Azure Security – Protecting the Platform

Aligned with Microsoft Certification Exam AZ-500

ine.com

Tracy Wallace

Azure Solutions Architect Expert

twallace@ine.com

@TracyWallaceINE

linkedin.com/in/tracy-wallace-746482a

Course Topics

Implement Network Security
Implement Host Security
Configure Container Security
Implement ARM Security

AZ-500 Objective Domains

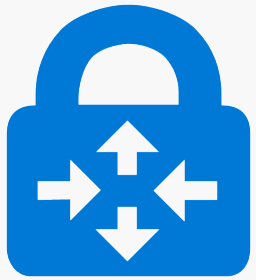
- Manage identity and access (30 - 35%)
- **Implement platform protection (15 - 20%)**
- Manage security operations (25 - 30%)
- Secure data and applications (20 - 25%)

Exam AZ-500: Microsoft Azure Security Technologies

- Implement advanced network security
  - + Secure the connectivity of virtual networks - VPN authentication, BYO Key for Express Route encryption, Point to site, Site tsite
  - + configure Network Security Groups (NSGs) and Application Security Groups (ASGs)
  - + create and configure Azure Firewall
  - + Configure Azure Front Door service as an Application Gateway
  - + configure a Web Application Firewall (WAF) on Azure Application Gateway
  - + configure Azure Bastion
  - + configure a firewall on a storage account, Azure SQL, KeyVault, or App Service
  - + implement Service Endpoints
  - + implement DDoS
- Configure advanced security for compute
  - + configure endpoint protection
  - + configure and monitor system updates for VMs in Azure
  - + configure authentication for containers
  - + configure security for different types of containers
  - + implement vulnerability management
  - + configure isolation for AKS
  - + configure security for container registry
  - + implement Azure Disk Encryption
  - + configure security for Azure App Service
  - + configure SSL/TLS certs
  - + configure authentication
  - + configure automatic updates

