ASE for compliant environments

April 11th, 2018

sourced

About the presenters

David Christensen

Cloud Architect, Sourced

David is a twenty year IT veteran who has helped a variety of enterprises transform and deliver tangible business results through Cloud and DevOps solutions. David continues to embrace and champion enterprise Cloud and DevOps solutions that not only impact Sourced Groups client's businesses, but also continue to position Sourced Group as a global technology leader. In addition, David is one of the organizers of the Toronto Azure Group.

Zach Koncir

Cloud Architect, Sourced

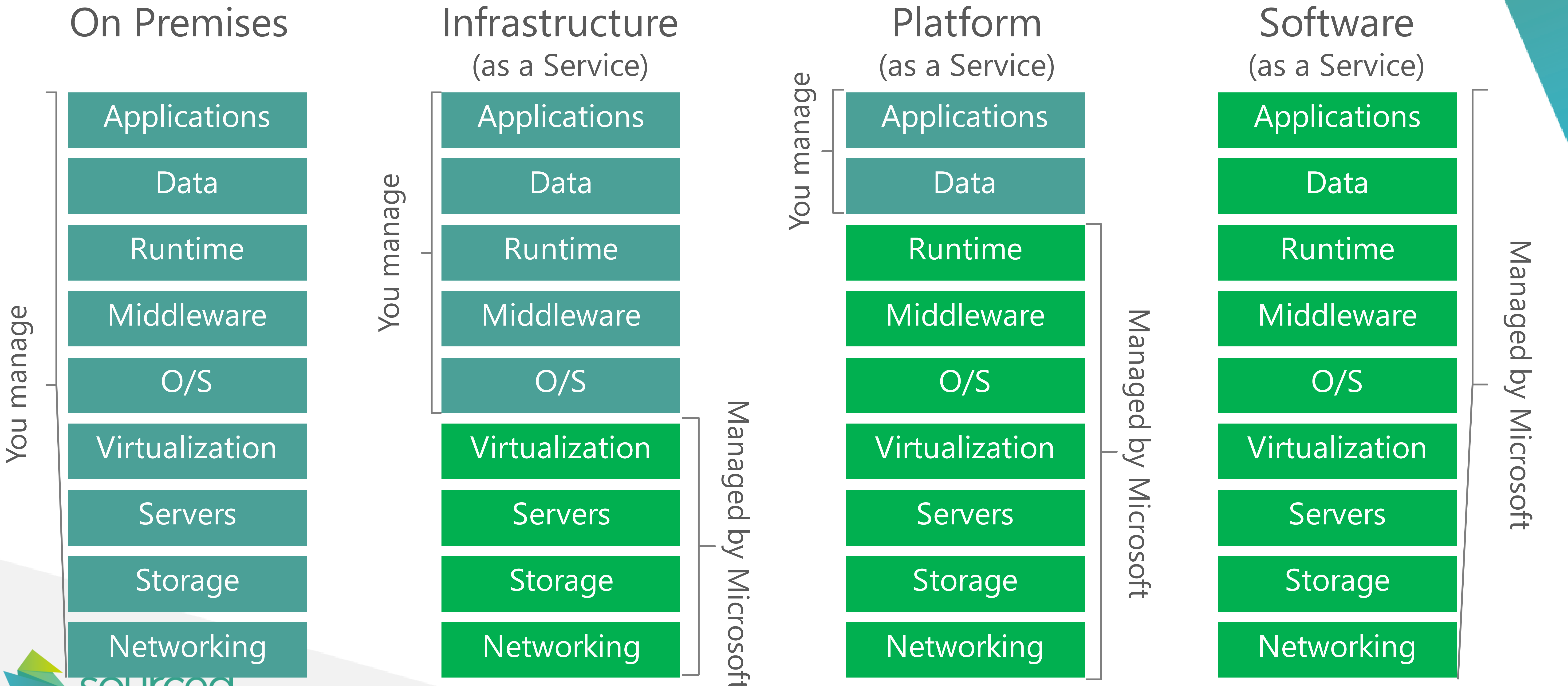
Zach is a technology professional with over 10 years of systems development experience who has focused heavily on public cloud solutions and automation. Zach has spent 2 years at Sourced Group delivering complex Cloud and DevOps transformative solutions for Canada's largest FSI's.

sourced

Agenda

- Background
- Challenge
- Intro to ASE
- ASE in compliant environments
- Demo
- Other considerations

Cloud Models



On Premises

You manage

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Infrastructure (as a Service)

You manage

- Applications
- Data
- Runtime
- Middleware
- O/S

Managed by Microsoft

- Virtualization
- Servers
- Storage
- Networking

Platform (as a Service)

You manage

- Applications
- Data

Managed by Microsoft

- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Software (as a Service)

Managed by Microsoft

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Azure App Service

- A cloud app platform for delivering modern enterprise apps across cloud and mobile devices.

- An integrated offering that delivers features and capabilities from a number of existing Azure services

