Beyond Public Endpoints: Securing Azure PaaS

Aidan Finn, MVP

Cloud Mechanix

Introducing Aidan Finn

- Cloud Mechanix
- 18 year MVP – currently Microsoft Azure
- Based in Kildare, Ireland (+5 hours from EST)
- Working as consultant/sys admin since 1996
- Windows Server, Hyper-V, System Center, desktop managment, and Azure

- http://aidanfinn.com
- http://cloudmechanix.com
- @joe_elway

Cloud Mechanix – Azure Consulting & Training

- Design and fix Azure foundations
- Remove risk before it becomes incident
- Enable your team, not dependency
- Microsoft best practices, real-world experience

http://cloudmechanix.com

Discount Code For MC2MC

Ant0205

€350/person

In The Beginning …

Windows Azure Was Born

- Announced Oct 2008, GA Feb 2010
  - AWS launched March **2006**
- Microsoft focused on developers:
  - Make it easy to adopt
- PaaS only offerings at first (not complete):
  - Web/Worker role
  - Storage Account
  - Azure SQL
  - Azure AppFabric

Chasing The Competition

- Wanted to make Azure easier to test and adopt
- Shaped the deployment experience to be easy
- The result – weakened:
  - Network security
  - Regulatory compliance
  - Industrial compliance
- But the dev got a website up quickly

Demo

Public Endpoints

Some Public Endpoint Incidents

- Azure Cosmos DB
  - Wiz, 2021
  - Disclosed any Azure customer could access customer data using Jupyter Notebook
- Storage Account – Blob
  - Microsoft, 2022
  - 2.4 TB of customer/partner data shared publicly without authentication
- Storage Account – Blob
  - EY, 2025
  - 4TB of SQL Server backups shared publicly

Issues

- Common patterns:
  - Public endpoints enabled by default
  - No Private Endpoint / VNET isolation
  - Misconfigured access controls (ACLs, tokens, APIs)
  - Lack of Azure Policy enforcement
- Legacy Azure configurations
  - The tyranny of the default
- Compounded by lack of
  - Knowledge
  - Governance

Can We Use Resource Firewalls?

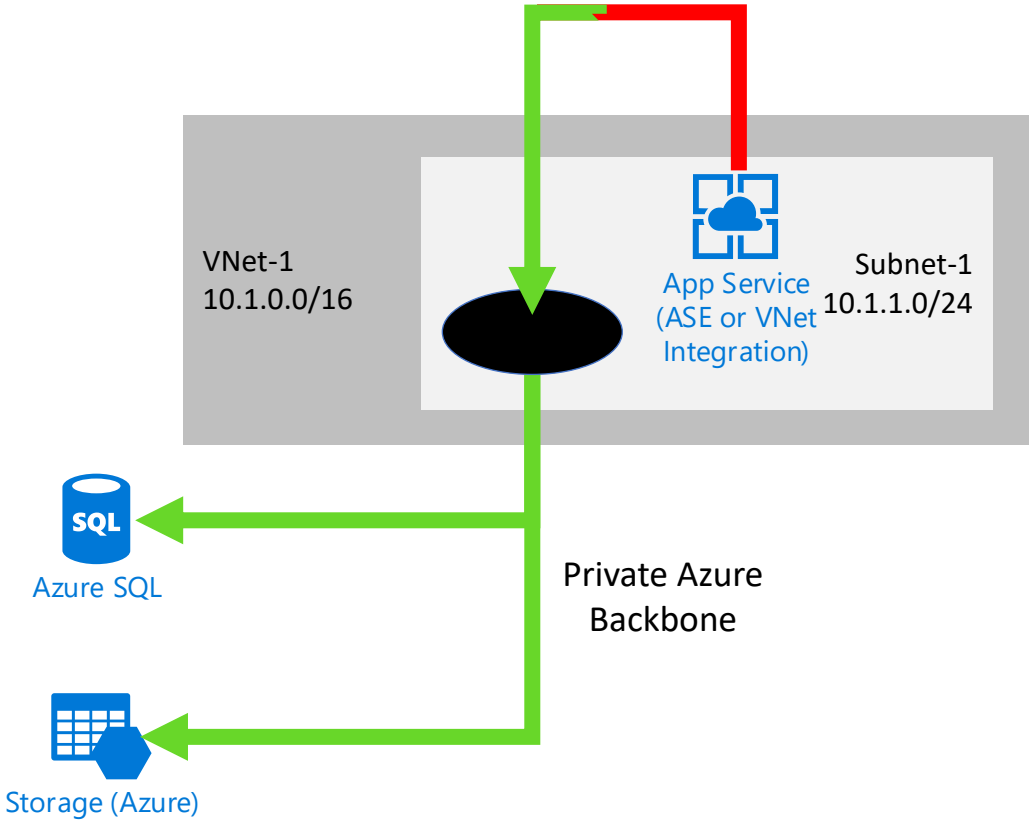
- Yes but …
- Highly distributed
- Varied:
  - Resource support
  - Implementation models
- Relying on opt-in by developers/operators

Public Endpoint Alternatives

- Service Endpoints
- Private Endpoints
- Network Security Perimeter
- Virtual Network integration
- Virtual Network injection

Service Endpoint

PaaS: Virtual Network Service Endpoints



- Enabled per subnet
- Support for limited resource types (18), including:
  - Microsoft.Storage
  - Microsoft.Web
  - Microsoft.KeyVault
- Reroutes traffic to PaaS resource over Azure backbone
  - Public endpoint still exists
  - Connections limited to subnets/VNets

Service Endpoint Policy

- The risk:
  - Service Endpoints allow uncontrolled egress to all instances of a resource type
- The theory:
  - Restrict access to specific instances of resources
- In practice:
  - Supports only Storage Accounts
- May be useful in *limited* scenarios

