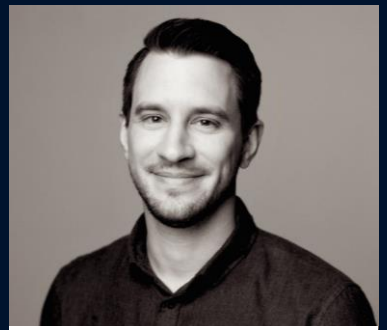
nic Cloud Connect

Mats Estensen

Deciphering Azure Private Endpoints

Mats Estensen



devoteam

- mats.estensen@devoteam.no
- Find me online: @matsest (GitHub, LinkedIn)
- Web: mxe.no

- 🥷 Cloud and DevOps Architect @ Devoteam M Cloud
- 🛠️ 9 yrs of infra engineering / consultancy + infra dev/ops experience
- Working on:
  - 💡 Enablement and adoption of cloud platforms in cloud transformation
  - ☁️ Cloud architecture
  - 🤖 Automating … everything
- Personal: Music fanatic 🎸, skydiver 🪂, skateboarder 🛹 and following Strømsgodset ⚽

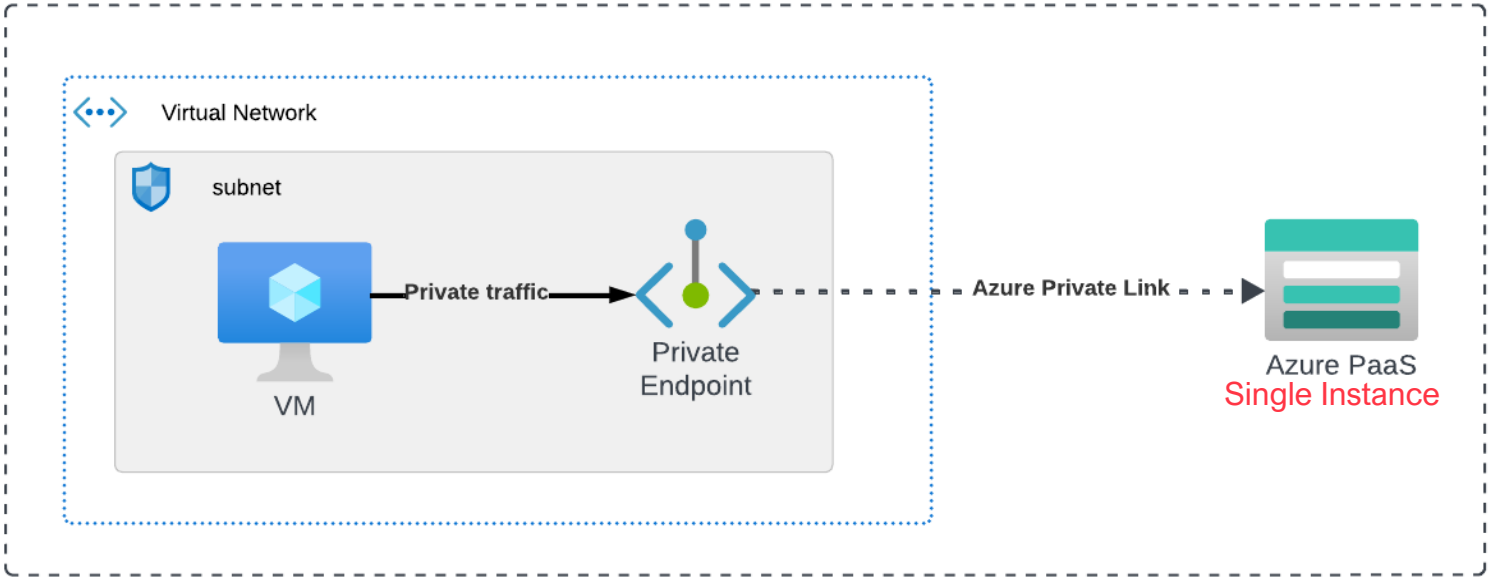
This session

- 🧐 What are private endpoints?
- 👀 Seeing is believing
- 👉 When should we use private endpoints?
- ☠️ Pitfalls and gotchas

nic Cloud Connect

PRIVATE ENDPOINTS?

What are Private Endpoints?



Bringing public Azure cloud services into your own virtual network

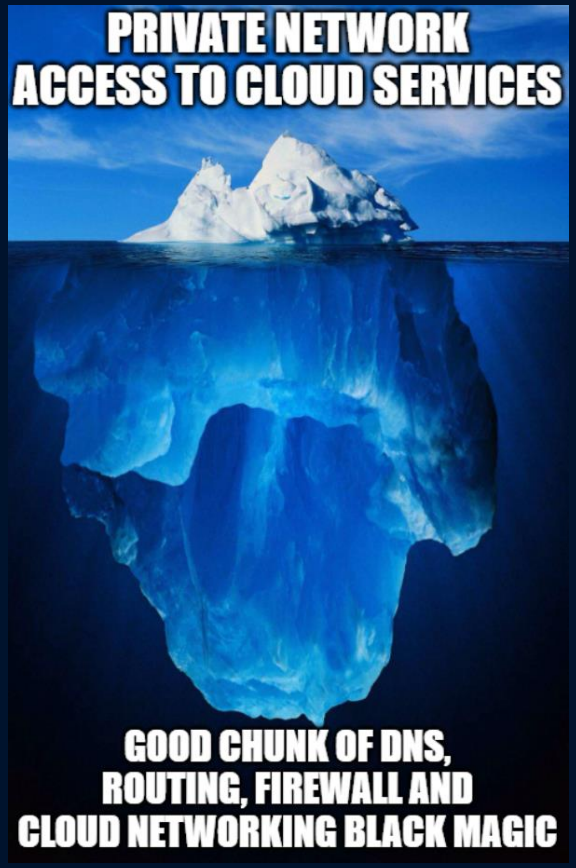
Why are people interested in private endpoints?

- Increasing support across services in Azure driven by enterprise customer demand

- Big focus from MS and other cloud vendors
  - Security benchmarks in Azure Policy
  - Service-specific security baseline recommendations
  - Enterprise-Scale / CAF design areas
  - Mentioned in (almost) every MS Learn documentation page regarding networking security

- Looks like a obvious quick-win for security?
  - “Privately access services on the Azure platform”
  - “Protection against data leakage”

Why am I talking about private endpoints?



nic Cloud Connect

By enabling private endpoints you …

- ☑ Do: Enable *private* network access to your PaaS resource
- ❌ Do not: Secure the PaaS resource by all means
  - Does also not disable public access by itself (with some exceptions)

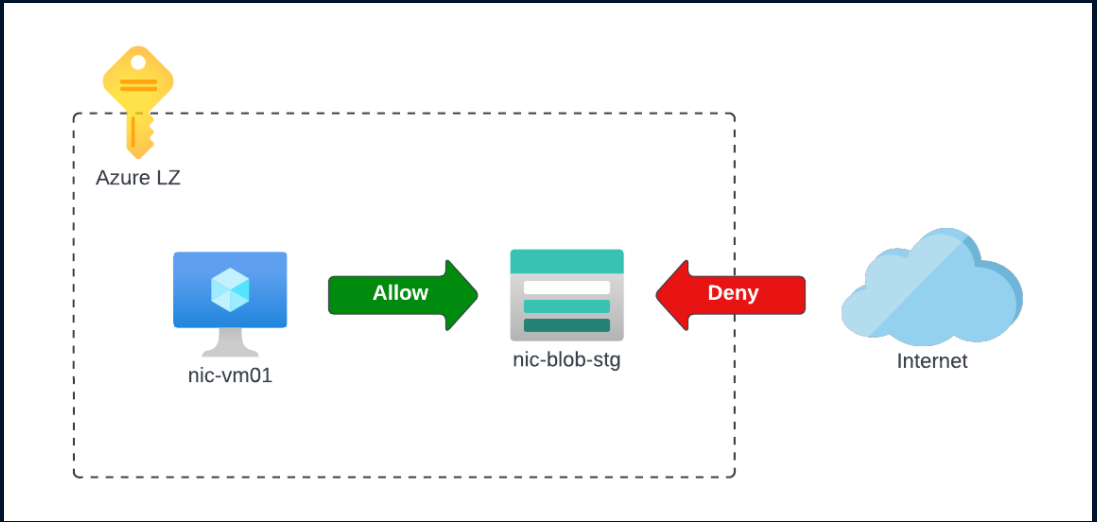
Considerations:

- Most PaaS Resources in Azure are natively designed for public consumption
- Secure defaults?
- Private networks are not inherently «secure» - even in the cloud
- Your service still runs in the public cloud! This cloud «perimeter» is a blurry line

DEMO

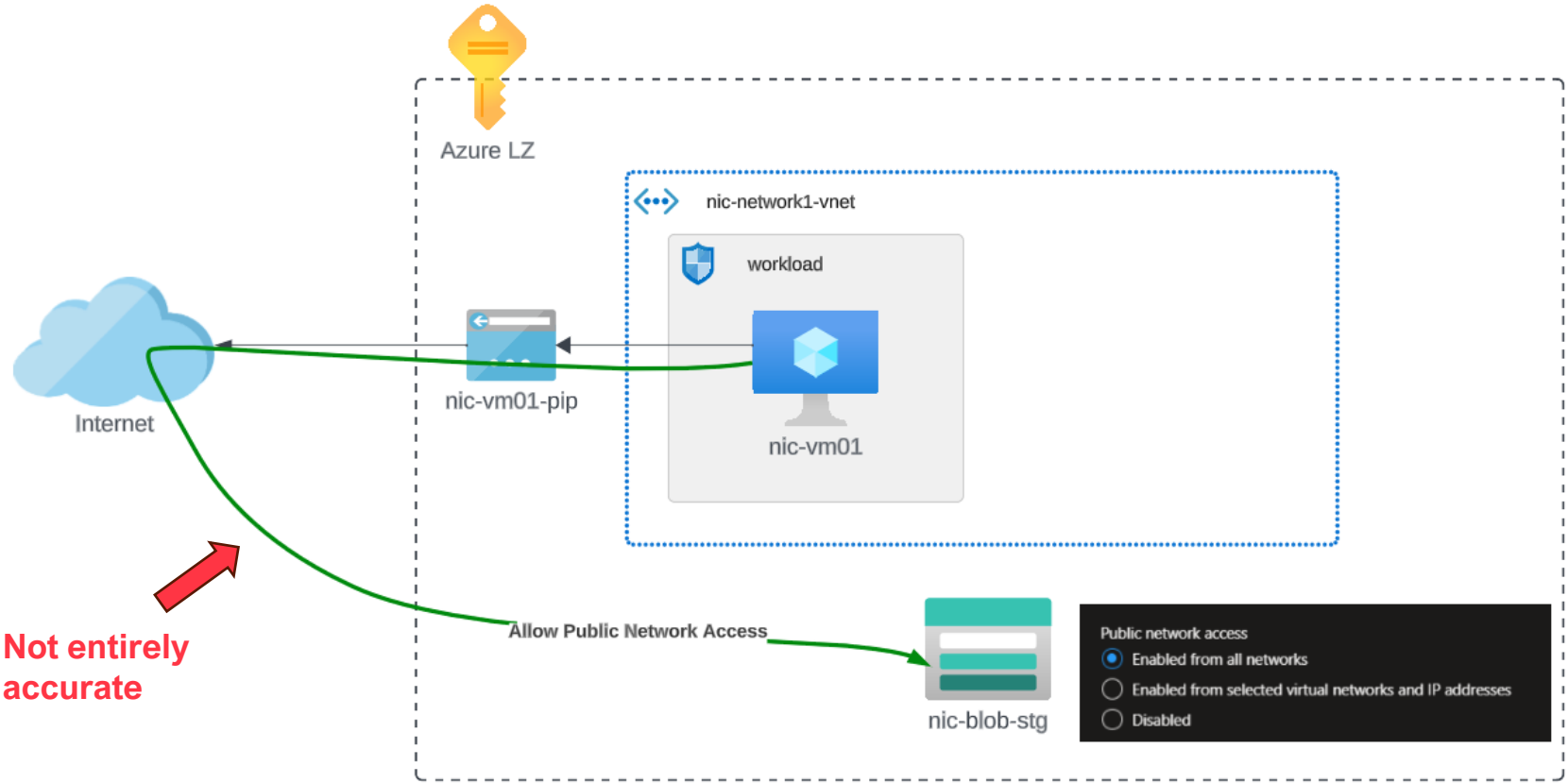
PaaS Networking - Azure Storage example

- *PrivateCorp* have top secret files on Azure Blob Storage
- Must limit access to their files from dedicated servers running in Azure
- What are their options?



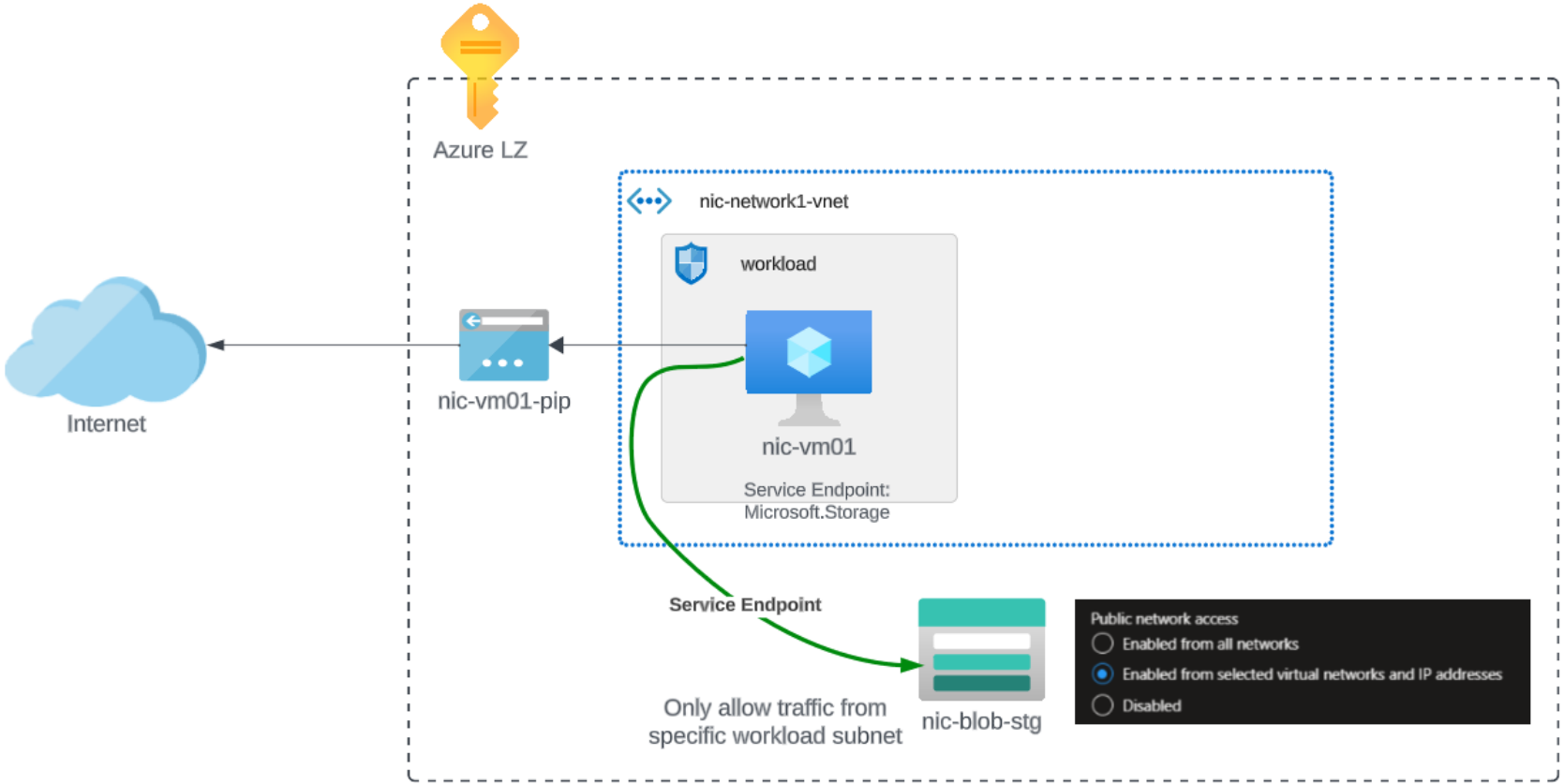
Option 1: Public

- Keep public access
- Implement secure authentication settings (Managed Identity on VM, secure stg. acc. config)