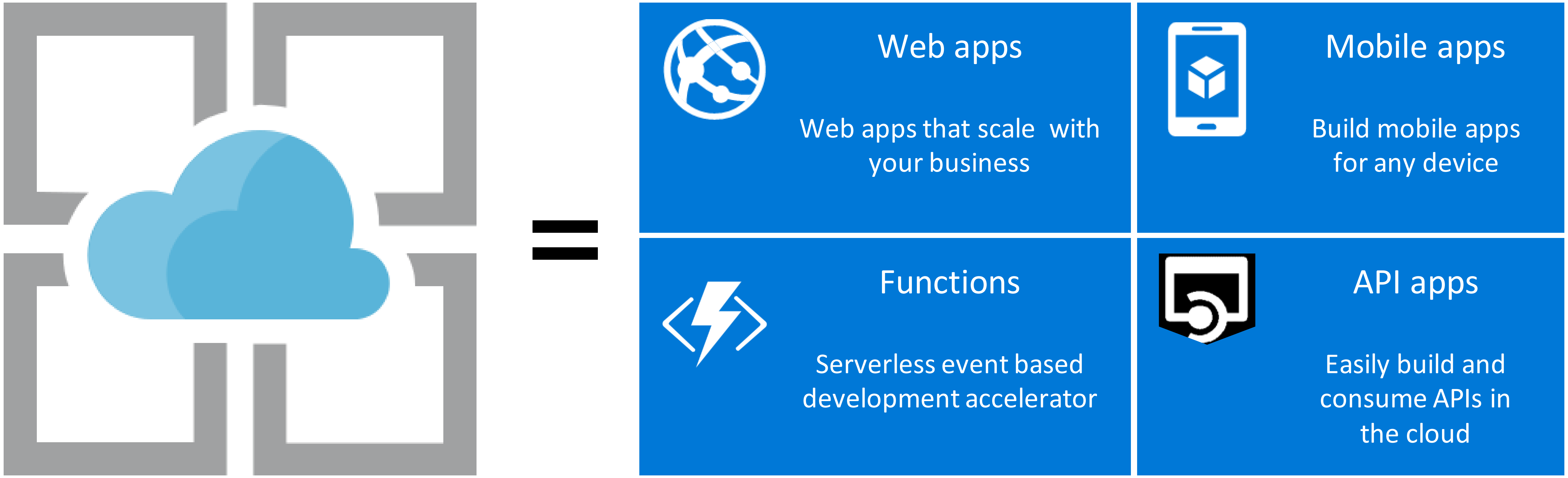
Enterprise Grade Apps

Fully Managed Platform

High Productivity Development

sourced

Azure App Service



Web apps

Web apps that scale with your business

Mobile apps

Build mobile apps for any device

Functions

Serverless event based development accelerator

API apps

Easily build and consume APIs in the cloud

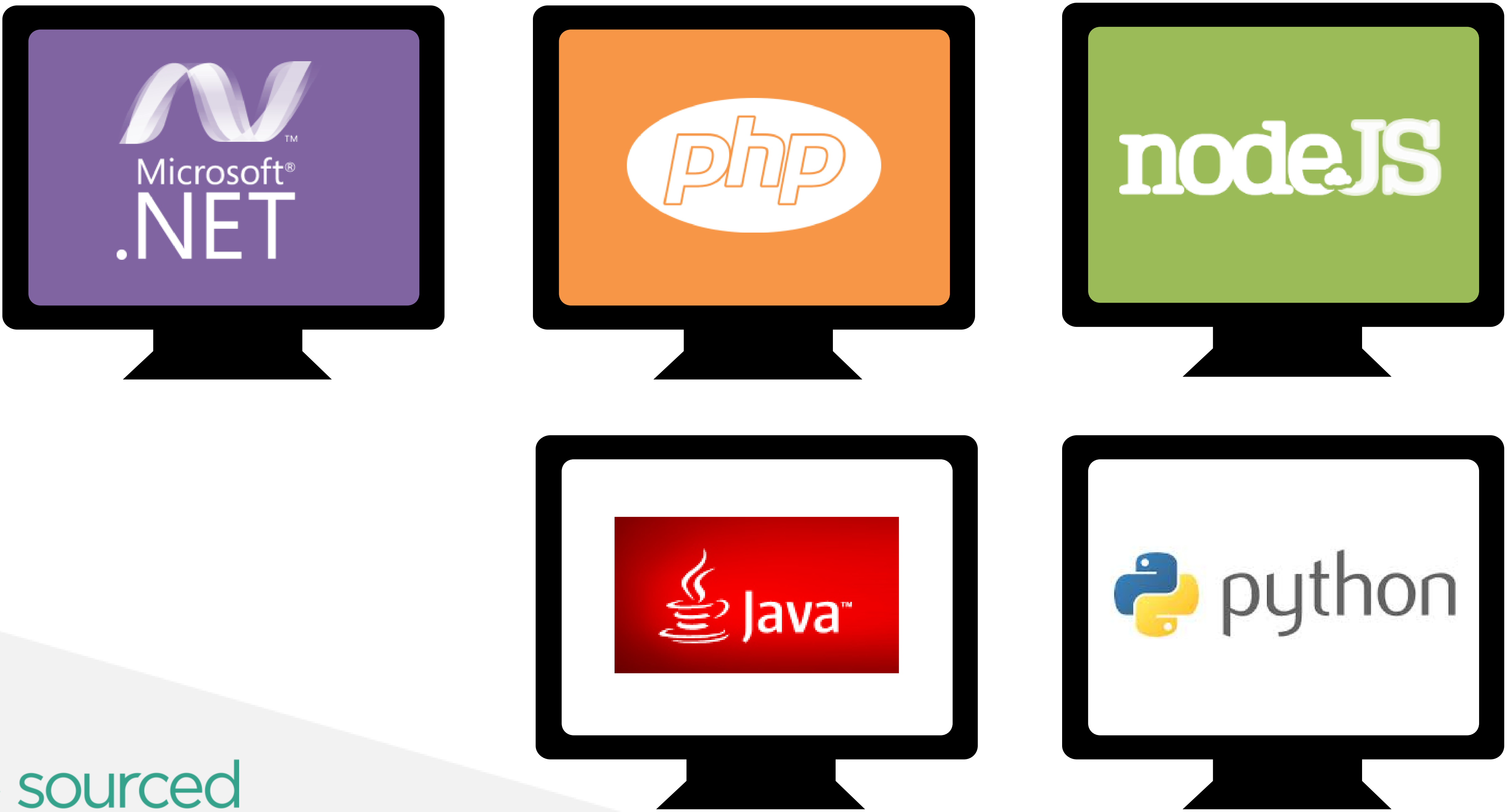
App Service Plan

- The core component of App Services:
- Represents the features and capacity of your Apps
- Can be shared across Apps or isolated for specific workloads
- Tiered service levels based on capacity and features…and price!
- All Apps in a Service Plan share the same resources
- Cost is defined by the service plan not the number of Apps you have

