Using VNETs in PaaS solutions

Tomasso Groenendijk

Insight

Tomasso Groenendijk
EMEA Solution Architect

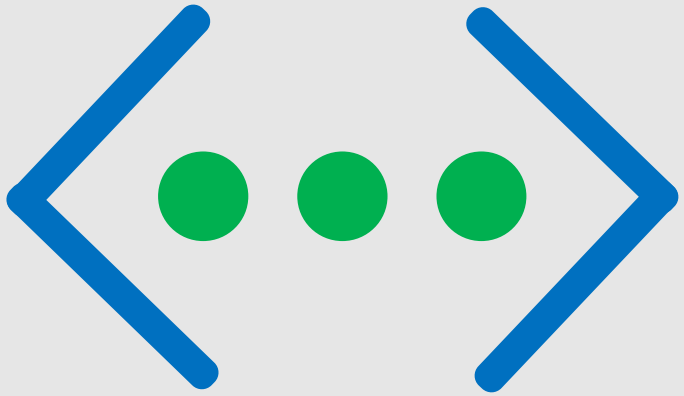
@tlagroenendijk

linkedin.com/in/tomassogroenendijk

ithero.nl

Microsoft® MVP Most Valuable Professional

Azure Virtual Network (VNet)



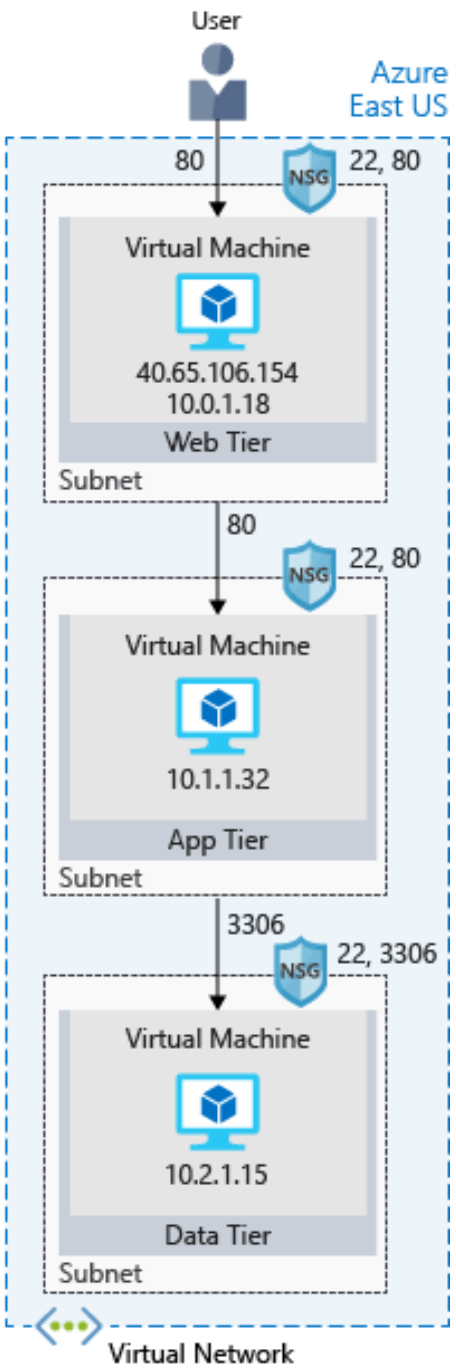
Azure Virtual Network enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks

Azure Virtual Network provides the following key capabilities:

- Isolation and segmentation
- Communicate with the internet
- Communicate between Azure resources
- Communicate with on-premises resources