Demo

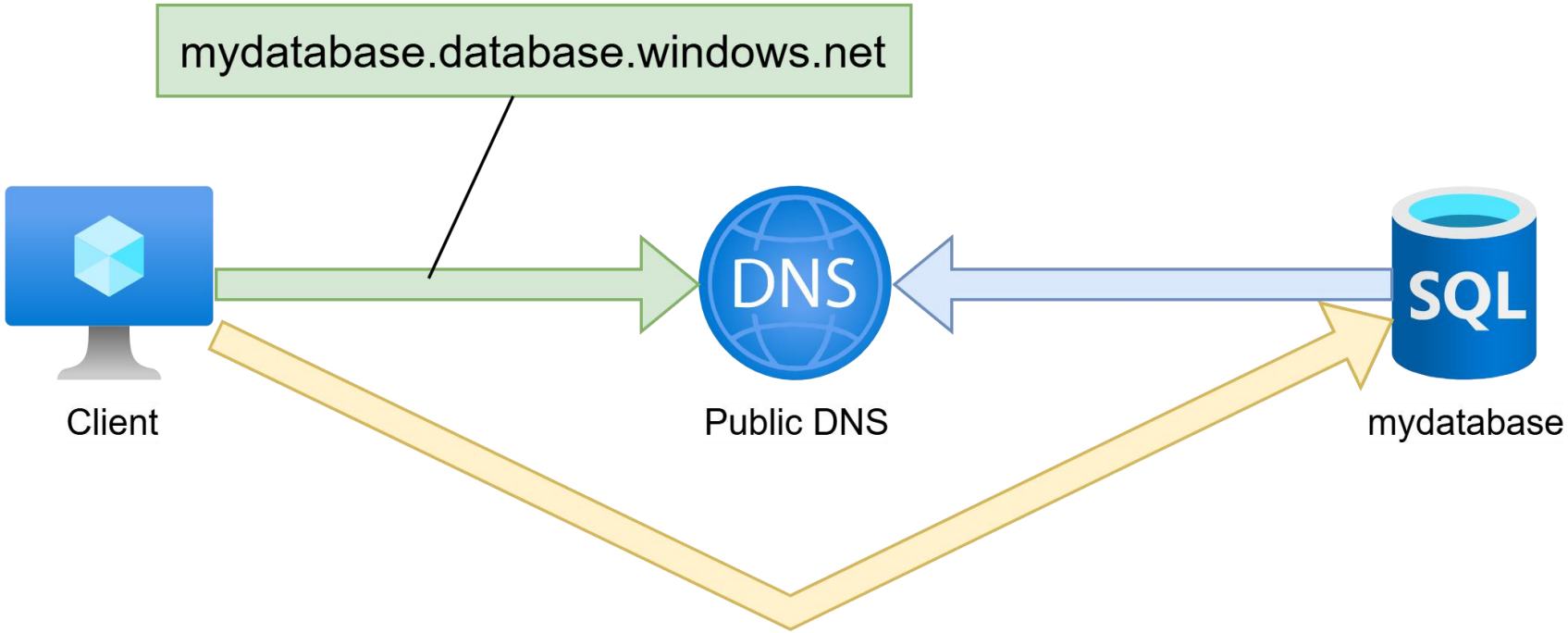
Service Endpoints

Service Endpoint Opinions

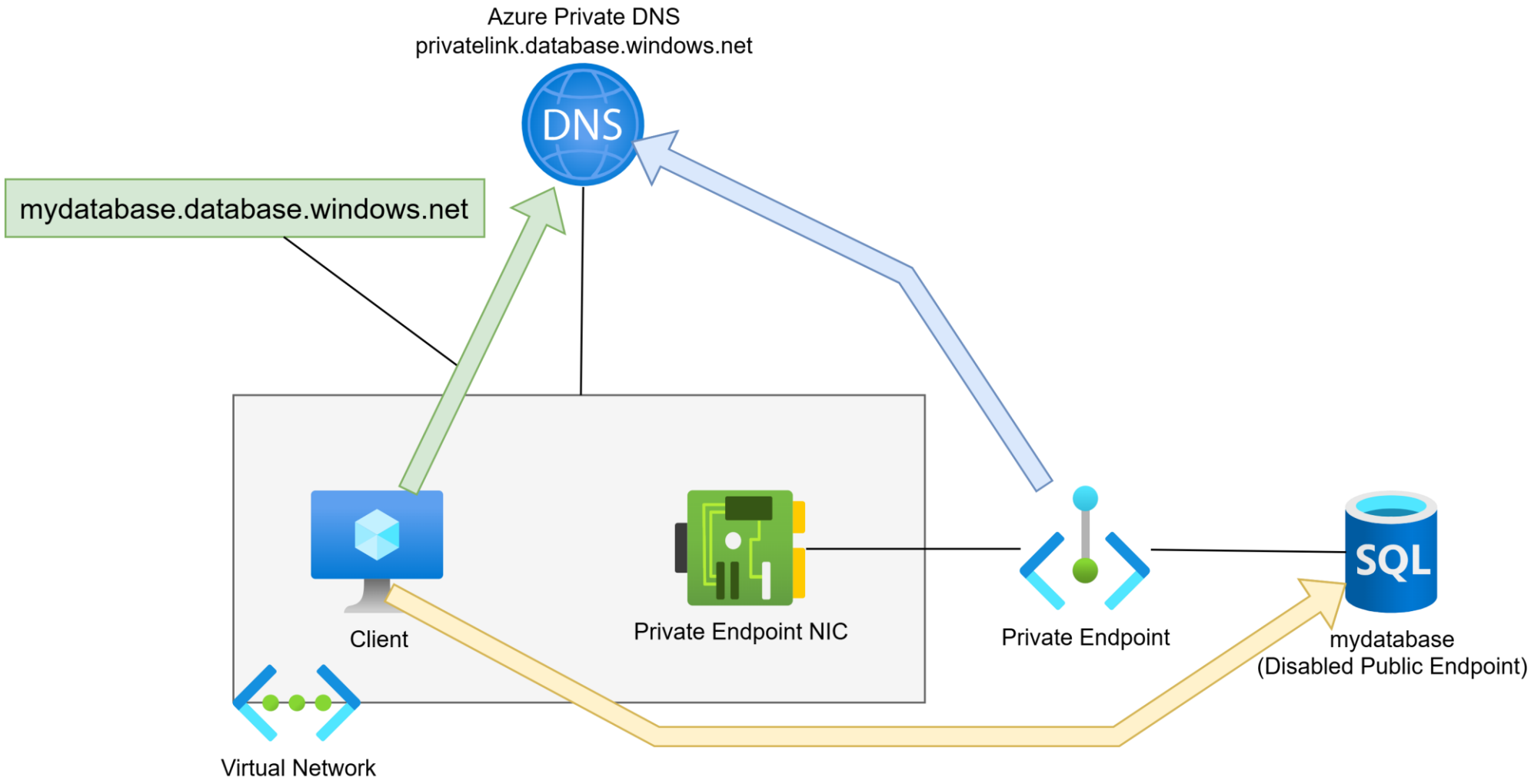
- Very simple to use
- Does not control egress
  - From PaaS compute resources
  - From client subnets to Service Endpoint resource type
- All of the other options are superior
- Very rare occasions where other options do not suit
- Consider all other options first