App Service Plan

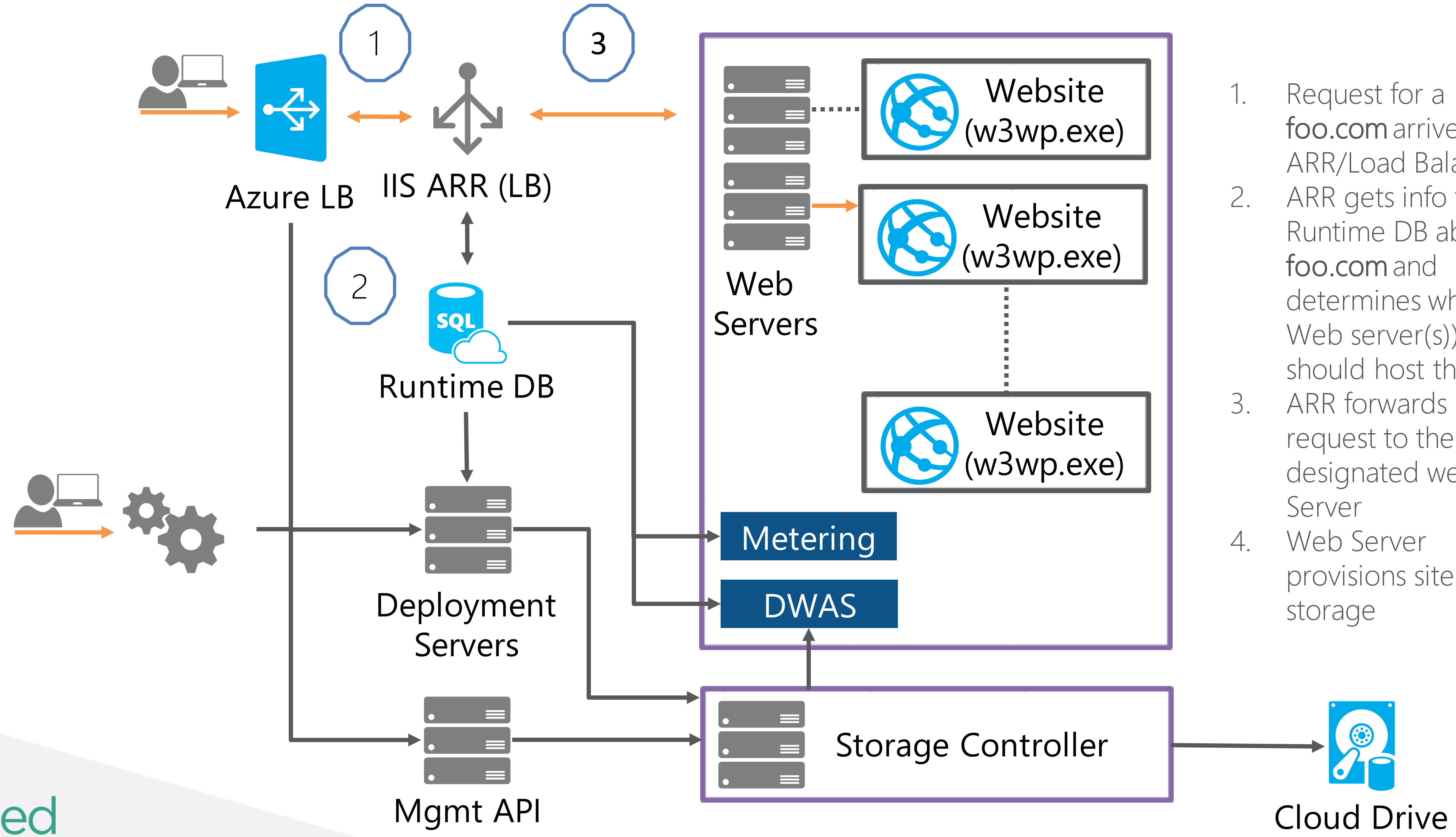
App Service Plans are the
underpinning service for your
Azure Apps

Supported Web Frameworks



Classic ASP as well or any custom FastCGI Handler

Underlying hosting environment



1. Request for a foo.com arrives to ARR/Load Balancer
2. ARR gets info from Runtime DB about foo.com and determines which Web server(s)) should host the site.
3. ARR forwards request to the designated web Server
4. Web Server provisions site from storage

sourced

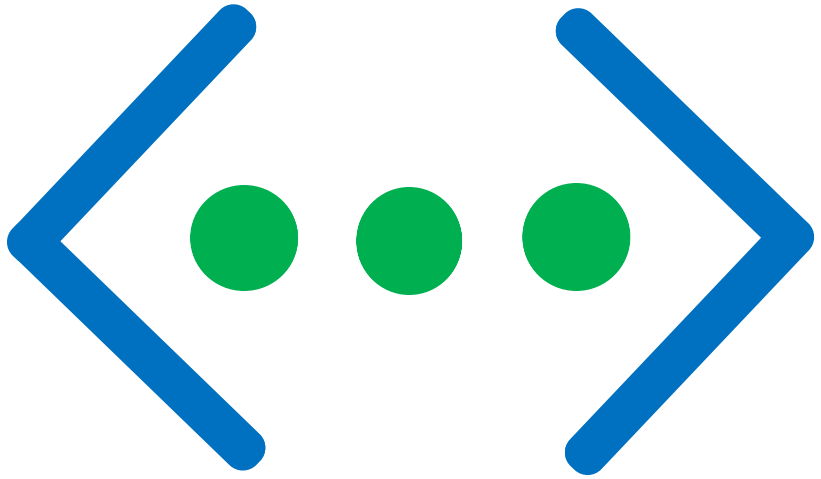
Challenges for App services in the enterprise

- Internet facing
- Multi-tenant
- Monitoring and Auditing

Introducing App Service Environment (ASE)

sourced

Azure Virtual Network(VNet)

