



Azure Networking Inside and Out

Mustafa Toroman

Saša Kranjac





Thank you, sponsors!

DATA ONE

Alegri



Nigel Frank
International

The Global Leader in Microsoft Recruitment

arvato
BERTELSMANN



Azure Saturday 2018



Speaker Introduction

- Mustafa Toroman
- Senior System Engineer @ Authority Partners
- @toromust
- <http://toroman.cloud/>
- Microsoft Azure MVP
- MCSE, MCP, MCSA, MCITP, MCSD, MCT, MS v-TSP



Speaker Introduction

- Saša Kranjac
- CEO and Security Expert @ Kranjac - IT Training and Consulting
- @SasaKranjac
- MCSE, MCP, MCSA, MCITP, MCT, MCT Regional Lead, Certified EC-Council Instructor, CEH

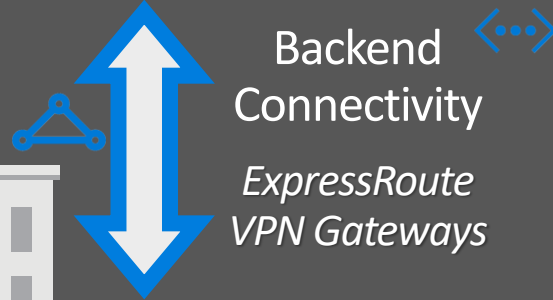
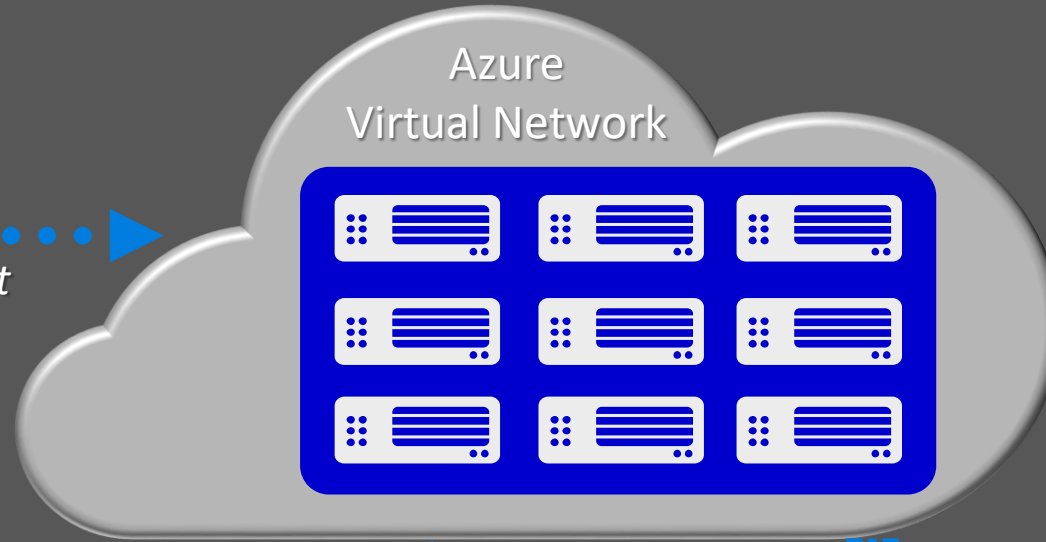




Users
Internet

Front-End Access

- Dynamic/Reserved Public IP addresses
- Direct VM access, ACLs for security
- Load balancing
- DNS services: hosting, traffic management
- DDoS protection



Virtual Network

“Bring Your Own Network”

Segment with subnets and security groups

Control traffic flow with User Defined Routes

Backend Connectivity

Point-to-site for dev / test

VPN Gateways for secure site-to-site connectivity

ExpressRoute for private enterprise grade connectivity



Public IP Addresses in Azure

Can be used for instance (VM) level access or load balancing

Instance-level IP

Internet IP assigned exclusively to a single VM Entire port range is accessible by default