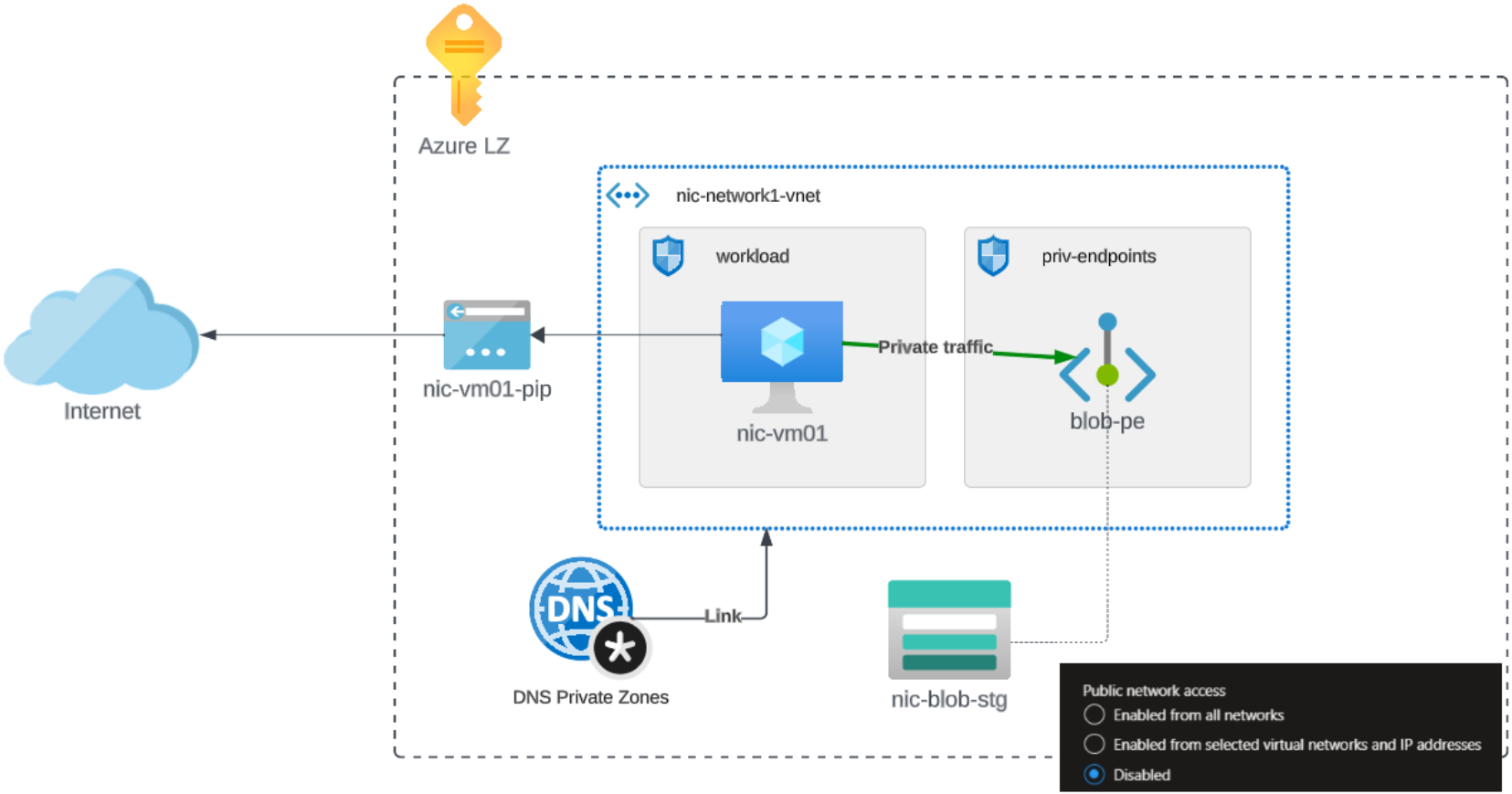
Option 2: Service Endpoints

- Restrict public access
- (Still) implement secure authentication settings



Option 3: Private Endpoints

- Actively disable public access
- (Even still) implement secure authentication settings



Comparison (Storage example)

	Public Access	Service Endpoint	Private Endpoint
Traffic Flow	Over Internet* - Public IP	Microsoft backbone – Public IP	Within virtual network(s) – Private IP
PaaS Network FW (inbound)	Enabled from all networks**	Enabled from specific subnets	Disabled (NSG active if network policy enabled)
Source NSG filtering (outbound)	Internet	Storage service***	Specific private IP
Additional Configuration	None	Service Endpoint in subnet, NSG	Private Endpoint, Private DNS Zones, Subnet configuration, NSG
Additional Cost	None	None	~80 NOK/month (PE) + PE traffic in/out (+ DNS)

* Inter-region traffic will stay within Azure Region DC
** Can't use VM PIP as whitelisted source within region
*** Use service endpoint network policy for per storage account filtering

What can go wrong?

Cloud Misconfigurations

Below are a few examples of cloud misconfigurations and statistics.

1. In February 2022, a misconfiguration in Google Cloud Storage resulted in the exposure of the personal information of over 23 million customers of a sports retailer.
2. In March 2022, a misconfigured storage bucket in Microsoft Azure led to the leak of financial data and personally identifiable information (PII) of more than 5 million users of a health app.
3. In April 2022, a misconfiguration in Amazon Web Services (AWS) was responsible for the leak of 533 million Facebook user records.
4. In May 2022, a cloud misconfiguration at McDonald's exposed employee information, including Social Security numbers and bank account details, of nearly 12,000 workers across North America.

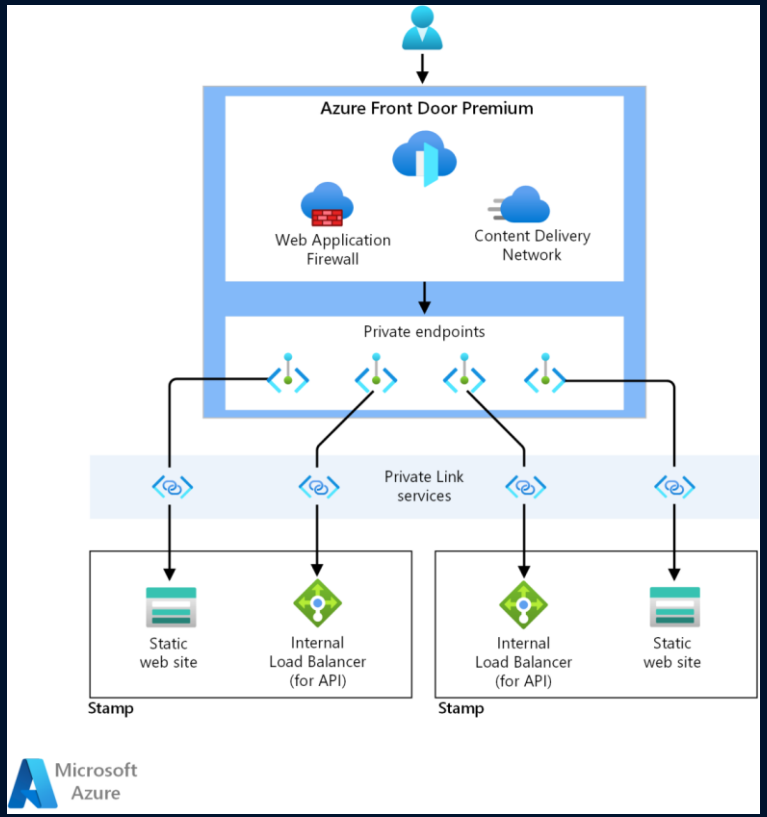
Cloud Security Threats and Predictions in 2023 | CSA (cloudsecurityalliance.org)

What can go wrong? (Storage example)

	Public Access	Service Endpoint	Private Endpoint
Risk: Public Network Exposure	Inherent	One click away	One click away(!)
Risk: Unauthorized Access	One click away	One click away	One click away
Impact: Auth-related Misconfiguration	High	Medium	Medium
Probability: Other Misconfigurations	Low	Low	Medium-High
Impact of Other Misconfigurations	High	Medium	Medium
Configuration Complexity	Low	Low	Medium-High