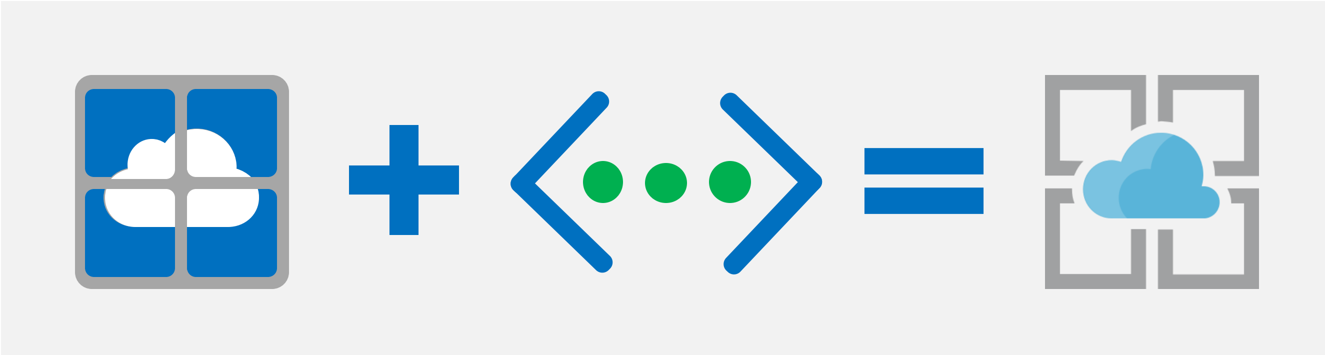


- Private network in the Azure cloud
  - Usually uses RFC1918 private IP addresses
- Enables network based security and isolation
  - Control access with Network Security Groups (NSGs)
- Can be used with VPNs to create hybrid cloud applications
  - Customers can control routes for IP traffic to go through those VPNs

App Service Environment (ASE)

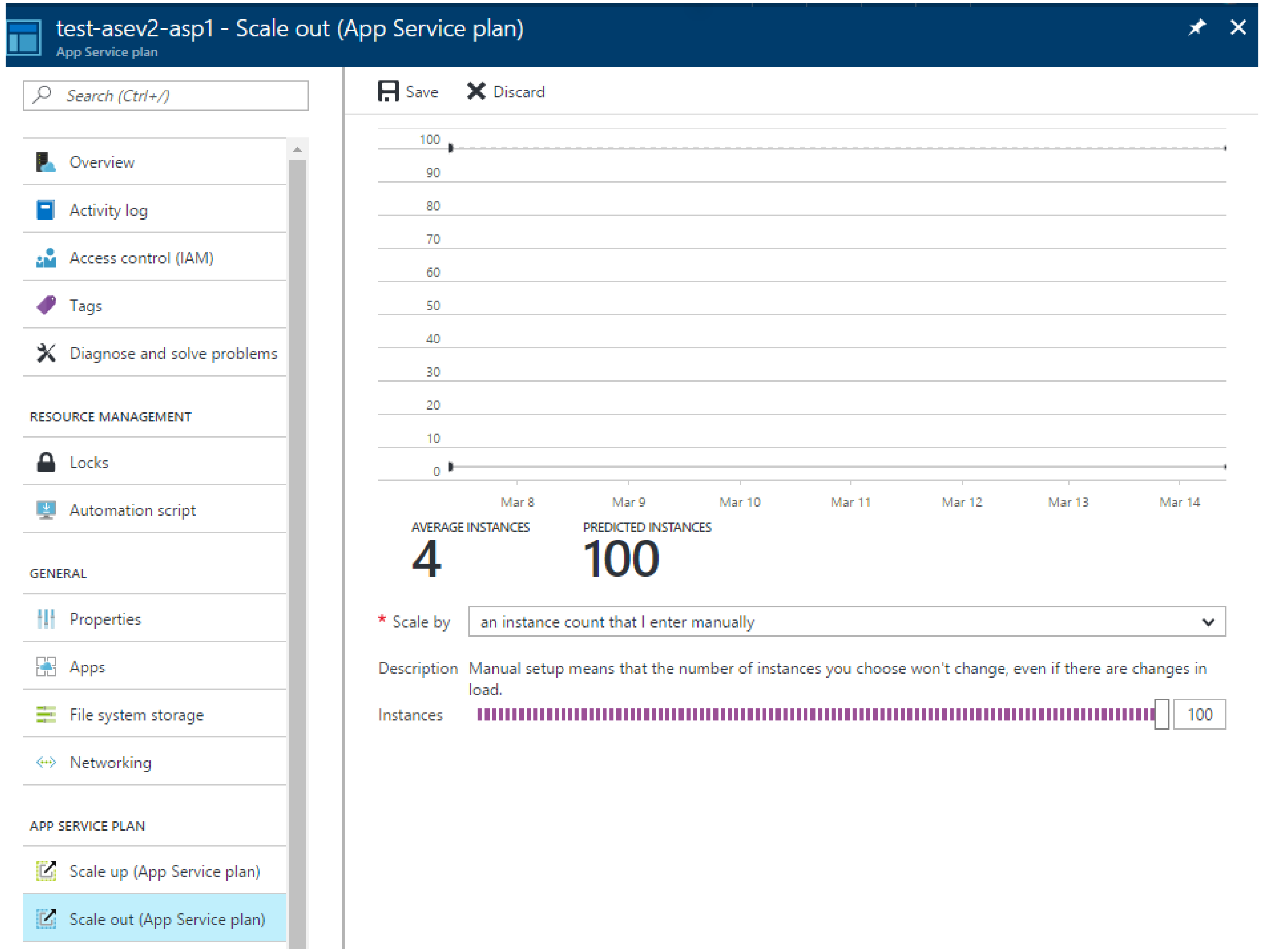
- The ASE is a deployment of the Azure App Service into a subnet of a customer’s Azure Virtual Network

- The ASE provides:
  - Network isolation for apps
  - Larger scale than multi-tenant
  - More powerful hosts
  - Ability to work with all VPN types



Scaling out App Service plans (ASPs) in ASE

- In ASE you can scale to 100 ASP instances
- That can be:
  1 ASP with 100 instances,
  100 ASPs with 1 instance each,
  or anything in between.



test-asev2-asp1 - Scale out (App Service plan)

