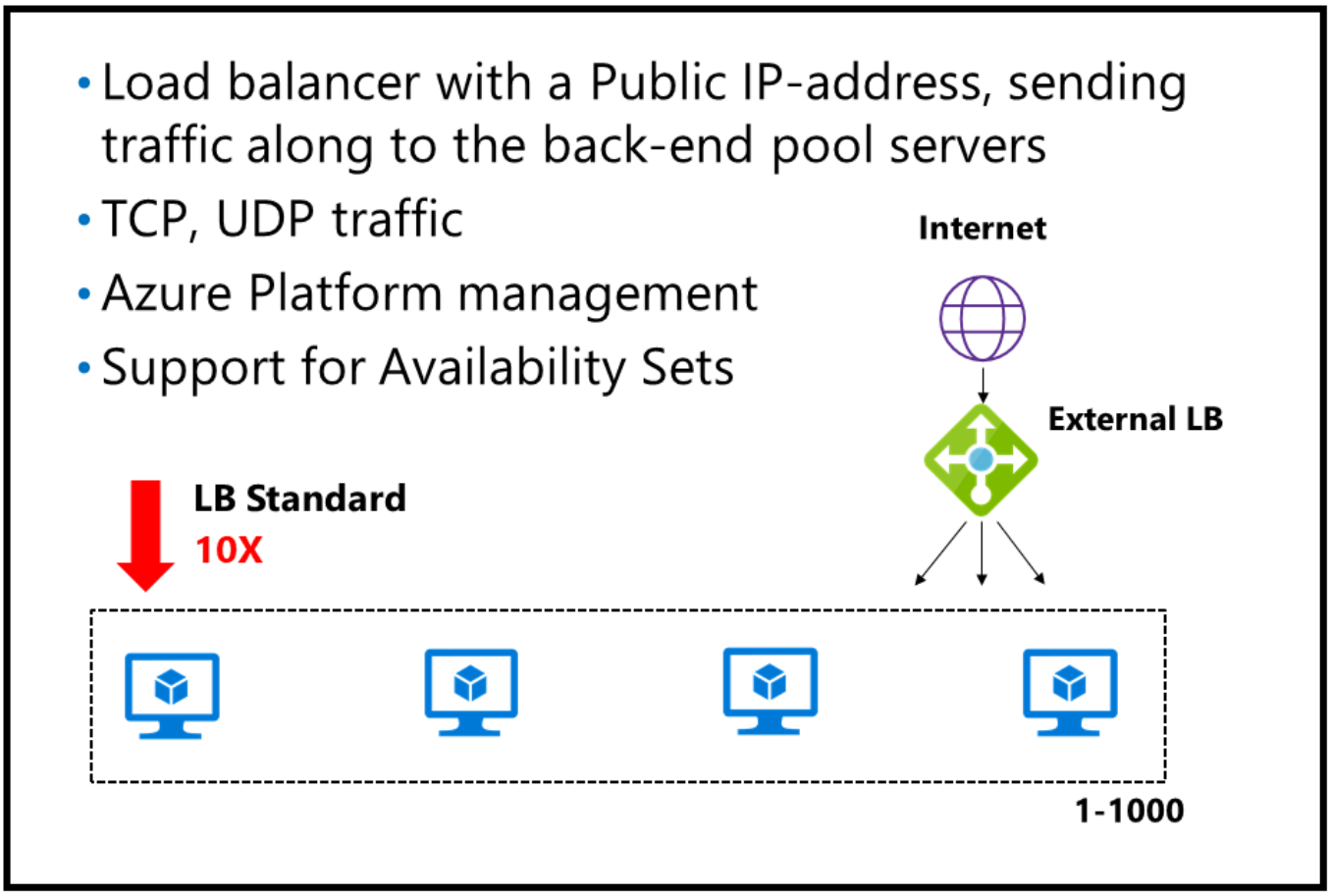
Load Balancing Solutions



Azure provides several built-in Azure Load Balancing Solutions:

- Azure Load Balancer
- Azure Application Gateway
- Azure Marketplace Load Balancing Appliance
- Azure Traffic Manager

Azure Load Balancer



Starting with Azure Load Balancer, it is important to point out it can be configured both as an “external load balancer,” or as an “internal load balancer,” where one cannot act as both external and internal at the same time.

In the scenario of an Azure external load balancer, the load balancer front-end is configured with a Public-facing IP-address, sending all traffic along to the back-end pool servers, using their internal IP-addresses.

Azure Load Balancers can handle almost any TCP or UDP traffic; use case scenarios include RDS (Remote Desktop Services Farm), Linux SSH server connectivity load balancing, or any other application-specific traffic.

In relation to Azure Virtual Machine Availability Sets, where you deploy multiple instances of the same Virtual Machine, it is thanks to Azure Load Balancer functionality; an Availability Set can grow to 10x the number of instances (100 to 1000 in a single Availability Set).

Pretty similar in functionality is an Azure Internal Load Balancer. The main difference is that this solution doesn’t have a Public-facing IP-address, and all communication is based on internal IP-addressing and IP-routing.

A typical use case for this setup is like the diagram shown, where you want to load balance incoming traffic between Azure Subnets or Azure VM Availability Sets. The external Load Balancer takes care of the incoming web traffic to the Web Server AVSet, where any Web Server VM can communicate with the Database Server backend, using the internal Azure Load Balancer option.

Azure Load Balancer existed in a **Basic** edition, which gave you the following characteristics:

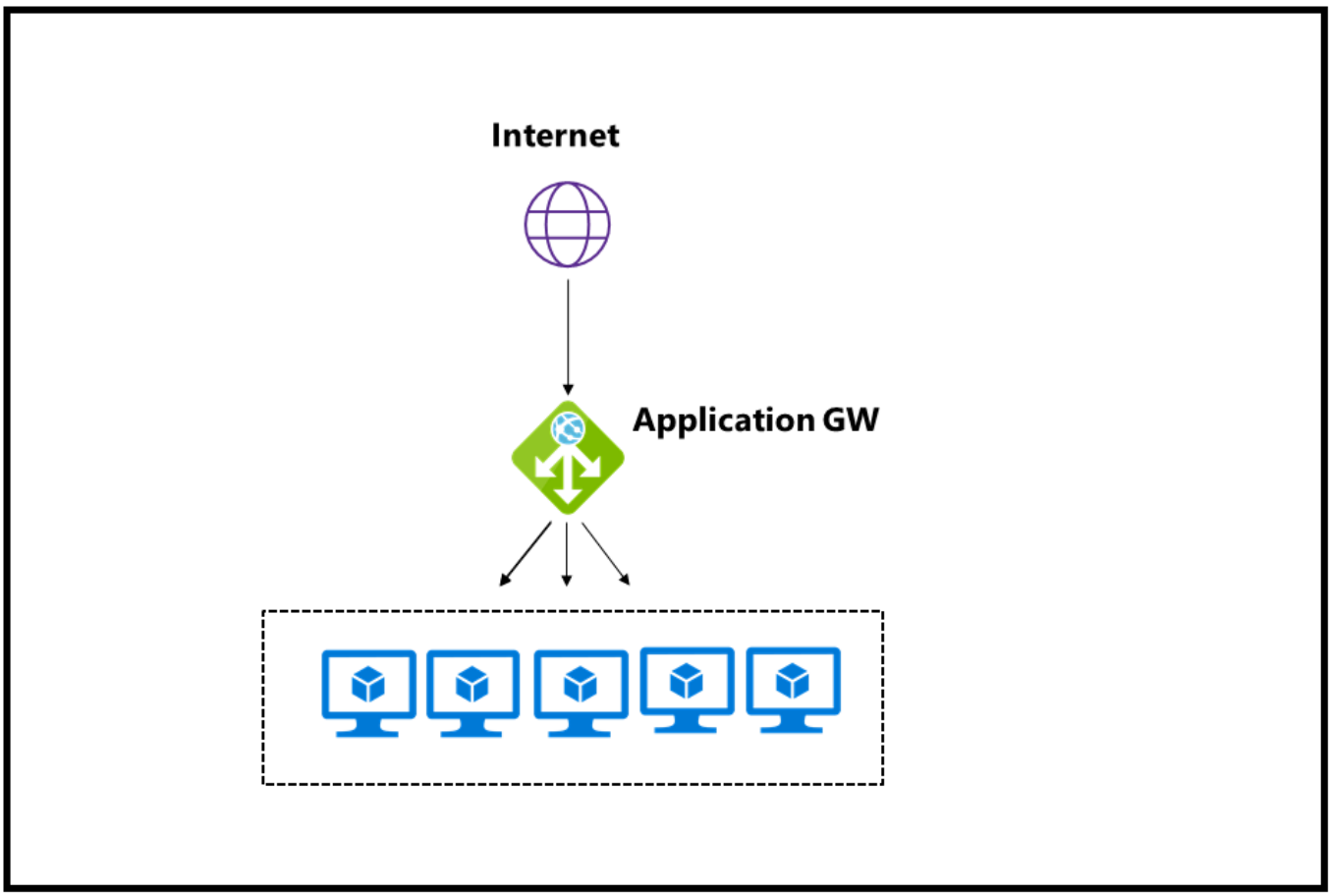
- Up to 100 backend instances
- Single Availability Set
- Basic NAT and Probe health status

- No HA Ports
- Network Security Groups (NSG) are optional
- No cost related to using this Azure Load Balancer solution

While Azure Load Balancer was and still is a viable solution, it also had some technical limitations. Some of these are resolved in the **Standard** SKU of the Azure Load Balancer, giving you the following characteristics:

- Up to 1000 backend instances
- Availability Sets are not required; providing support for Availability Zones
- Integrated Frontend and Backend health metrics
- Support for HA Ports
- Network Security Groups are required during configuration and deployment

Azure Application Gateway



Another Azure Load Balancing solution on the platform is **Azure Application Gateway**. While mostly similar in functionality than the Azure Load Balancer, we like to focus on its specifics:

- Load Balancing, active on Layer 7 of the network stack; this mainly means it is “application

intelligent.”