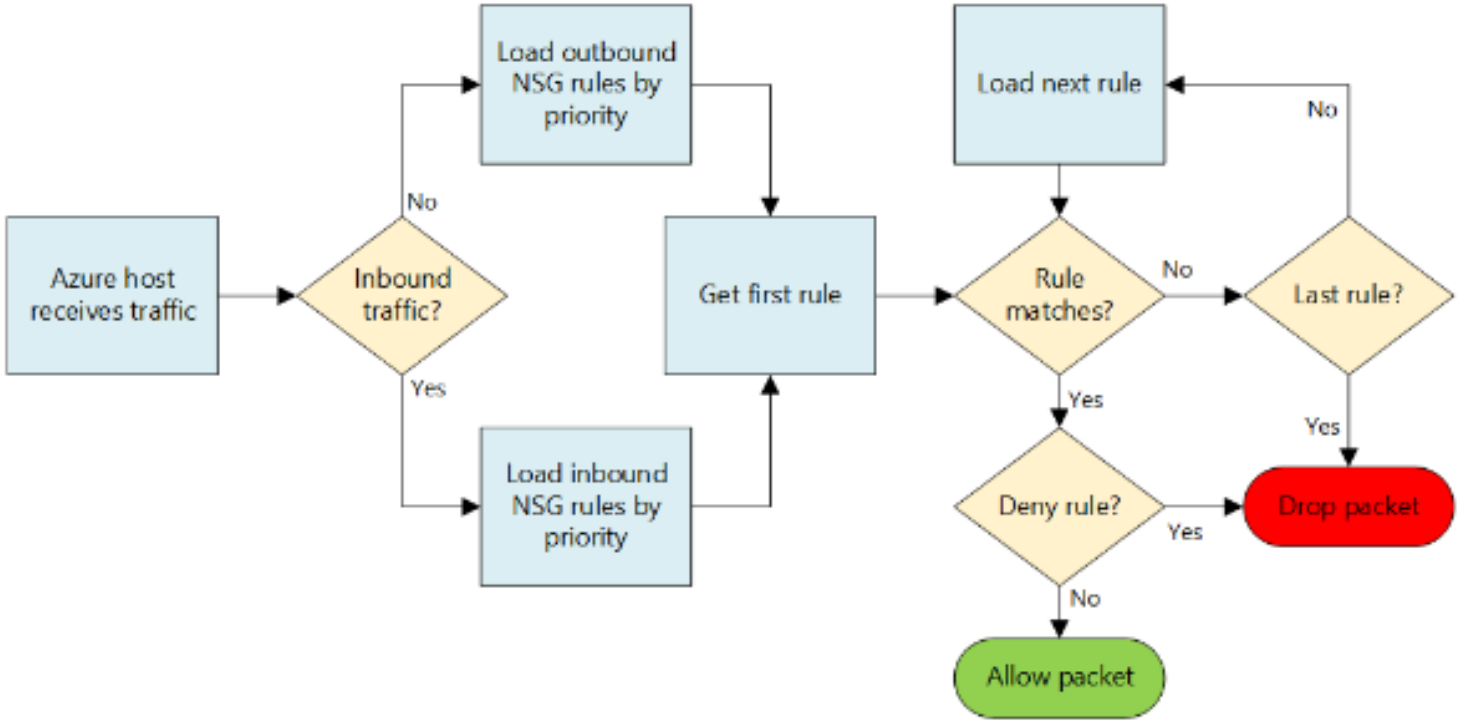
Azure infrastructure services hierarchy

- Subscription
- Location
- Resource group
- Virtual network
- Subnet
- Availability set
- Load balancer
- Network security group
- Virtual machine



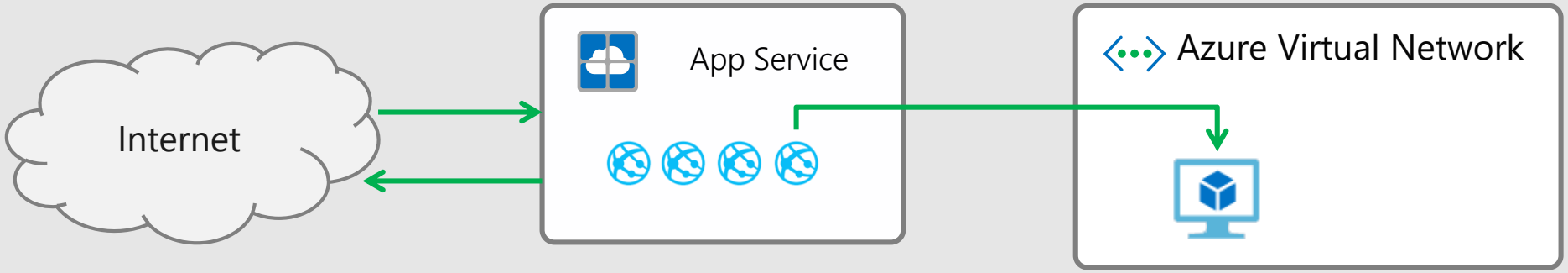
Network Security Group

- You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group.
- A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.



VNet Integration

Access resources in your Azure VNet



Outbound backend calls from your app can reach private IP addresses in your Azure Virtual Network or go out to the internet through a set of addresses shared with other apps.

You can reach on premises resources if VNet uses a Site to Site VPN. The current feature does not work with ExpressRoute or Service Endpoints.

App Service Environment (ASE)

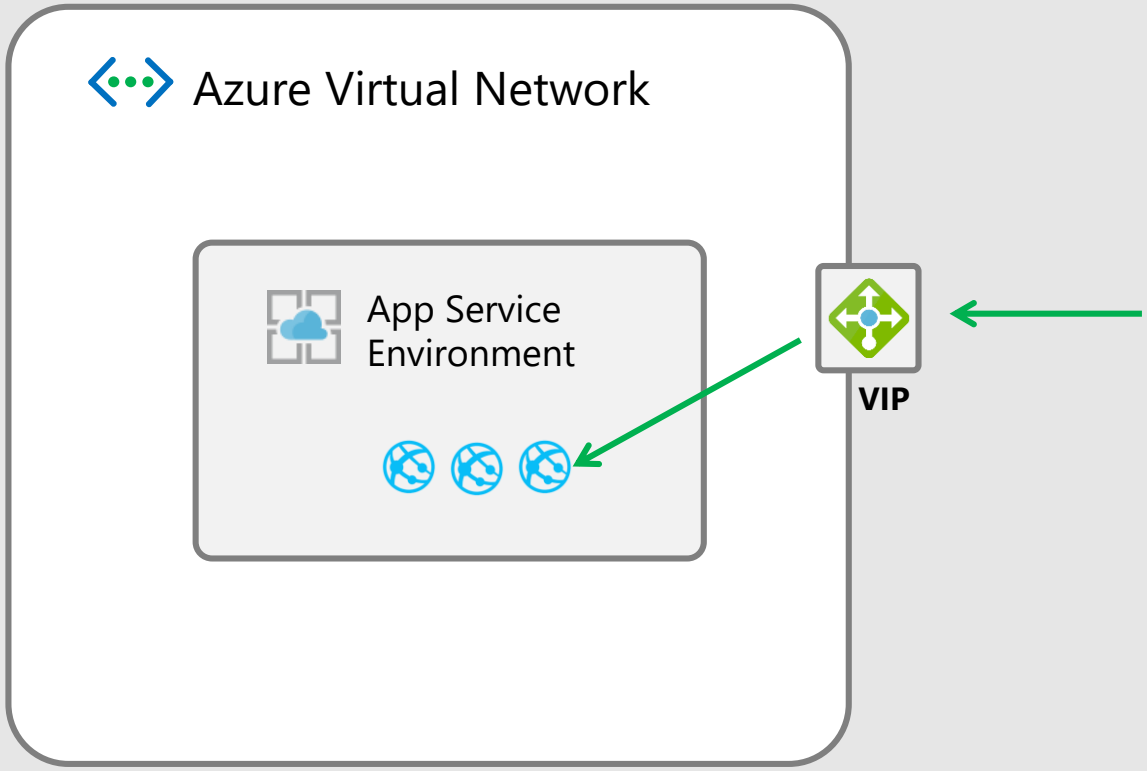
The ASE is a deployment of the Azure App Service into a subnet of a customer's Azure Virtual Network