App Service plan

AVERAGE INSTANCES 4

PREDICTED INSTANCES 100

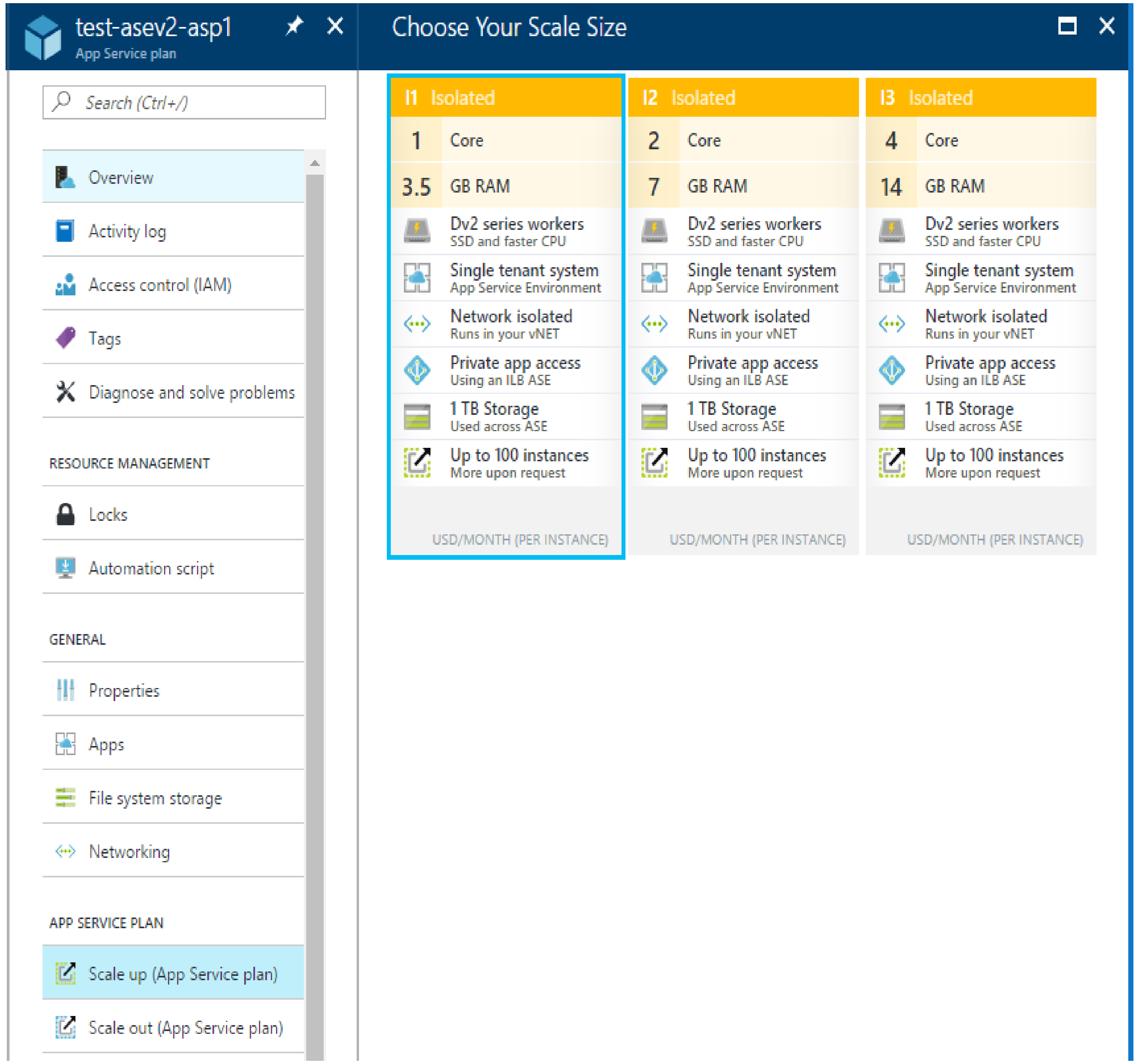
* Scale by: an instance count that I enter manually

Description: Manual setup means that the number of instances you choose won't change, even if there are changes in load.

Instances: 100

Isolated – Pricing plan just for ASE apps

- One fee for the ASE plus Isolated App Service plan fees
- ASE ownership fee does not change with the size of the ASE and covers all infrastructure including automatically scaled components
- ASP fees let you pay for what you use
- Prices vary between regions.



test-asev2-asp1
App Service plan

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

RESOURCE MANAGEMENT

Locks
Automation script

GENERAL

Properties
Apps
File system storage
Networking

APP SERVICE PLAN

Scale up (App Service plan)
Scale out (App Service plan)