- Main features Application Gateway provides, compared to Azure Load Balancer, are:
  - HTTP/HTTPS traffic only, no other ports allowed
  - SSL Offloading
  - Cookie Affinity
  - Web Application Firewall (WAF)
  - URL Based Routing

  In the scenario of **URL based Routing**, Application Gateway recognized the incoming web request and based on the URL information; it will redirect traffic to the correct destination. Besides main URL redirection, this can also be used on subheaders. For example, in the given scenario, web requests to the http://www.domain2.com/finance web app will be redirected to WebAV1, where all requests to the http://www.domain2.com/sales web app, will be redirected to another WebAV2 availability set.

  In regards to **SSL Termination**, Azure App Gateway provides the following capabilities:

- SSL Offloading, by importing the SSL Certificate onto the App Gateway; traffic to the backend servers don’t require HTTPS communication, also that would still be an option
- HTTP to HTTPS redirect; this means that, whenever a user is connecting to the web app using HTTP, the request will be redirected to HTTPS, forcing SSL Tunneling for this given request.

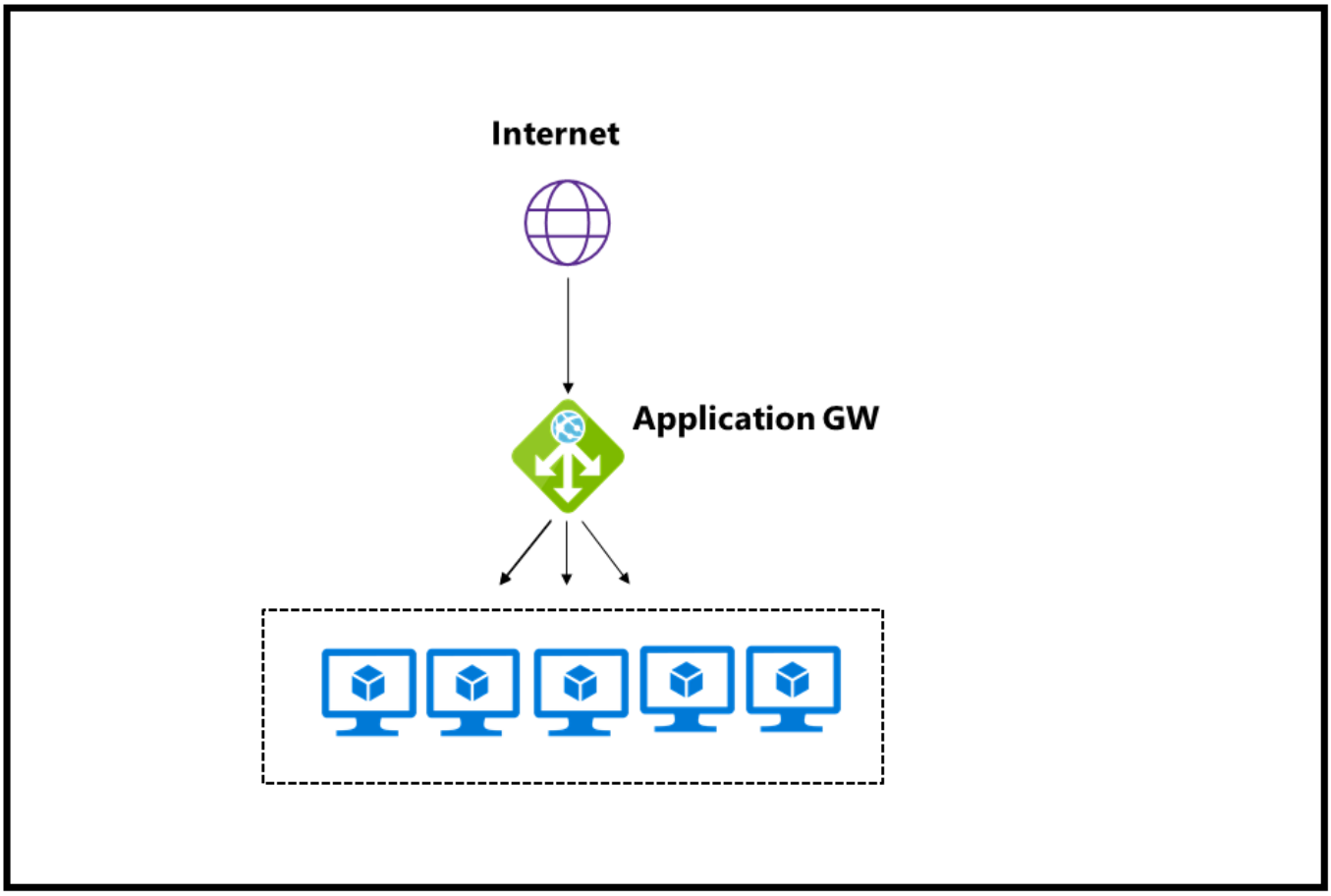
  The last feature of Azure Application Gateway we want to discuss here is **Web Application Firewall** (WAF).

  Based on industry-standard rules for WAF, CRS 2.2.9 and CRS 3.0, Azure Application Gateway provides protection against several common attacks and threats on application workloads:

- SQL Injection
- Cross-site scripting
- Protocol violations
- Generic attacks
- HTTP rate limiting
- Scanner detection
- Session fixation

- LFI/RFI

Azure Load Balancing Marketplace Appliances



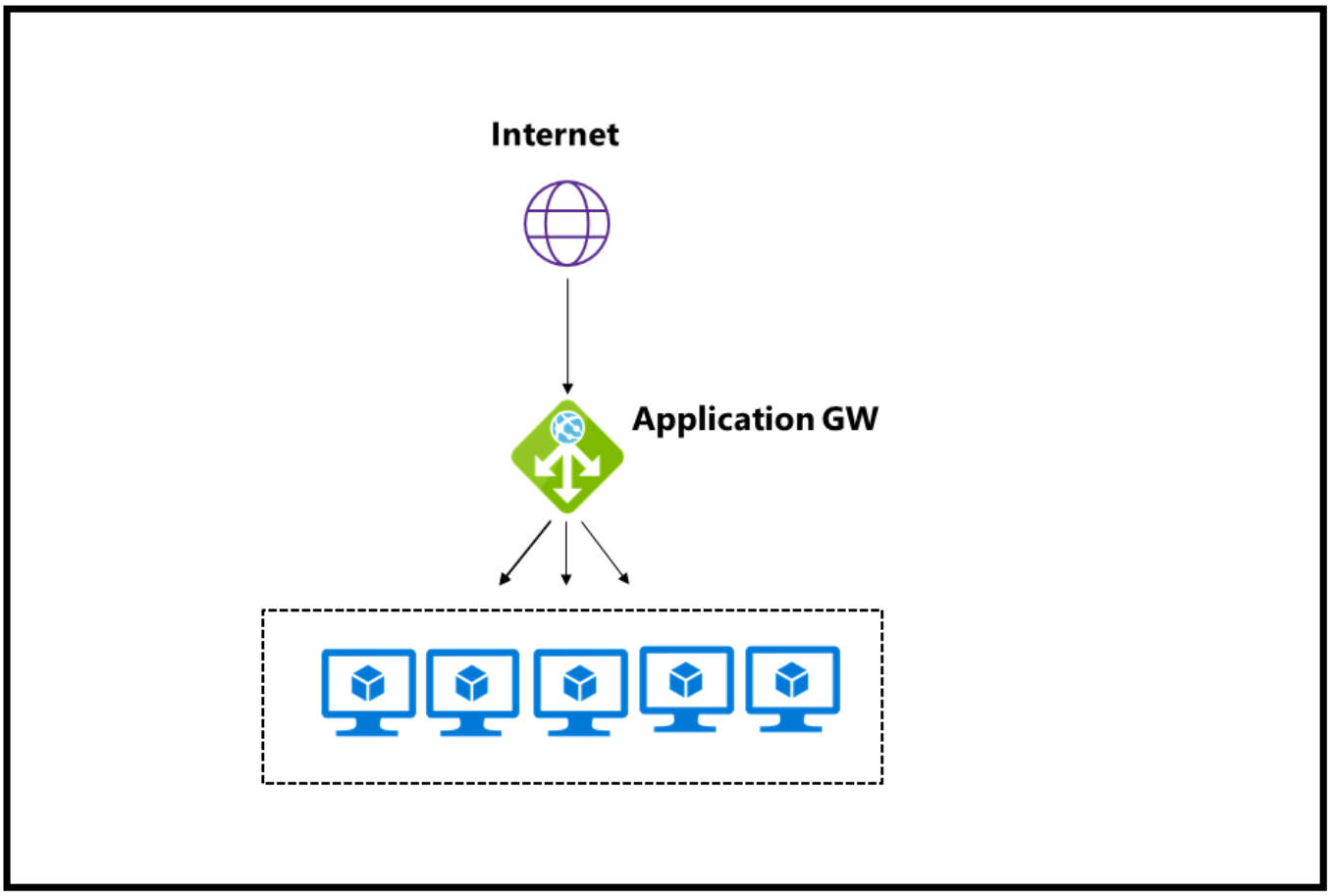
Where both Azure Load Balancer and Azure Application Gateway are an interesting option, directly built into the Azure Platform and offered “as a service,” the capabilities around management, monitoring and control might be too limited for certain organizations. In that scenario, one can deploy a third-party Azure Marketplace appliance.

