

# Using VNETs in PaaS solutions

Tomasso Groenendijk



# Tomasso Groenendijk

## EMEA Solution Architect



@tlagroenendijk



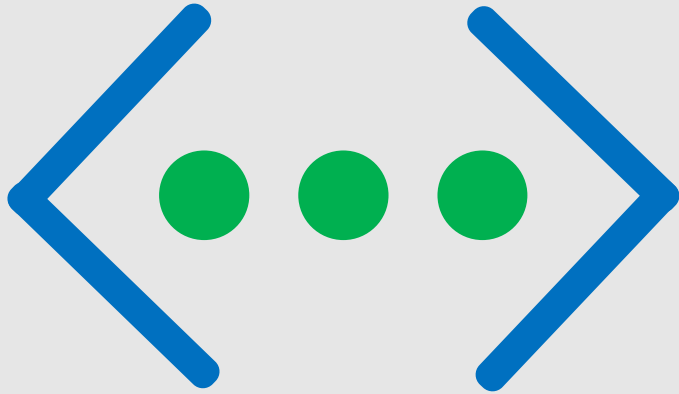
[linkedin.com/in/tomassogroenendijk](https://www.linkedin.com/in/tomassogroenendijk)



[ithero.nl](https://ithero.nl)



# Azure Virtual Network (VNet)



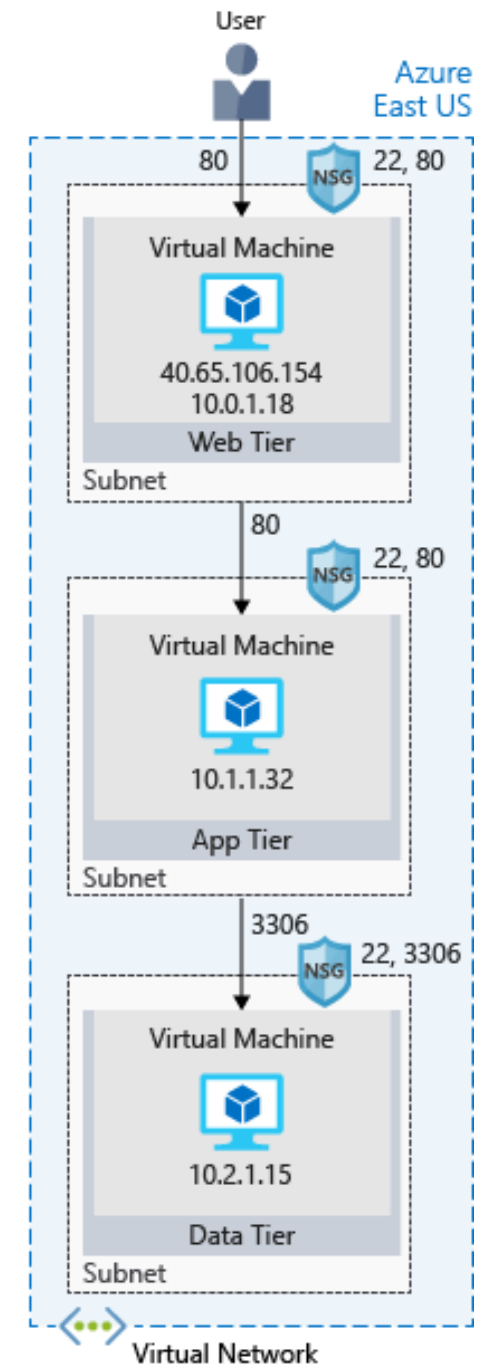
Azure Virtual Network enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks

Azure Virtual Network provides the following key capabilities:

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

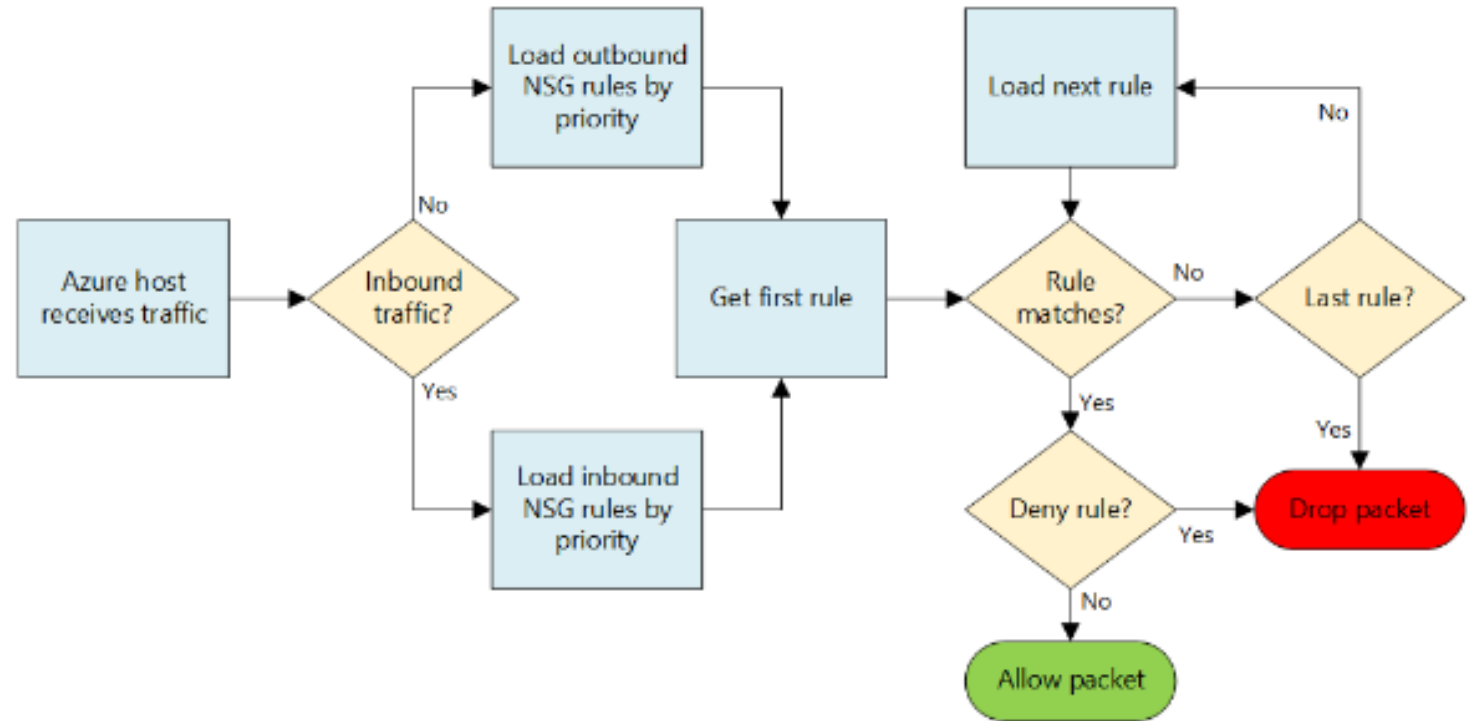
# Azure infrastructure services hierarchy