Pre-requisites

Azure Fundamentals
Azure Administrations

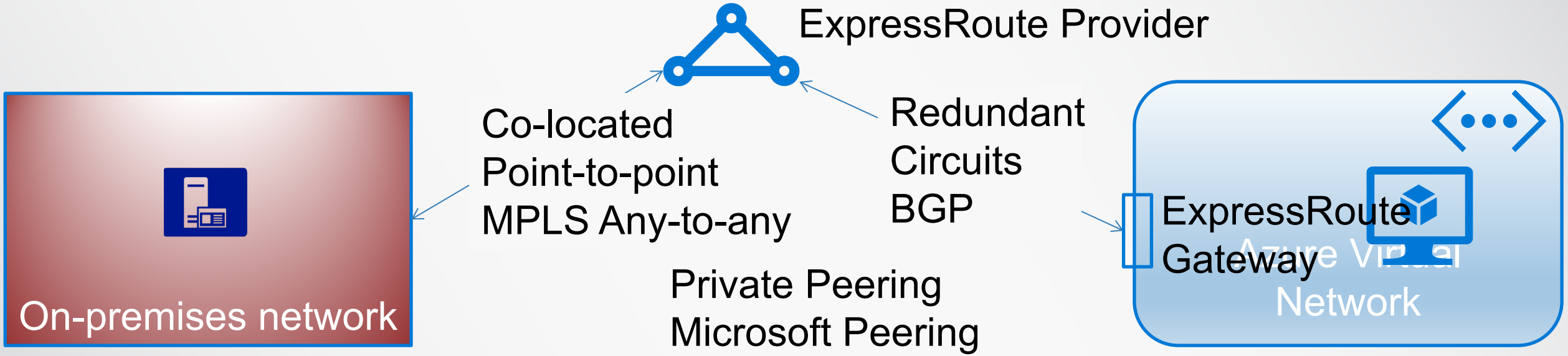


Virtual Network Connectivity

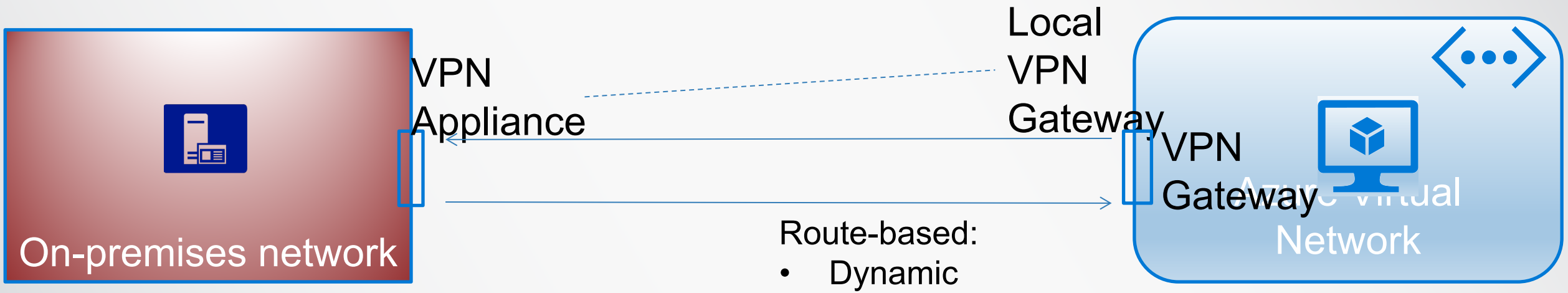
Virtual Network Connectivity

- ExpressRoute
- VPN Gateway
- Virtual network peering

ExpressRoute



VPN Gateway



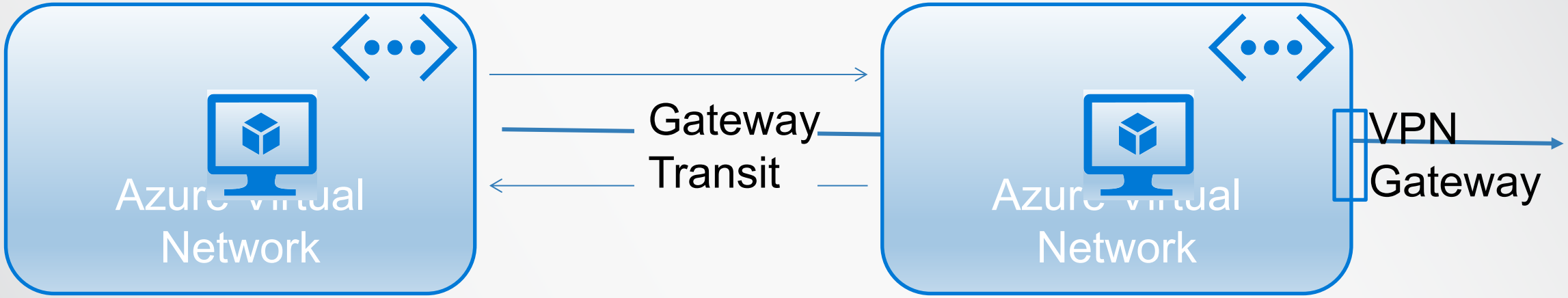
Route-based:

- Dynamic
- BGP
- Active-active
- Full featured
- Custom IKE/IPSec policy

Policy-based:

- Static
- Basic tier
- One route
- Limited P2S

Virtual Network Peering



Virtual Network Connectivity Take-aways

- ExpressRoute – physical options, peering options
- Site 2 Site – Encryption