Private Endpoint

Default Connectivity



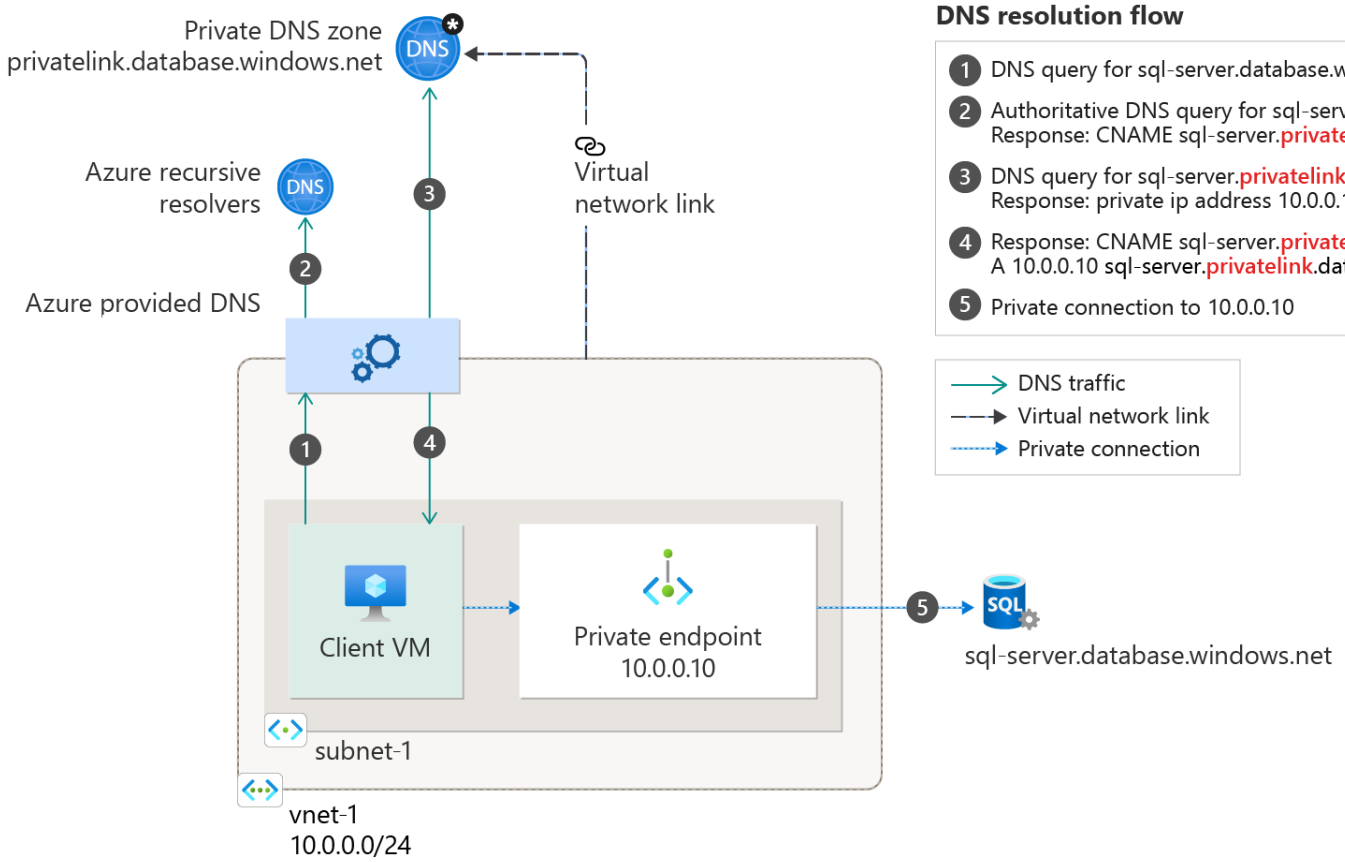
Private Endpoint Overview



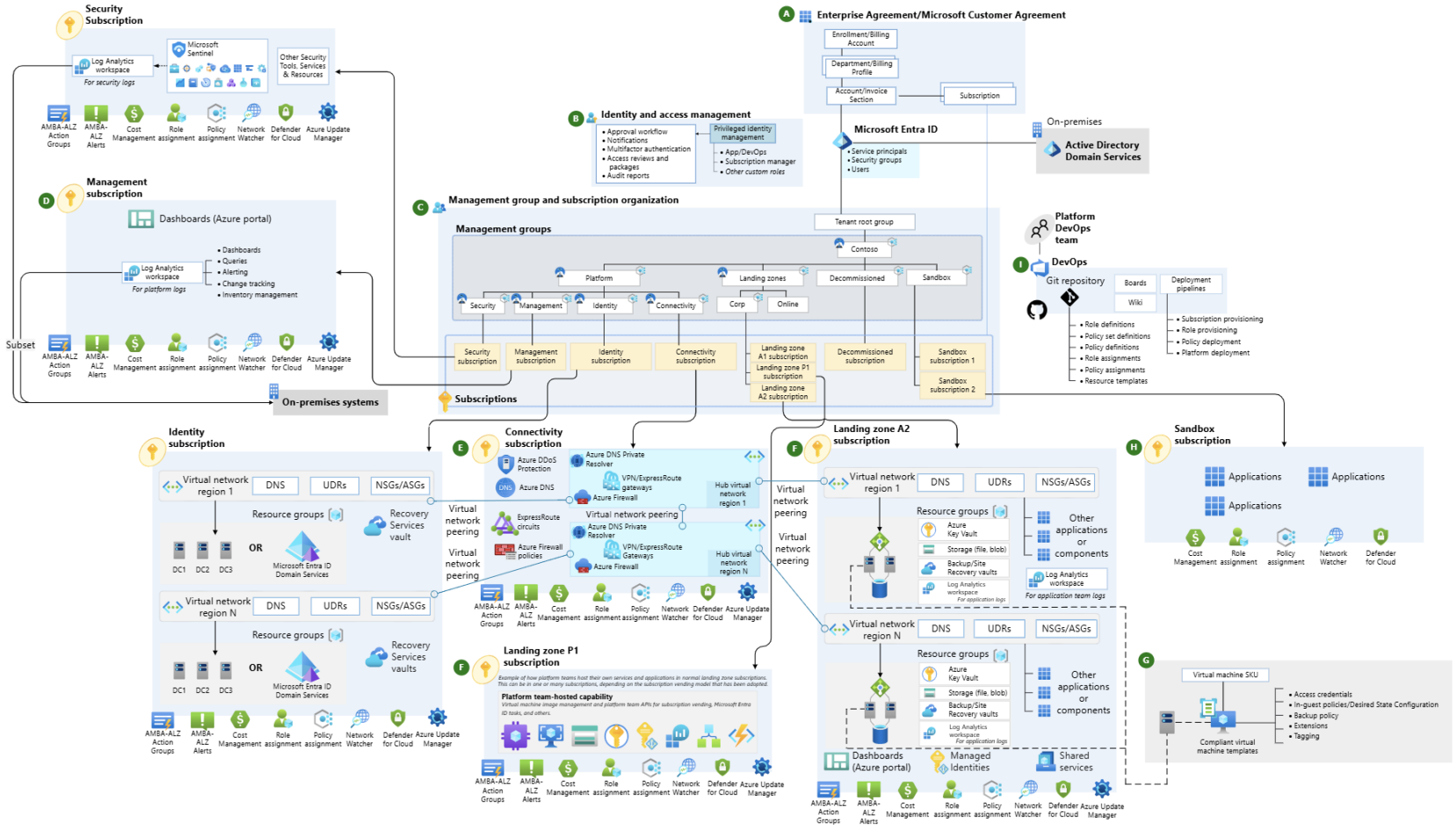
Private Endpoint Notes

- Created for specific resources/services only
  - Egress to other resources subject to network controls
- A private endpoint supports ingress only
  - Requests & responses
  - No outbound requests
- Availability depends on resource tier:
  - All tiers: Storage Account, Key Vault
  - Moderate tiers: App Services Basic+
  - Premium only: Service Bus, we're looking at you
- It's always DNS