The ASE provides:

- Network isolation for Apps
- Larger scale then multi-tenant
- More powerfull hosts
- Ability to work with all VPN types

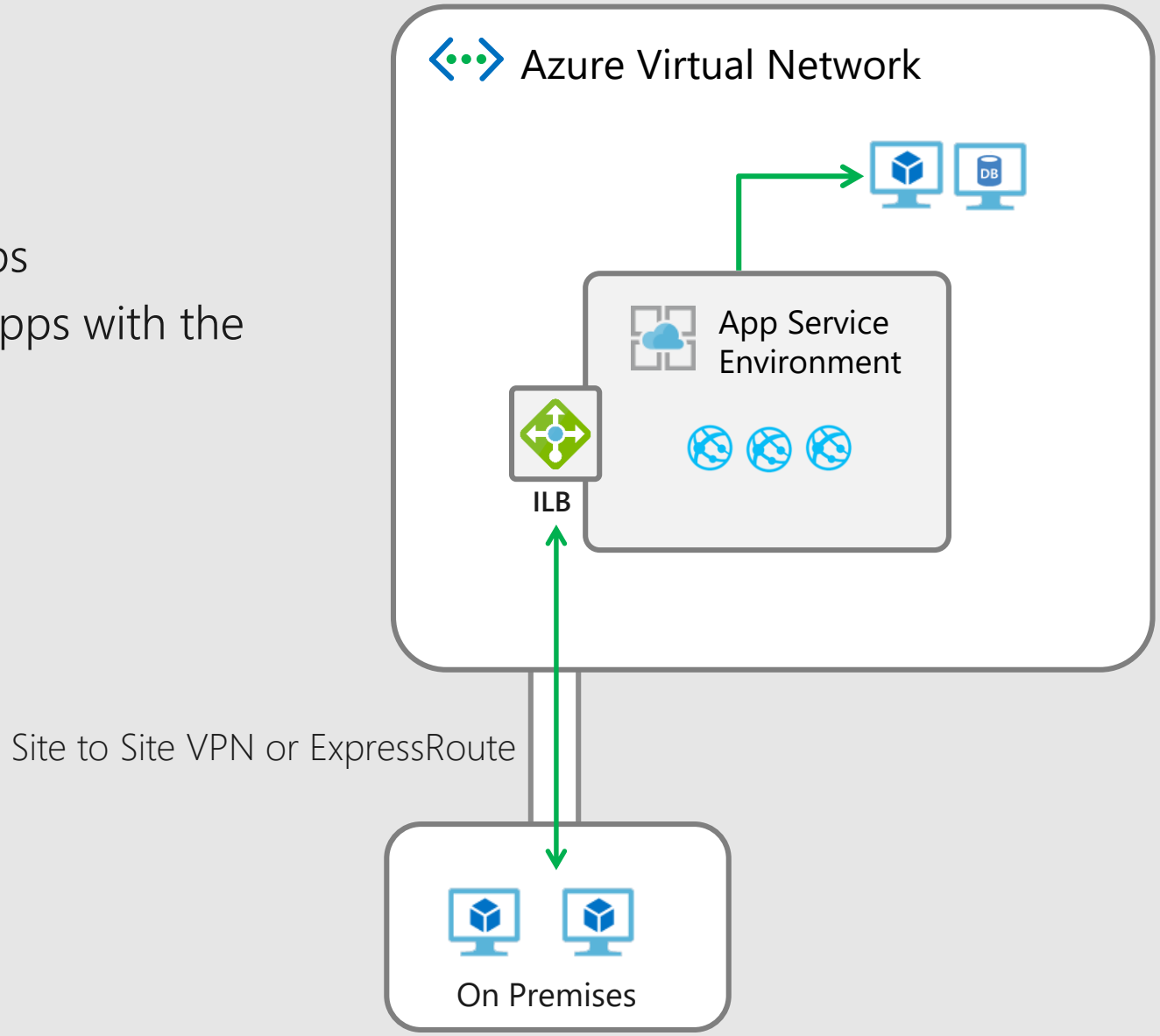
External ASE

- Assign an IP SSL Address to a single app
- Use NSGs to lock down access to that app
- Enables things like hosting a public app that calls an API App that only apps in the ASE can reach