- Point 2 Site – Authentication options
- Peering options

Configure Remote Access Management

Configure Remote Access Management

- Gateway Access
- Network Security Groups
- Demo: Just-In-Time Access
- Firewalls
- Azure Load Balancer
- Bastion Host
- Demo: Bastion Host

Configure Remote Access Management

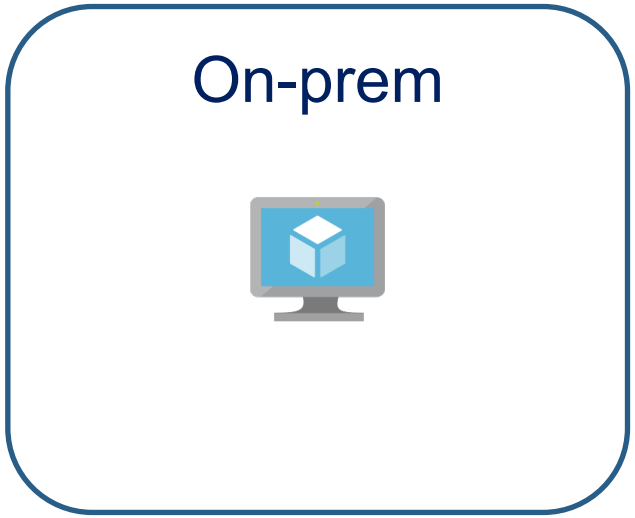
Gateway Access

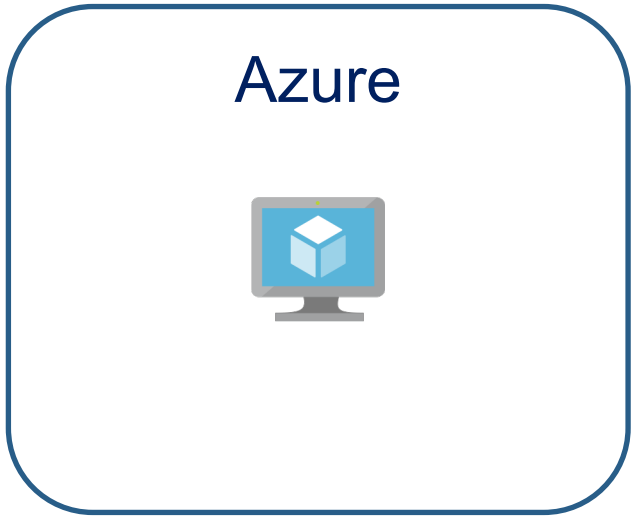
Network Security Groups

Firewalls

Azure Load Balancer

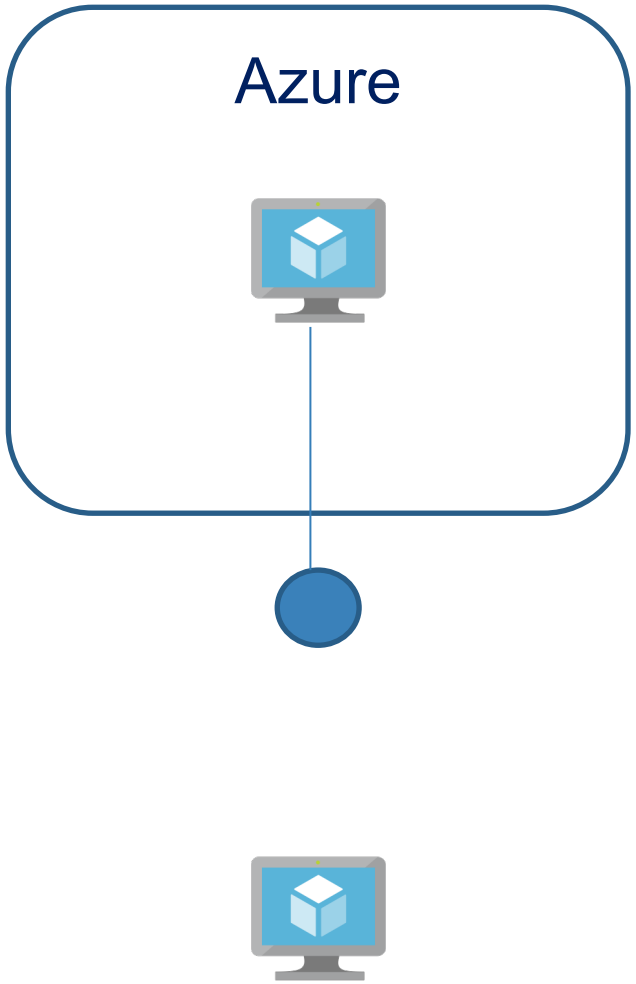
Bastion Host





Configure Remote Access Management

- Gateway Access
- Network Security Groups
- Firewalls
- Azure Load Balancer
- Bastion Host