The “common” vendors from the on-premises world are present in an Azure Appliance alternative. Support is initially provided by Microsoft, backed by SLA’s, and acting as a SPOC.

Most flavors support 2 different licensing models to choose from:

- BYOL – Bring Your Own License; this is an ideal candidate if you are removing or downsizing on your on-premises running third-party load balancer. Depending on the specific licensing terms of the vendor, one can reuse the license key on the Azure VM Appliance.
- Pay-Per-Use; in this model, the monthly Azure VM consumption cost is based on the VM Size allocation to the Appliance, as well as a monthly licensing fee for the third party load balancing application within the VM.

Azure Traffic Manager



Traffic Manager

Microsoft Azure Traffic Manager allows you to control the distribution of user traffic to your specified endpoints, which can include Azure cloud services, websites, and other endpoints. Traffic Manager works by applying an intelligent policy engine to Domain Name System (DNS) queries for the domain names of your Internet resources. Your Azure cloud services or websites can be running in different datacenters across the world.

Traffic Manager is very flexible because it allows you to mix various endpoints behind the same DNS name. Traffic Manager can be used in a variety of scenarios but most use cases fall in the following scenarios:

- **Failover**: Traffic Manager can poll to determine if and endpoint is online or offline. The endpoints are then ordered in a priority list. By default, traffic routes to the first endpoint. If the first endpoint is down, traffic routes to the next endpoint (2) in the list. Traffic Manager will route requests to the endpoint that is the highest in the priority list and is still online. Using this method, you can have Traffic Manager route traffic to primary or backup datacenters/services for a simple failover scenario.
- **Geography**: Traffic Manager uses an Internet Latency Table to determine the endpoint that is "closest" to the client that is making a request. Using this method, an application can be hosted in West Europe and West US. A user from Denmark can reasonably expect to be served by the endpoint residing in the West Europe datacenter and should experience lower latency and higher responsiveness.
- **Distribution**: Traffic Manager can distribute traffic in a near-random way to distribute traffic evenly across a set of endpoints. If a specific endpoint is down, the traffic is distributed evenly across the remaining endpoints. The distribution can optionally be weighted so that

certain endpoints receive more requests than others. The weighted distribution is especially useful if you want to distribute a small subset of your traffic to a hot disaster recovery site that is using smaller service tiers but keep the majority of your traffic to a primary site that is using larger service tiers.

Using Traffic Manager with Web Apps

Traffic Manager can be integrated with Web Apps easily. When you configure a Traffic Manager profile, the settings that you specify provide Traffic Manager with the information needed to determine which endpoint should service the request based on a DNS query. No actual endpoint traffic routes through Traffic Manager.

The below diagram shows how Traffic Manager directs users to one of a set of endpoints.

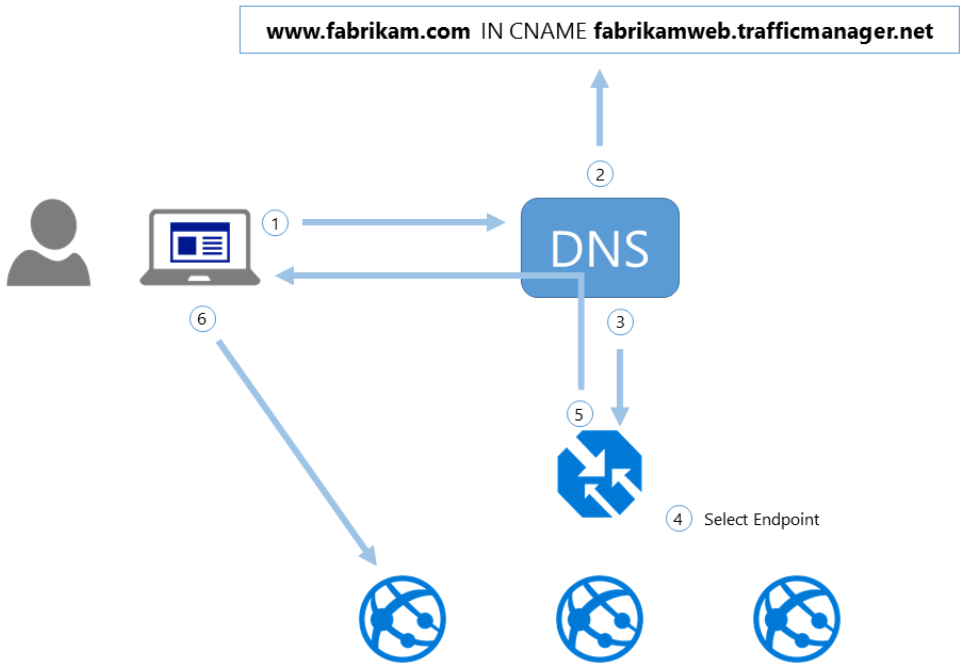


FIGURE 8.2: TRAFFIC MANAGER WORKFLOW

1. **User traffic to company domain name**: The client requests information using the company domain name. The goal is to resolve a DNS name to an IP address. Company domains must be reserved through normal Internet domain name registrations that are maintained outside of Traffic Manager. In Figure 1, the example company domain is www.fabrikam.com.

2. **Company domain name to Traffic Manager domain name**: The DNS resource record for the company domain points to a Traffic Manager domain name maintained in Azure Traffic Manager. This is achieved by using a CNAME resource record that maps the company domain name to the Traffic Manager domain name. In the example, the Traffic Manager domain name is fabrikamweb.trafficmanager.net.

3. **Traffic Manager domain name and profile**: The Traffic Manager domain name is part of the Traffic Manager profile. The user's DNS server sends a new DNS query for the Traffic

Manager domain name (in our example, fabrikamweb.trafficmanager.net), which is received by the Traffic Manager DNS name servers.

4. **Traffic Manager profile rules processed**: Traffic Manager uses the specified load balancing method and monitoring status to determine which Azure or other endpoint should service the request.

5. **Endpoint domain name sent to user**: Traffic Manager returns a CNAME record that maps the Traffic Manager domain name to the domain name of the endpoint. The user's DNS server resolves the endpoint domain name to its IP address and sends it to the user.

6. **User calls the endpoint**: The user calls the returned endpoint directly using its IP address.

Lesson 3: External Connectivity

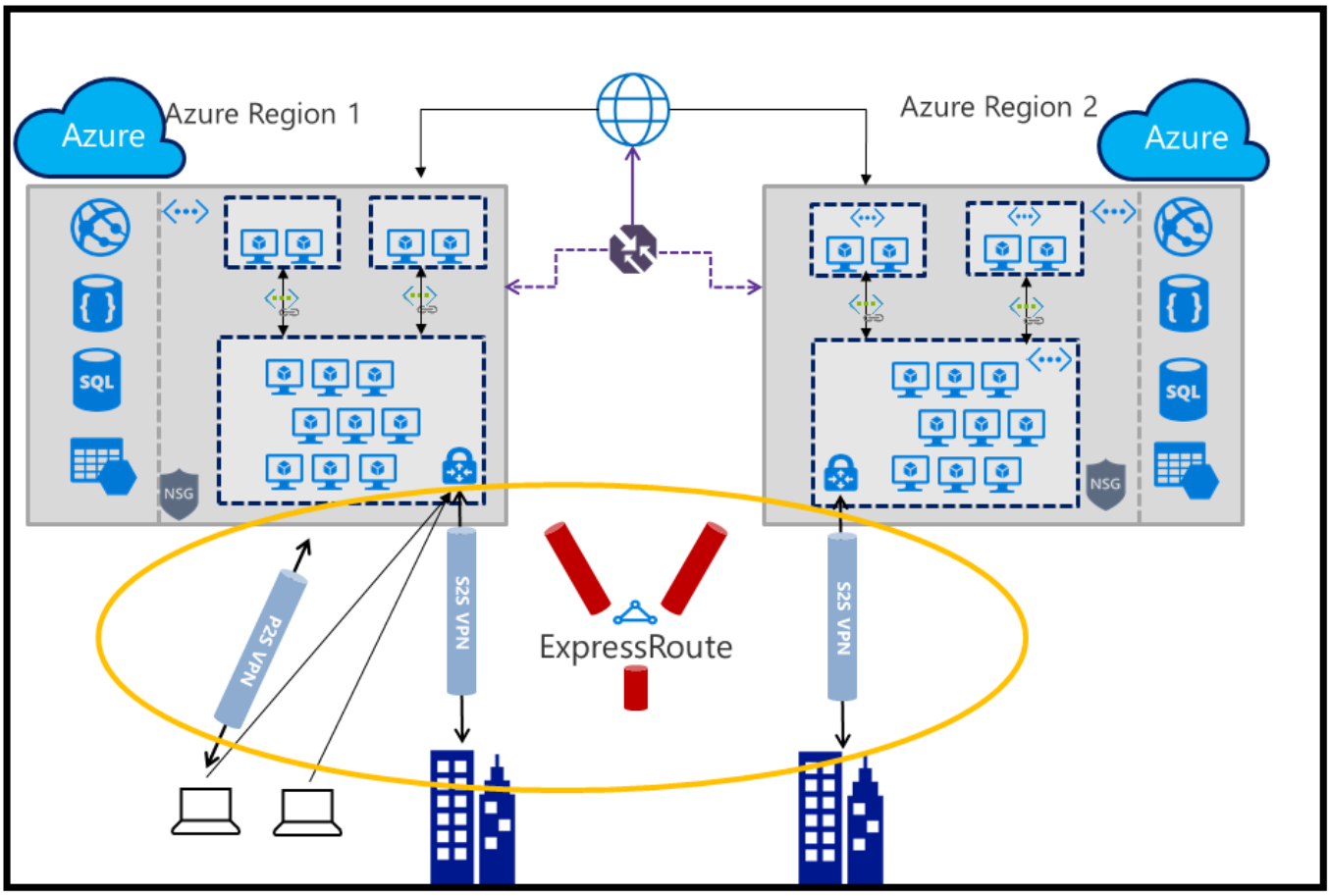
Azure Hybrid Connectivity discusses several options available within the Azure Platform, to establish end-to-end hybrid connectivity. This can be between an on-premises network and one or more Azure regions, or between multiple Azure regions. This lesson discusses some reference architectures, the different solutions available for each challenge, and some overall guidelines and concepts.