USECASES

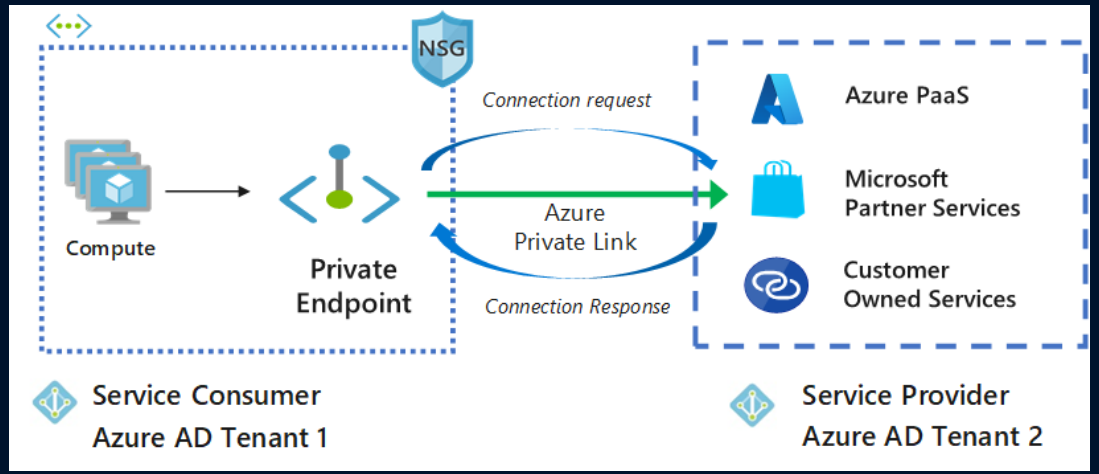
Use case: Making your backend services privately networked



- **Challenge:** Require privately networked lower tiers (API, Data, etc)
- **What:** N-tier design with secure public-facing services
- **Examples:** Application Gateway, Front Door, API Gateway

Networking and connectivity for mission-critical workloads on Azure - Azure Architecture Center | Microsoft Learn

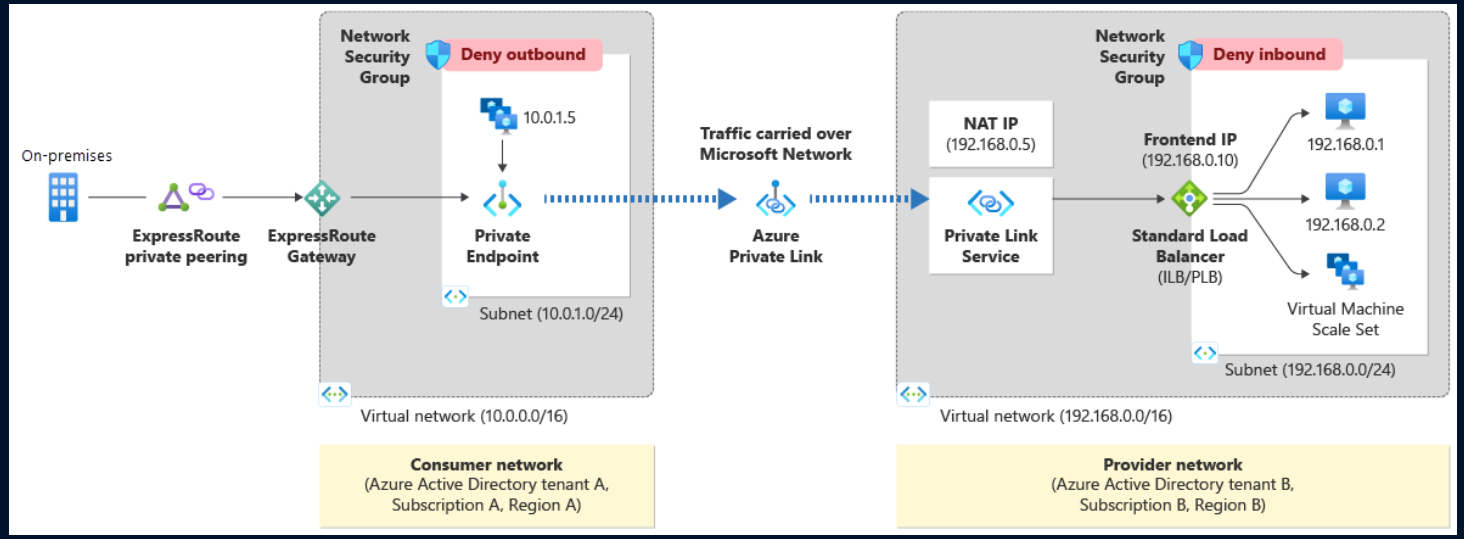
Use case: Connecting to a private service in another tenant



- **Challenge:** Secure private networking without VPN
- **What:** Provider / consumer pattern across tenants
- **Examples:** Give a client/partner access to your storage account for delivering files

Manage Azure Private Endpoints - Azure Private Link | Microsoft Learn

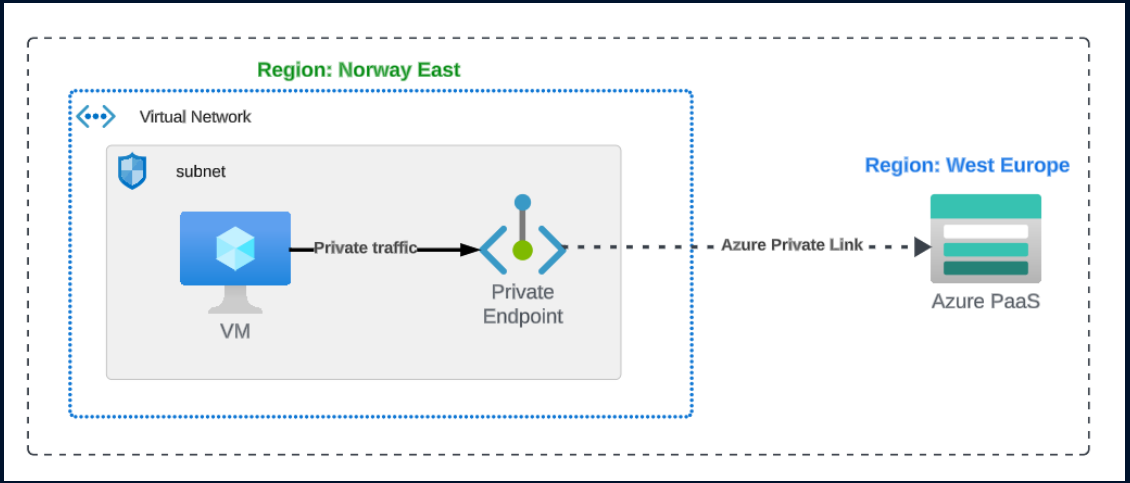
Use case: Connecting to a private service in another tenant 2



Can also be done with custom IaaS based solutions using Azure Private Link Service

[What is Azure Private Link service? | Microsoft Learn]

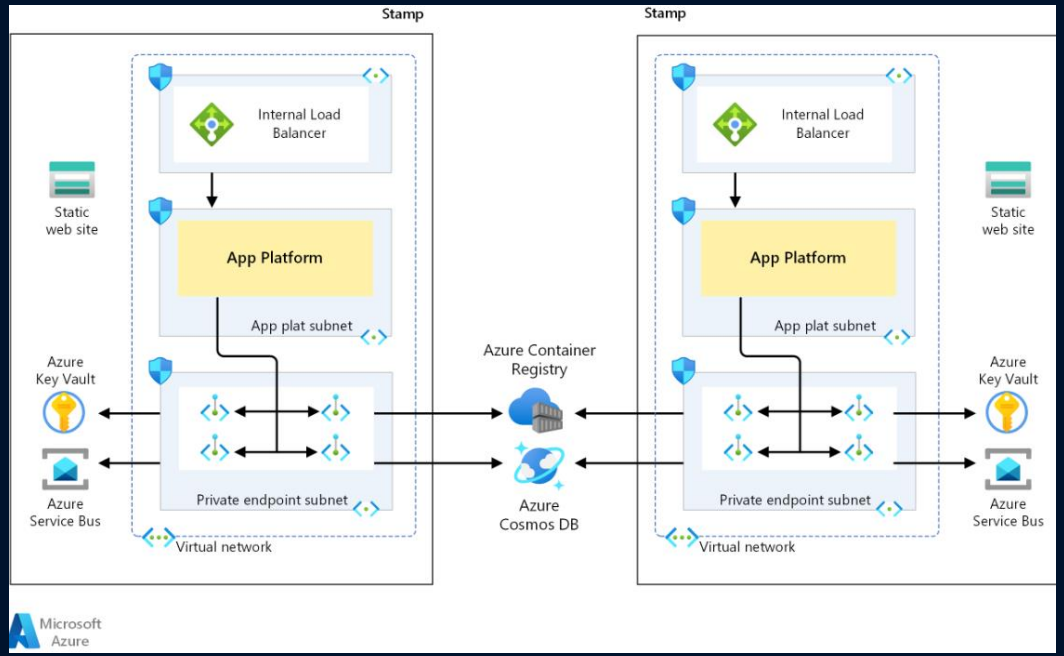
Use case: Connecting to other resources in other regions