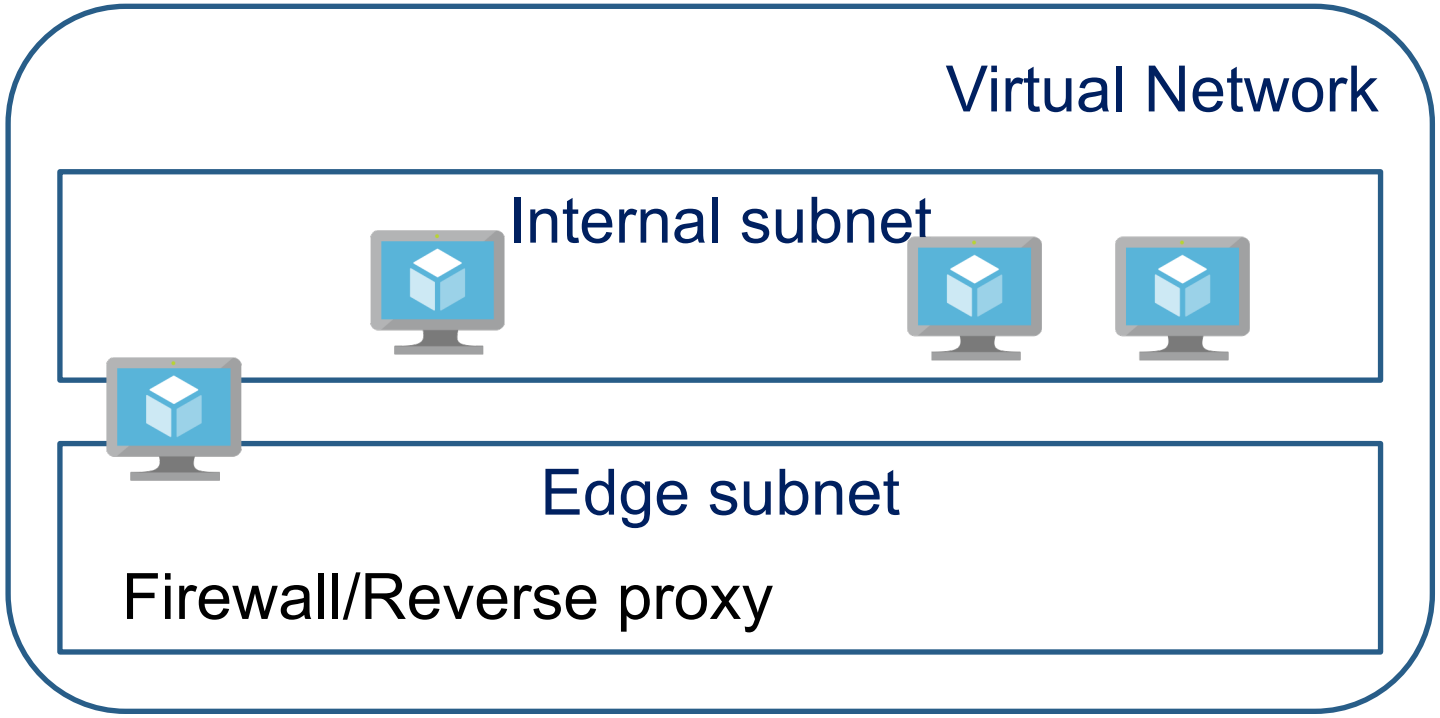


Only recommended with just-in-time administrative acc

Demo: Just-In-Time Access

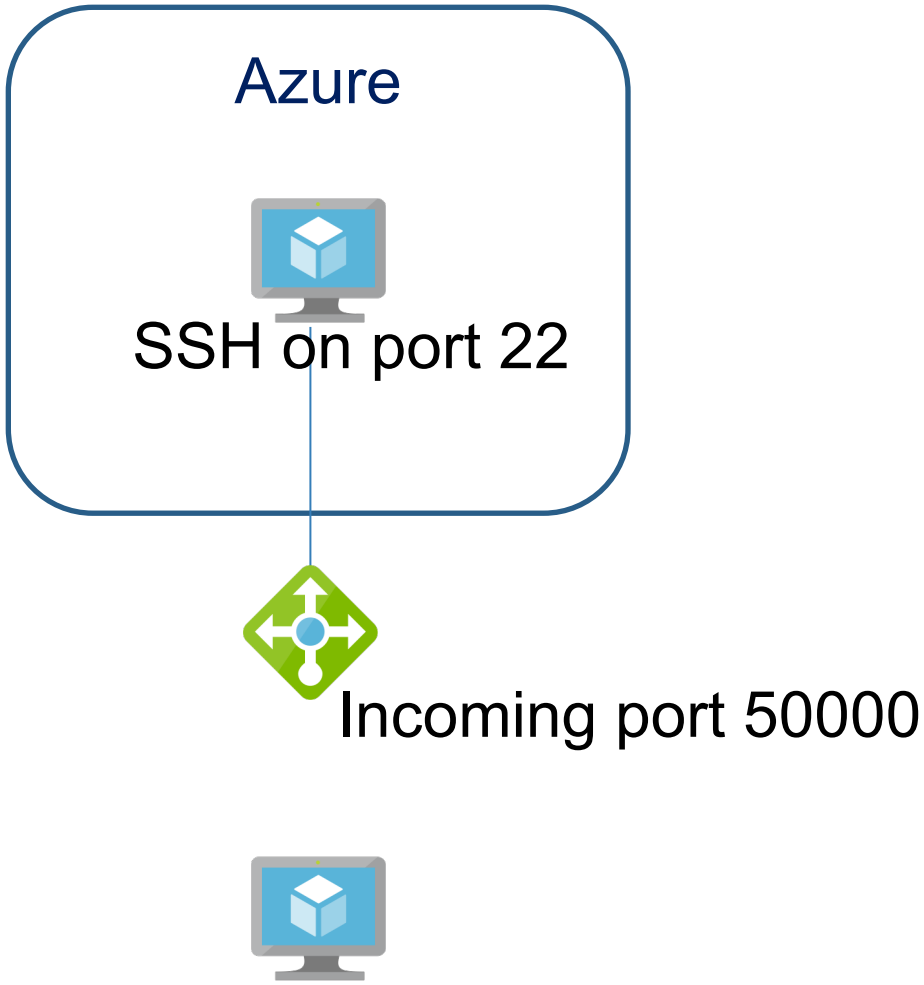
Configure Remote Access Management

- Gateway Access
- Network Security Groups
- Firewalls
- Azure Load Balancer
- Bastion Host



Configure Remote Access Management

- Gateway Access
- Network Security Groups
- Firewalls
- Azure Load Balancer
- Bastion Host



Don't do this

Configure Remote Access Management

Gateway Access

Network Security Groups

Firewalls

Azure Load Balancer

Bastion Host

- HTTPS connection
- Access from portal
- RBAC
- No administrative ports exposed
- One bastion host per network

Demo: Bastion Host

Azure Firewall

Azure Firewall

- What is Azure Firewall?
- Azure Firewall Features
- Demo: Azure Firewall

What is Azure Firewall?

- Whiteboard

Azure Firewall Features

- L3 – L7 policies
- Microsoft threat intelligence
- High availability
- High scalability
- Multiple public IP addresses
- DNAT/SNAT
- Integrated monitoring
- Compliance certifications

Demo: Azure Firewall

Azure Front Door Service

Azure Front Door Service

- Azure Front Door
- Front Door Components
- Demo: Azure Front Door

Azure Front Door

Azure Front Door

- Smart health probes
- URL-based routing
- Multiple-site hosting
- Session affinity
- Secure Sockets Layer (SSL) termination
- Custom domains and certificate management
- Web Application Firewall
- URL redirection
- URL rewrite