Lesson objectives

After completing this lesson, you will be able to:

- Understand Azure Hybrid Connectivity
- Architecting Azure VNET Peering and understanding the use cases
- Understanding the differences between Site-to-Site VPN and Point-to-Site VPN
- Understand the key capabilities and characteristics of Azure ExpressRoute

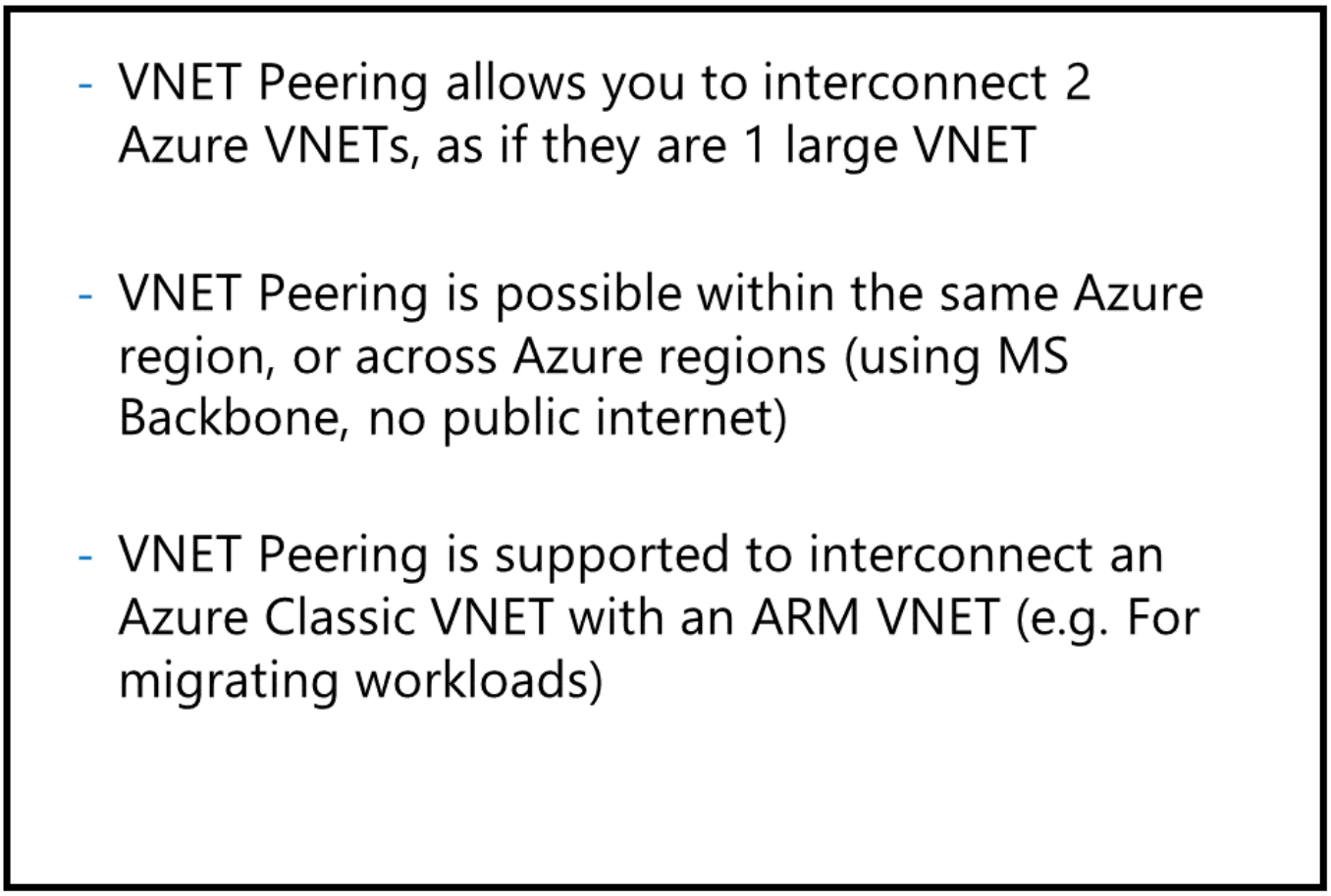
On-Premises to Azure Connectivity



There are three primary options to connect your on-premises data center to Azure:

Connectivity	Benefits
ExpressRoute	• ExpressRoute as primary cross-premises connectivity • Multiple circuits for redundancy & better routing • ExpressRoute-VPN co-existence for highly available, redundant paths
Site-to-Site VPN	• S2S VPN over Internet for remote branch locations • BGP & active-active configuration for HA and transit
Point-to-Site VPN	• P2S VPN for mobile users & developers to connect from anywhere with macOS & Windows • AD/radius authentication for enterprise grade security

VNET Peering



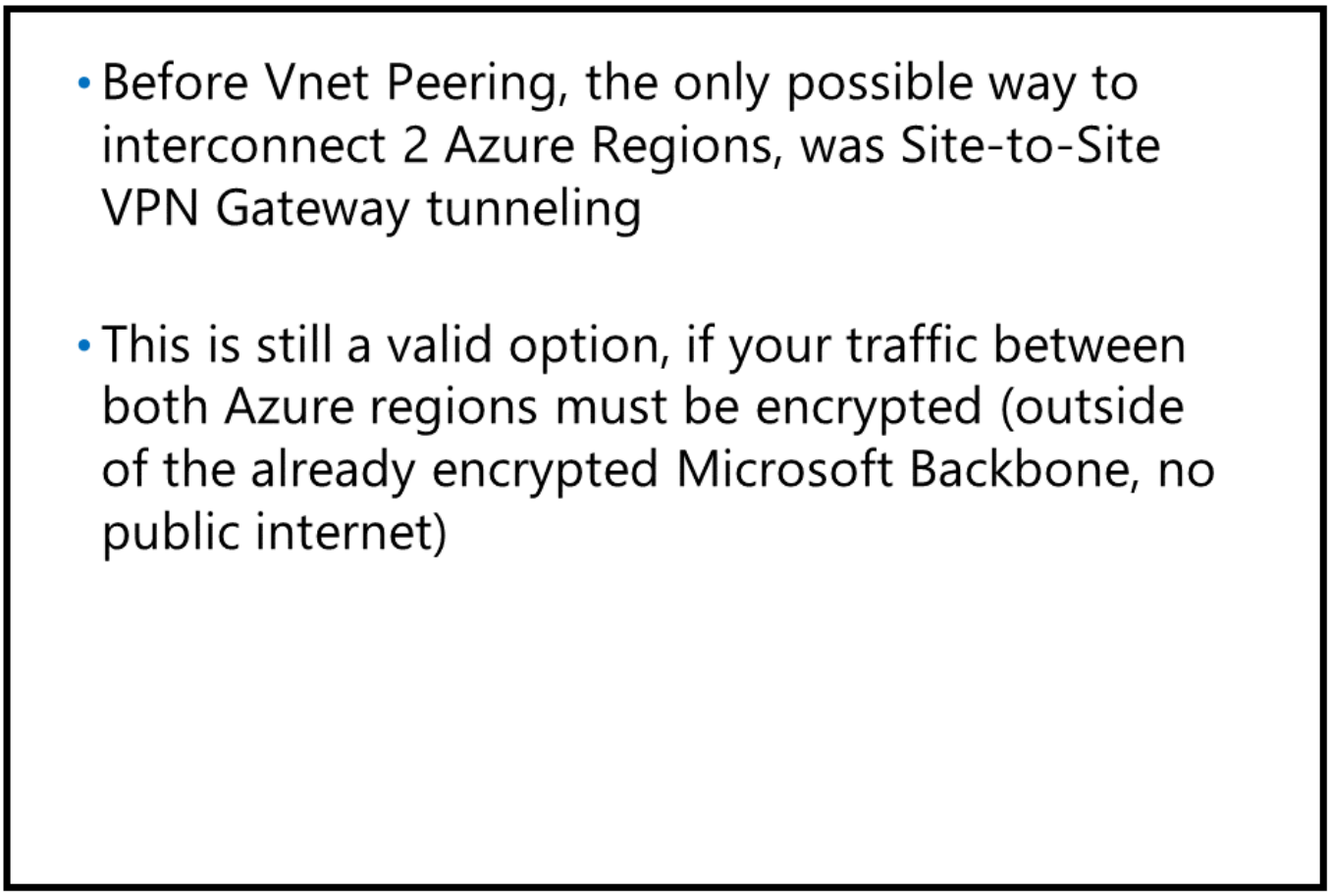
VNET peering allows you to interconnect 2 Azure Regions with each other, using the Microsoft Backbone (not the public internet). Communication relies on internal IP addressing.