ILB ASE

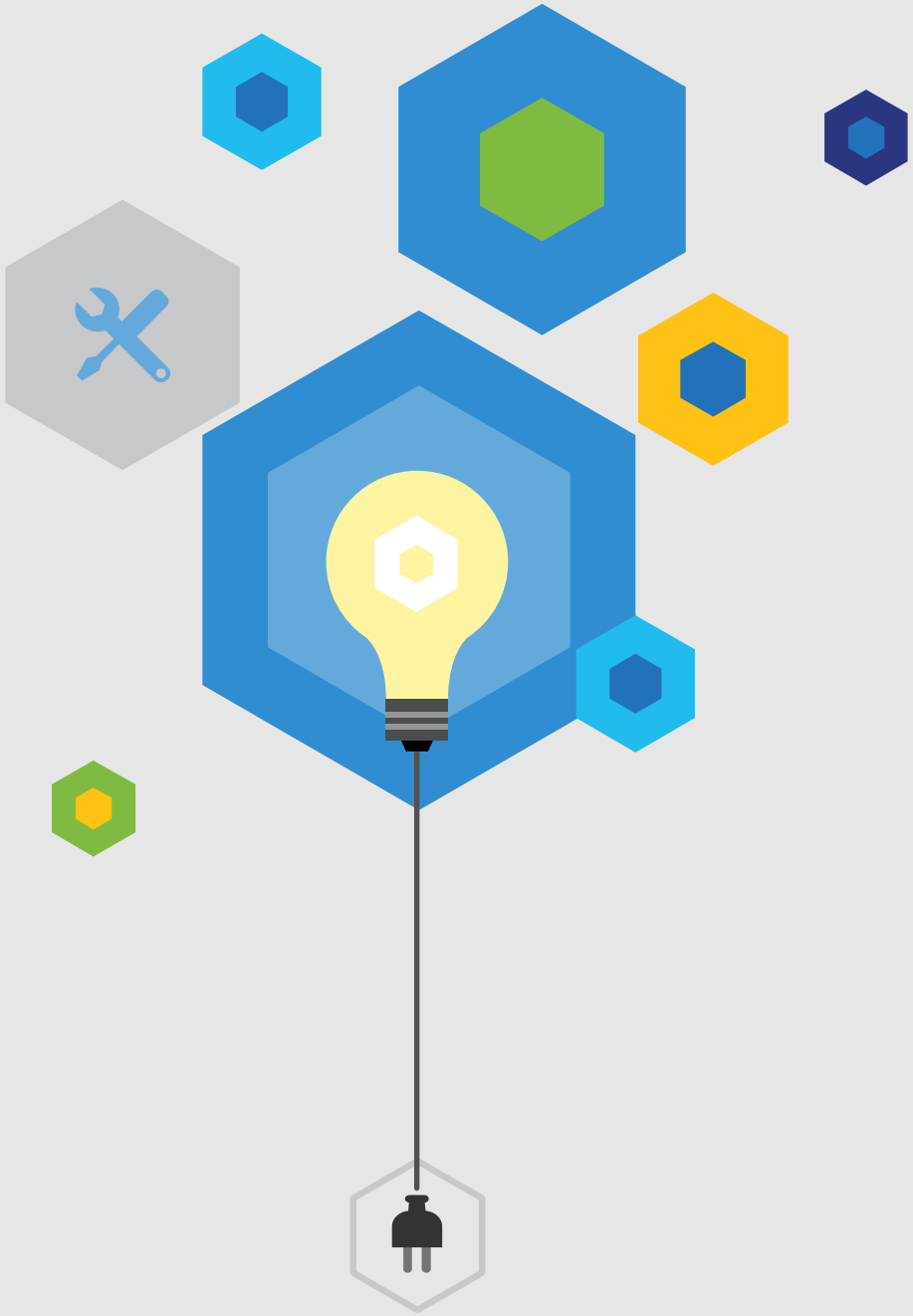
- Private IP address for your apps
- Use your own DNS and host apps with the DNS names you want to use



Demo

The following topics are shown:

- ASE
- Virtual Network
- Isolated App Service Plan
- Isolated Web App



Virtual Network Service Endpoints

Endpoints allow you to secure your critical Azure service resources to only your virtual networks.

Service endpoints provide the following benefits:

- Improved security for your Azure service resources
- Optimal routing for Azure service traffic from your virtual network
- Simple to set up with less management overhead