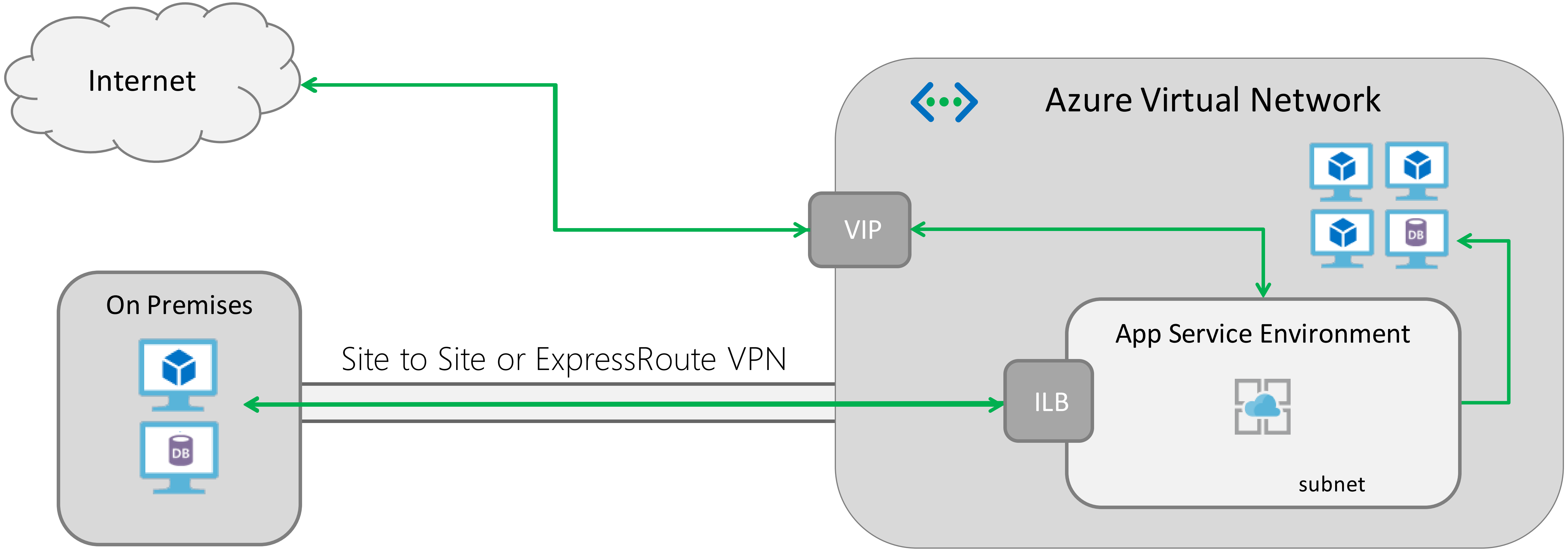
Choose Your Scale Size

I1 Isolated	I2 Isolated	I3 Isolated
1 Core	2 Core	4 Core
3.5 GB RAM	7 GB RAM	14 GB RAM
Dv2 series workers SSD and faster CPU	Dv2 series workers SSD and faster CPU	Dv2 series workers SSD and faster CPU
Single tenant system App Service Environment	Single tenant system App Service Environment	Single tenant system App Service Environment
Network isolated Runs in your vNET	Network isolated Runs in your vNET	Network isolated Runs in your vNET
Private app access Using an ILB ASE	Private app access Using an ILB ASE	Private app access Using an ILB ASE
1 TB Storage Used across ASE	1 TB Storage Used across ASE	1 TB Storage Used across ASE
Up to 100 instances More upon request	Up to 100 instances More upon request	Up to 100 instances More upon request
USD/MONTH (PER INSTANCE)	USD/MONTH (PER INSTANCE)	USD/MONTH (PER INSTANCE)

sourced

ASE High Level Networking

An ASE is a deployment of the Azure App Service into a subnet in a customer's Azure Virtual Network



sourced

App Service Environment endpoints

Internet accessible endpoint:

- All app inbound and outbound traffic flow through a public VIP
- App hostnames are in public DNS
- App names have the form **<appname>.<ASEname>.p.azurewebsites.net**
- Certificates are created with your ASE
- Type of ASE commonly called the external ASE or public ASE

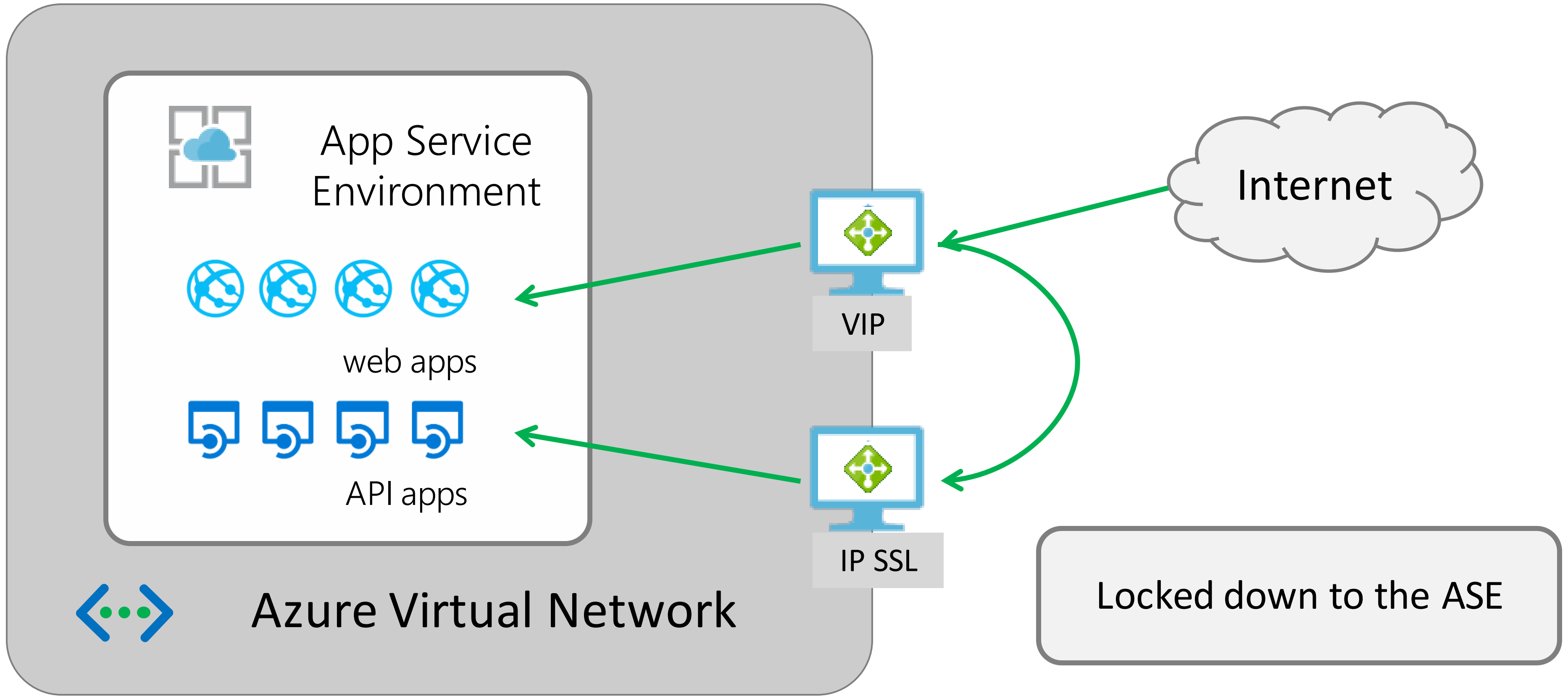
Azure virtual network address endpoint:

- All app inbound flows in to an address in the subnet used by the ASE
- App outbound to the internet goes though a public VIP
- App hostnames need to be managed in a customer DNS
- User defines domain for the ASE that apps are made in
- Certificates need to be provided by the customer
- Type of ASE commonly called the ILB ASE as it uses an Internal Load Balancer