Here are some of the primary features of VNET Peering:

- VNET Peering allows you to interconnect 2 Azure VNET as if they are 1 large VNET
- VNET Peering is possible within the same Azure region, or across Azure regions (using MS Backbone, no public internet)
- VNET Peering is supported to interconnect an Azure Classic VNET with an ARM VNET (e.g., For migrating workloads)

If VNET peering is not an option, because you might want to encrypt your traffic within the VNET tunnel, one can still deploy a VPN Gateway on both Azure Regional VNETs and creating a Site-to-Site VPN tunnel across those regions.

Multi-Region VPN Connectivity



Forced Tunneling

By using Forced Tunneling, Azure traffic can be rerouted to an on-premises virtual network, to be routed through an existing Site-to-Site VPN or ExpressRoute, into the internal Azure VNET.

This is a massive improvement from a security standpoint, as your internal Azure VMs are no longer accessible through the public internet.

Securing Access to PaaS Services

A similar concept now exists, to limit network access to PAAS Services in Azure. In a typical scenario, these PAAS services are/were accessible from the public internet. But that's not what all customers want. Maybe you want your application services endpoints in PAAS to be only accessed from the internal Azure VNETs.

The solution to this is using VNET service endpoints, where you define which PAAS services are no longer accessible through the public internet.

Note: For now, this feature is only available to Azure Storage Accounts, SQL DB Services in PAAS and Web Apps. More PAAS Services will be integrated with this feature soon enough.

Lesson 4: Secure Connectivity

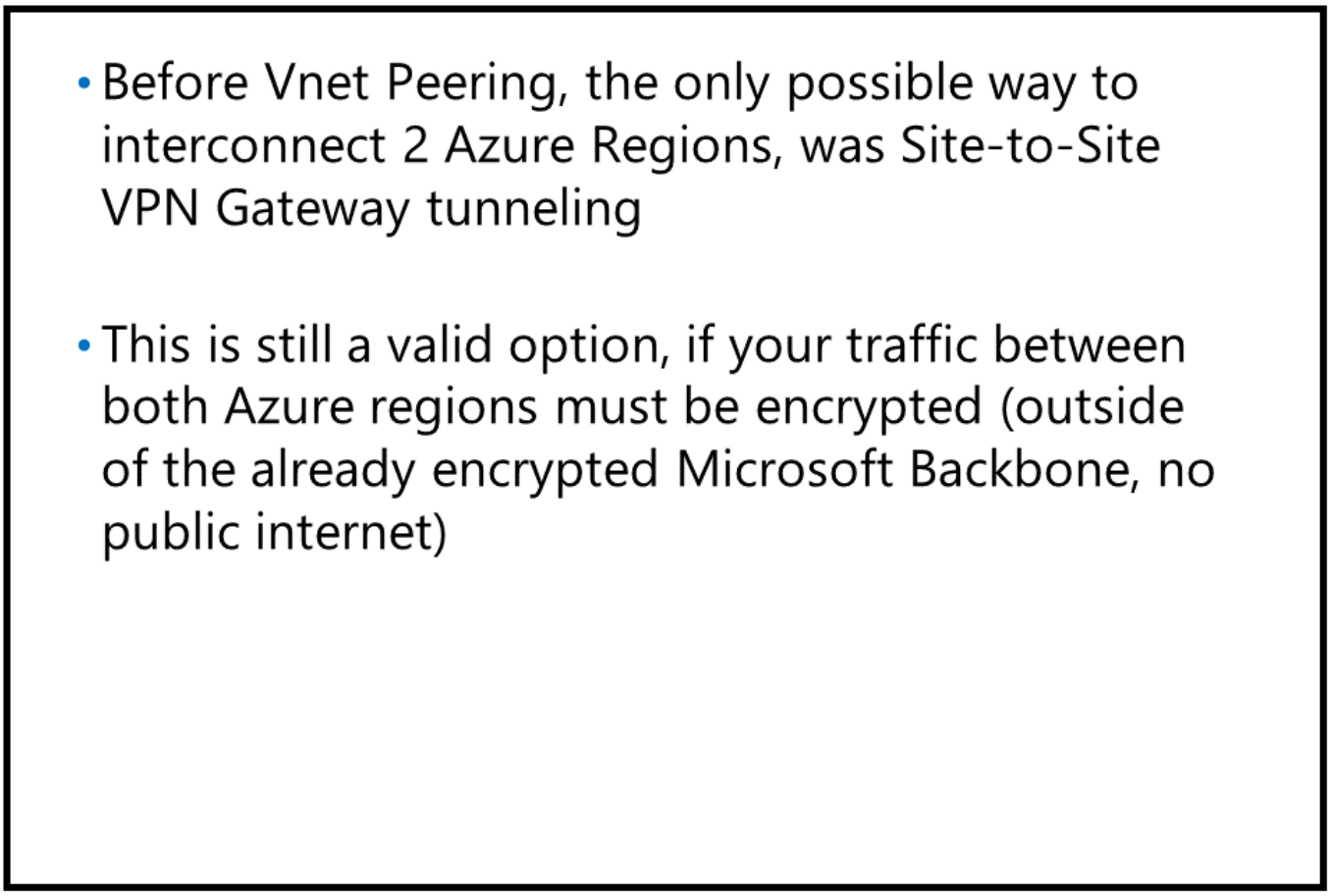
This lesson briefly talks about Network Security Groups and how they can be used to secure connections in a hybrid or external connectivity scenario.

Lesson objectives

After completing this lesson, you will be able to:

- Determine how and when to use Network Security Groups to secure access to and from a VM.

Network Security Groups



Network security groups are different than endpoint-based ACLs. Endpoint ACLs work only on the public port that is exposed through the input endpoint. An NSG works on one or more VM instances and controls all the traffic that is inbound and outbound.

You can associate an NSG to a VM, or to a subnet within a VNet. When associated with a VM, the NSG applies to all the traffic that is sent and received by the VM instance. When applied to a subnet within your VNet, it applies to all the traffic that is sent and received by ALL the VM instances in the subnet. A VM or subnet can be associated with only 1 NSG, and each NSG can contain up to 200 rules. You can have 100 NSGs per subscription.on the VM.

Managing Network Security Groups

A NSG is a top level object that is associated to your subscription. An NSG contains access control rules that allow or deny traffic to VM instances. The rules of an NSG can be changed at any time, and changes are applied to all associated instances.

A network security group has a Name, is associated to a Region, and has a descriptive label. It contains two types of rules, Inbound and Outbound. The Inbound rules are applied on the incoming packets to a VM and the Outbound rules are applied to the outgoing packets from the VM. The rules are applied at the host where the VM is located. An incoming or outgoing packet has to match an Allow rule for it be permitted, if not it will be dropped.

Rules are processed in the order of priority. For example, a rule with a lower priority number (e.g. 100) is processed before rules with a higher priority numbers (e.g. 200). Once a match is found, no more rules are processed.

Default Network Security Group Rules

An NSG contains default rules. The default rules cannot be deleted, but because they are assigned the lowest priority, they can be overridden by the rules that you create. The default rules describe the default settings recommended by the platform. While connectivity to the Internet is allowed for Outbound direction, it is by default blocked for Inbound direction. There is a default rule to allow Azure's load balancer (LB) to probe the health of the VM. You can override this rule if the VM or set of VMs under the NSG does not participate in the load balanced set.

Inbound

NAME	PRIORITY	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT
ALLOW VNET INBOUND	65000	VIRTUAL_NETWORK	*	VIRTUAL_NETWORK	*
ALLOW AZURE LOAD BALANCER INBOUND	65001	AZURE_LOADBALANCER	*	*	*
DENY ALL INBOUND	65500	*	*	*	*

Outbound

NAME	PRIORITY	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT
ALLOW VNET OUTBOUND	65000	VIRTUAL_NETWORK	*	VIRTUAL_NETWORK	*
ALLOW INTERNET OUTBOUND	65001	*	*	INTERNET	*
DENY ALL OUTBOUND	65500	*	*	*	*