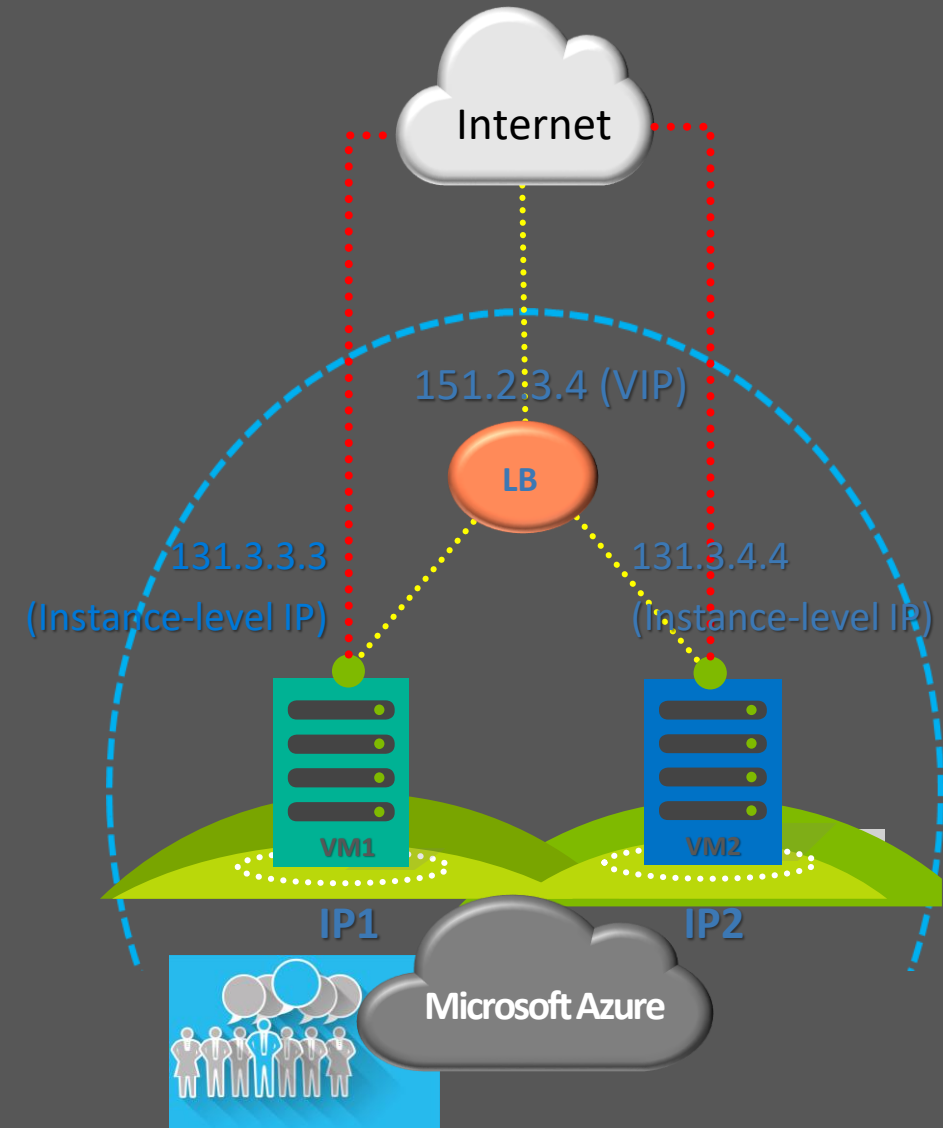
Primarily for targeting a specific VM

Load balanced IP (VIP)

Internet IP load balanced among one or more VM instances

Allows port redirection

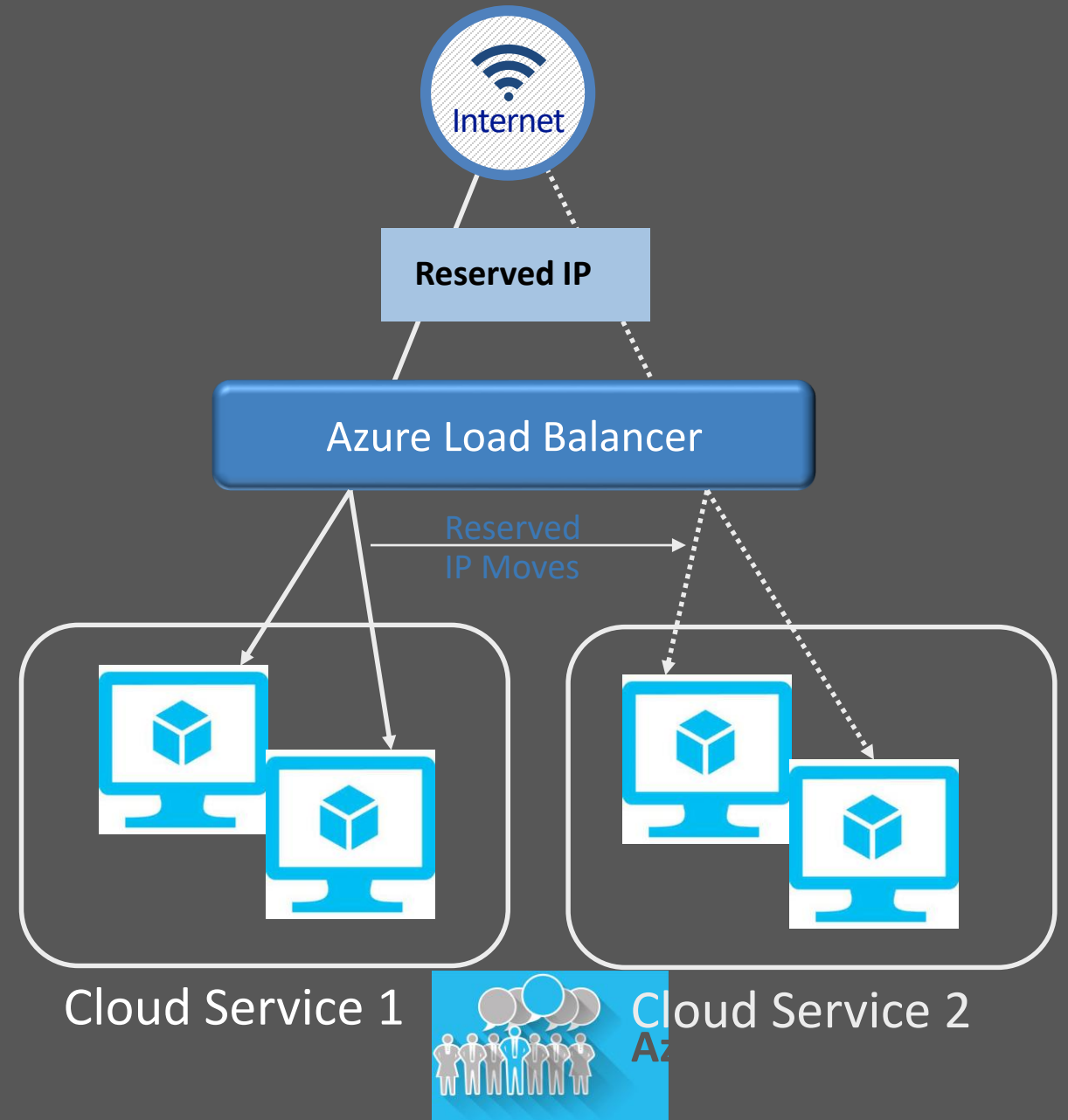
Primarily for load balanced, highly available, or auto-scale scenarios