- **Challenge:** Main network infrastructure in region 1 – access service in region 2
- Avoid complex peerings
- **What:** Multi-region private connectivity
- **Examples:** Place PaaS near other service in region 2

What is a private endpoint? - Azure Private Link | Microsoft Learn

Use case: Shared service in separate networks



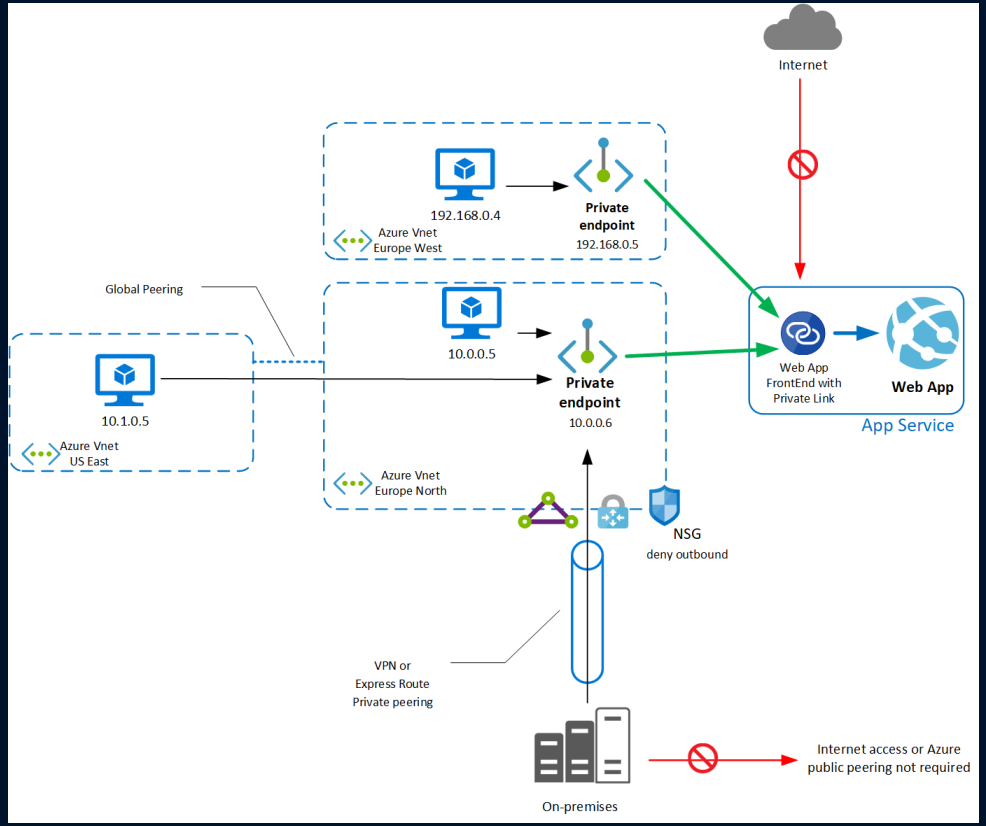
- **Challenge:** Avoid duplicate geo-replicated services
- Avoid unnecessary peerings
- Overlapping private IPs?

- **What:** Expose more than one private endpoint for a service (DNS!)

- **Examples:**
  - DR designs
  - Shared services

Networking and connectivity for mission-critical workloads on Azure - Azure Architecture Center | Microsoft Learn

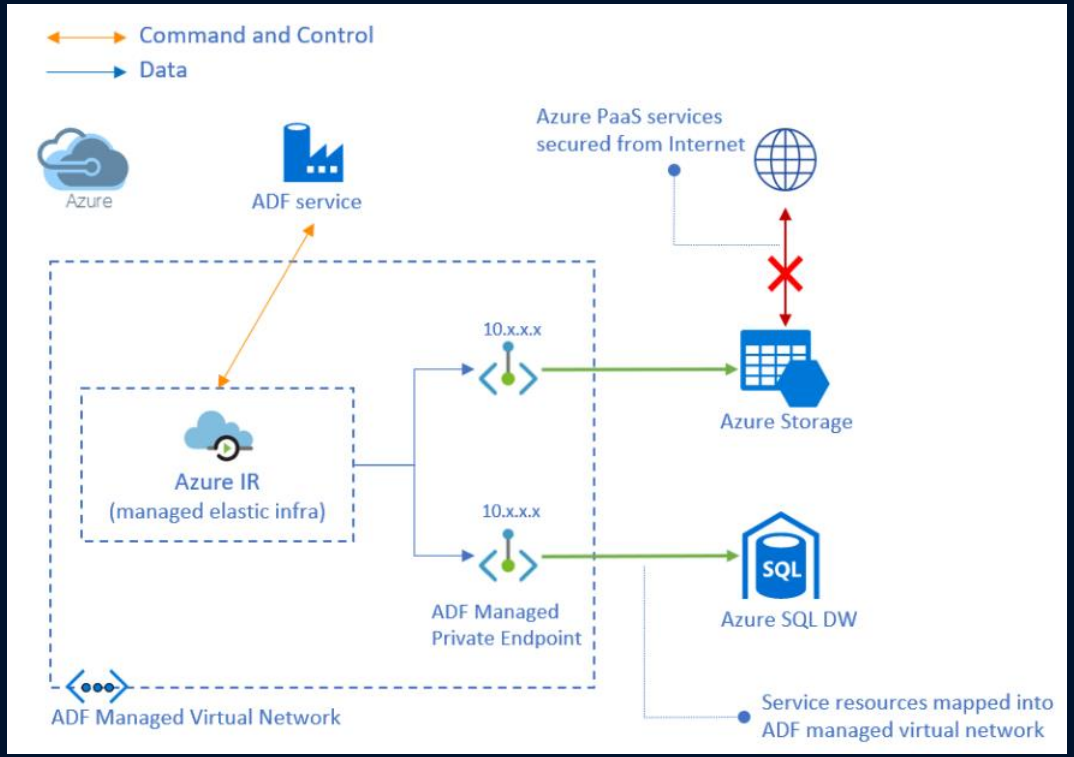
Use case: Accessing PaaS privately in hybrid scenarios



- **Challenge:** Access PaaS from secured private networks
- **What:** Private endpoint + ExpressRoute/VPN
- **Examples:**
  - Ports/protocols not open towards Internet
  - Utilize cloud resources in hybrid scenarios

[Connect privately to an App Service apps using private endpoint - Azure App Service | Microsoft Learn]

Use case: Data Integrations with private endpoints



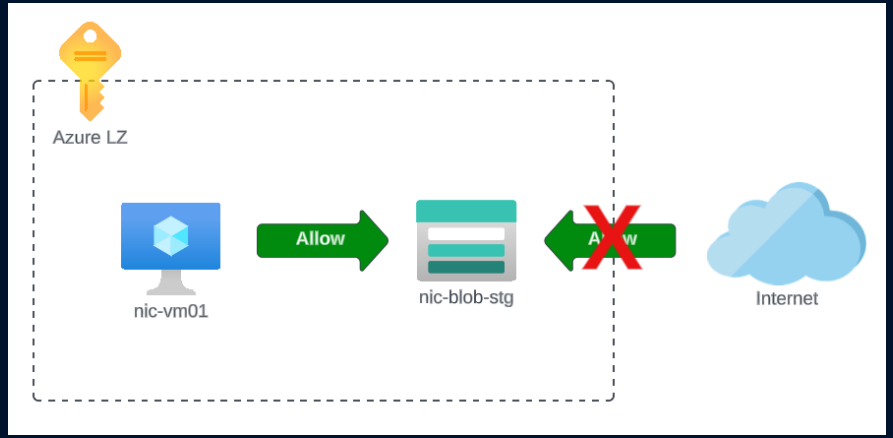
- **Challenge:** Complex networking or limited vnet integration
- **What:** Managed Virtual Network with managed Private Endpoint
- **Examples:** Azure Data Factory, Azure Purview, Azure Data Explorer, Azure Synapse

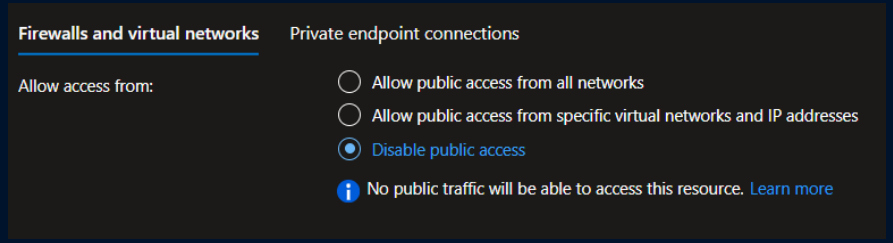
Managed virtual network and managed private endpoints - Azure Data Factory | Microsoft Learn

GOTCHAS

Gotcha – Public Access Not Disabled

- Explicitly disable public access after configuring PE
- Some exceptions like App Service
- **Recommendation:**
  - Implement Azure Policy to audit / enforce this!