Lesson 5: Networking Case Study

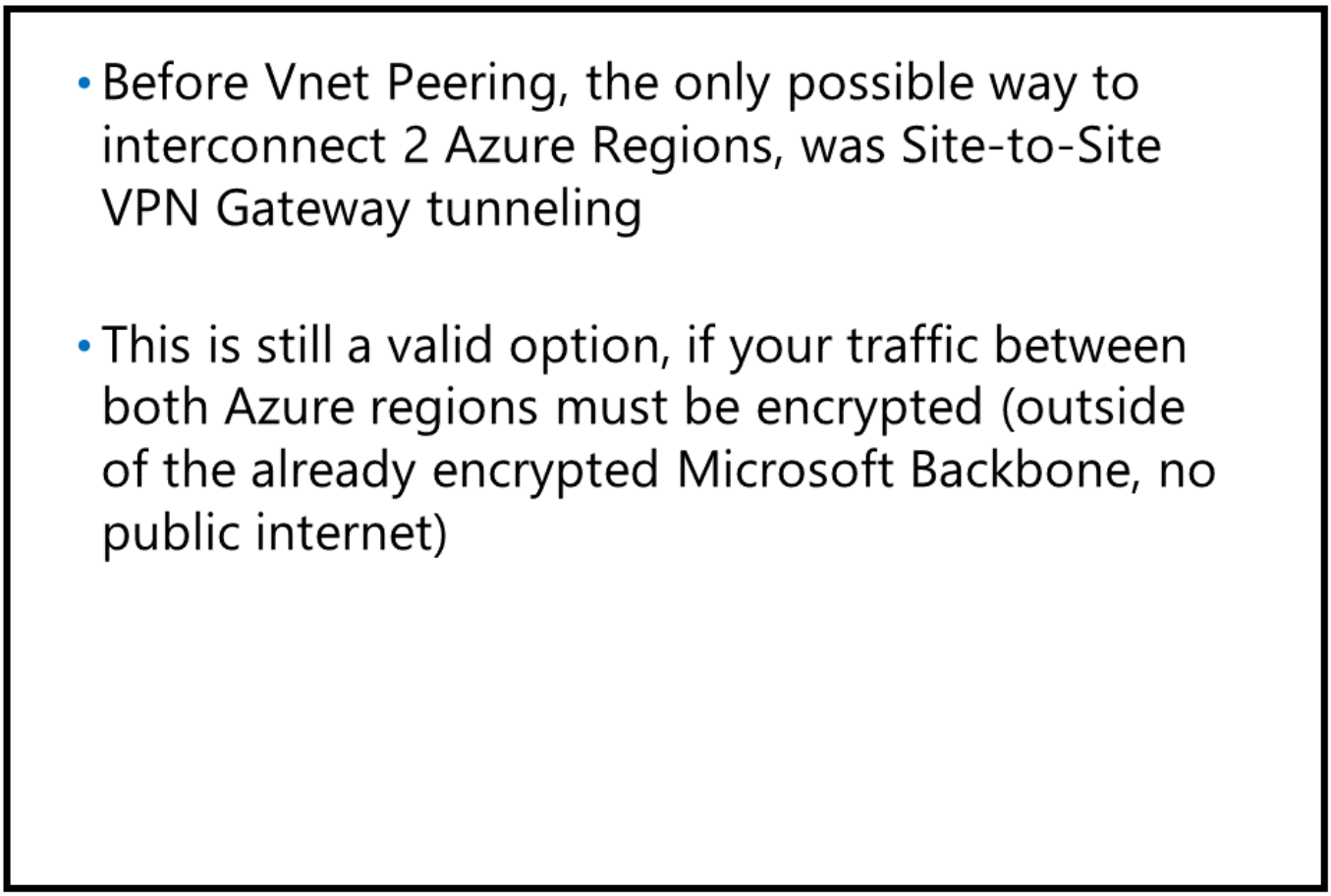
In this case study, we will look at a customer problem that requires an architectural recommendation.

Lesson objectives

After this case study, you should:

- Identify customer problems as they are related to networking.
- Design a solution that will meet the customer's objectives.
- Ensure your designed solution accounts for customer objections.

Case Study Overview



Who is the Customer?

Fabrikam Residences (http://fabrikamresidences.com) is a national real estate services group whose rapid growth was being slowed by an expensive and unresponsive datacenter infrastructure.

Fabrikam has two data centers in the United States, but it really doesn't want to be in the datacenter business. "We are a national real estate firm," says Craig Jones, Chief Information Officer for Fabrikam. "We want to make investments that support our core business, and buying and managing servers is not our core business. In fact, we have what we call a DOS strategy 'don't own stuff.' We were not an asset-intensive organization in any area but IT, where we had many underutilized assets."

What Does the Customer Already Have?

Fabrikam has about 250 servers in its datacenter in California, and another 110 in its Virginia datacenter, and hundreds of servers scattered across several branch offices throughout the United States. Fabrikam ended up overprovisioning servers each time it deployed an application to ensure that capacity would be there at peak times. This meant that millions of dollars' worth of hardware and software was sitting idle much of the time.

In addition to the primary data centers, Fabrikam also has several branch offices scattered across the United States that have connectivity to the primary data center through an MPLS based wide area network. Their partner is a Microsoft Azure ExpressRoute partner. To reduce costs, Fabrikam has made the decision to move its West coast datacenter to a colocation site in Silicon Valley and to virtualize the remainder of the servers in its branch offices and Virginia data center into the cloud. Fabrikam's current virtualization and management solution is based on System Center so a solution that integrates well with these known tools is ideal.

What is the Customer's Goal?

Fabrikam Residences would like to eventually migrate the majority of their workloads to Azure. There are several workloads that will be migrated, but the most critical for Fabrikam is their CRM application.

The CRM application is a custom web application that runs on IIS 8 and SQL Server 2012 that stores sensitive documents for all of their customer's transactions. This application needs to perform well at peak time while mitigating the problem of overprovisioned capacity. The centralized nature of the application means that any downtime will block the activity of a significant portion of the company so the solution must be highly available. Due to the sensitive nature of this application security is key so access to the application is restricted to only authorized users from the corporate network including branch offices.

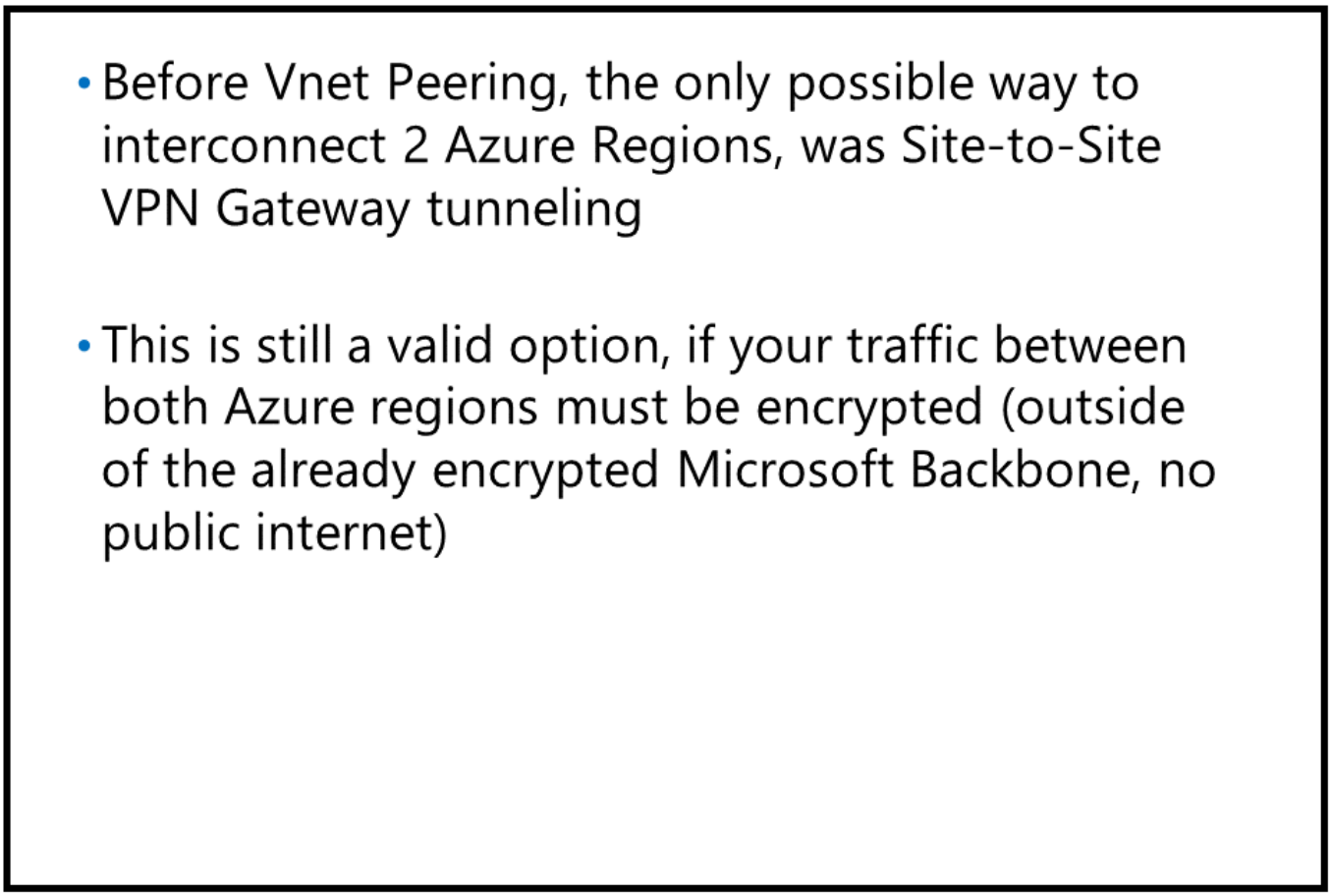
What Does the Customer Need?

- Reduce the number of existing on-premises servers through public cloud consolidation to reduce the costs of their current overprovisioned deployments. Servers running in the Virginia data center and remote branch offices will be moved to the closest Azure region. Due the sheer amount of servers being virtualized latency and performance of the network is a big concern.
- Because of the sensitive nature of the data that Fabrikam Real Estate works with ensuring the security and privacy of their infrastructure connects through is critical.
- As part of the migration efforts the CRM application must be deployed in a way that mitigates their current problem of overprovisioning capacity when not needed but able to scale to meet peak demand. The CRM application must be highly available and only accessible from the corporate intranet.

What Things Worry the Customer?