Microsoft Docs



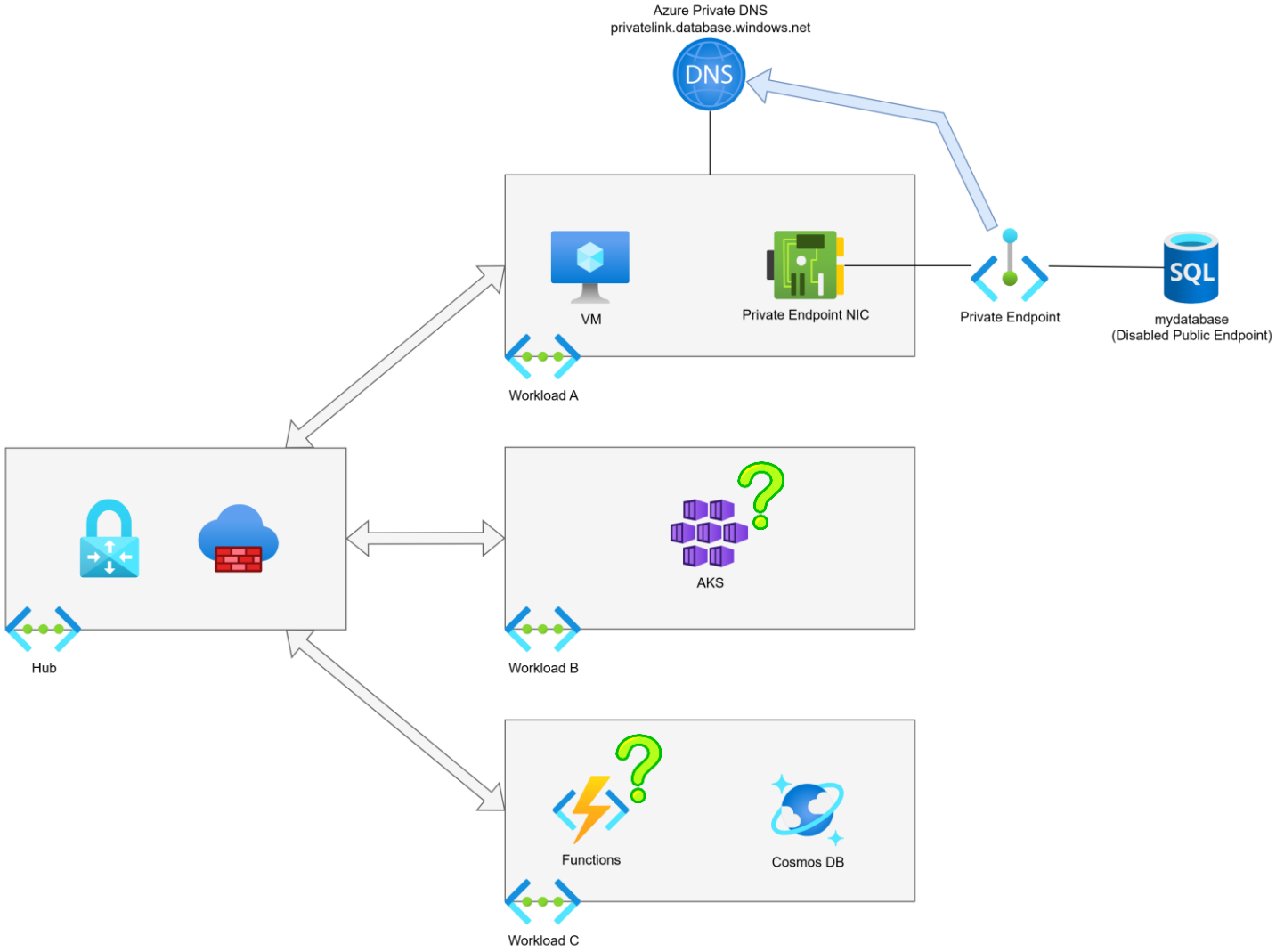
What About Landing Zones?



Microsoft Azure

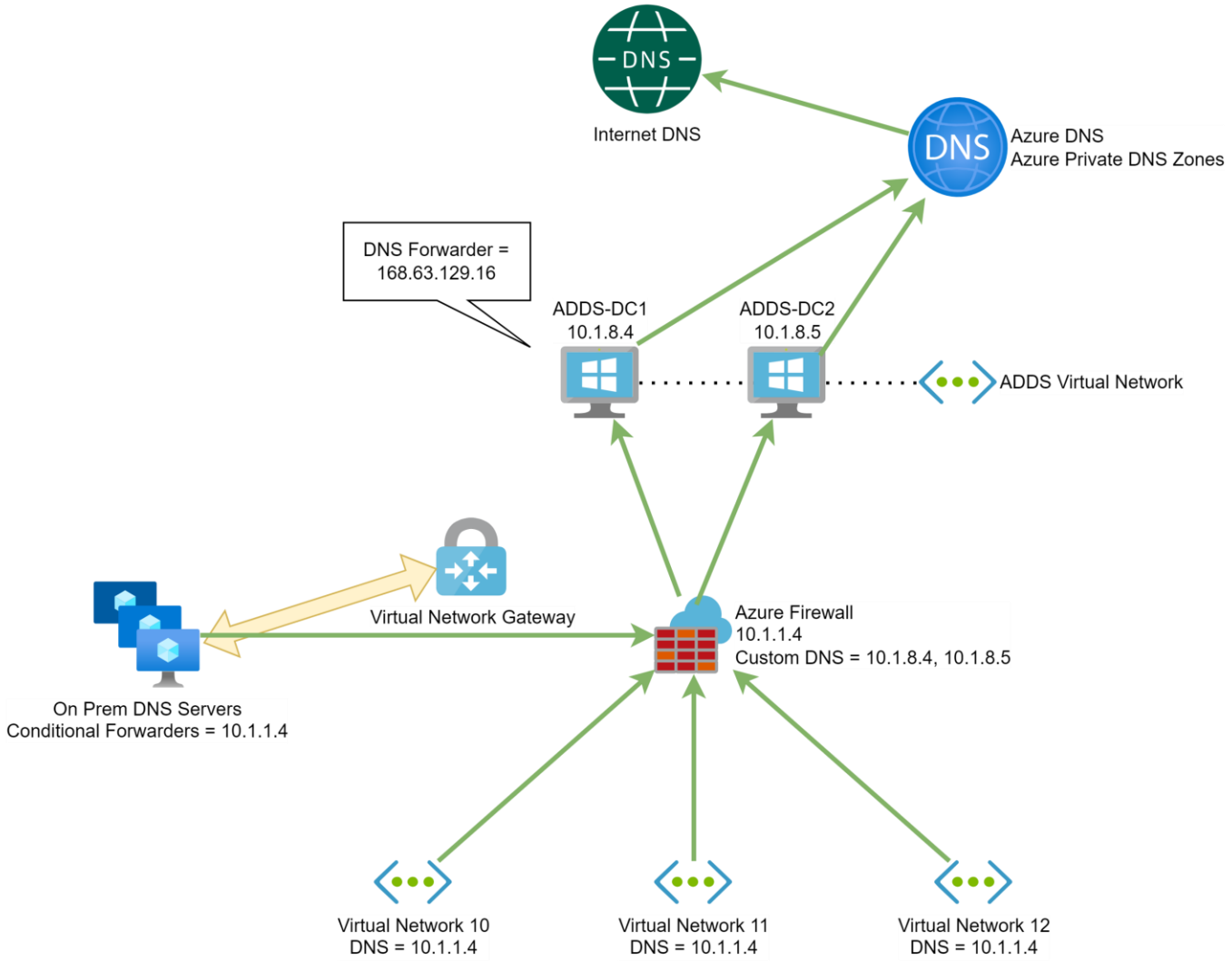
Version: 2025-07-07

DNS Fragmentation Breaks Integration



Real World: Scalable Enterprise DNS

- "DNS servers" deployed to dedicated application zone
  - Windows/Bind/Azure Private DNS Resolver
- Azure Firewall forwards to DNS servers
  - Can use FQDNs in Network Rules
- On-prem DNS servers use conditional forwarers
- No need for "DMZ DNS" servers