Deployment Patterns

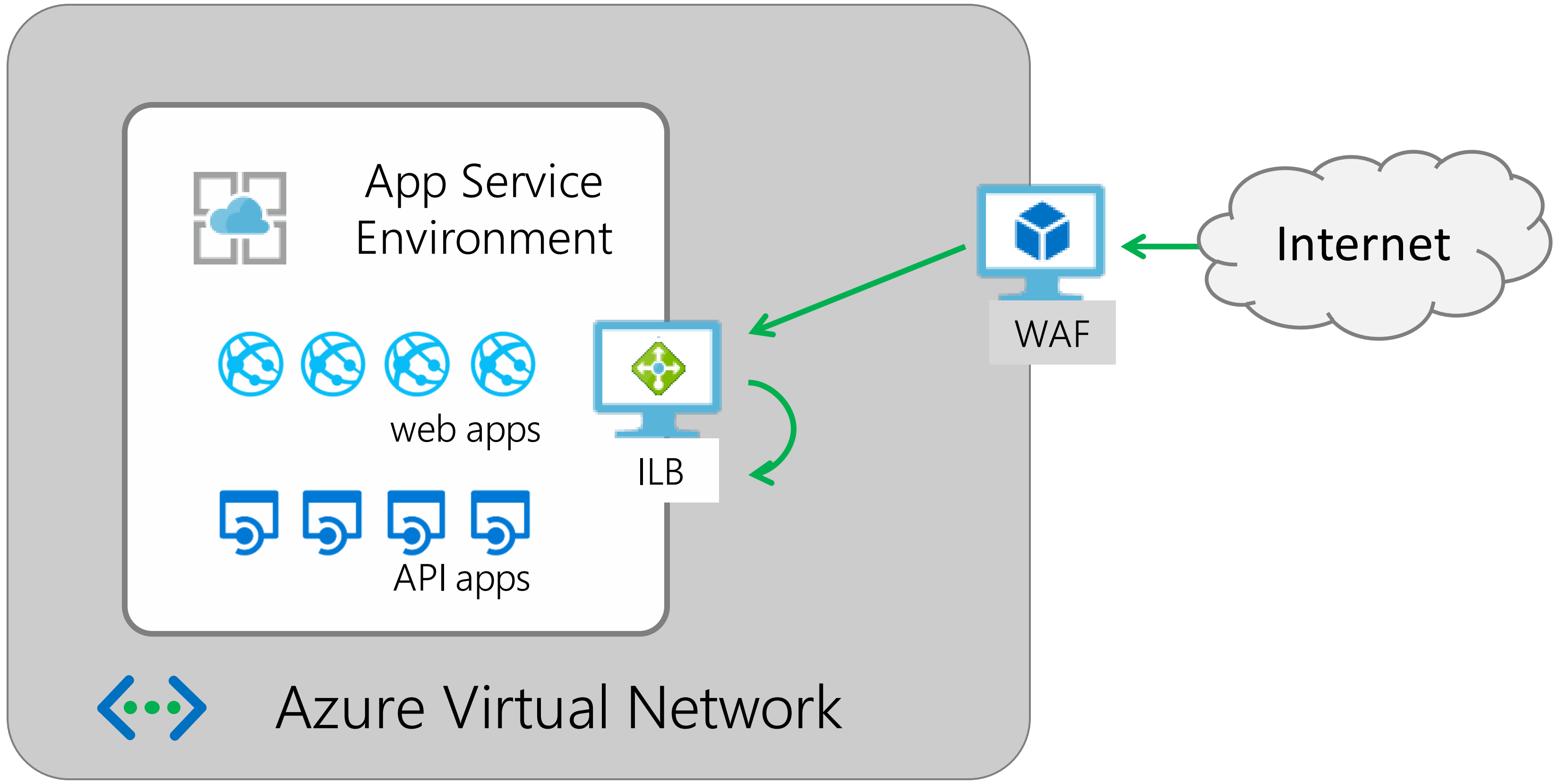
sourced

External ASE



- Assign an address to a single app using IP-based SSL
- Use Network Security Groups to lock down access to that app.