Retain your IP addresses

IPs on existing services can be reserved

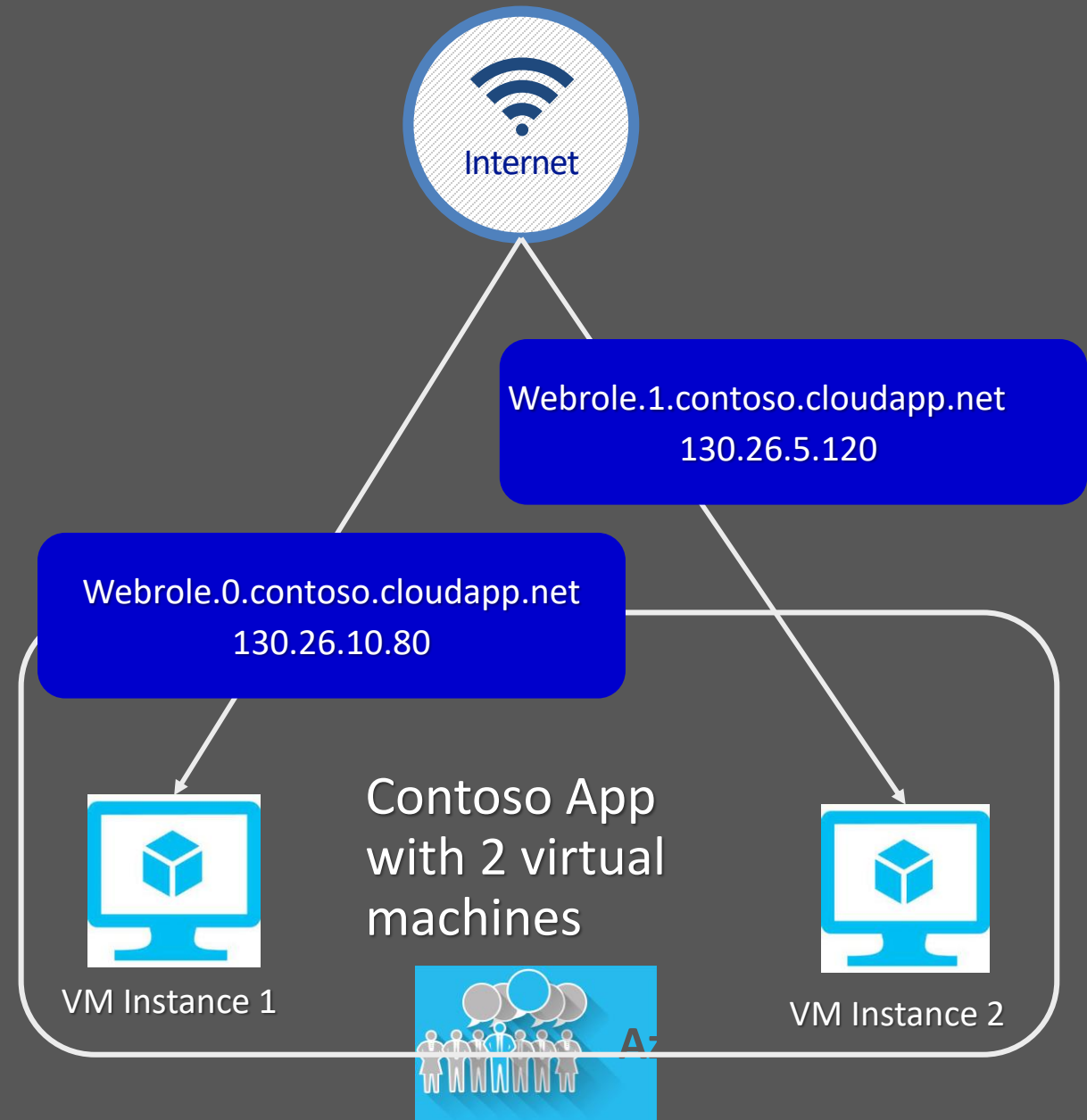
IPs can be moved between services in seconds