Demo

Private Endpoint

Tips

- Do not assume that the public endpoint is disabled automatically!
- Use Virtual Network Flow Logging for troubleshooting
- Enable subnet Network Policies for Private Endpoint – **off by default**:
  - Route Tables: Disable creation of route to the Private Endpoint /32 prefix in the GatewaySubnet
  - Network Security Groups: Enable support for NSG rules
- Use Azure Policy to disable public endpoints automatically
  - See “public network access” in Azure Policy definitions
  - See “Audit Public Network Access” Azure Policy initiative

Some Negatives

- You still run on shared compute
  - Microsoft-managed VMs in a Microsoft tenant
  - Shared pool of compute with other customers
- Can be complicated at scale:
  - 1 App Service plan with 20 app services >
  - 20 private endpoints!
- The resources have no public endpoint
  - Requires self-hosted agents/runners for DevOps/GitHub
  - Developer experience is changed to private only – see VPN & support tickets

Private Endpoint Opinions

- Should be considered the default PaaS privacy option
- Offers complete client-server privacy
- Use Azure Policy to enforce public endpoint disablement
  - Where supported
- There are times when:
  - Dedicated compute is preferred, leading to simpler networking
  - Developers want more simplicity

Network Security Perimeter

Service Endpoint & Private Endpoint

- Service Endpoint:
  - Easy
  - Lacks control
- Private Endpoint:
  - Brings a lot of control
  - Can be a heavy experience for developers

Network Security Perimeter (NSP)

- Brings control to public endpoints
- Create a permitter
- Associate PaaS resources with the NSP
- Create ingress and egress access rules in the NSP
- Manage all access rules for all associated resources in one NSP

Supported Resources

Private link resource name	Resource type	Availability
Azure Monitor	Microsoft.Insights/dataCollectionEndpoints Microsoft.Insights/ScheduledQueryRules Microsoft.Insights/actionGroups Microsoft.OperationalInsights/workspaces	Generally available
Azure AI Search	Microsoft.Search/searchServices	Generally Available
Cosmos DB	Microsoft.DocumentDB/databaseAccounts	Public Preview
Event Hubs	Microsoft.EventHub/namespaces	Generally Available
Key Vault	Microsoft.KeyVault/vaults	Generally Available
Service Bus	Microsoft.ServiceBus/namespaces	
SQL DB	Microsoft.Sql/servers	Public Preview
Storage	Microsoft.Storage/storageAccounts ** Static websites must be disabled*	Generally Available
Azure OpenAI service	Microsoft.CognitiveServices(kind="OpenAI")	Public Preview
Microsoft Foundry	Microsoft.CognitiveServices(kind="AIServices")	Generally Available

Supported Access Rules Types

Direction	Access rule type
Inbound	Subscription-based rules
Inbound	IP-based rules (check respective onboarded private link resources for v6 support)
Outbound	FQDN-based rules

Profiles

- Network Security Perimeter
- NSP contains 1 or more profiles
- Profiles contain 1 or more access rules

Demo

Network Security Perimeter

Limitations

- Number of network security perimeters: Supported = 100/subscription
- Profiles per network security perimeters: Supported = 200
- Number of rule elements per profile: Supported = 200 inbound and 200 outbound
- Number of PaaS resources across subscriptions associated with the same network security perimeter: Supported = 1000
- Currently, service endpoint traffic can be denied even when an inbound rule allows 0.0.0.0/0
  - Recommended to use private endpoints for IaaS to PaaS communication

Tips

- Profiles have two modes:
  - Learning Mode: Observe actual traffic
  - Enforced Mode: Apply the access rules
- Recommendation for existing/dev workloads:
  - Enable Learning Mode for the profile(s)
  - Observe & tune rules
  - Apply Enforced Mode
- Configure public network access for PaaS resources to Secured By Perimeter
  - A resource property > publicNetworkAccess: 'SecuredByPerimeter'