Azure Generally available

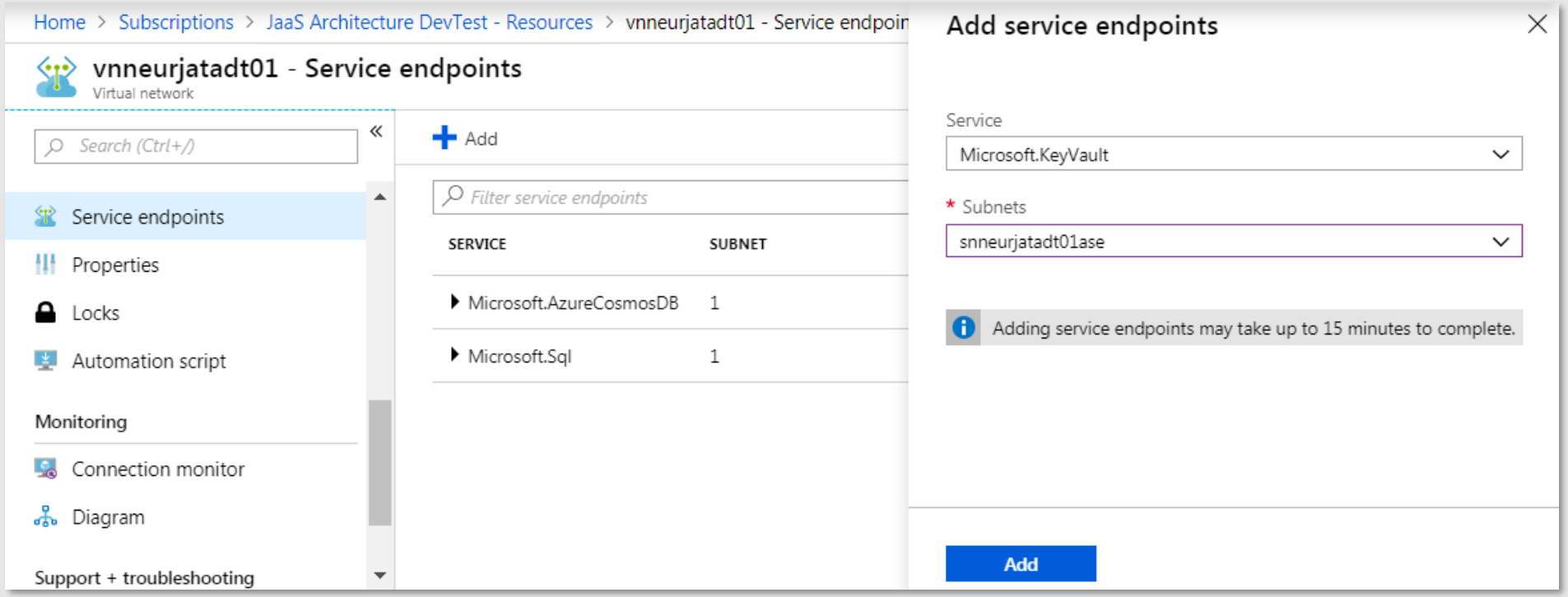
- Azure Storage
- Azure SQL Database
- Azure SQL Data Warehouse
- Azure Database for PostgreSQL server
- Azure Database for MySQL server
- Azure Database for MariaDB
- Azure Cosmos DB
- Azure Key Vault
- Azure Service Bus
- Azure Event Hubs
- Azure Data Lake Store Gen 1

Public Preview

- Azure Container Registry

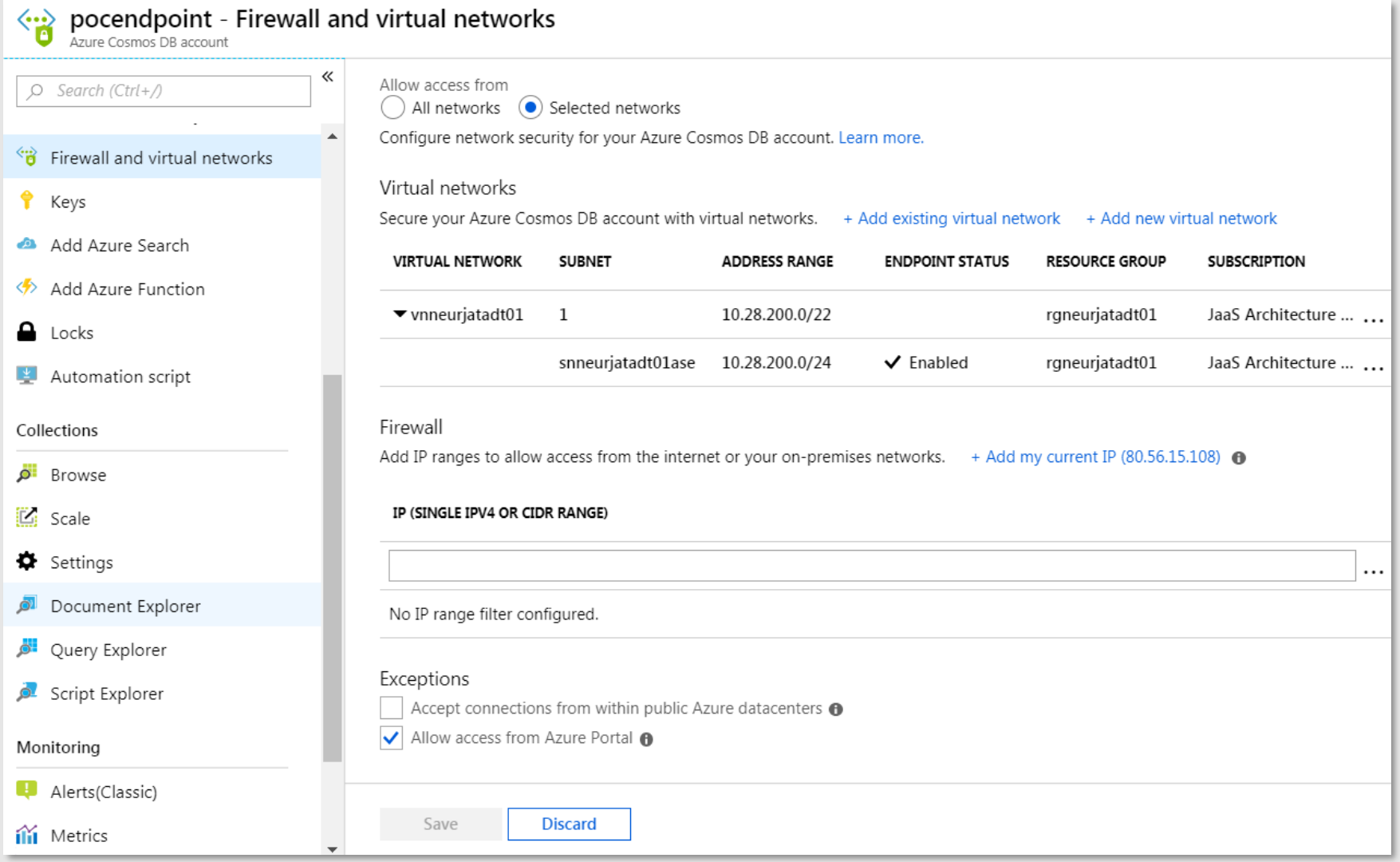
Configure service endpoint for an existing Azure virtual network and subnet

- From All resources blade, find the virtual network you want to configure service endpoint for Azure Cosmos DB.
- Navigate to the Service endpoints blade and make sure that the subnet of the virtual network has been enabled for the "Azure.CosmosDB" service endpoint.