FQDN access to a virtual machine

Available for virtual machines and web/worker roles

Automatic DNS registration/de-registration during
scale-up, scale-down



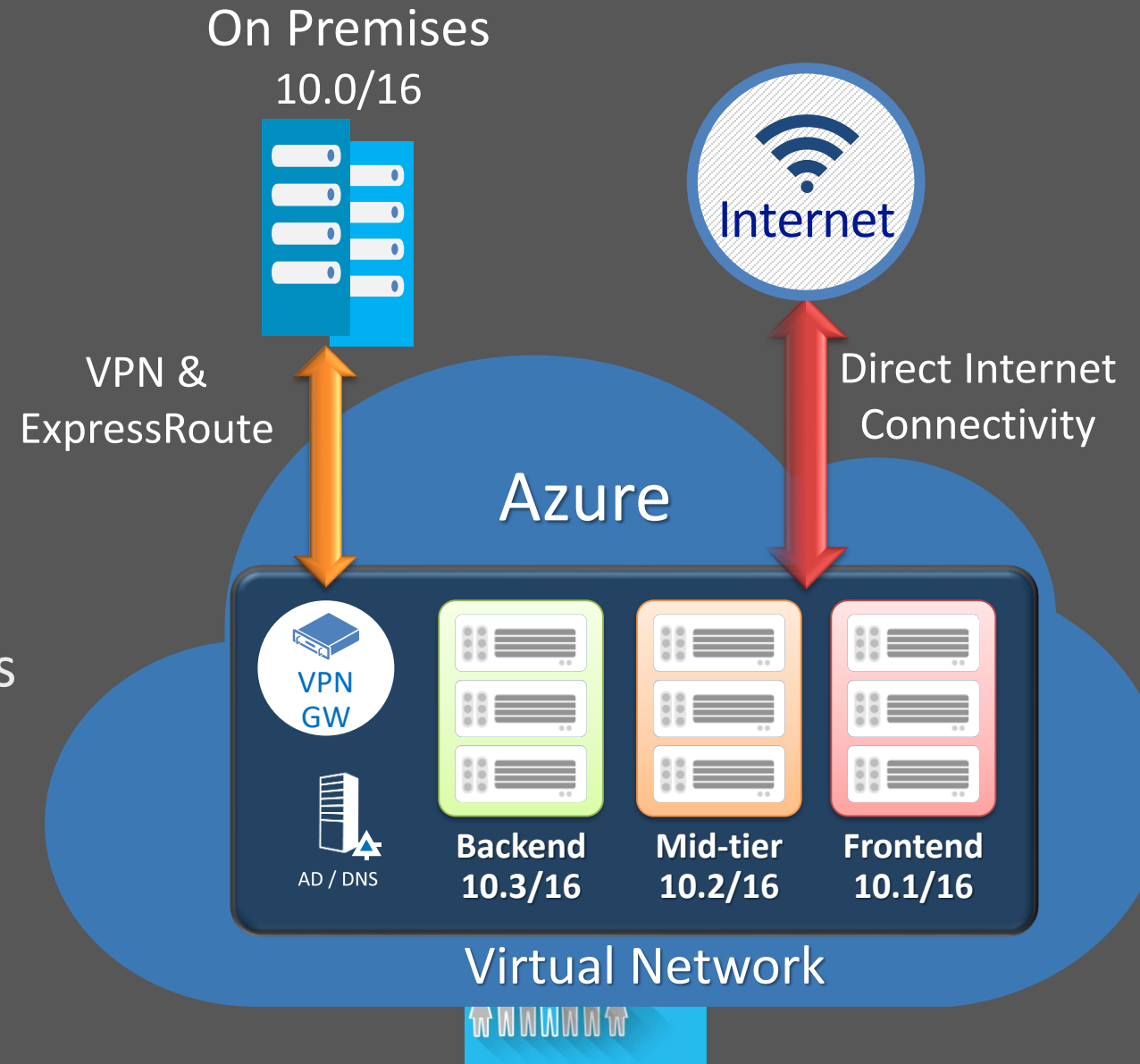
Bring your own network

Create subnets with your private or public IP addresses

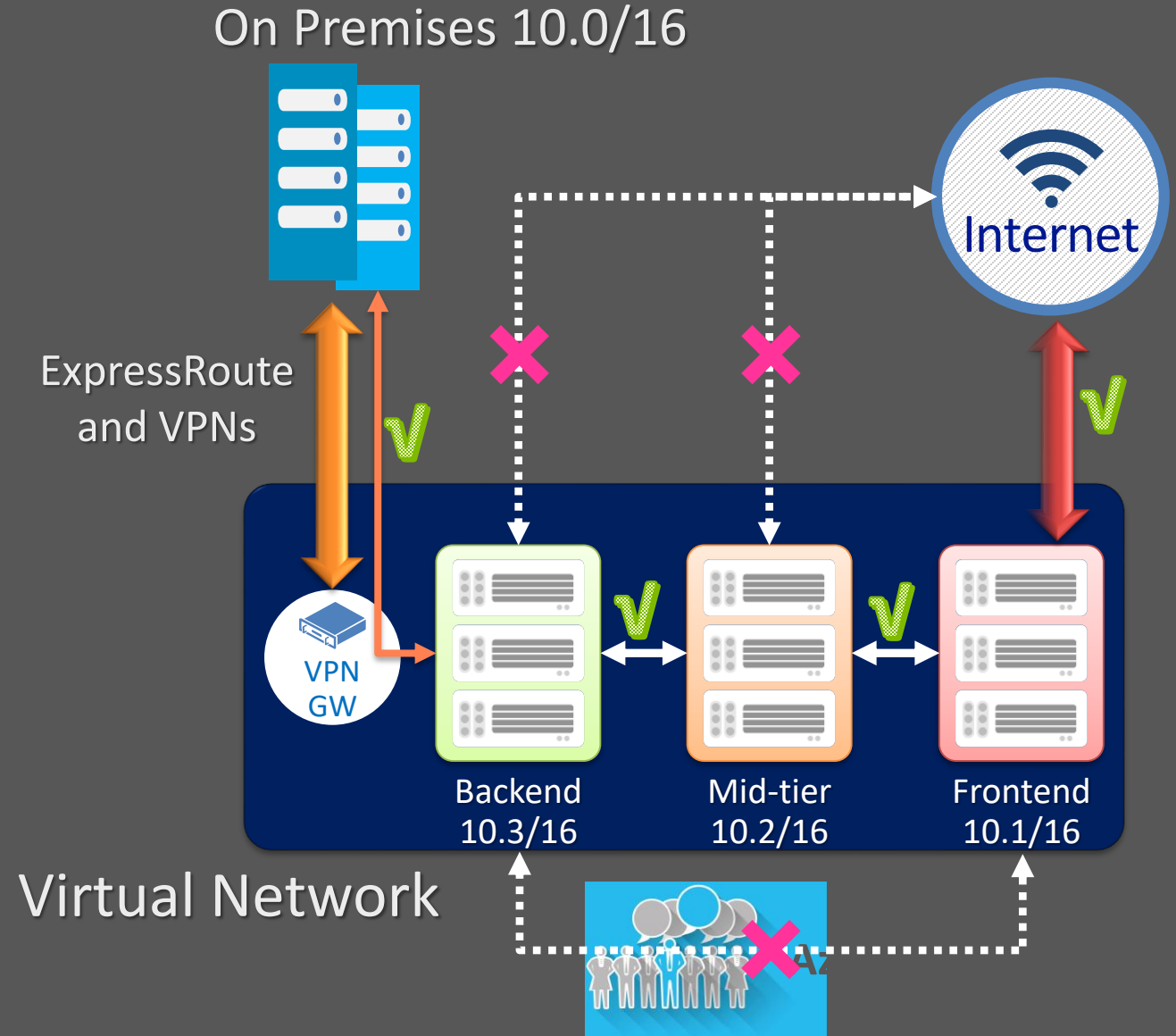
Bring your own DNS or use Azure-provided DNS