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



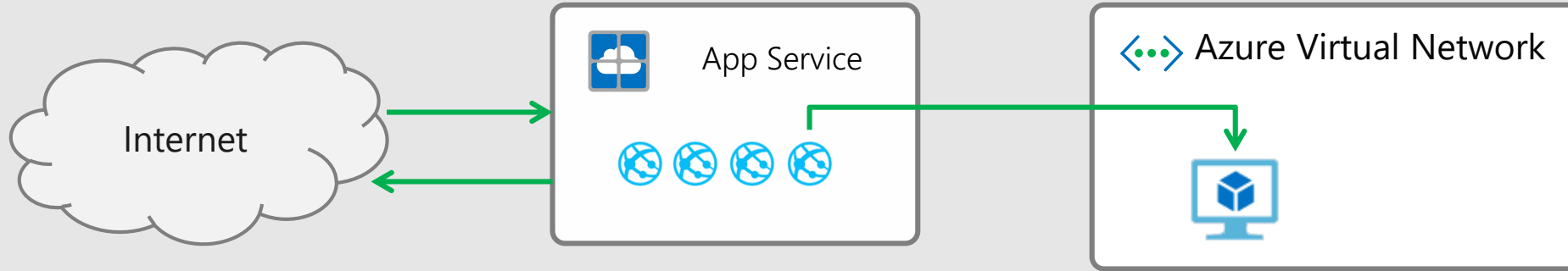
# Network Security Group

- 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

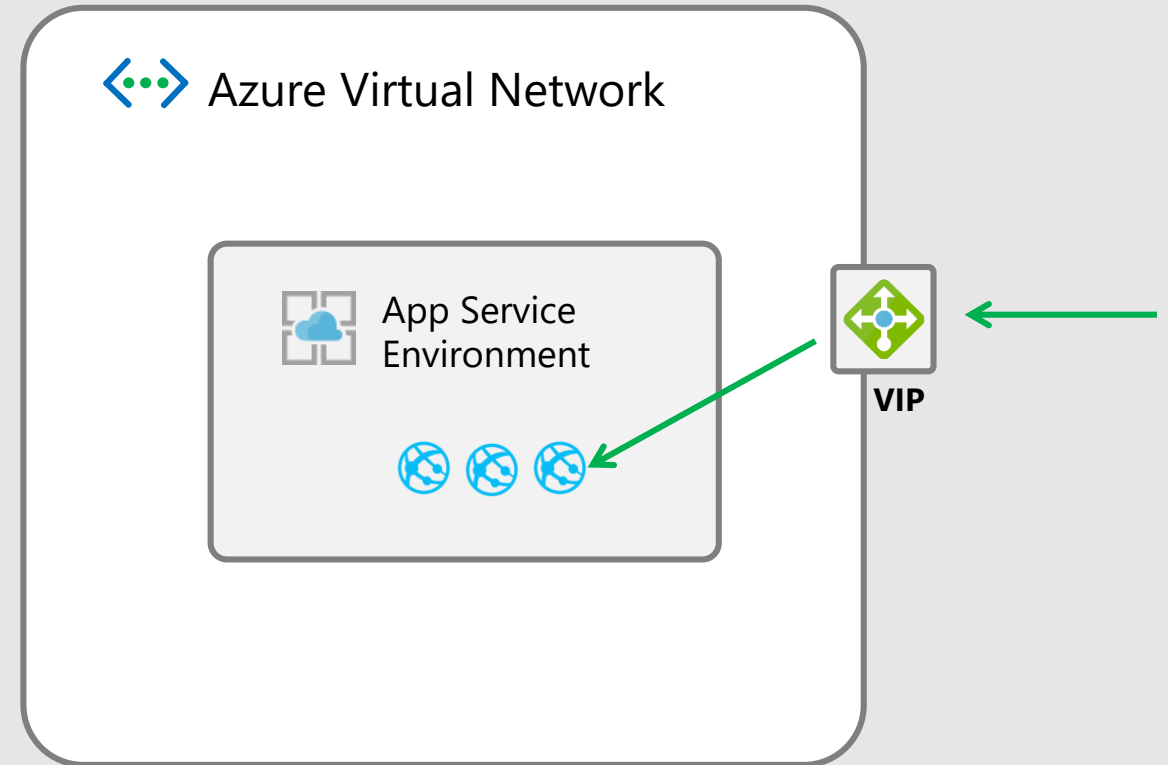
The ASE provides:

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



# External ASE

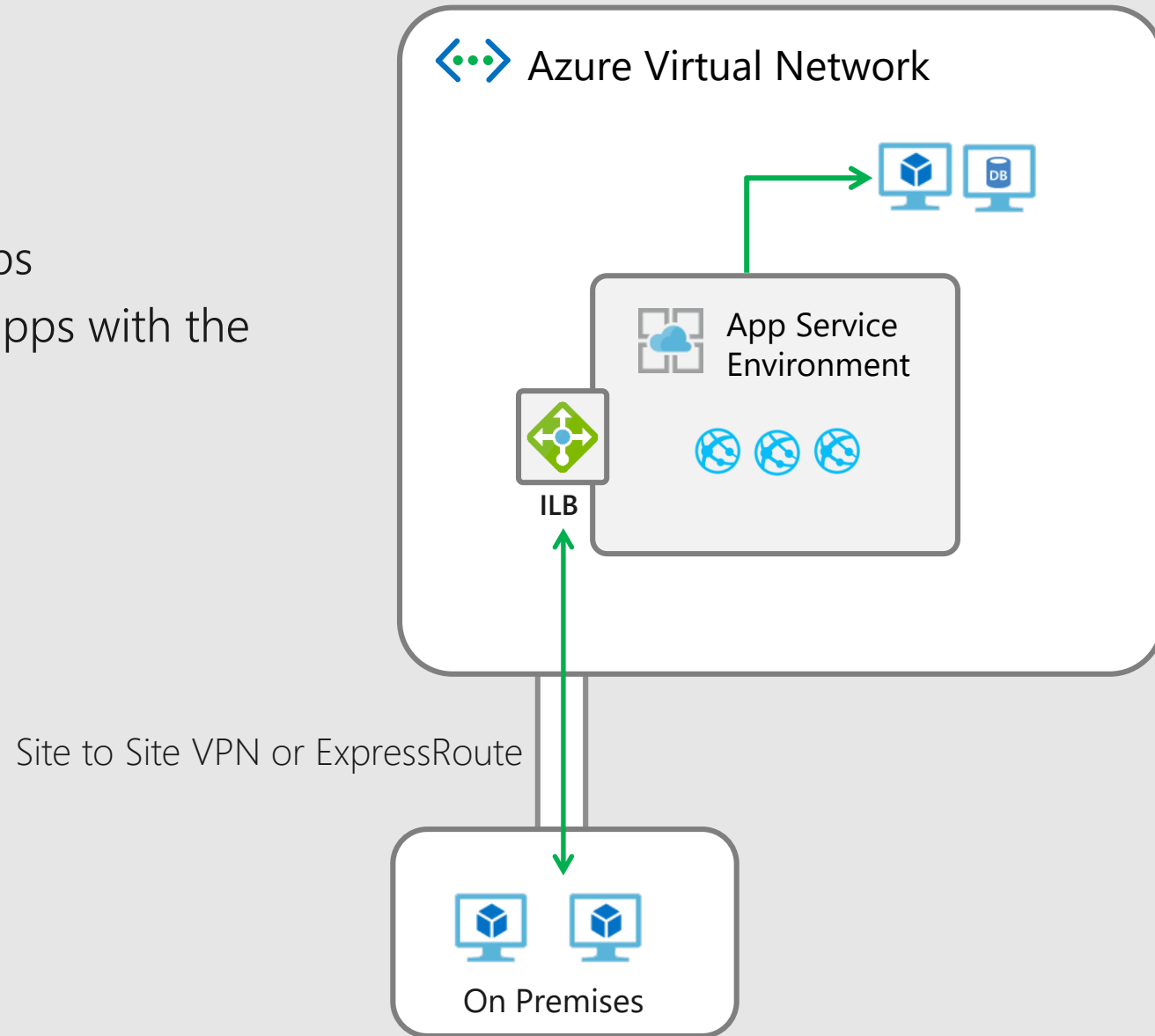
- Assign an IP SSL Address to a single app
- Use NSGs to lock down access to that app
- Enables things like hosting a public app that calls an API App that only apps in the ASE can reach