- We have a national business and we need connectivity that can accommodate connectivity from coast-to-coast.
- Our workloads are very seasonal. I do not want to pay for more resources than I need.
- The data that crosses our network is very confidential. Is Azure secure?
- I need to deploy an intranet-based solutions and I have heard that Azure requires an on-premises load-balancer for internal facing workloads.
- I have heard that the public IP address of an Azure deployment can change and break my application.
- My workloads require static IP addresses. I have heard Azure does not support this scenario.
- I have some workloads that require multiple network interfaces on my virtual machines.
- Some deployments require the segmenting of network traffic. Does Azure support this?

Case Study Solution



Preferred Target Audience

Craig Jones, Chief Information Officer for Fabrikam

The primary audience is the business decision makers and technology decision makers. From the case study scenario, this would include the IT Director, Network Administrator and Security Lead.

Preferred Solution

Fabrikam Residences went with Azure ExpressRoute. They already had a relationship with a Network Service Provider and their MPLS WAN was already in place so it made logical sense to extend their network with Azure. ExpressRoute provides the secure and private connection they need to ensure the privacy of their customer records along with the high speed and low latency connectivity their workloads require.

The first step was to configure ExpressRoute by first contacting AT&T and start the onboarding process for ExpressRoute.

After a circuit was in place with their provider, the next step was to implement Azure Virtual Networks in each of the regions where they would be migrating workloads to the cloud.

They connected the virtual networks across several regions where their branch offices are located to the ExpressRoute circuit using the PowerShell New-AzureDedicatedCircuitLink cmdlet.

The next step was to deploy Active Directory in each of the regions. Each Active Directory DC should be deployed with a static IP into a subnet that does not contain non-static IP based VMs. There should be at least two DCs for redundancy and deployed into an availability set. An Active Directory site should be configured so authentication requests stay local.

The final step was to architect the solution for their CRM solution to ensure it met the requirements of being secure, highly available, and easily scalable for peak demand. The CRM web servers are deployed into an availability set and auto scale is configured to avoid over provisioning. Access to CRM is through an internally load-balanced endpoint and the SQL Server deployment uses AlwaysOn availability groups as well as an internal load balanced IP for the listener.

Example of a Preferred Solution

Deploying ExpressRoute with MPLS Network

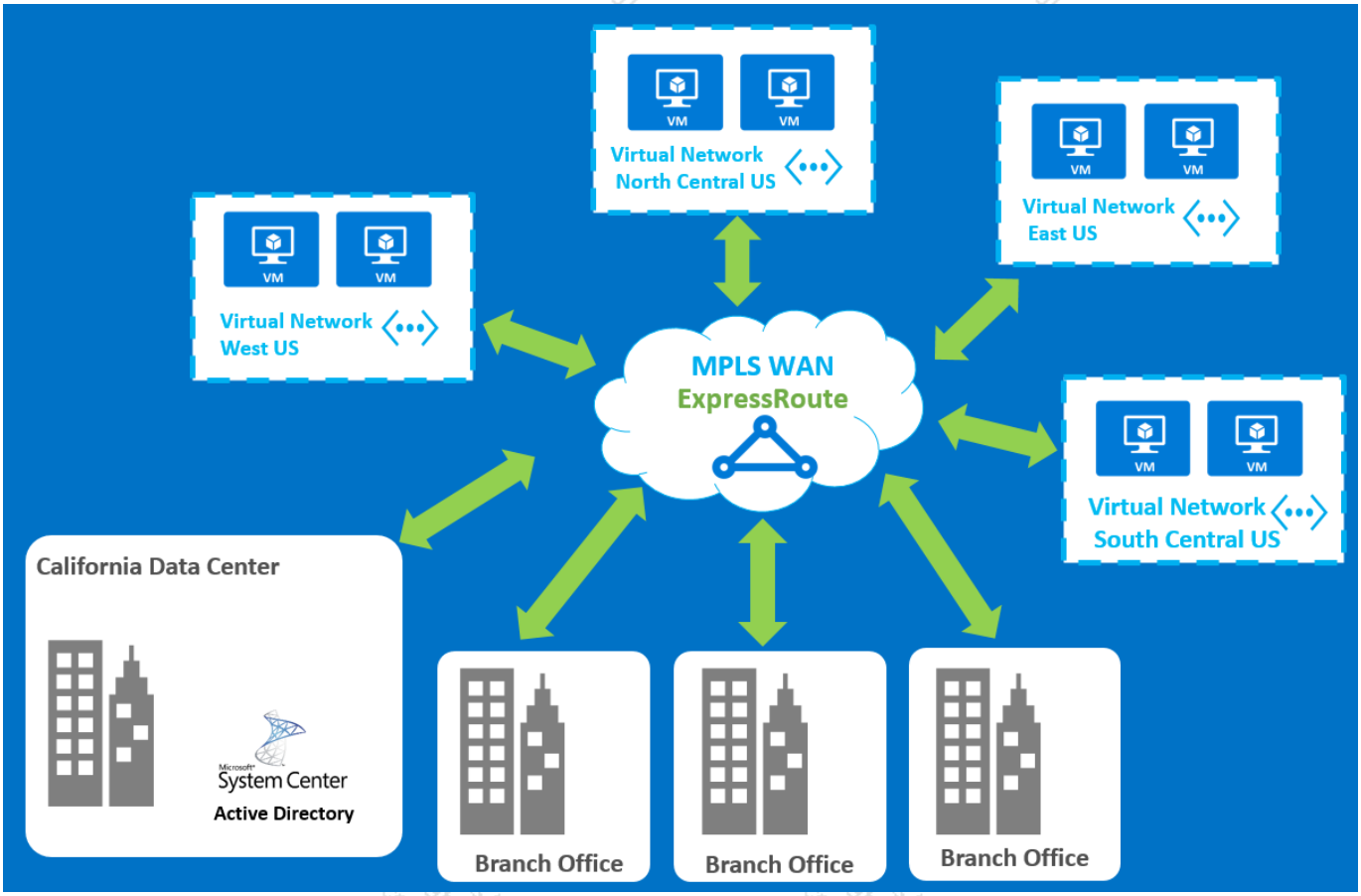


FIGURE 8.3: DEPLOYING EXPRESSROUTE

Each region should have at least two domain controllers configured within an availability set. Active Directory sites and site links should be configured to authentication to the local DCs first.

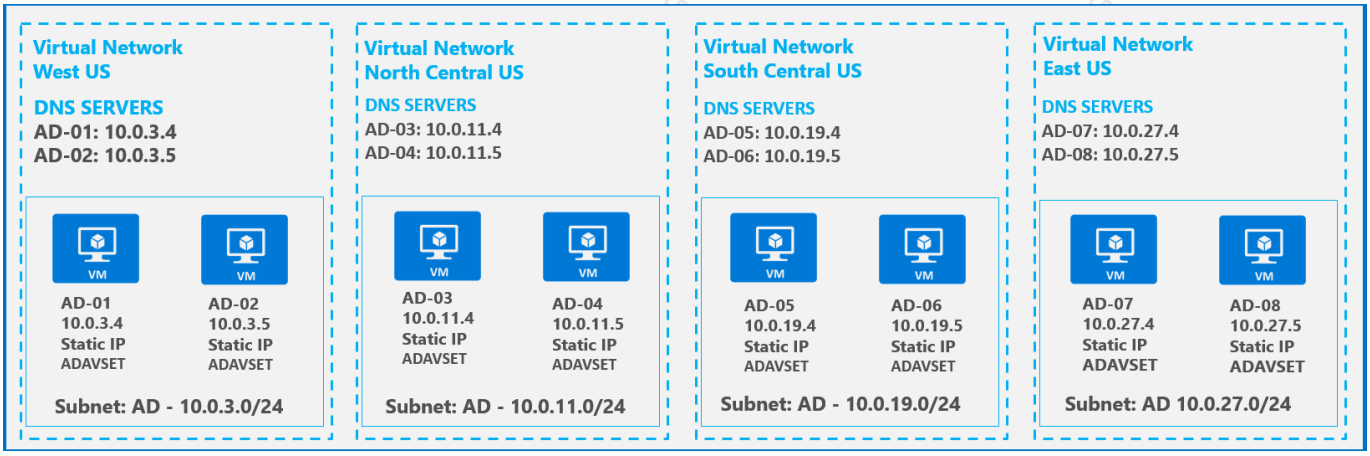


FIGURE 8.4: DEPLOYMENT OF ACTIVE DIRECTORY

The CRM webservers are deployed with auto scale enabled and configured using the internal load balancer. SQL Always On is configured using the internal load balancer.