Front Door Components

Demo: Azure Front Door

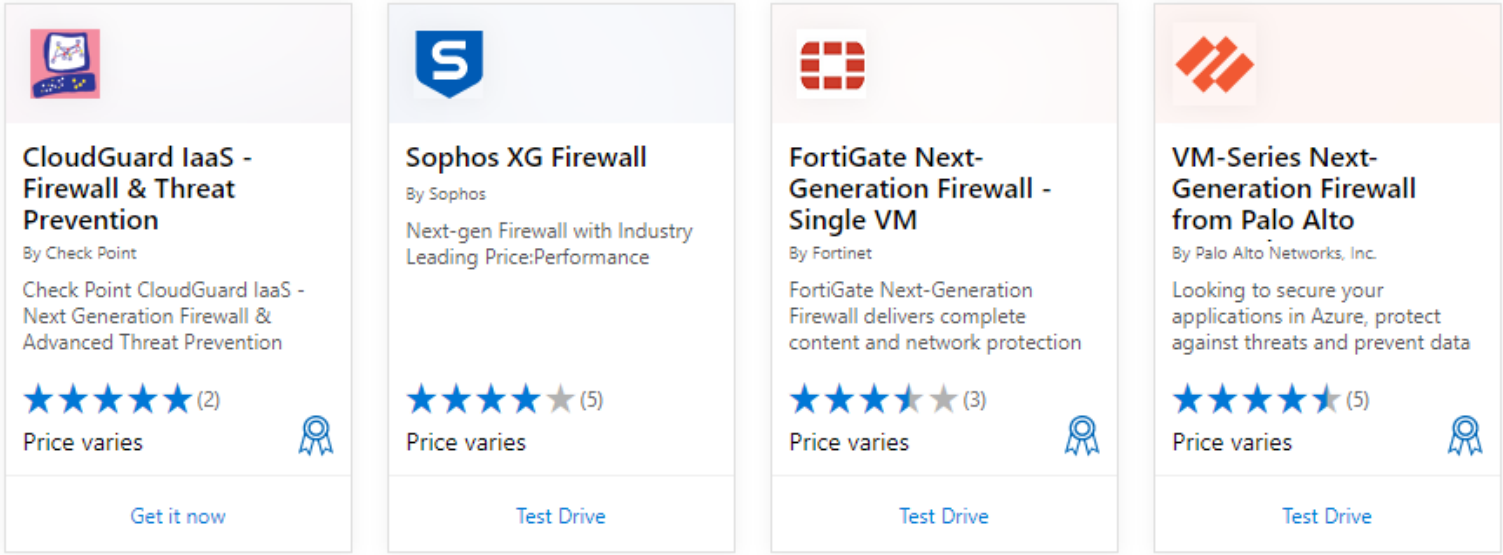
Firewall Appliances

Firewall Appliances

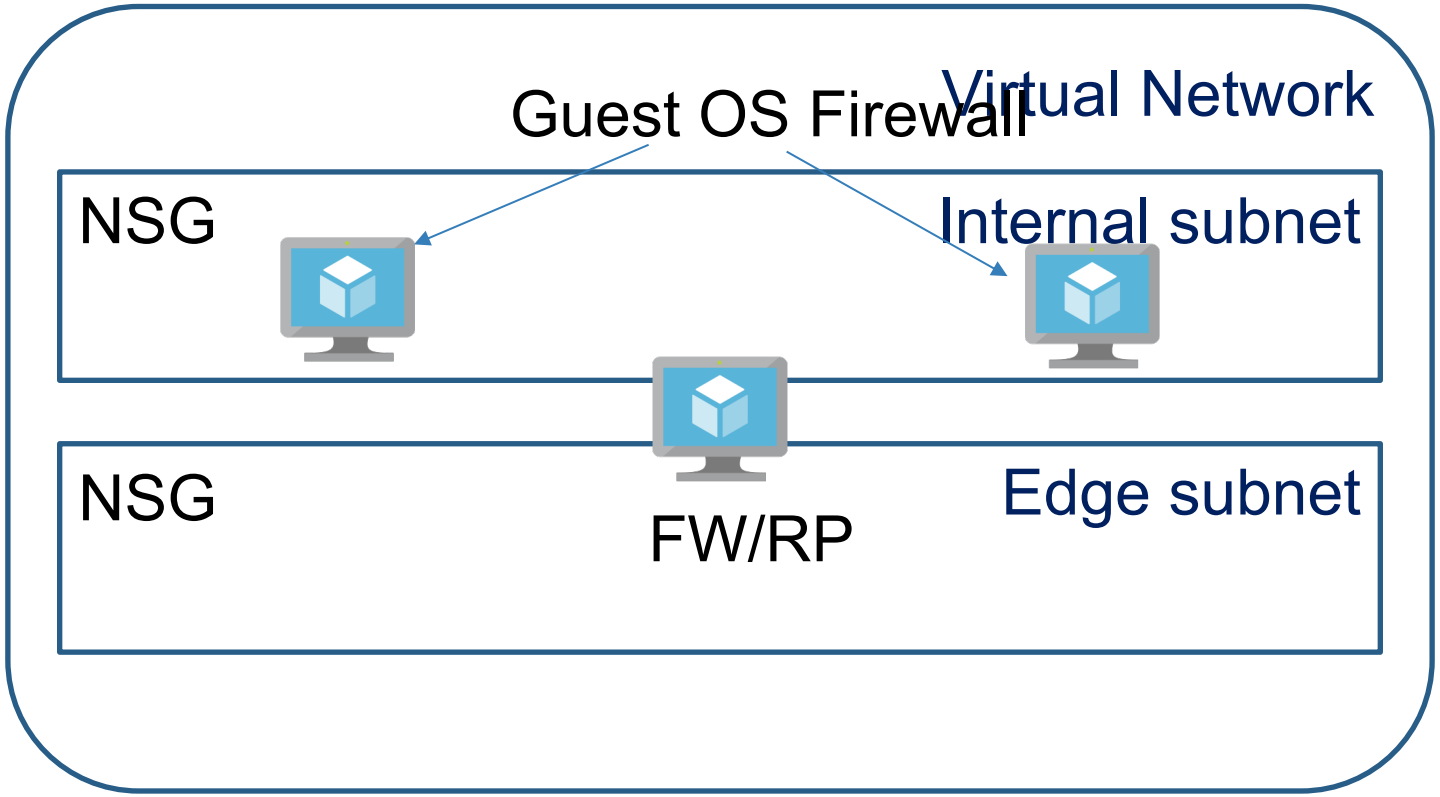
- Vendor Firewalls
- Secured Network Topologies
- Demo: pfSense Firewall