# ILB ASE

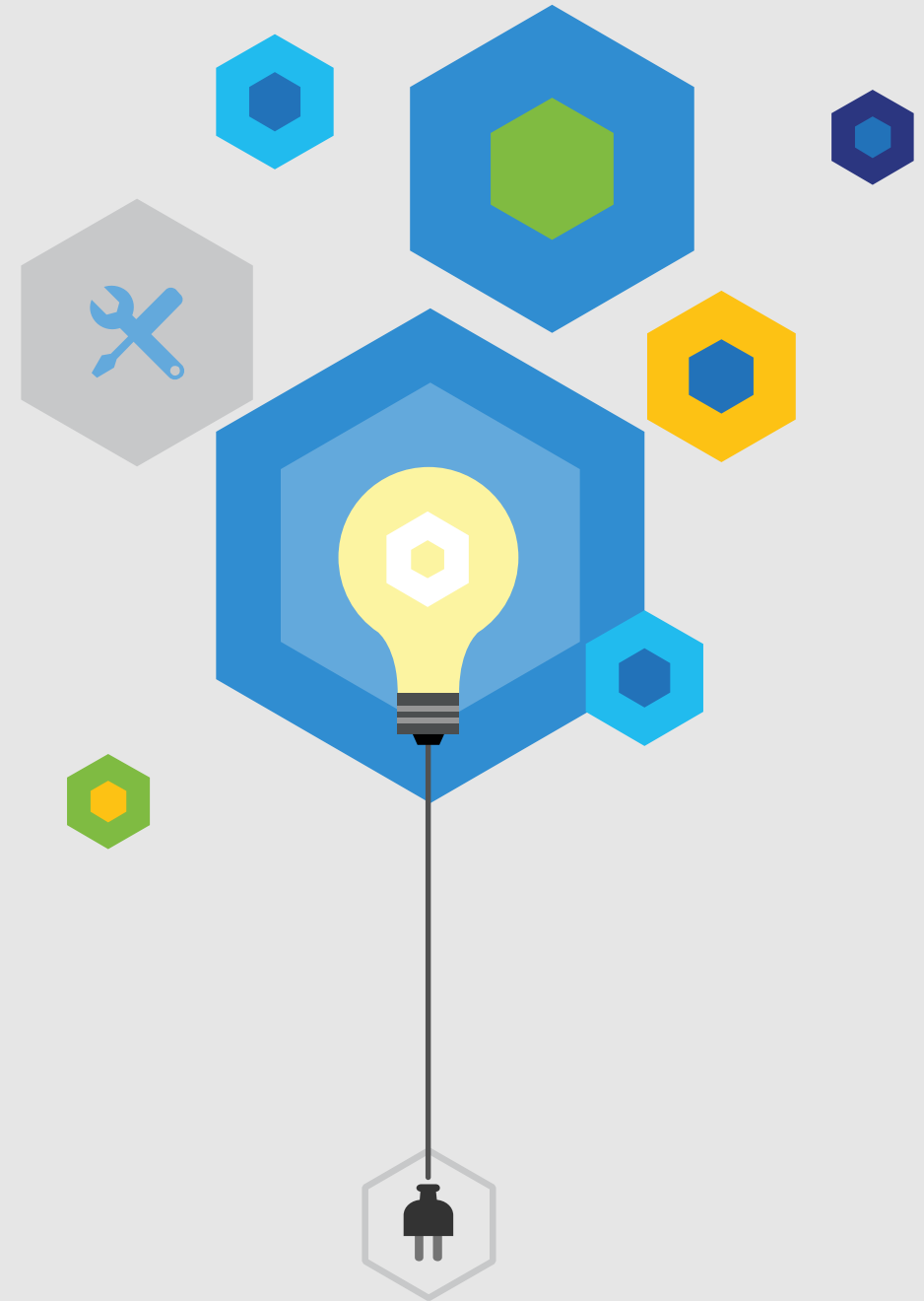
- Private IP address for your apps
- Use your own DNS and host apps with the DNS names you want to use



# 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.

The screenshot displays the Azure portal interface for configuring service endpoints on a virtual network. The main blade, titled 'vnneurjatadt01 - Service endpoints', shows a list of configured endpoints:

SERVICE	SUBNET
Microsoft.AzureCosmosDB	1
Microsoft.Sql	1

The 'Add service endpoints' dialog is open, showing the configuration for a new endpoint:

- Service:** Microsoft.KeyVault
- Subnets:** snneurjatadt01ase

An information message states: 'Adding service endpoints may take up to 15 minutes to complete.' An 'Add' button is visible at the bottom of the dialog.

# 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.

**pocendpoint - Firewall and virtual networks**  
Azure Cosmos DB account

Search (Ctrl+)

Firewall and virtual networks

Keys

Add Azure Search

Add Azure Function

Locks

Automation script

Collections

Browse

Scale

Settings

Document Explorer

Query Explorer

Script Explorer

Monitoring

Alerts(Classic)

Metrics

Allow access from  
☐ All networks ☒ Selected networks

Configure network security for your Azure Cosmos DB account. [Learn more.](#)

Virtual networks  
Secure your Azure Cosmos DB account with virtual networks. [+ Add existing virtual network](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
▼ vnneurjatadt01	1	10.28.200.0/22		rgneurjatadt01	JaaS Architecture ...
	snneurjatadt01ase	10.28.200.0/24	✓ Enabled	rgneurjatadt01	JaaS Architecture ...