Secure access to an Azure Cosmos DB account by using Azure Virtual Network service endpoint

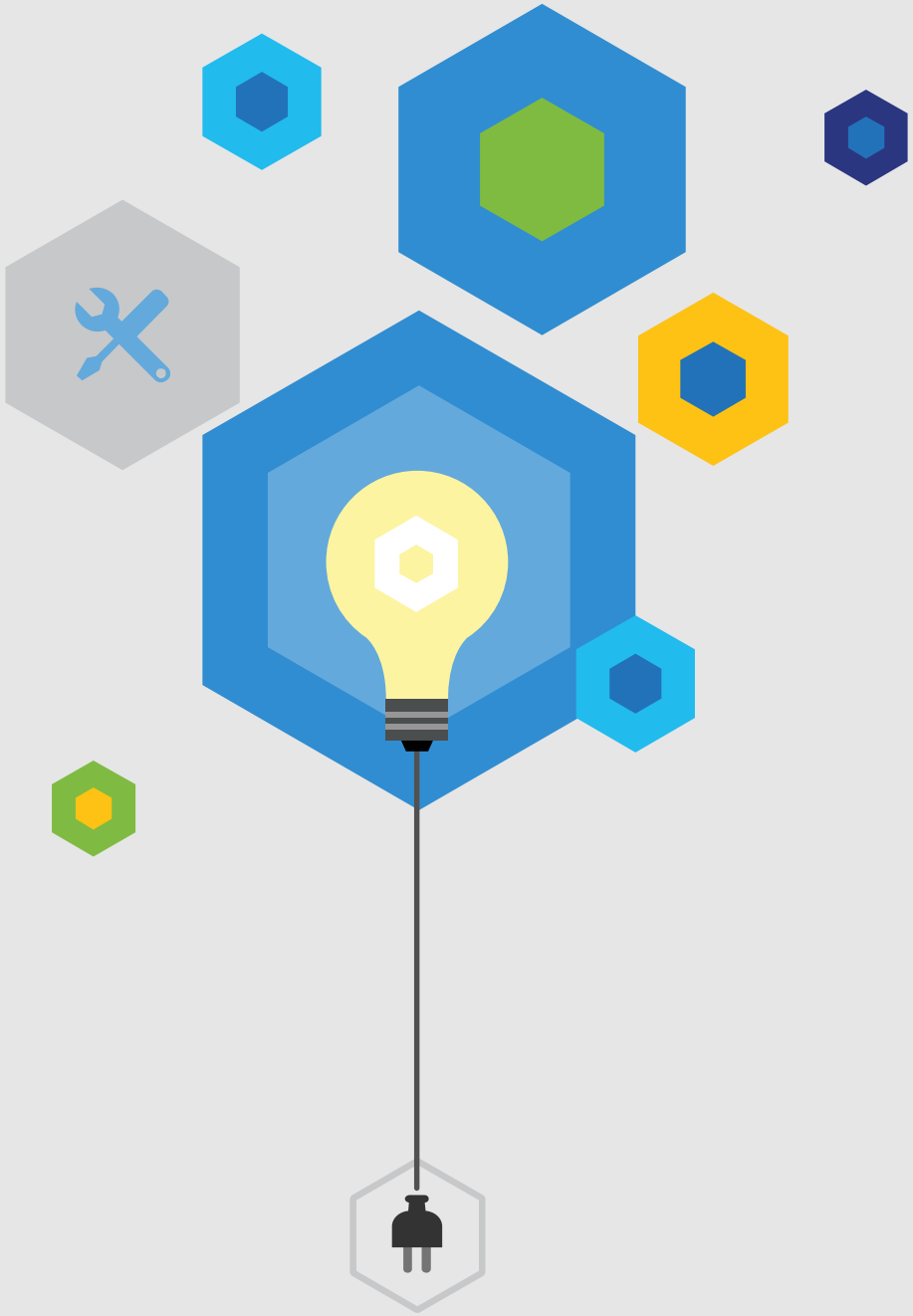
By enabling a Service Endpoint, traffic is ensured an optimal and secure route to the Azure Cosmos DB.