Vendor Firewalls

Over 20 templates and over 25 virtual machine images



Secured Network Topologies



Demo: pfSense Firewall

Deploy Network Security Groups

Deploy Network Security Groups

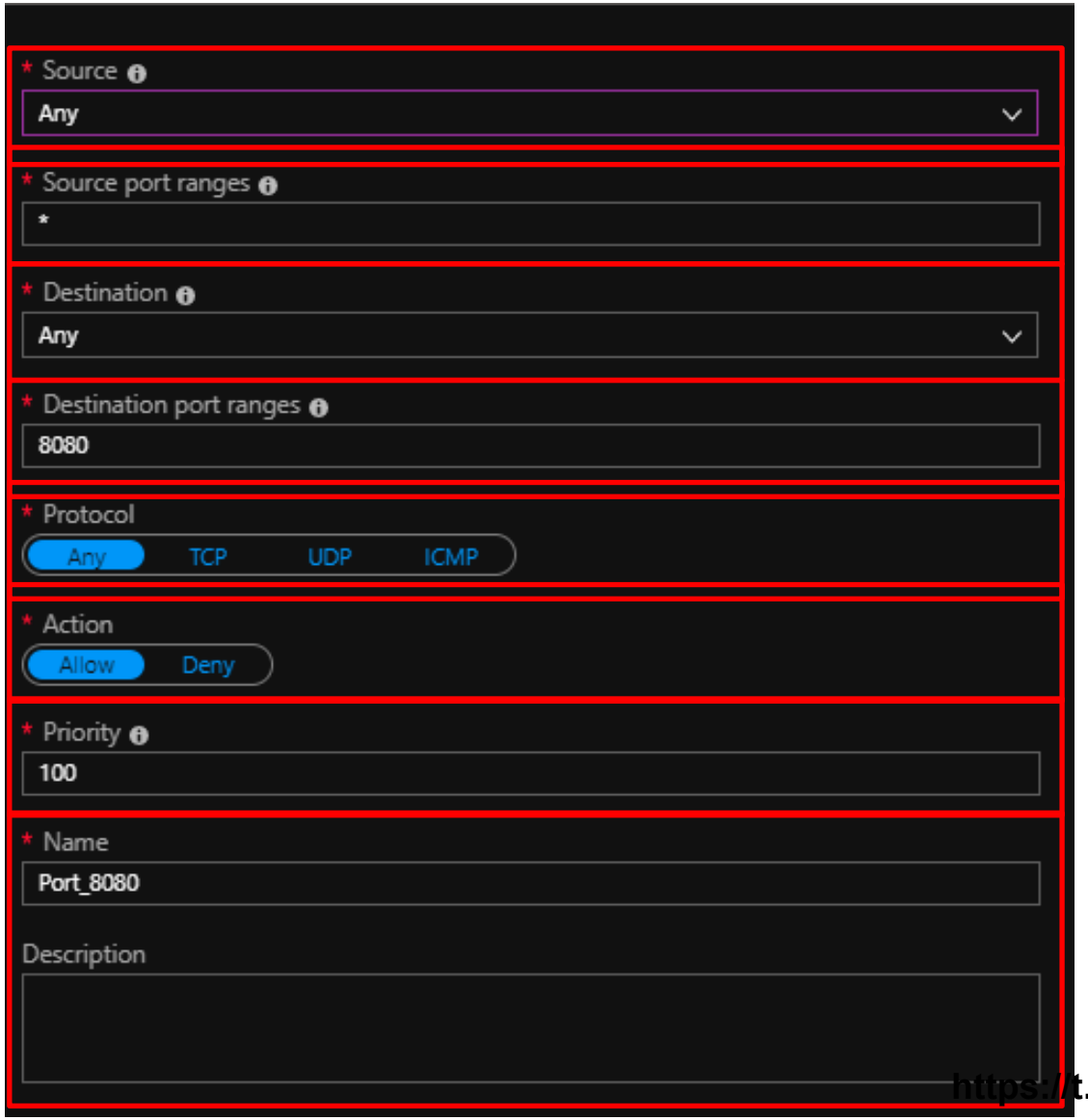
- Network Security Group Overview
- Common Ports
- NSG Rules
- Service Tags
- Application Security Groups
- Demo: Apply Azure NSGs

Network Security Group Overview

Common Ports

Service	Standard Port
RDP	3389
SSH	22
WinRM	5985 (HTTP) / 5986 (HTTPS)
HTTP	80
HTTPS	443
DNS	53
LDAP	389
SMB	445
FTP	20,21

NSG Rules



IP addresses
Service tag

Port (80)
Port range (50-60)
Port ranges (80, 443, 100-110)

Unique
Low number to high number
100 to 4096

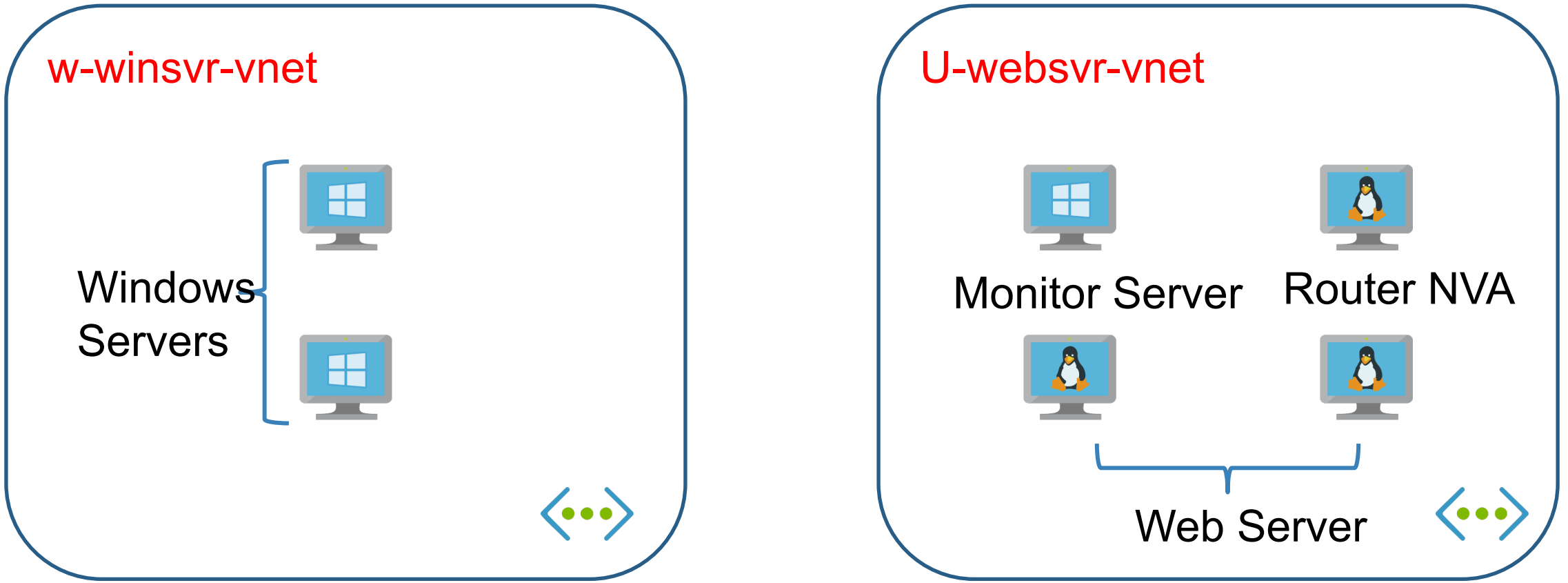
Service Tags

- Simplify Azure related addressing
- Internet
- Network
- Azure Services
  - storage
  - SQL
  - load balancer
  - many more