Secure with Network Security Group ACLs

Control traffic flow with User Defined Routes



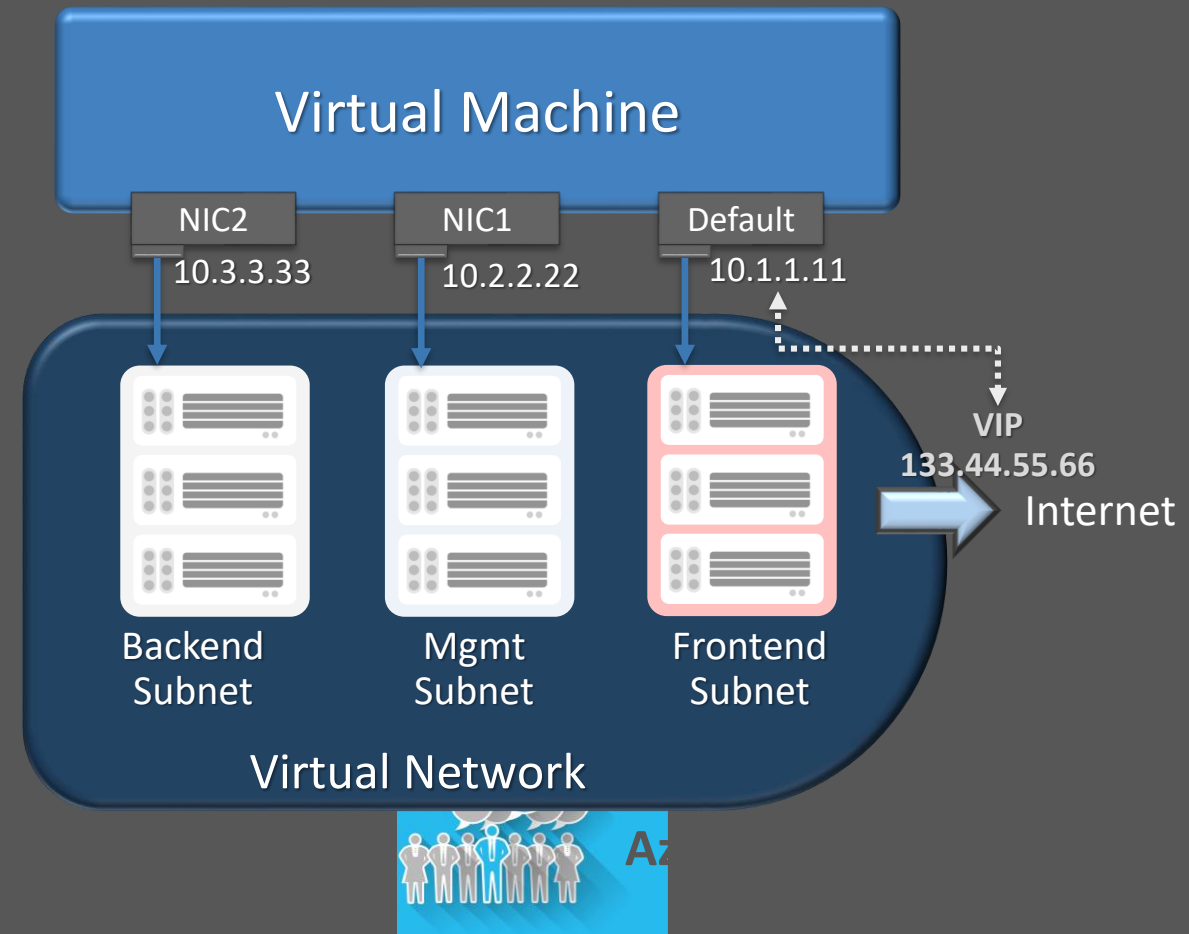
Segment network to meet security needs
Can protect Internet and internal traffic
Enables DMZ subnets
Associated to subnets/VMs and now NICs
ACLs can be updated independent of VMs

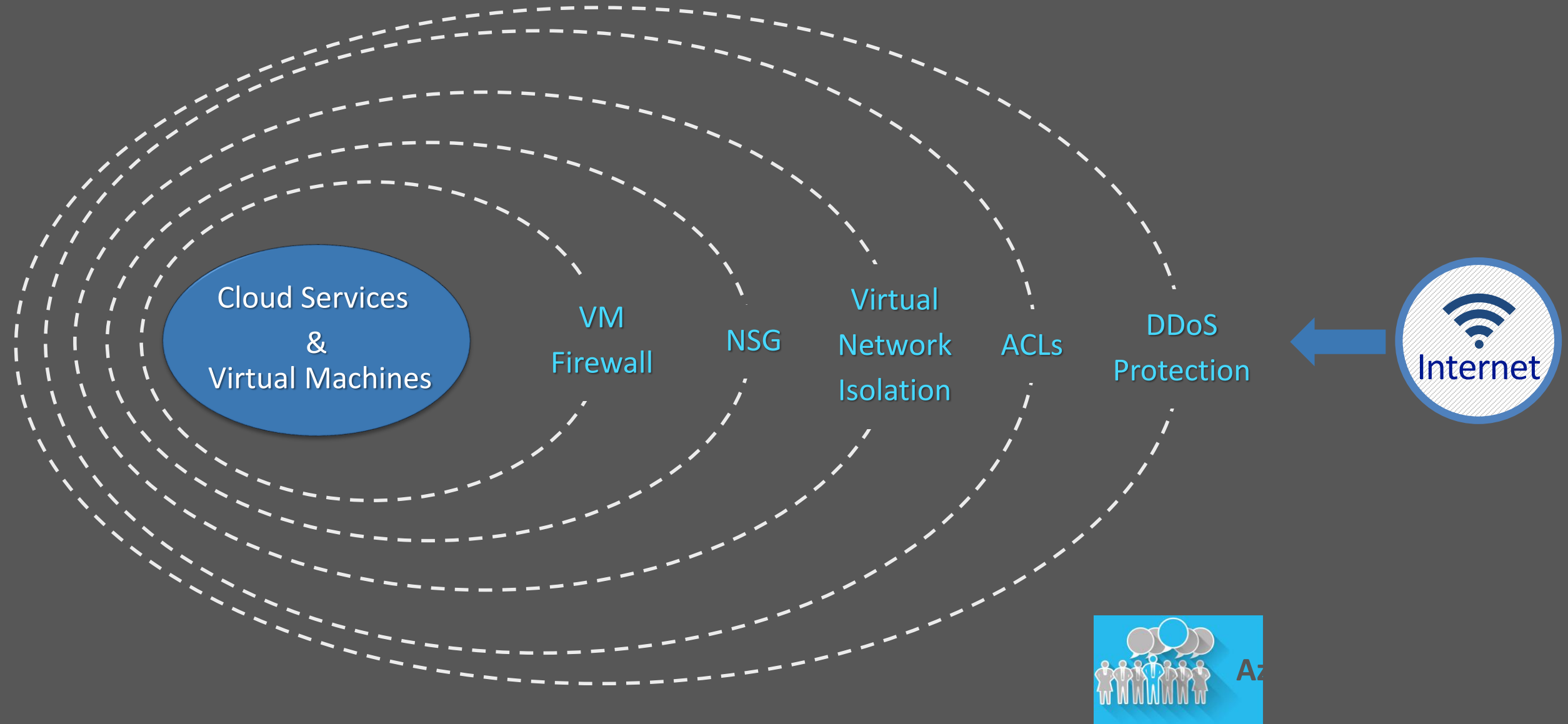


Up to 16 NICs per VM

NSG and Routes on all NICs

Can separate frontend, backend, and management





Overview

VMs that perform specific network functions

Focus: Security (Firewall, IDS , IPS), Router/VPN, ADC (Application Delivery Controller), WAN Optimization