Network Security Perimeter Opinions

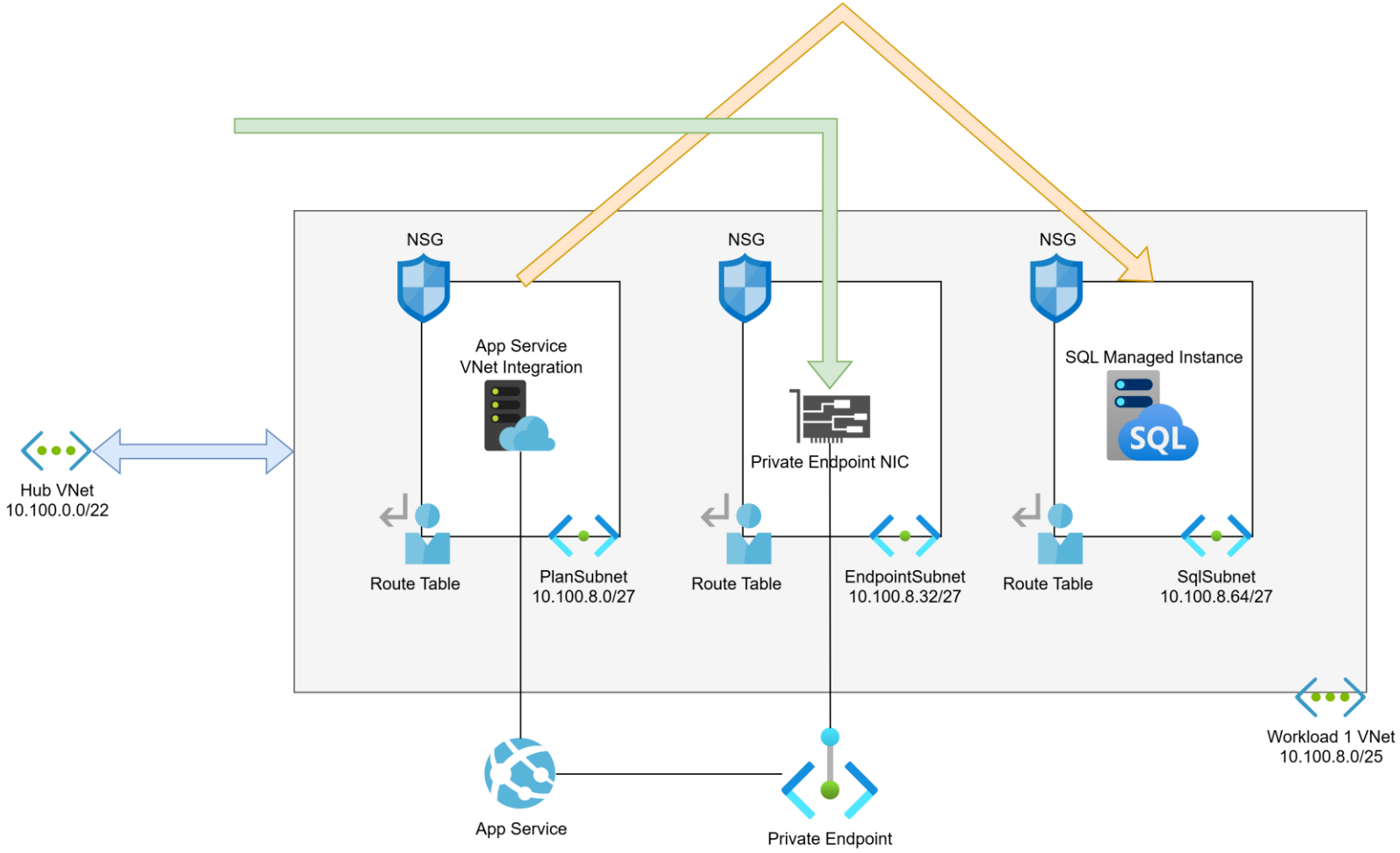
- NSP is quite basic
  - But it is very simple
- Resource support is very limited
  - Compared to broad support for Private Endpoint
- Sources are limited to:
  - Subscriptions
  - IP addresses/prefixes
  - No selection of specific resources
- Very limited resource type support
- Today, I view it as “better than nothing” for developer-centric environments
- Maybe with time …

Virtual Network Integration

Integration Overview

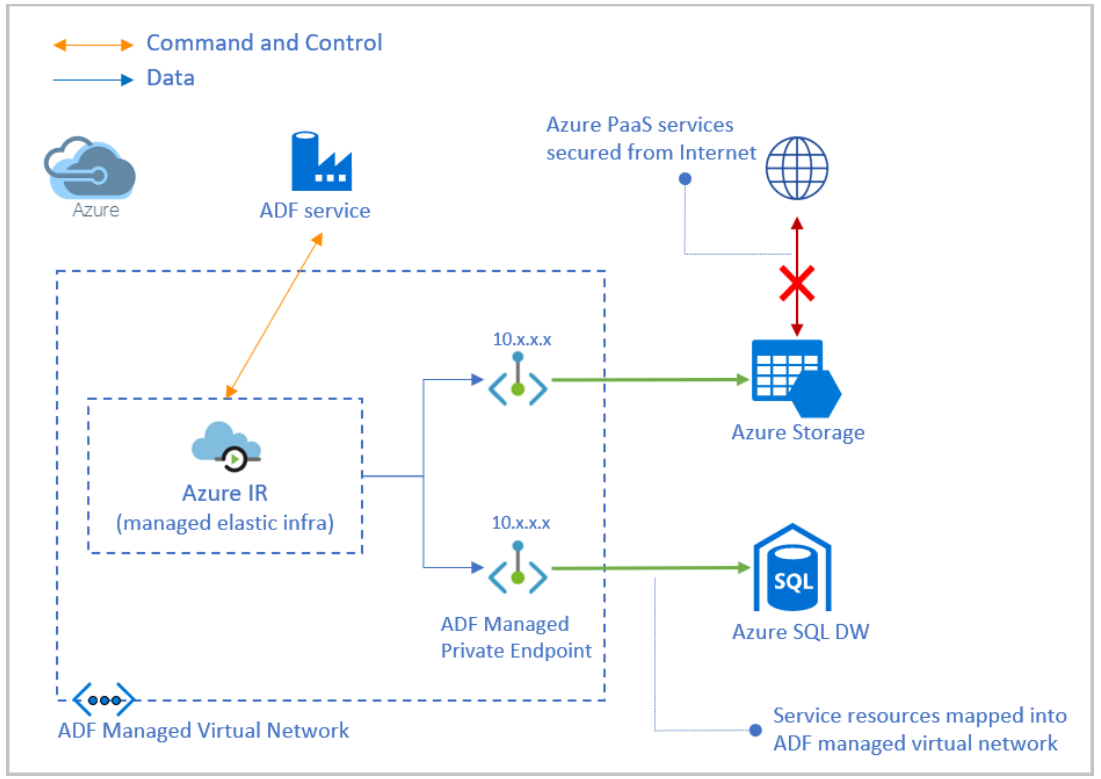
- A PaaS resource is connected to a Virtual Network
  - Enabling egress
  - Sometimes ingress
- The resource is still “separate”
- Example: App Service Regional VNet Integration
  - Allows outbound connectivity over a private network
- *Sometimes* compliments Private Endpoint:
  - Inbound: Private Endpoint
  - Outbound: VNet integration