Application Security Groups

Demo: Apply Azure NSGs

Demonstration Architecture



Configure VM Security

Configure VM Security

- VM Hardening
- Security Center
- Endpoint Protection
- Demo: Security Center for VMs
- System Updates

VM Hardening

- Manage access to the VM resources
- Use complex, randomize passwords for administrative accounts
- Deploy VMs based on hardened images using templates
- Manage (automate) updates
- Implement a backup solution
- Monitor VMs
  - Enroll VMs in Security Center
  - Implement SEIM
- Encrypt disk volumes
  - Use key encrypting key
- Implement multi-level firewalling (host and system)

Security Center

- Free tier – basic policy and security score
- Vulnerability scanning
- Workload specific white-listing
- Just-in-time access
- Security Alerts

Endpoint Protection

- Security Center validates presence of anti-malware software on VMs
- Monitors efficacy of endpoint protection
- Does NOT provide direct protection*
- Currently monitored endpoint protection (As of April 2020)
  - Windows Defender
  - System Center endpoint protection
  - Trend Micro
  - Symantec
  - McAfee
  - Sophos

*Endpoint protection can be installed via an extension

Demo: Security Center for VMs

System Updates

System Updates

- Update management solution
- Runs on top of log analytics
- Track and manage updates and patches for Windows and Linux
- Components
  - Log Analytics agent for Windows or Linux
  - PowerShell Desired State Configuration (DSC) for Linux
  - Automation Hybrid Runbook Worker
  - Microsoft Update or Windows Server Update Services (WSUS) for Windows machines
- Supported OSs
  - Windows 2012 + - full support
  - Windows 2008 R2 – assessments only
  - CentOS 6 (x86/x64) and 7 (x64)
  - Red Hat Enterprise 6 (x86/x64) and 7 (x64)
  - SUSE Linux Enterprise Server 11 (x86/x64) and 12 (x64)
  - Ubuntu 14.04 LTS, 16.04 LTS, and 18.04 (x86/x64)

Container Security

Container Security

- Container Resource Protection
- Container Authentication
- Demo: ACR Authentication
- Container Isolation
- Container Networking
- Demo: Container Networking

Container Resource Protection

- RBAC
- Vulnerability scanning of Azure container registries
- Agent-based threat monitoring for IaaS container solutions
- Agentless threat monitoring for Azure Kubernetes service
- Security hardening
  - Center for Internet Security (CIS) Docker Benchmark policy monitoring
  - IaaS and Kubernetes

Container Authentication

- Azure container instances – no explicit authentication
- Containers hosted on Azure VM (IaaS) – administrator login
- Azure container registry
  - Azure AD (user, service principal)
  - Managed identity – effectively service principal
  - AKS – integrated on provisioning – managed identity
  - Admin user
  - Repository-scoped access token

Demo: ACR Authentication

Container Isolation

- Container Instances
  - Hyper-V isolation
  - Each container group is isolated
  - No shared kernel
- IaaS
  - VM level isolation
  - Azure dedicated hosts

Container Networking

- Azure container registry – Service endpoint in preview (April 2020)
- IaaS – standard networking – NSG, firewall, etc.
  - Docker networking definition and designation
- Container instance – port mapping
- Azure Virtual Network container network interface plug-in

