This document is a treatment for a video that shows commonly used Azure networking services and demonstrates their benefits.

As a treatment, it focuses more on the message we intend to convey and less on presentation elements like visuals and the exact wording of the narration.

Only a few abbreviations are used because much of the message is likely to be conveyed by the narration. If an abbreviation is needed to make a visual element fit, the narration should be adjusted to match.

Section headers are used to organize the message and are not intended to be included in the video. Think of them as scene headers, i.e. sluglines, in a screenplay or video script.

To make it easier to find text that can benefit by being supported with visual elements, such blocks of text contain the phrase **SHOWN HERE** _.

Azure networking for data centers

Many organizations have an on-premises data center, such as the one **SHOWN HERE**. The networking environment for a datacenter is usually divided into logical security zones. Typically, there is an internal security zone that contains the internal and trusted networked elements and a perimeter zone. A perimeter zone is often referred to as a "demilitarized zone" or DMZ because it shields the internal zone from untrusted accessors.

Physical components in a datacenter

The datacenter and other networked components in the organization connect to the Internet via physical devices on a physical network. The types of devices are routers, switches, firewalls, and so on that control the flow of network traffic between the logical security zones.

An Azure virtual network for a datacenter

Azure provides virtual networks with the same kind of logical security

zones while managing the physical network and components that support them.

While there is only one virtual network **SHOWN HERE**, it is common to have multiple virtual networks. If there is more than one Azure virtual network, each virtual network is isolated from the others. Hence, the network traffic flowing in and out of one virtual network does not interfere with the others.

When an Azure virtual network is initially set up, it is, by default, connected to the internet. You can modify that connection. You can implement and manage your own firewalls to control the flow of traffic between zones, if you choose. In Azure, firewalls are implemented as virtual machines, or VMs.

VMs built and optimized for a special purpose, such as providing firewalls, are called network virtual appliances, or NVAs. The Azure Marketplace has pre-configured firewall NVAs from several vendors that can be deployed in your virtual network.

An Internet-facing 3 tier application

In the example **SHOWN HERE**, an Internet-facing 3 tier application is deployed in the on-premises datacenter. Servers, both physical and virtual, are deployed to run applications.

The 3 tiers used by the application are presentation, business logic, and data. The presentation and business logic tiers are deployed in the DMZ, whereas the data tier is deployed in the internal zone. Internet traffic communicates inbound to the presentation tier, but not with the business logic or data tiers.

Within a zone, the network could be segmented into separate virtual local area networks or VLANs. And, the presentation and business logic tiers might be deployed in different VLANs. A switch, firewall, or both might control the flow of traffic differently between the VLANs.

The business logic tier communicates outbound to the internet, whereas

the data tier doesn't communicate with the internet at all. It only communicates with the business logic tier.

Load balancing with in Azure

For the high availability, multiple servers are added in each of the 3 tiers, as **SHOWN HERE**.

The example application includes multiple servers deployed in each tier with a load balancer that balances traffic across the servers in each tier.

In Azure, you can deploy the same application, but all of the servers are virtual servers and the network segments are subnets rather than VLANs. Similar to your on-premises application deployment, you can deploy the tiers into different subnets. You can load balance any network traffic to different servers in the same tier with an Azure load balancer.

If you're load balancing web traffic, you can offload SSL processing to an Azure application gateway, and inspect the traffic for security threats. Both load balancer and application gateway regularly check the response of each server in the tier. If a server stops responding, both services stop sending traffic to the server. You can use the two services together for higher scale, availability, security, and performance.

More ways to increase availability with Azure

As is **SHOWN HERE**, for additional levels of availability and performance, you can deploy VMs for a tier across multiple Azure regions, and direct traffic across the regions with Azure Traffic Manager.

Azure provides several platform as an application services, or PaaS services. If your application uses PaaS services for each tier, you may not need VMs at all.

Azure DNS

In an on-premises datacenter, you may have a DNS server in your perimeter zone that resolves name lookup requests for internet-facing

services. You could deploy a VM in your Azure perimeter zone with DNS resolver capability.

However, rather than managing a DNS server, you can use the Azure DNS service. It resolves public name lookup requests, but because it's a service, you don't have to manage VMs.

Azure for internal use

You no doubt have applications in your on-premise datacenter that are for internal use only. Such applications don't communicate with the internet, but like the application in the perimeter zone, you can use the Azure Load Balancer and Application Gateway to load balance internal only traffic too, as **SHOWN HERE**. You can also use the Azure DNS service for resolving internal-only host names.

Controlling access to a datacenter

In the configuration **SHOWN HERE**, the only way to access either zone in Azure is from the internet. In most cases, you don't want to allow any internet access to resources in the internal zone. Also you probably don't want to provide inbound internet access to all resources in the perimeter zone, such as to the business logic servers.

There are several ways you can provide access to your virtual network from your on-premises network. When you're just getting started with Azure, you can implement a point to site VPN connection from one or more individual computers in your organization.

A point to site connection requires no special hardware on your premises and typically doesn't even require changes to your existing firewall. Your computer connects to an Azure network gateway through a virtual private network, or VPN, over the internet. The gateway is deployed in your Azure virtual network. Once connected, each computer can access the VMs in the virtual network.

When several entities in your organization need access to the virtual network, managing many individual point to site connections can be

unwieldy. In this case, you can implement a site to site VPN connection.

A site to site connection does require you to have an on-premises gateway that connects to an Azure network gateway. Once the connection is established, any authorized entity in your organization can access the resources in the virtual network.

You use both point to site, and site to site, VPN connections to provide a secure tunnel over the internet between your on-premises gateway, or computer, and an Azure virtual network.

Azure ExpressRoute

If you don't want traffic between a virtual network and your premises or computers to traverse the internet, you can use the Azure ExpressRoute service. As **SHOWN HERE** ExpressRoute is a dedicated connection between an entity, a service provider, and Azure. Traffic never traverses the internet, even through a tunnel.

Azure Networking - The Big Picture

We've covered a few of the more common uses of Azure Networking, but if you need it, there's more. As you explore Azure Networking in depth, it helps to remember the following points...

- In Azure, a virtual network provides a secure boundary that separates your resources from Azure resources used by others.
- Azure DNS provides name resolution for your Azure resources.
- You can extend your on-premises network to your virtual network with:
    - a VPN tunnel through the internet provided by a VPN gateway
    - a dedicated, private connection provided by ExpressRoute
- You can provide scalability, high-availability, and performance for your applications with any combination of:
    - A load balancer to balance any network traffic
    - An application gateway to allow inspection and balancing of web traffic
    - Traffic Manager, for directing traffic across multiple regions