List of built-in policy initiatives - Azure Policy | Microsoft Learn

Gotcha – Private Data vs Control Plane

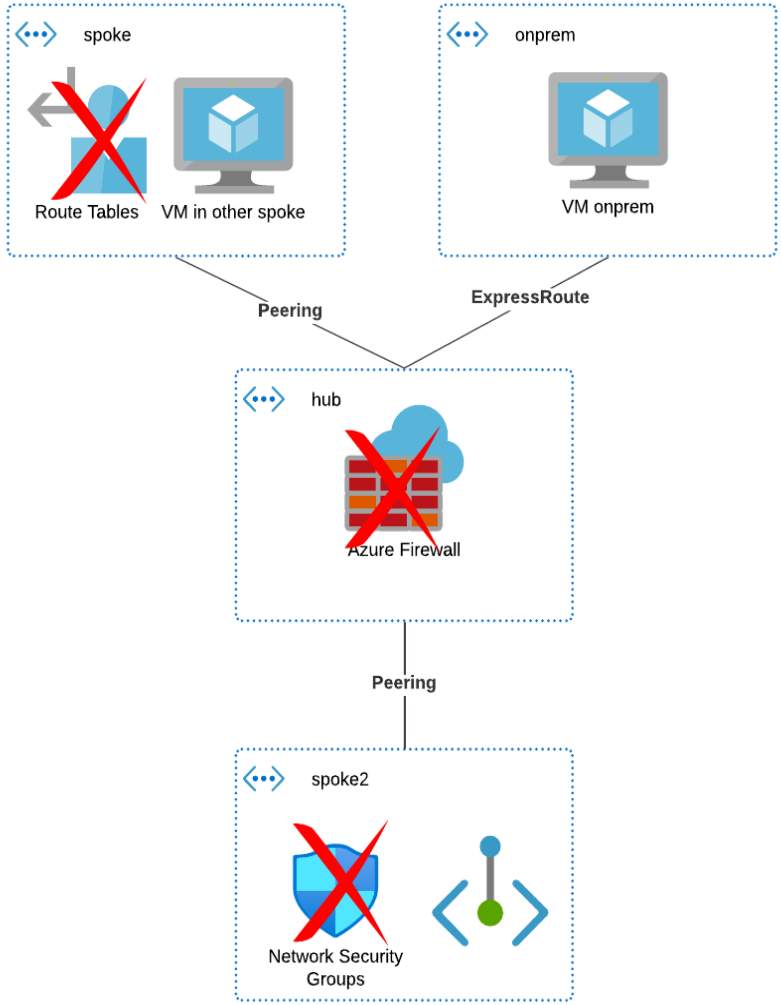
- The control plane (ARM) is always publicly available!
- Control plane and data plane might have separate roles (accesses)
- If you are authorized, you can still **manage** it from the “outside”
  - Including enabling public access!
- **Recommendation:**
  - Get control of your RBAC (data + control)
  - Use conditional access for Azure + PIM
  - Audit and log in both planes

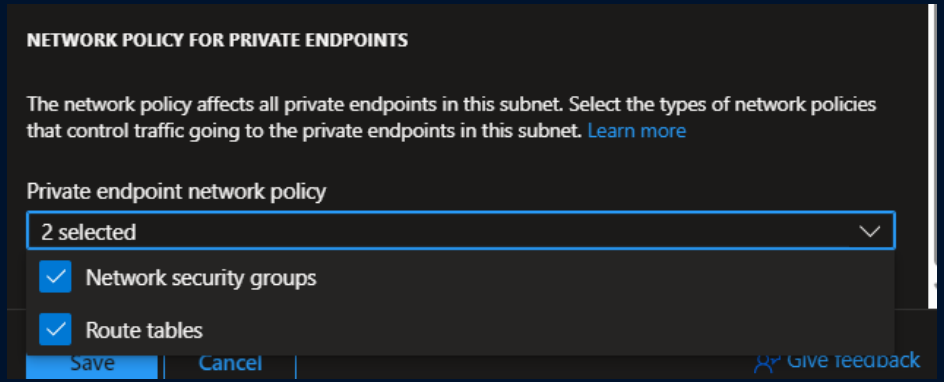
Control plane and data plane operations - Azure Resource Manager | Microsoft Learn

Gotcha – PE in hub and spoke

- By default Private Endpoints..
  - propagates a /32 route
  - Does not respect UDR
  - Does not respect NSG
- Possible consequences
  - Bypassing firewall(s)
    - From onprem
    - Between spokes
  - Bypassing NSGs
- Remediation:
  - Network policy on subnets
  - Debug routing to verify

[Manage network policies for private endpoints - Azure Private Link | Microsoft Learn]






```
},
"policyRule": {
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Network/virtualNetworks/subnets"
      },
      {
        "value": "[length(field('Microsoft.Network/virtualNetworks/subnets/privateEndpoints[*]'))]",
        "greater": 0
      },
      {
        "field": "Microsoft.Network/virtualNetworks/subnets/privateEndpointNetworkPolicies",
        "notEquals": "Enabled"
      }
    ]
  },
  "then": {
    "effect": "[parameters('effect')]"
  }
}
```

Gotcha – PE Network Policy

- By default Network Policy is disabled on subnets
- Portal creation of private endpoints will attempt to disable them at most times
- Remediation:
  - Azure Policy to audit/enforce
  - Include secure defaults in subnet IaC module

[Manage network policies for private endpoints - Azure Private Link | Microsoft Learn]

Gotcha – Logging and visibility

DNS, Routing or Firewall misconfigs will cause all sorts of weird issues!

PE have limitations:

- **No NSG flow logs**
- No effective routes
- No effective security rules

Remediation:

- Use logging of PaaS service to support traditional network logs
- Inspect cross-spoke and cross-prem with firewall
- «Manual» debugging and packet capturing (e.g. Wireshark)

Limitation	Description
Effective routes and security rules unavailable for private endpoint network interface.	Effective routes and security rules won't be displayed for the private endpoint NIC in the Azure portal.
NSG flow logs unsupported.	NSG flow logs unavailable for inbound traffic destined for a private endpoint.

Azure Firewall scenarios to inspect traffic destined to a private endpoint - Azure Private Link | Microsoft Learn

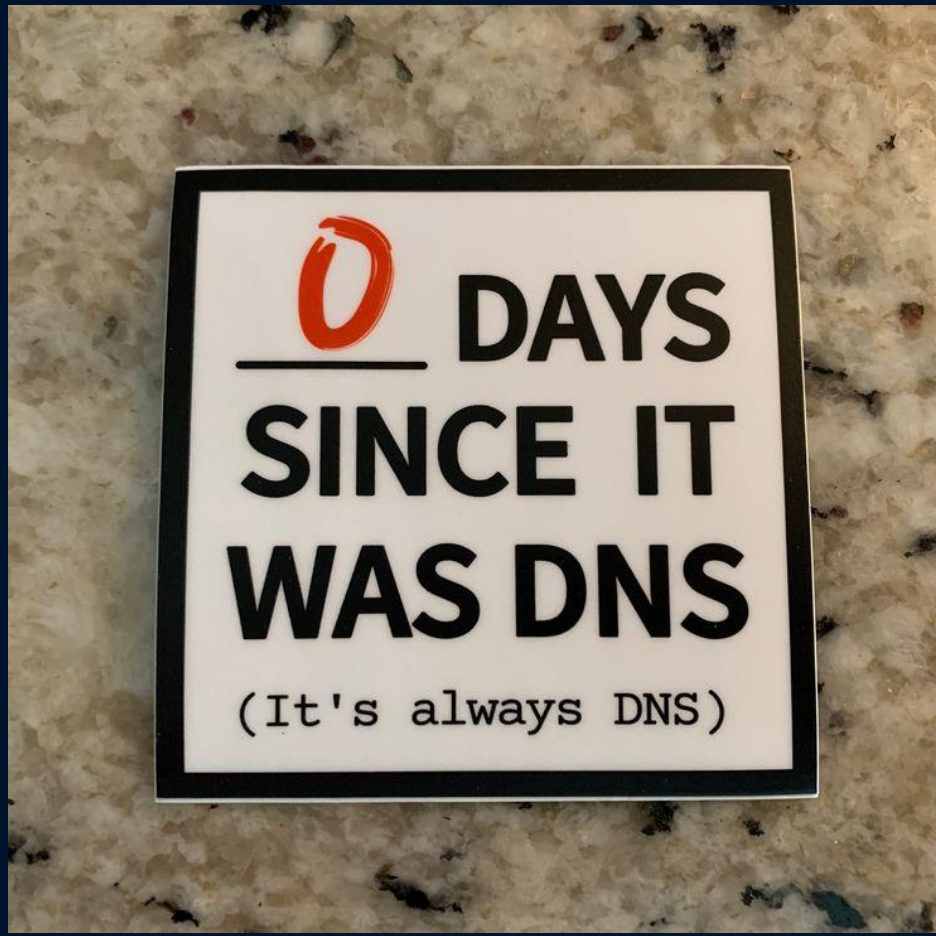
Troubleshoot Azure Private Endpoint connectivity problem