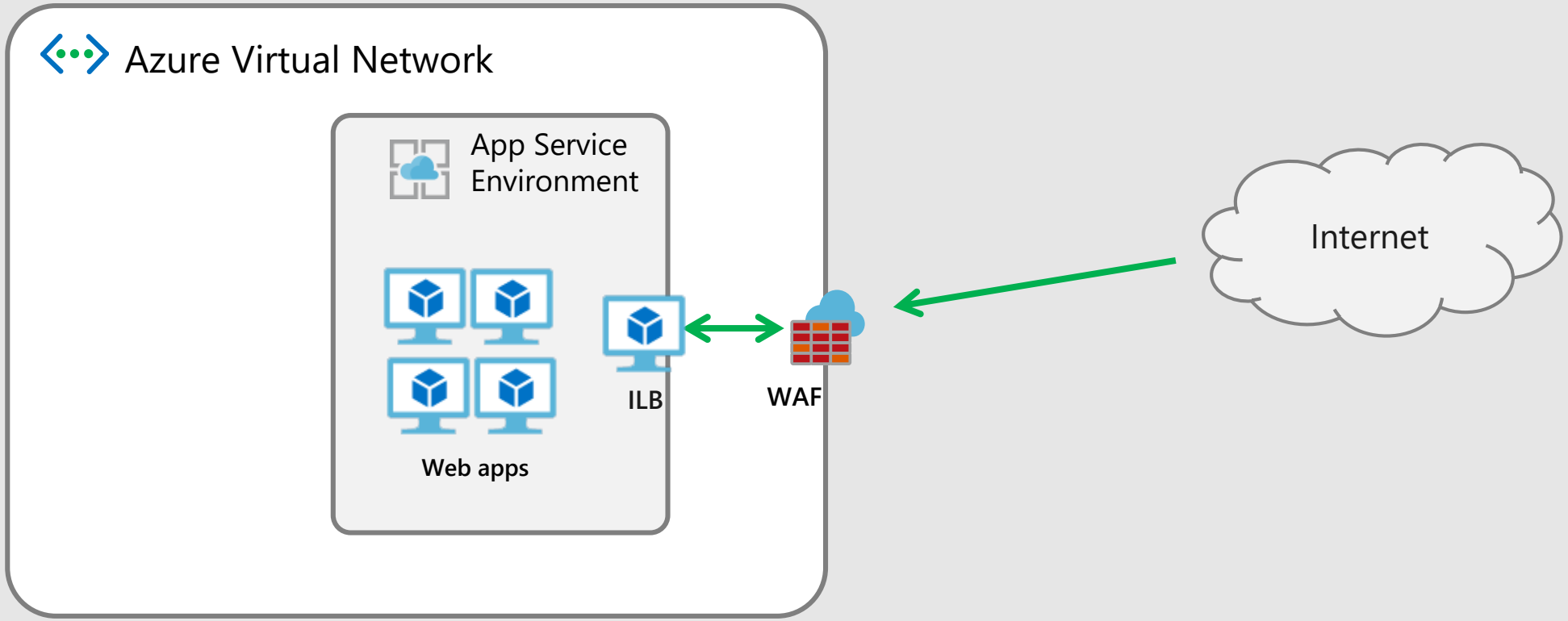
Demo

The following topics are shown:

- Service endpoints

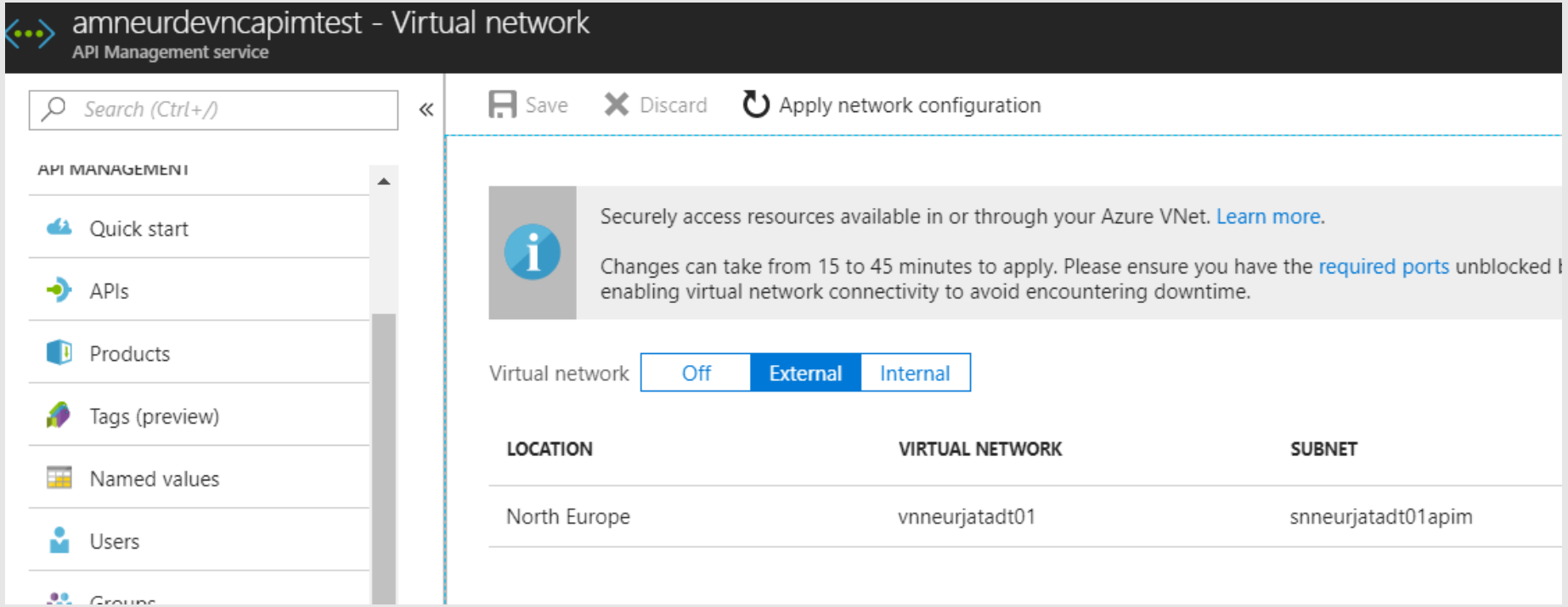


ILB ASE with Web Application Firewall (WAF)