Firewall  
Add IP ranges to allow access from the internet or your on-premises networks. [+ Add my current IP \(80.56.15.108\)](#)

IP (SINGLE IPV4 OR CIDR RANGE)

No IP range filter configured.

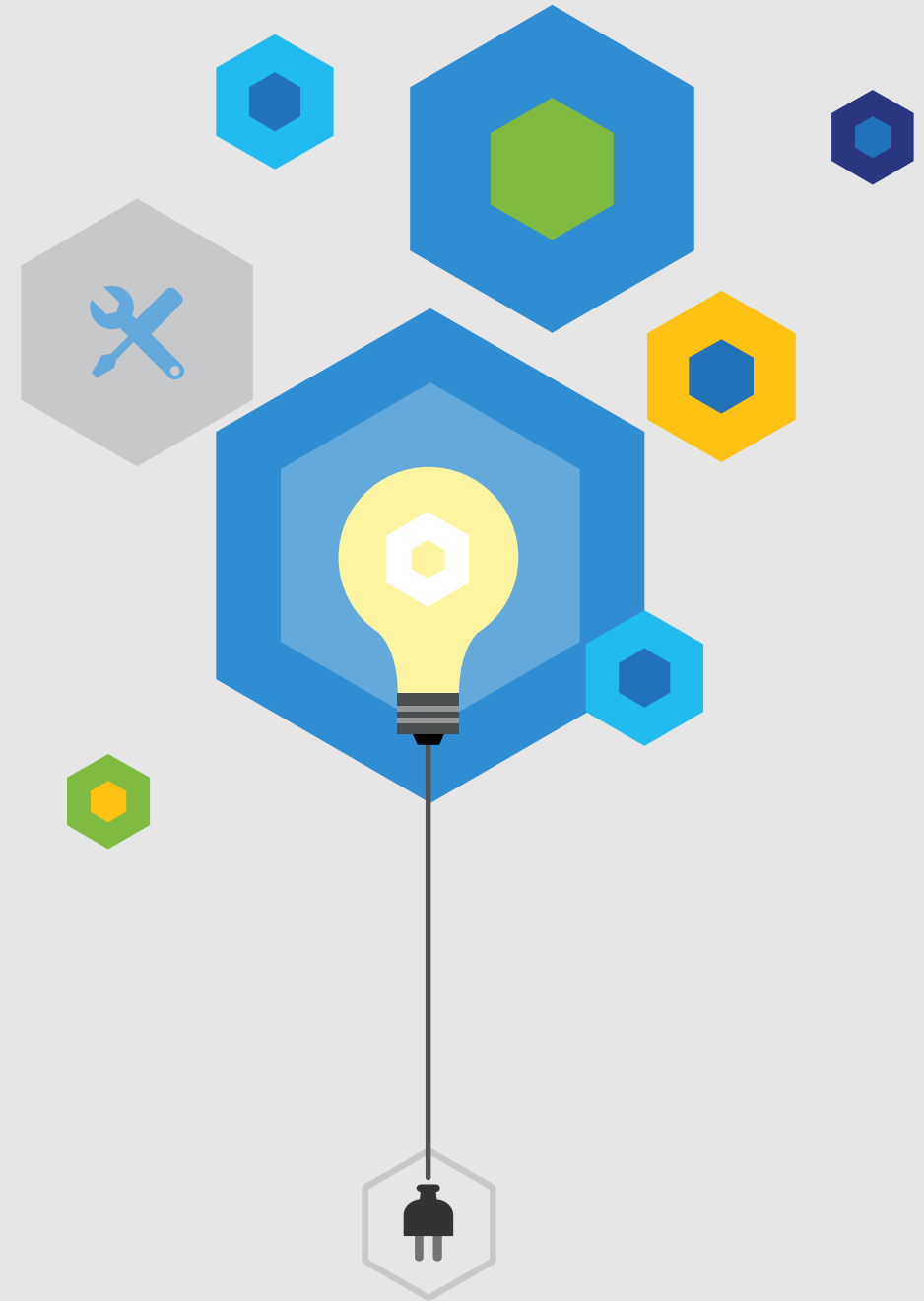
Exceptions  
☐ Accept connections from within public Azure datacenters  
☒ Allow access from Azure Portal