Gotcha – DNS

Challenges:

- Central DNS resolution
  - Hybrid scenarios
  - Cross-spoke
  - Integration with existing DNS
- Central DNS registration
  - Access Control
  - Automation

[Azure Private Endpoint DNS configuration | Microsoft Learn]

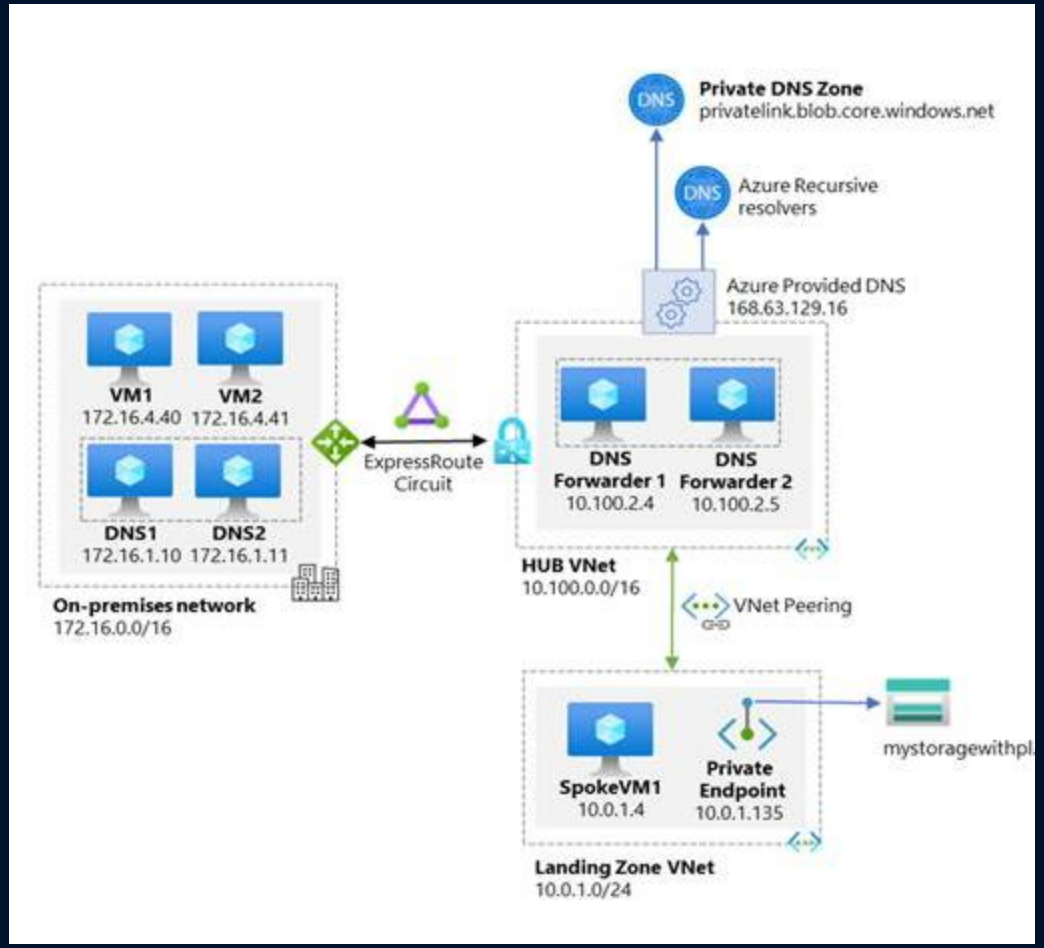


Gotcha – Central DNS Resolution

Remediation:

- DNS Forwarder solution for hybrid-scenarios (VMs or Private Resolver)
- Configure Azure Firewall as DNS?
- Automate DNS settings on Vnets (Policy/bootstrapping)

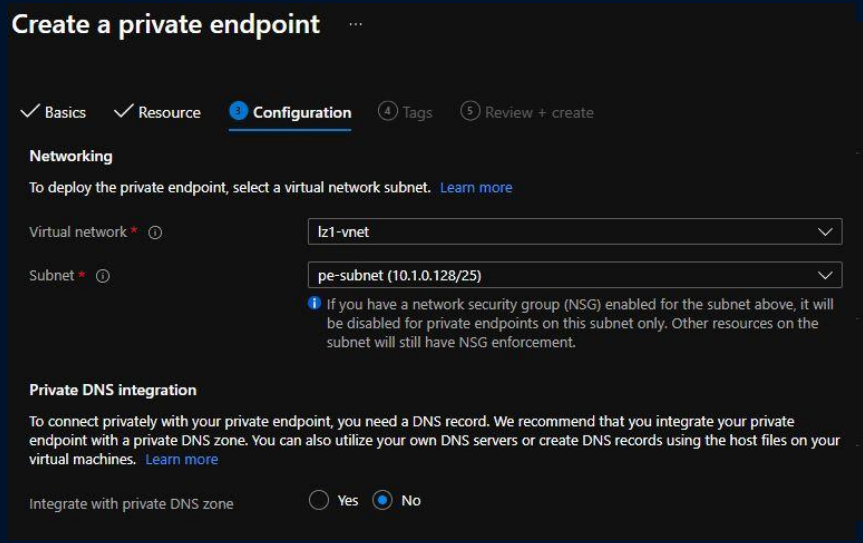
[Azure Private Endpoint DNS configuration | Microsoft Learn]

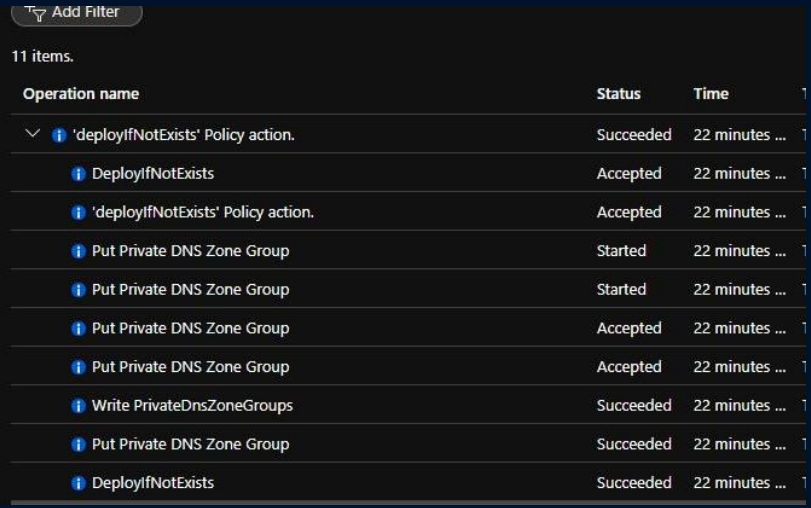


Gotcha – DNS Registration

Remediation:

- DINE policy for auto-registering (note: specific for groupId!) BuiltIn + Custom





Private Link and DNS integration at scale - Cloud Adoption Framework | Microsoft Learn

Gotcha – DNS Registration

Example:

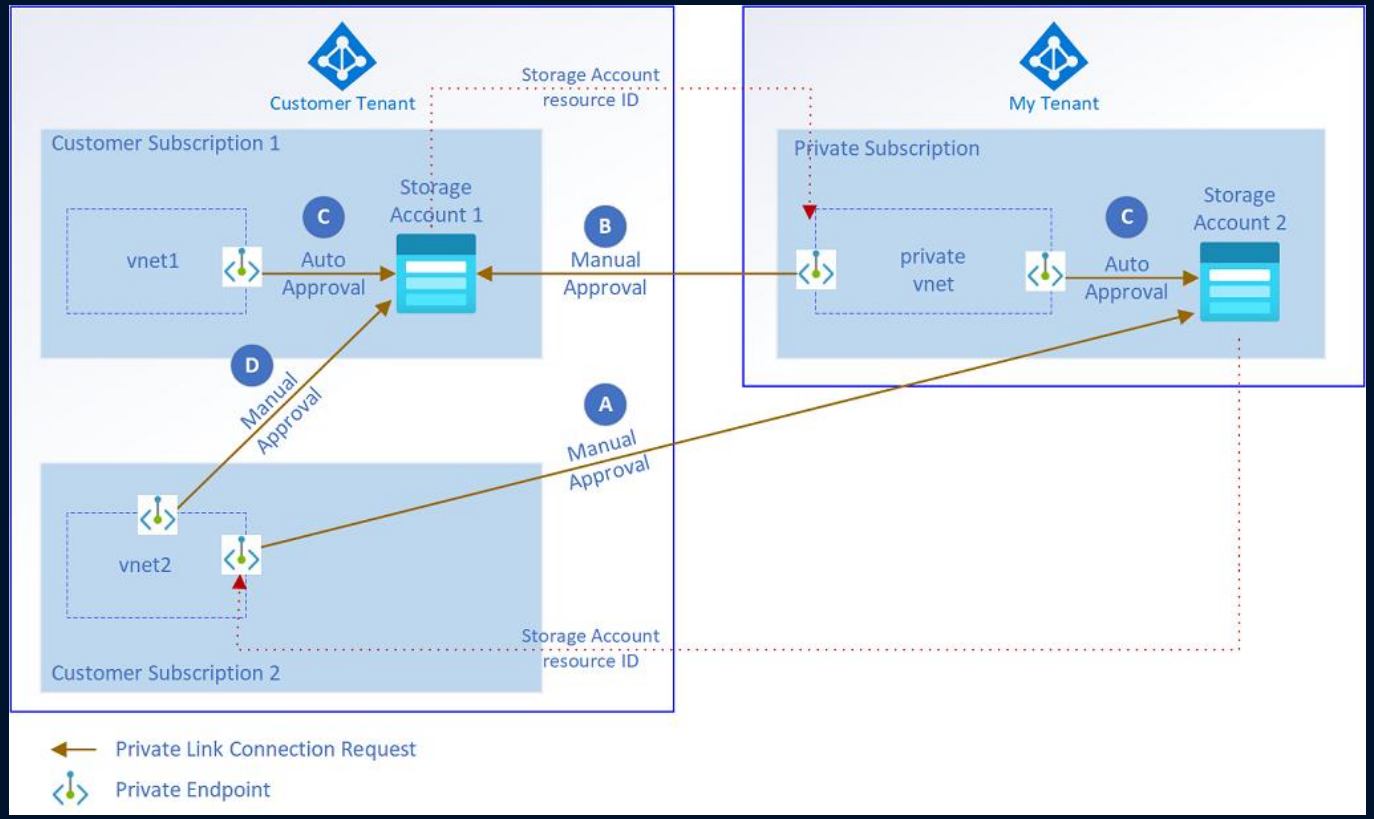
- Azure Static Web Apps can use .[n].azurestaticapps.net
  - Will need privatelink.[n].azurestaticapps.net zones
  - No deterministic DNS Zone => «dynamic» policy

- Remediation: Custom policy

Request: DINE policy for private endpoint -> private DNS zone linking with static webapps · Issue #1223 · Azure/azure-policy (github.com)

Private Link and DNS integration at scale - Cloud Adoption Framework | Microsoft Learn

Gotcha: Cross-tenant Data Exfiltration



Cross-tenant secure access to apps with private endpoints - Azure Architecture Center | Microsoft Learn

Limit cross-tenant private endpoint connections in Azure - Cloud Adoption Framework | Microsoft Learn

Gotcha: Mix Storage Private Endpoints with public

Storage access constraints for clients in VNets with private endpoints

Clients in VNets with existing private endpoints face constraints when accessing other storage accounts that have private endpoints. For example, suppose a VNet N1 has a private endpoint for a storage account A1 for Blob storage. If storage account A2 has a private endpoint in a VNet N2 for Blob storage, then clients in VNet N1 must also access Blob storage in account A2 using a private endpoint. If storage account A2 does not have any private endpoints for Blob storage, then clients in VNet N1 can access Blob storage in that account without a private endpoint.

This constraint is a result of the DNS changes made when account A2 creates a private endpoint.

PrivateLink/Issue-Customer-Unable-to-Access-PaaS-AfterPrivateLink at master · dmauser/PrivateLink (github.com)

RECOMMENDATIONS

NIC Cloud Connect

Private Endpoints status

- It's still *relatively* new… (initial GA 2020/02)
- Multiple services got support for PE/PL since then – still some in preview

- 2023/01: ASG support for Private Endpoints GA
- 2022/10: Static IP support GA, Custom NIC name GA
- 2022/08: NSG support GA, UDR support GA

nic Cloud Connect

Private Endpoints specific recommendations

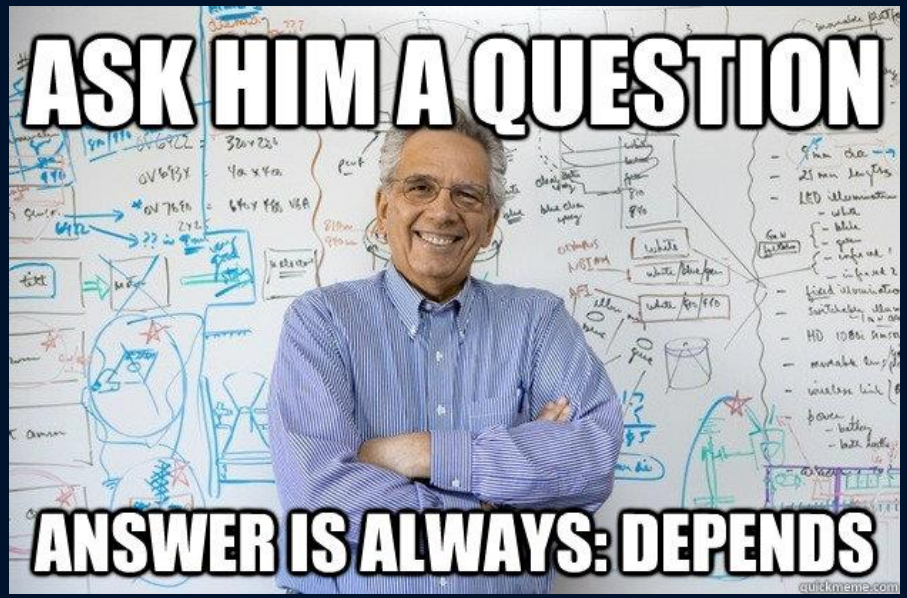
- Use **network policy** on subnets
- Review and verify your hybrid/private **DNS design**
- Treat **routing** rigorously
- Filter and log traffic with a **firewall**
- Explicitly **disable public access**
- Use Azure Policy to enforce or audit configurations
  - Audit cross-tenant private links
  - Audit / enforce landing zones that should have private endpoints
  - Network policy on subnets
  - Register endpoints in central private DNS zones

Private Endpoints Considerations

- Always understand **your use case** (requirements, context, risks, architecture)
- Be aware of additional **complexity** (filtering, routing, DNS) and private endpoint gotchas
- User **misconfigurations** is one of the most prevalent risks
- Bring along **traditional networking principles**, but explore new **cloud capabilities** and patterns
- Understand the **Azure services** you choose to use
- Networking is just one piece of the security puzzle – **never trust, always verify**!
- Review the **CAF Connectivity to Azure PaaS services** design considerations and recommendations

nic Cloud Connect

Should you use Azure Private Endpoints?



When you do – do it right!

nic Cloud Connect

Oslo Spektrum
November 7 - 9

Thank you!

Slides will be available at GitHub github.com/matsest

Deciphering Azure Private Endpoints

Mats Estensen

@matsest

mats.estensen@devoteam.no