API Management

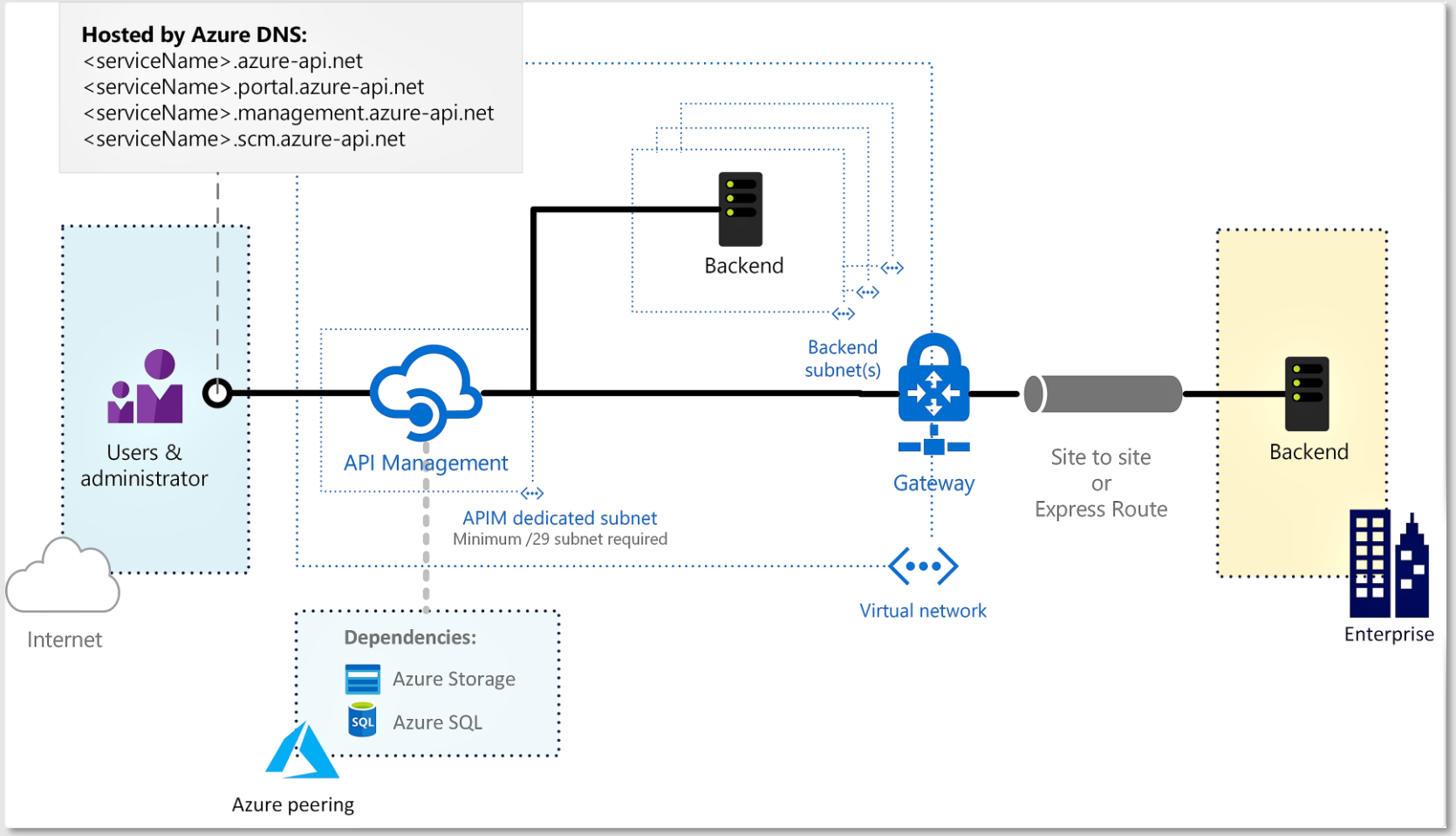
- API Management is configured as “External”
- Allows External IP address to be exposed for public connections
  - Internal VNET integration for accessing internal resources such as ASE hosted Azure functions



Using Azure API Management with virtual networks

External

- the API Management gateway and developer portal are accessible from the public internet via an external load balancer.
- The gateway can access resources within the virtual network.



API Management pricing

Pricing details

	CONSUMPTION PREVIEW	DEVELOPER	BASIC	STANDARD	PREMIUM
Purpose	Gateway component of API Management offered on a pay-per-use basis	Non-production use cases and evaluations	Entry-level production use cases	Medium-volume production use cases	High-volume or Enterprise production use cases
Price (per unit)	€1.475775[4] per million calls (1M calls for free[3])	~€40.51/month	~€124.11/month	~€579.11/month	~€2,357.17/month
Cache (per unit)	External only	10 MB	50 MB	1 GB	5 GB
Scale-out (units)	N/A (automatic scaling)	1	2	4	10 per region (call support to add more)
SLA	99.9%	No	99.9%	99.9%	99.95% [1]
Azure Active Directory integration	No	Yes	No	Yes	Yes
Virtual Network support	No	Yes	No	No	Yes
Multi-region deployment	No	No	No	No	Yes
Estimated Maximum Throughput[2] (per unit)	N/A (automatic scaling)	500 requests/sec	1,000 requests/sec	2,500 requests/sec	4,000 requests/sec

Questions

@tlagroenendijk

linkedin.com/in/tomassogroenendijk

ithero.nl