Save Discard

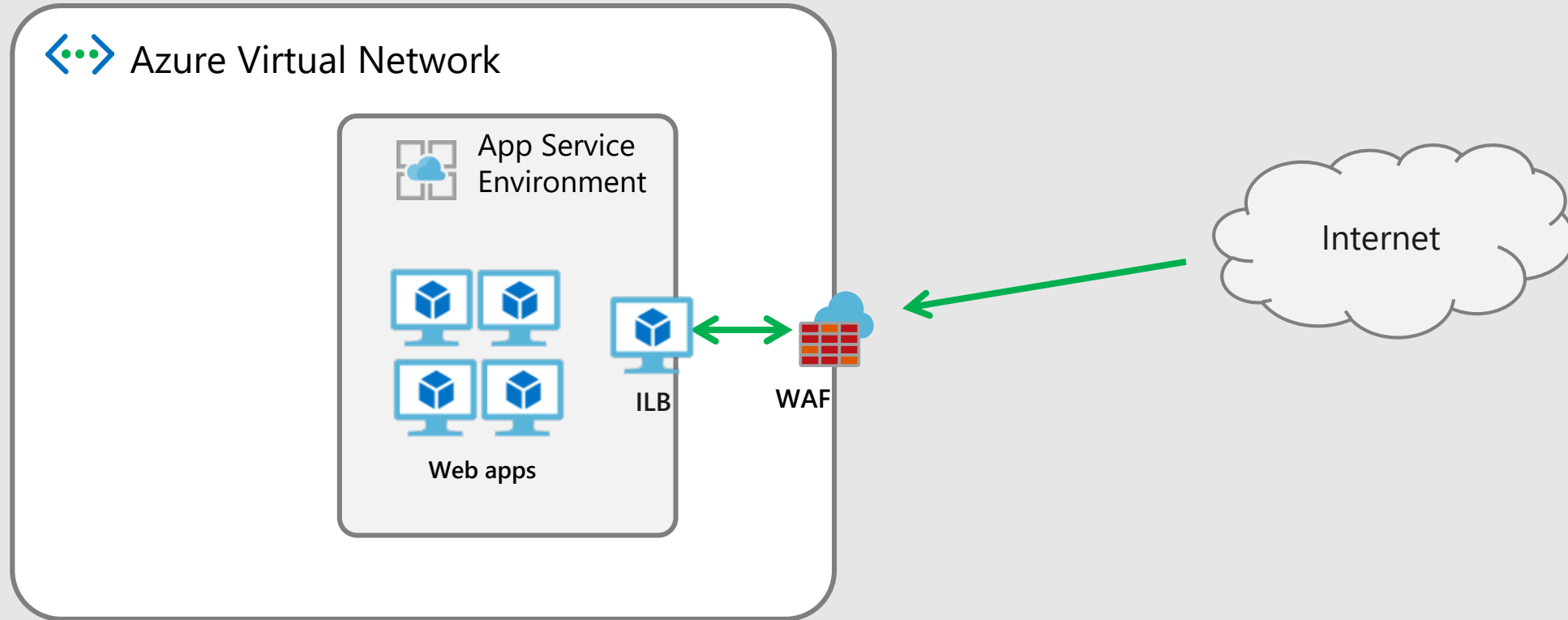
# Demo

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

The screenshot shows the Azure API Management console for the instance 'amneurdevncapimtest'. The left sidebar contains a navigation menu with options: Quick start, APIs, Products, Tags (preview), Named values, Users, and Groups. The main content area is titled 'Virtual network' and features a top bar with 'Save', 'Discard', and 'Apply network configuration' buttons. Below this, an information box states: 'Securely access resources available in or through your Azure VNet. Learn more. Changes can take from 15 to 45 minutes to apply. Please ensure you have the required ports unblocked I enabling virtual network connectivity to avoid encountering downtime.' The 'Virtual network' section has three tabs: 'Off', 'External' (which is selected), and 'Internal'. Below the tabs is a table with the following data:

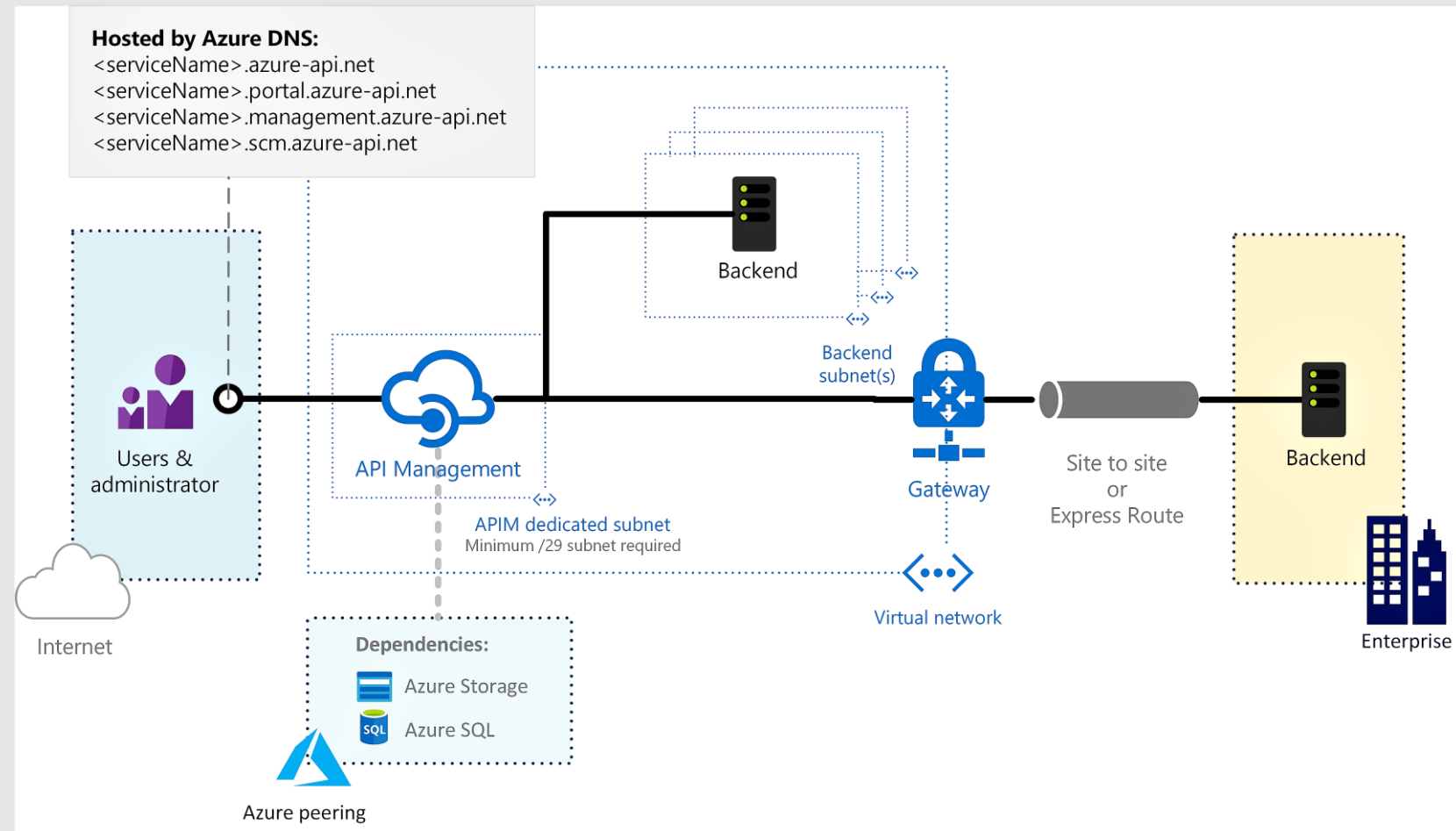
LOCATION	VIRTUAL NETWORK	SUBNET
North Europe	vnneurjatadt01	snneurjatadt01apim



# 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 <small>PREVIEW</small>	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 <sup>4</sup> per million calls (1M calls for free <sup>3</sup> )	~€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% <sup>1</sup>
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 <sup>2</sup> (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](https://www.linkedin.com/in/tomassogroenendijk)



[ithero.nl](https://ithero.nl)