Typically Linux or FreeBSD-based platforms

Scenarios

IT Policy & Compliance – Consistency between on premises & Azure

Supplement/complement Azure capabilities

Azure Marketplace

Available through Azure Certified Program to ensure quality and simplify deployment

You can also bring your own appliance and license

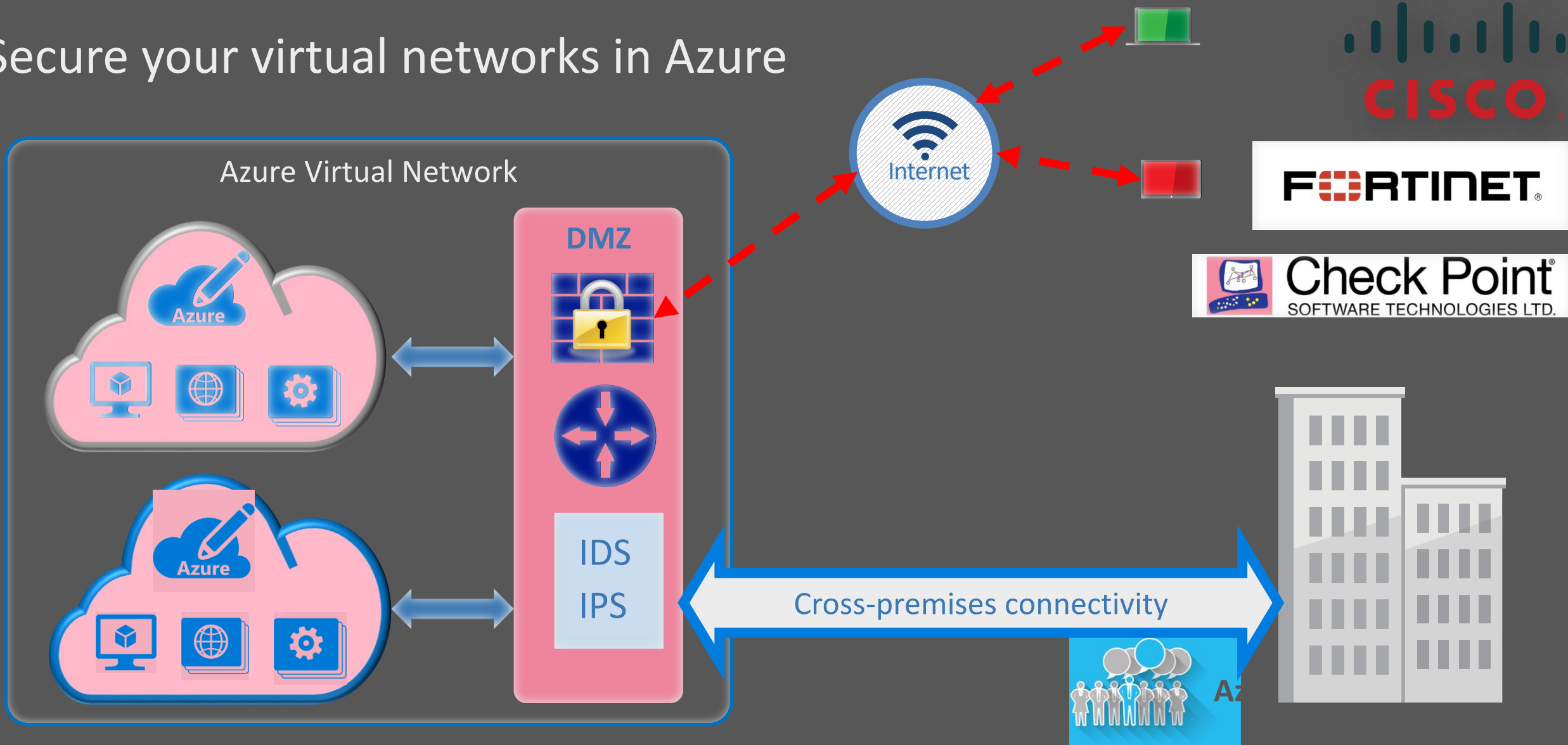
Microsoft
Azure

Certified

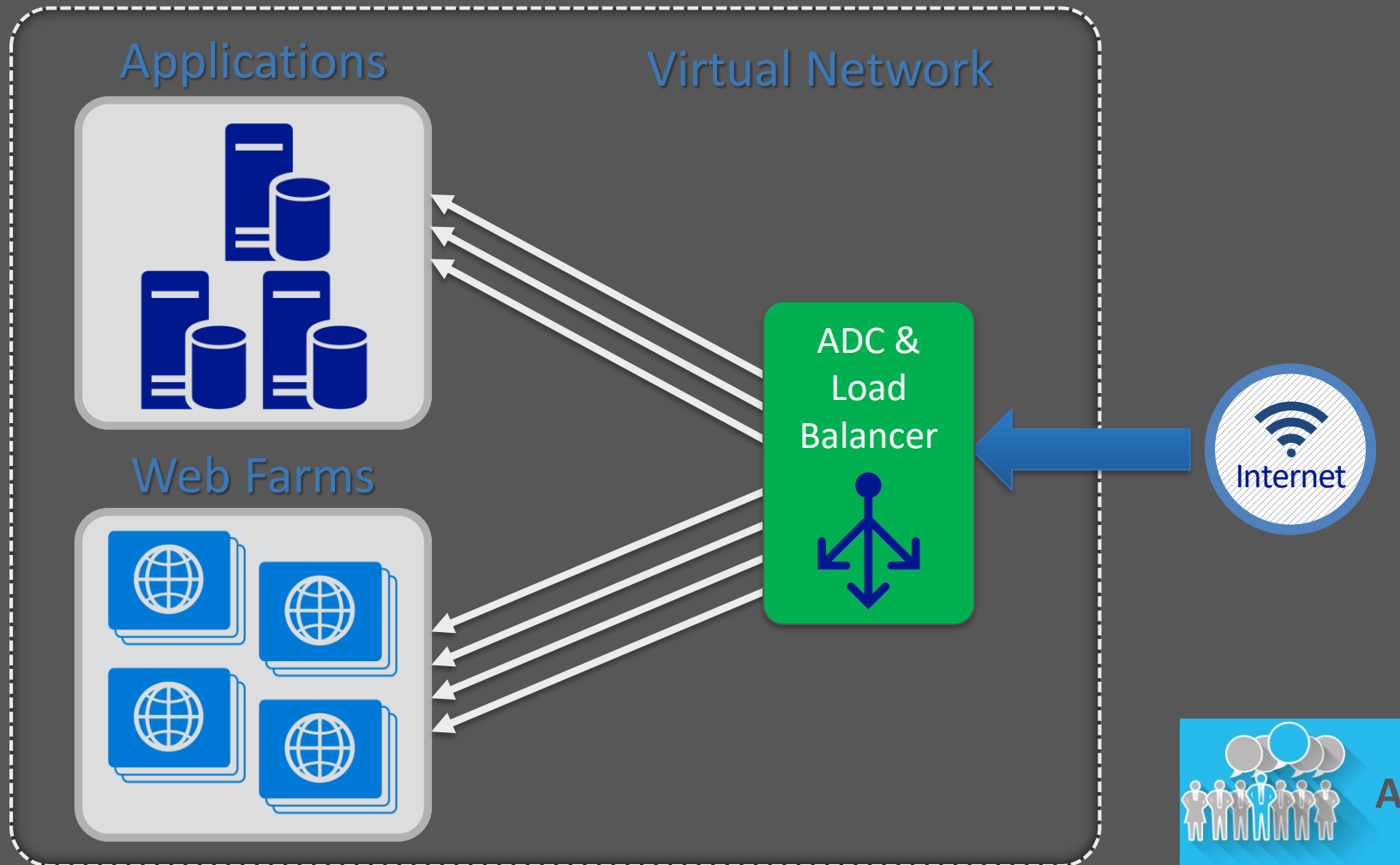


Virtual Appliances - Firewalls, IDS/IPS, VPNs

Secure your virtual networks in Azure











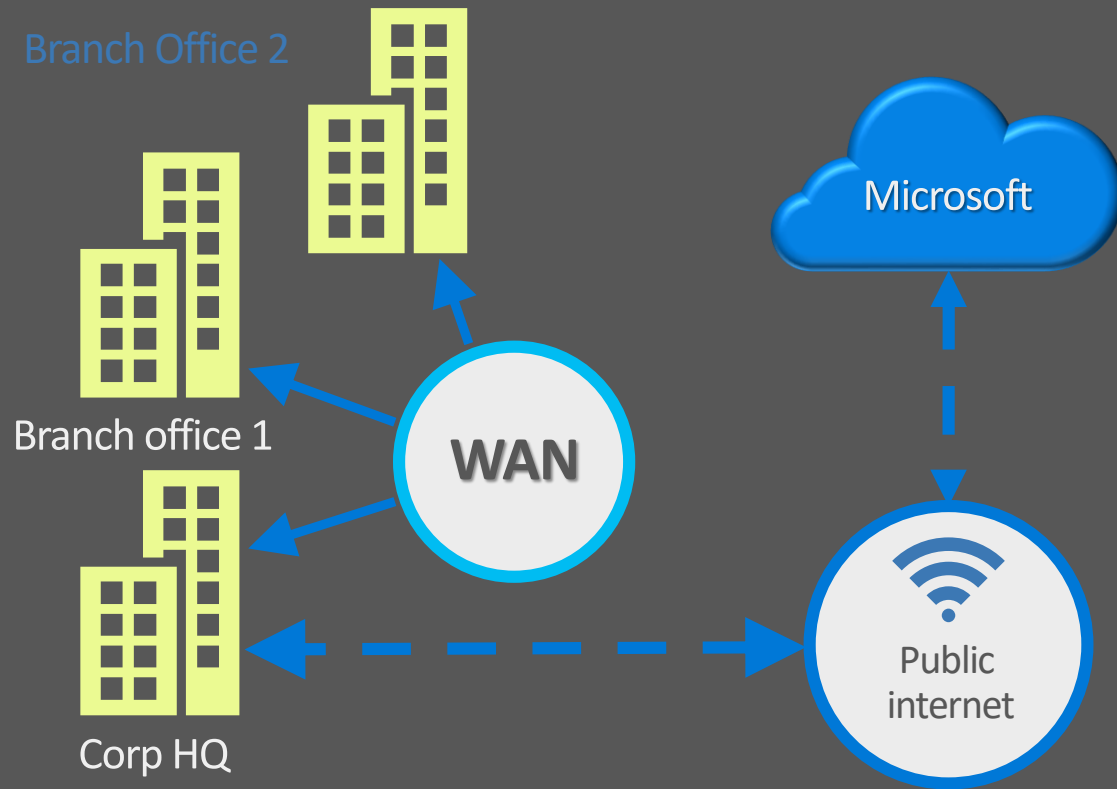
Scenario – Application Delivery Controller