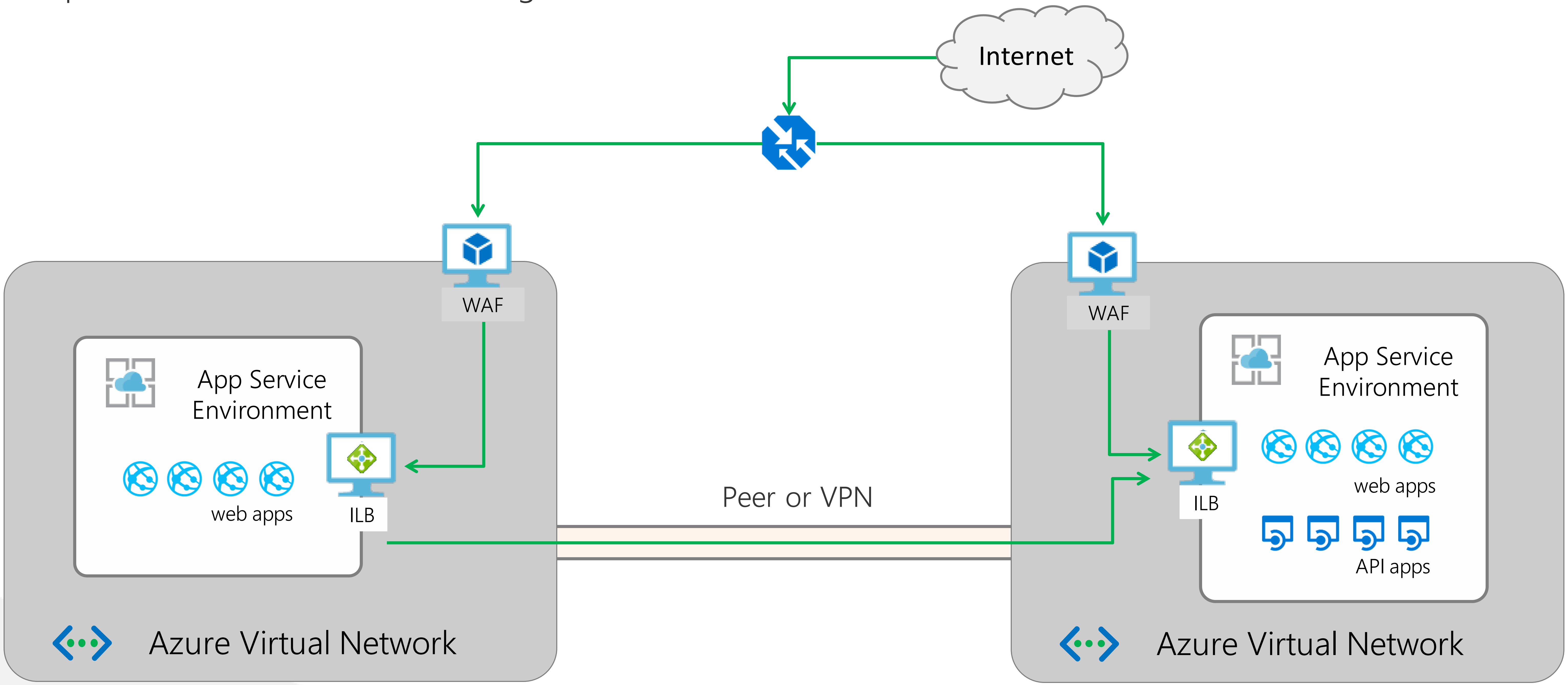
ILB with WAF



- Leverage the benefits of the WAF with a web app that calls back to an API app on the same ILB ASE. The traffic between the web and API apps stays in the VNet.

Geo distributed ILB ASE

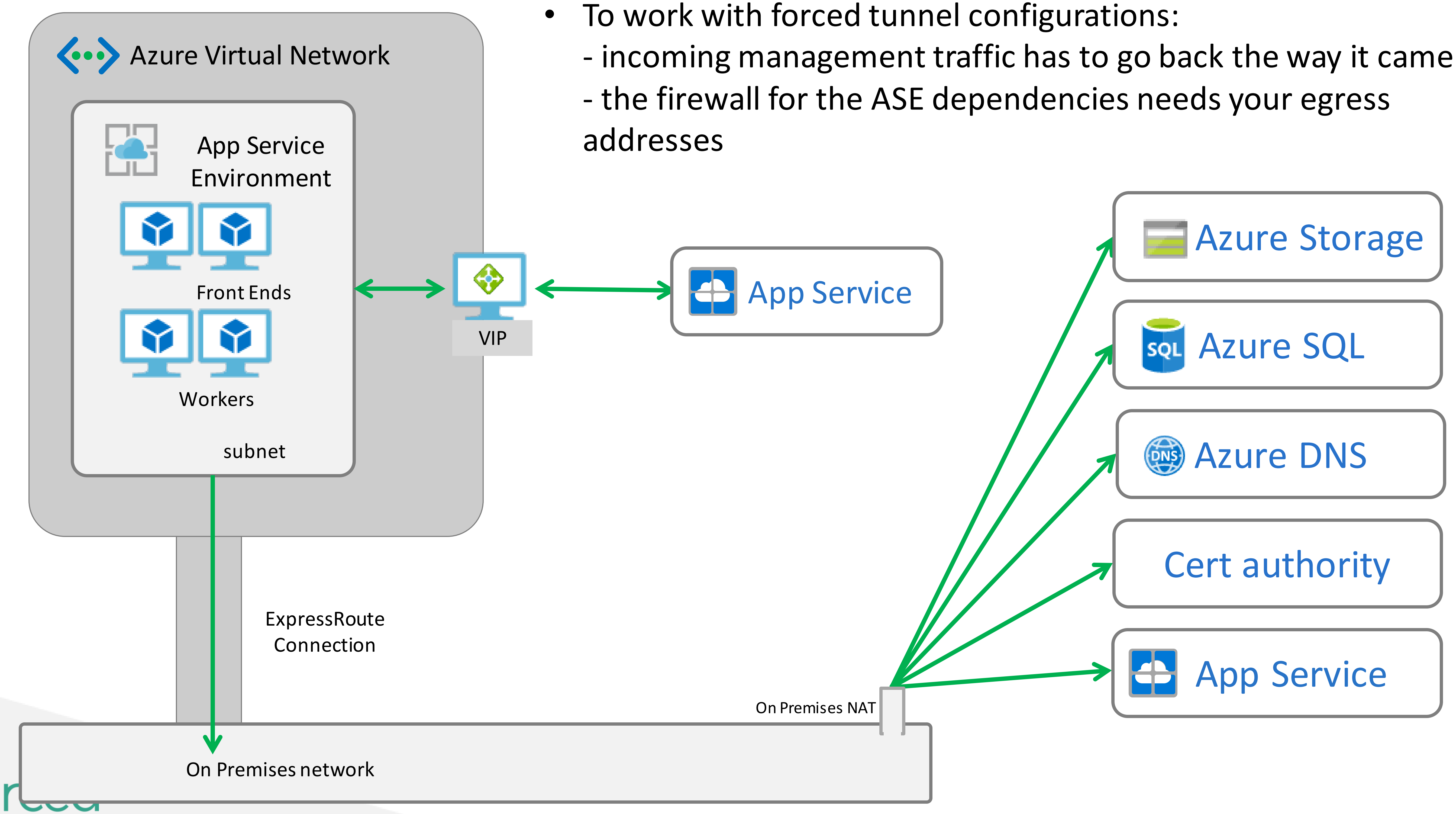
- Multiple ILB ASEs behind traffic manager.



sourced

Forced tunnel and ASE

- To work with forced tunnel configurations:
  - incoming management traffic has to go back the way it came
  - the firewall for the ASE dependencies needs your egress addresses



Supporting forced tunnel configuration

- To enable forced tunnel config on an existing ASE:
  - Create/edit the ASE subnet route table to include App Service management addresses for inbound traffic
  - Add your gateway/NAT addresses to the ASE firewall list

- To create an ASE in a force tunneled VNet:
  - Create/edit the ASE subnet route table to include App Service management addresses for inbound traffic
  - Create the ASE with a template and set your gateway/NAT addresses for the ASE firewall

Demo

sourced

App Service Environment - Demo

- Walkthrough – how to deploy an ILB ASEv2
- Overview components of WAF enabled Isolated App Service
- ASE ARM Template

Recent network improvements

- Create NSGs and UDRs on the ASE subnet
  - Only with ASEs made from the portal

- Published App Service management addresses
  - https://docs.microsoft.com/en-us/azure/app-service/app-service-environment/management-addresses
  - can be used with NSGs and UDRs

- Ability to adjust the SQL Server whitelist
  - Enable forced tunneling

- List of dependency hostnames (coming soon)
  - Provide a list of the dependency hostnames for an ASE

Questions?

sourced