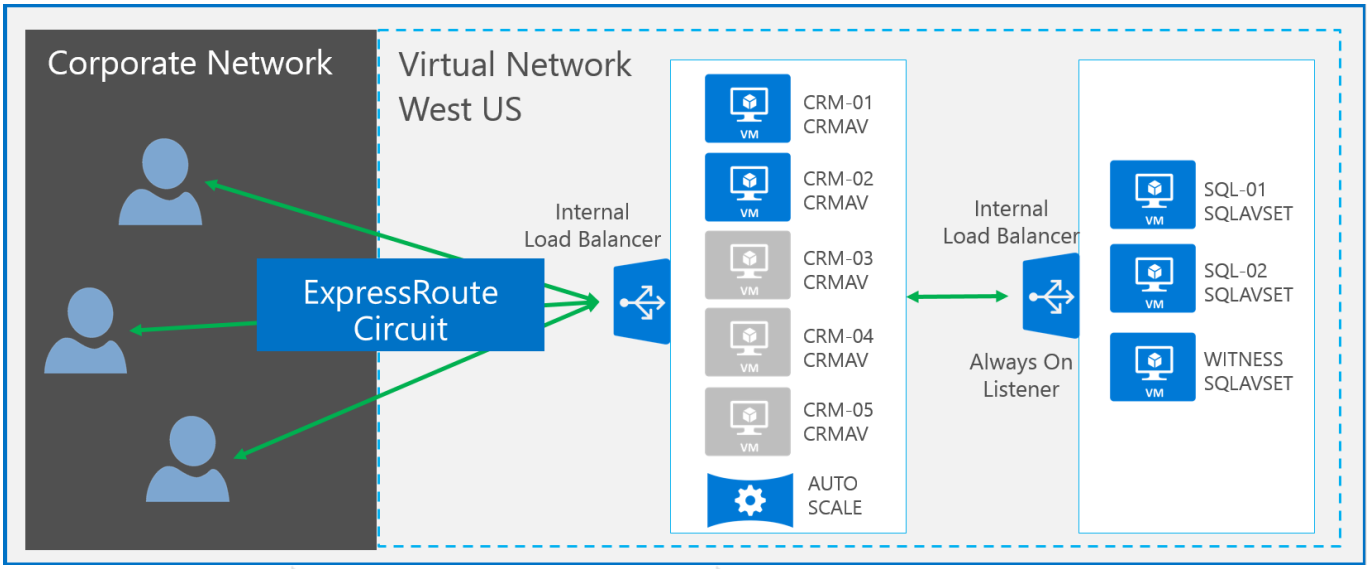


FIGURE 8.5: CUSTOM CRM APPLICATION DEPLOYMENT

Checklist of Potential Benefits

Increased Security/Privacy and Network Performance for Enterprise Connectivity

Azure ExpressRoute provides a dedicated connection between an organizations network to Microsoft Azure through an ExpressRoute partner. Your connection is dedicated bandwidth between your infrastructure and Microsoft Azure. This committed bandwidth and additional control gives you predictable network performance.

Your connection is private. Traffic that flows between your on-premises network and Microsoft Azure does not traverse the public Internet and is isolated using industry standard VLANs. ExpressRoute connections support high throughput and low latency for some of the most bandwidth hungry applications and workloads.

For workloads where large amounts of data are leaving the Microsoft Azure data center ExpressRoute can save significant amounts of money due to the included bandwidth and lower bandwidth costs that come with an ExpressRoute circuit.

Public Peering

In addition to providing private connectivity between your on-premises network and your Azure virtual networks you can enable public peering which provides private connectivity to a number of Azure public services.

Cross Region Connectivity

Azure ExpressRoute makes it simple to connect multiple virtual networks to the same ExpressRoute circuit as long as the virtual networks are on the same continent. This allows you to extend your on-premises network to multiple Azure regions.

Network Service Provider Model of ExpressRoute Provides a Simple Integration Point

Fabrikam already has an existing MPLS VPN with a Network Service Provider. With ExpressRoute choosing the Network Service Provider model the provider is responsible for onboarding your network into Azure. They take care of the routing configuration and ensuring everything works. You are still responsible for choosing your service tier and creating the circuit in Azure that they will setup. Bandwidth options for a Network Service Provider range from 10 Mbps all the way up to 1 Gbps. With a network service provider bandwidth is unlimited and not separately charged.

When a virtual network in Azure is configured in this manner the virtual network will be accessible to you just like any other site on your wide area network.

Checklist of Preferred Proof of Concept Potential Flow/Scope

- Objectives
  - Identify connectivity and latency requirements for proof of concept (regions and site connectivity).
  - Configure AD sites/subnets to ensure efficient replication and authentication for the sites.
  - Deploy custom CRM intranet based workload securely and without over provisioning.
  - Demonstrate that Azure Virtual Machines and Virtual Networks can deliver the connectivity requirements for the solution.
  - Address and resolve technical issues involved with connecting and deploying the virtual machines in the proof of concept.
- Flow/Scope of the proof of concept (a list of 2-3 bullets)
  - Contact Network Service Provider and sign up for Azure ExpressRoute
  - Provision a circuit in Azure and work with Network Service Provider to connect the new circuit to the existing MPLS network.
  - Identify services (virtual machines), regions and on-premises sites to design the network architecture.
  - Configure Azure Virtual Networks for connectivity
    - Design subnets for each virtual network to accommodate growth but not overlap any of the on-premises sites or other virtual networks.
    - Define the local network sites that the virtual networks will connect to. This may be other virtual networks (connecting across regions) or connecting to one or more of the branch offices.
    - Create the dynamic gateways at each virtual network site.
    - Connect each virtual network to the ExpressRoute circuit using the New-AzureDedicatedCircuitLink PowerShell cmdlet.
  - Deploy the virtual machines for Active Directory. There should be two domain controllers in an availability set for each virtual network. The virtual network should reference the IP addresses of both DCs. Sites and site links should be configured per virtual network to ensure Active Directory traffic stays local.
  - Deploy the virtual machines for the custom CRM intranet based workload into a virtual

network using an internal load balancer configuration for the web servers and another internal load balancer for the SQL Server Always On listener.

- Conditions of satisfaction / success criteria for the PoC
  - Demonstrate that Azure Virtual Networks and Virtual Machines can provide the connectivity requirements and capacity for their virtualization.
  - Ensure that AD replication and authentication occurs.
  - Ensure the CRM intranet solution scales without overprovisioning and connectivity is secure.
- Resources / Bill of Materials that you would use
  - Azure Virtual Networks and Virtual Machines
  - Azure ExpressRoute and Network Service Provider partner
  - Partner / MCS

Checklist of Preferred Objection Handled

- **We have a national business and we need connectivity that can accommodate coast-to-coast.**
- Microsoft Azure ExpressRoute can provide connectivity to virtual networks on the same continent. The virtual networks do not even have to reside in the same Azure Subscription.
- **I need to deploy an intranet-based solution and I have heard that Azure requires an on-premises load balancer for internal facing workloads.**
- Microsoft Azure now supports configuring an internal load-balancer using an internal IP address from your virtual network. You can load balance up to 50 virtual machines in a single load-balanced set.
- **I have heard that the public IP address of an Azure deployment can change and break my application.**
- Azure virtual machines now support reserved IP addresses. Reserved IPs allow you to assign an IP address to a virtual machine deployment as the public IP. Even if you shut down all of the virtual machines or delete them and recreate them you can re-use the reserved IP address.
- **My workloads require static IP addresses. I have heard Azure does not support this scenario.**

- Microsoft Azure now supports deploying virtual machines with static IP addresses in virtual networks.
- **Network security is critical to our business. Is Azure secure?**
- Customers often make broad statement that we cannot use public cloud because of the security concerns. We need to make sure we understand their specific concerns. Usually it fall in either of the four buckets
- **Trust** – To build trust make sure customer is aware of Microsoft history & experience of delivering cloud services at scale, take them to datacenter tours and take accountability of their success.
- **Privacy** - Privacy is one of the foundations of Microsoft's Trustworthy Computing. Microsoft has a longstanding commitment to privacy, which is an integral part of our product and service lifecycle. Share the Microsoft Azure Privacy Statement that describes the specific privacy policy and practices that govern customers' use of Microsoft Azure.
- **Compliance** - Microsoft partners with customers to help them address a wide range of international, country, and industry-specific regulatory requirements. Microsoft provides Microsoft Azure customers with detailed information about our security and compliance programs, including audit reports and compliance packages, to help customers assess our services against their own legal and regulatory requirements.
- Security of Infrastructure and services - Microsoft Azure runs in geographically dispersed datacenters that comply with key industry standards, such as ISO/IEC 27001:2005, for security and reliability. They are managed, monitored, and administered by Microsoft operations staff (Global foundation Services) that have years of experience in delivering the world's largest online services with 24 x 7 continuity.
- For more information, visit Microsoft Azure Trust Center and familiarize yourself with Microsoft Azure Security practices. (Links are provided further in this section)
- **AWS supports setting ACLs within subnets of their VPC.**
- Azure supports setting ACLs on endpoints. As a workaround you can isolate networks in this manner. You can also use the firewall within the guest OS (if Windows you can use Group Policy).

Reference Links: https://azure.microsoft.com/blog/new-windows-azure-network-security-whitepaper/

Reference Links: http://azure.microsoft.com/support/trust-center/

Customer Quote

“With our Microsoft cloud infrastructure, we have reduced our IT costs by 75 percent and gotten out of the business of owning so much IT stuff" – Craig Jones

Lab: Deploying Network Components for Use in Azure Solutions

Scenario

Your newest client has purchased a third-party web application that they have been custom branded and is ready for deployment. The web application is hosted on Linux servers using nginx as the web server. The CTO of your client’s company has specifically requested that the solution is triple-redundant at a minimum with three load-balanced machines hosting the web application.

Objectives

- Create an ARM Template for a Linux VM.
- Use the ARM copy Functionality to Duplicate Resources.
- Deploy a Load Balancer Resource Bound to Copied VMs.

Lab setup

Estimated Time: 60 minutes

Virtual machine: **20535A-SEA-ARCH**

User name: **Admin**

Password: **Pa55w.rd**

The lab steps for this course change frequently due to updates to Microsoft Azure. Microsoft Learning updates the lab steps frequently, so they are not available in this manual. Your instructor will provide you with the lab documentation.

Exercise 1: Create an ARM Template for a Linux VM

Exercise 2: Duplicate the VM Resources

Exercise 3: Create a Load Balancer Resource

Exercise 4: Cleanup Subscription

Review Question(s)

Module review and takeaways

Review Question(s)