Cross premises connectivity

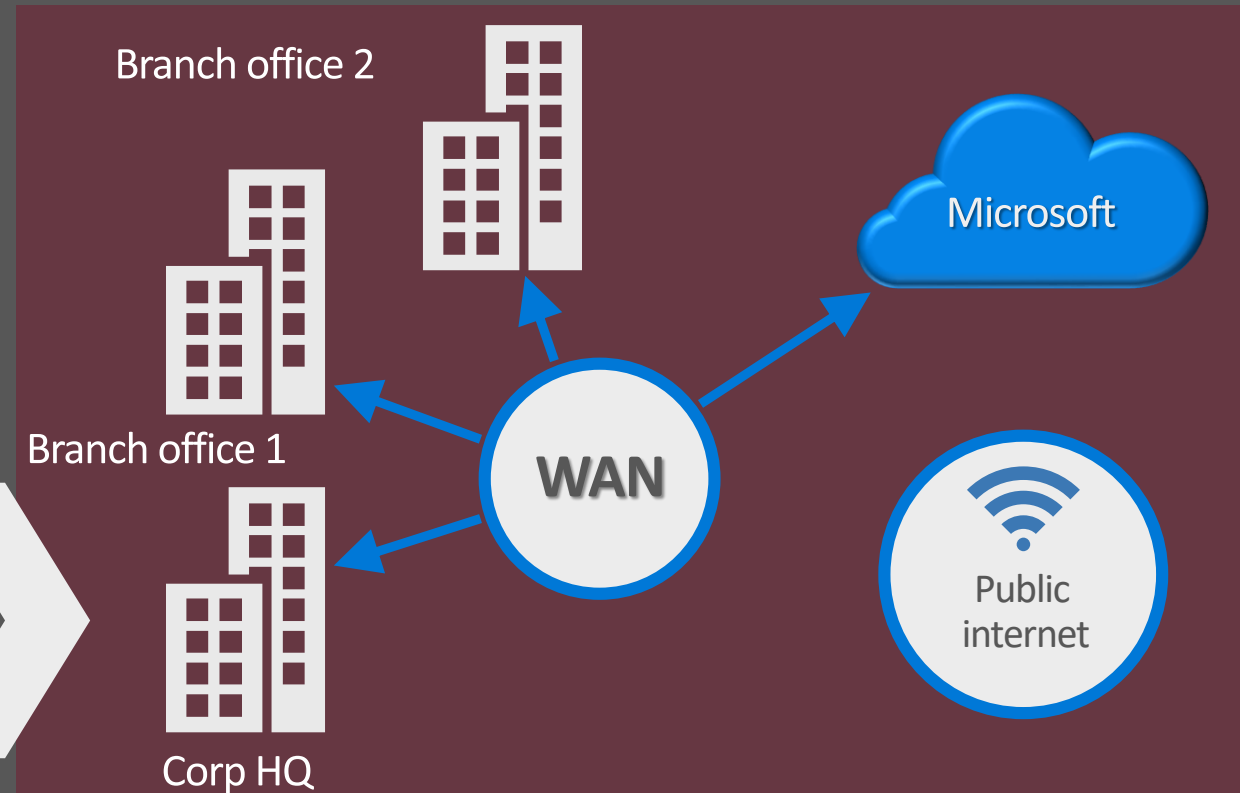


Cloud		Customer	Segment and workloads
	Internet Connectivity		<ul style="list-style-type: none"> • Consumers • Access over public IP • DNS resolution • Connect from anywhere
	Secure point-to-site connectivity		<ul style="list-style-type: none"> • Developers • POC Efforts • Small scale deployments • Connect from anywhere
	Secure site-to-site VPN connectivity		<ul style="list-style-type: none"> • SMB, Enterprises • Connect to Azure compute
	ExpressRoute private connectivity		<ul style="list-style-type: none"> • SMB & Enterprises • Mission critical workloads • Backup/DR, media, HPC • Connect to Microsoft services



IPsec VPN over Internet

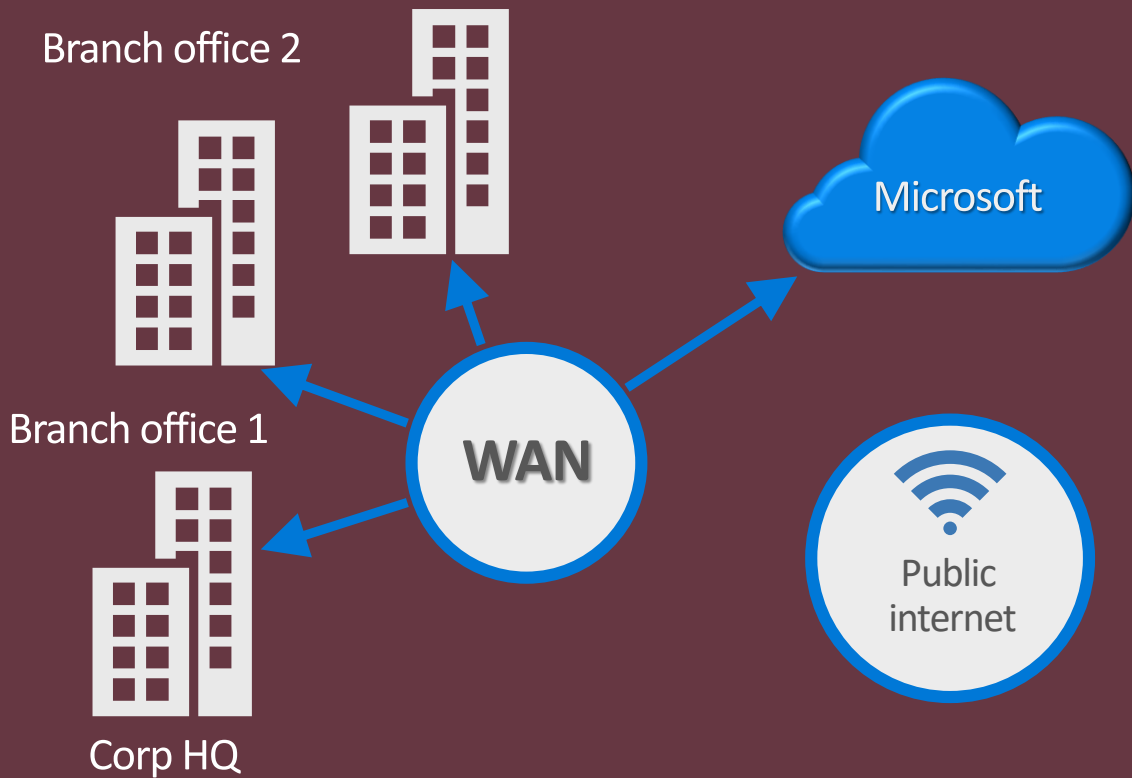
- ⌚ Encrypted data traverses Internet to reach Azure
- ⌚ Limited bandwidth and higher availability



Cloud on your WAN

- ⌚ Traffic flows directly from customer WAN to Microsoft
- ⌚ Reduces complexity
- ⌚ Lower latency, higher bandwidth and higher availability





ExpressRoute provides a private, dedicated, high-throughput network connection to Microsoft

Predictable performance



Security



High throughput



Lower cost



Az



Hammer Time!



<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>

<https://azure.microsoft.com/en-us/services/virtual-network/>

<https://docs.microsoft.com/en-us/azure/virtual-network/>

<https://docs.microsoft.com/en-us/azure/virtual-network/>

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

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices>

Q&A?



Thank you!