App Service Regional VNet Integration



There Are Variations

- Data Factory
  - Managed Virtual Network
- Logic Apps
- Azure Databricks
- Azure Synapse Analytics



Virtual Network Integration Opinions

- A necessary evil ☺
- Some PaaS resource require outbound connections to Virtual Networks
- Can make Virtual Networks complicated
  - Dedicated (“delegated”) subnets
  - Separated ingress/egress with Private Endpoints

Virtual Network Injection

Injection Overview

- Dedicated compute for PaaS resources hosted in a Microsoft tenant
  - You get your own footprint
  - Usually implies a substantial cost
- Complete injection into a Virtual Network (subnet)
  - Simplifies architecture
- Examples:
  - App Service Environment (ASE) / Isolated tier
  - SQL Managed Instance
  - API Management Premium v1/v2
  - Azure Cache for Redis Enterprise

Comparing Private Endpoint with Injection

App Services Standard

- 1 plan with 20 apps
- Dedicated subnet for VNet integration
  - Outbound communications
- 20 Private Endpoints
  - Inbound application traffic (sites)
- *Another* 20 Private Endpoints
  - For code deployment (SCM - sitesdev)

App Service Environment (ASE)

- 1 plan with 20 apps
- Dedicated subnet for the ASE

Virtual Network Integration

- The cleanest solution of all
  - Total privacy
  - Relatively simple networking – still requires dedicated subnet
- Unfortunately:
  - High cost resource tiers
  - Limited resource support
- How I would design PaaS networking in “my Azure v2”
  - Public endpoint being optional

Conclusions

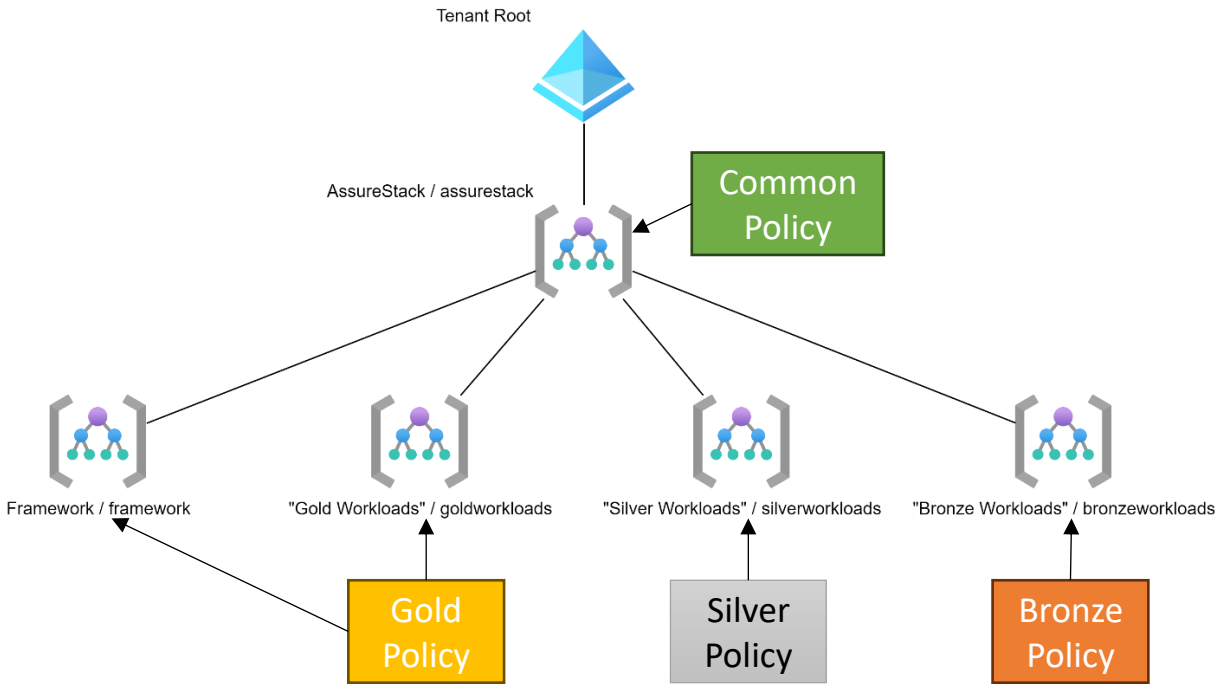
Wrapping Up

When To Use Which Option?

- Service Endpoint:
  - Rare Azure scenarios when it’s the only private option
- Private Endpoint:
  - Most occasions
  - Requires structure and planning
- Network Security Perimeter:
  - Developer-centric scenarios
  - Lacks micro-segmentation (Zero Trust)
- Virtual Network Integration
  - PaaS resources requirements
- Virtual Network Injection
  - PaaS resources requirements
  - When Private Endpoint isn’t scaling well

Security Policy Driven Approach

- Pre-decide your security questions
- Tiered Security Policy
  - Offering various levels of control
- Start with “minimal viable” security policy
- Apply using Azure governance features & org. processes
- Evolve over time via scheduled risk assessments



Thank You!

- Aidan Finn
- http://aidanfinn.com
- http://cloudmechanix.com
- @joe_elway

Online Course

Azure Operations for Small and Medium Businesses

April 13-14

Discount Code For NIC

Dub0128

€350/person