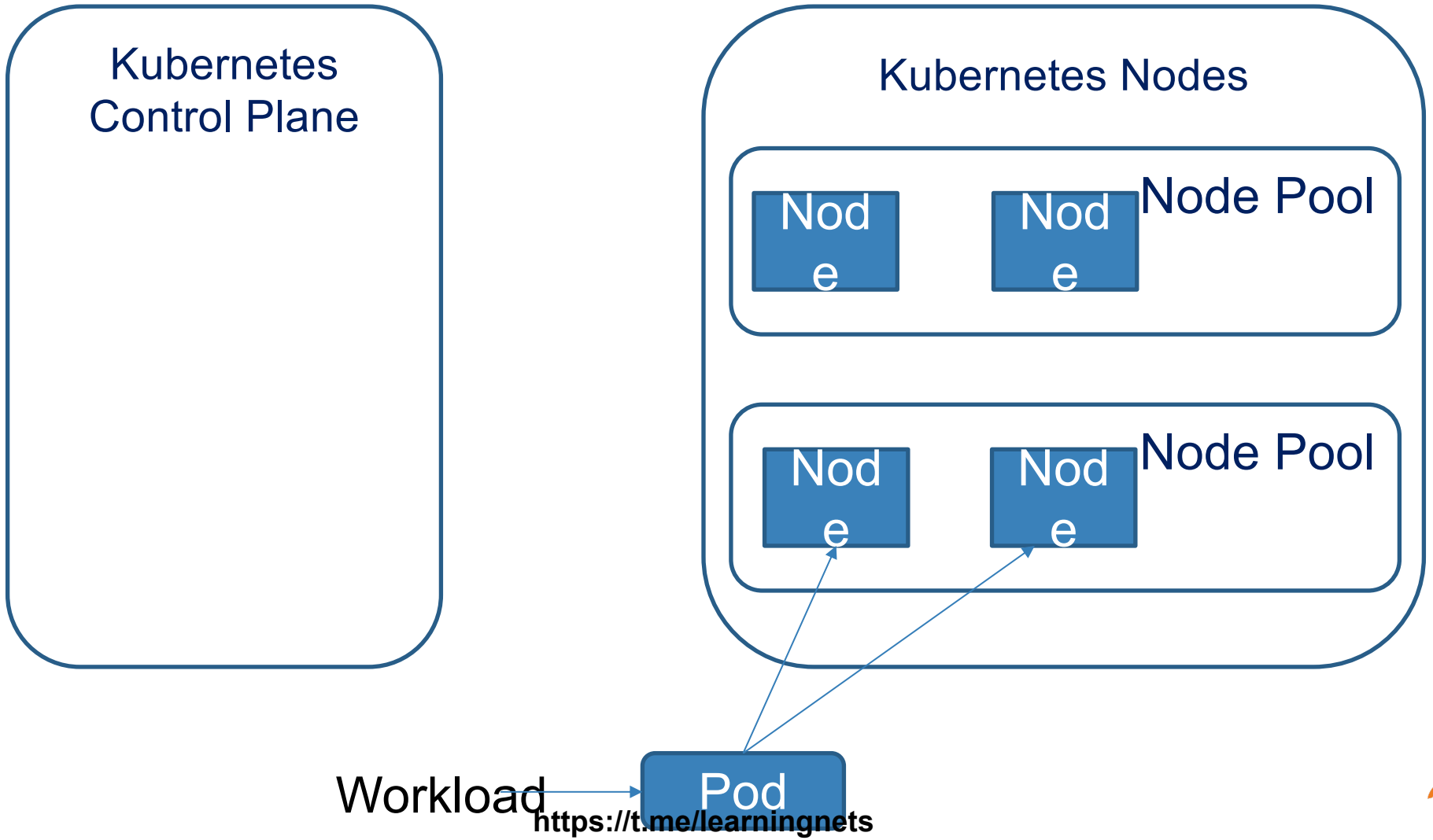
Demo: Container Networking

Configure AKS Security
Part I

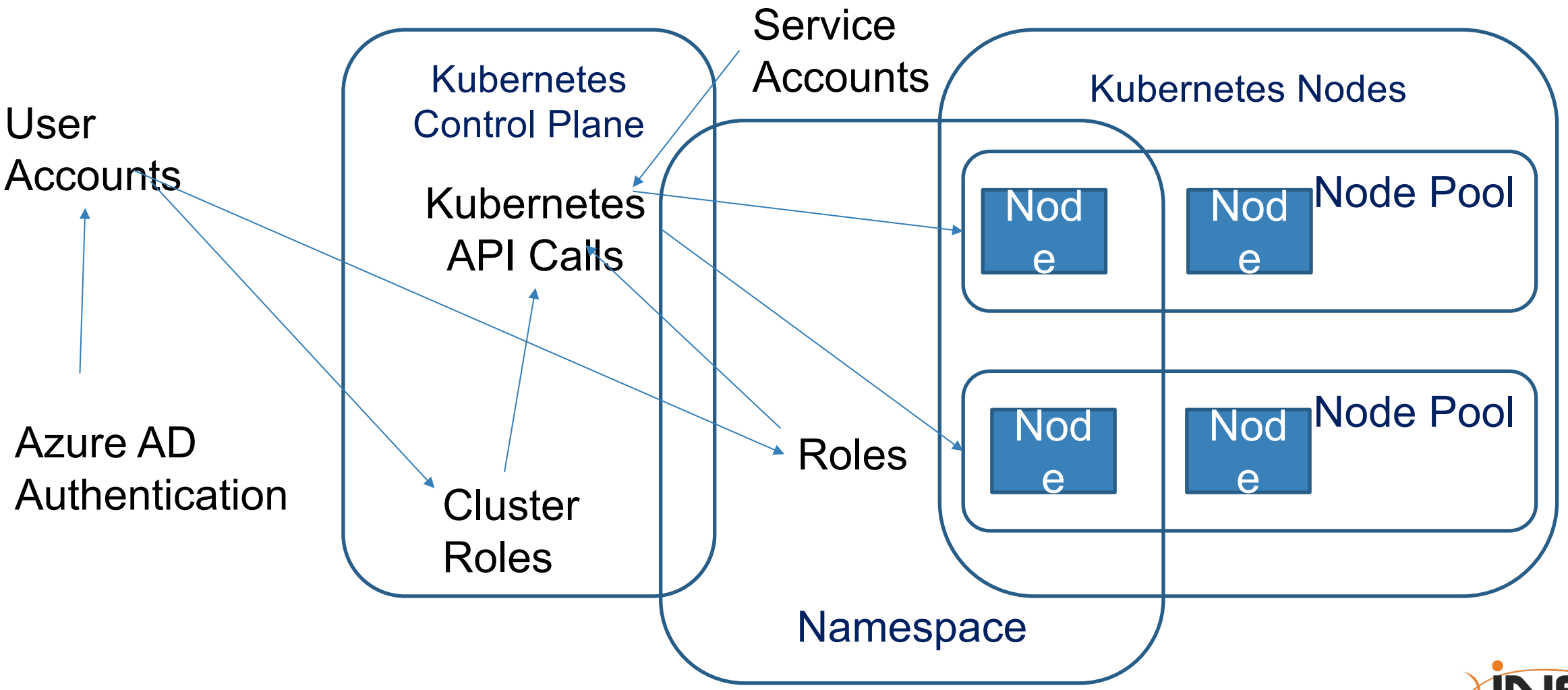
Configure AKS Security

- Azure Kubernetes Components
- RBAC and Azure AD for Kubernetes
- Kubernetes Updates and Patches
- Demo: Azure AD for Kubernetes

Azure Kubernetes Components



RBAC and Azure AD for Kubernetes

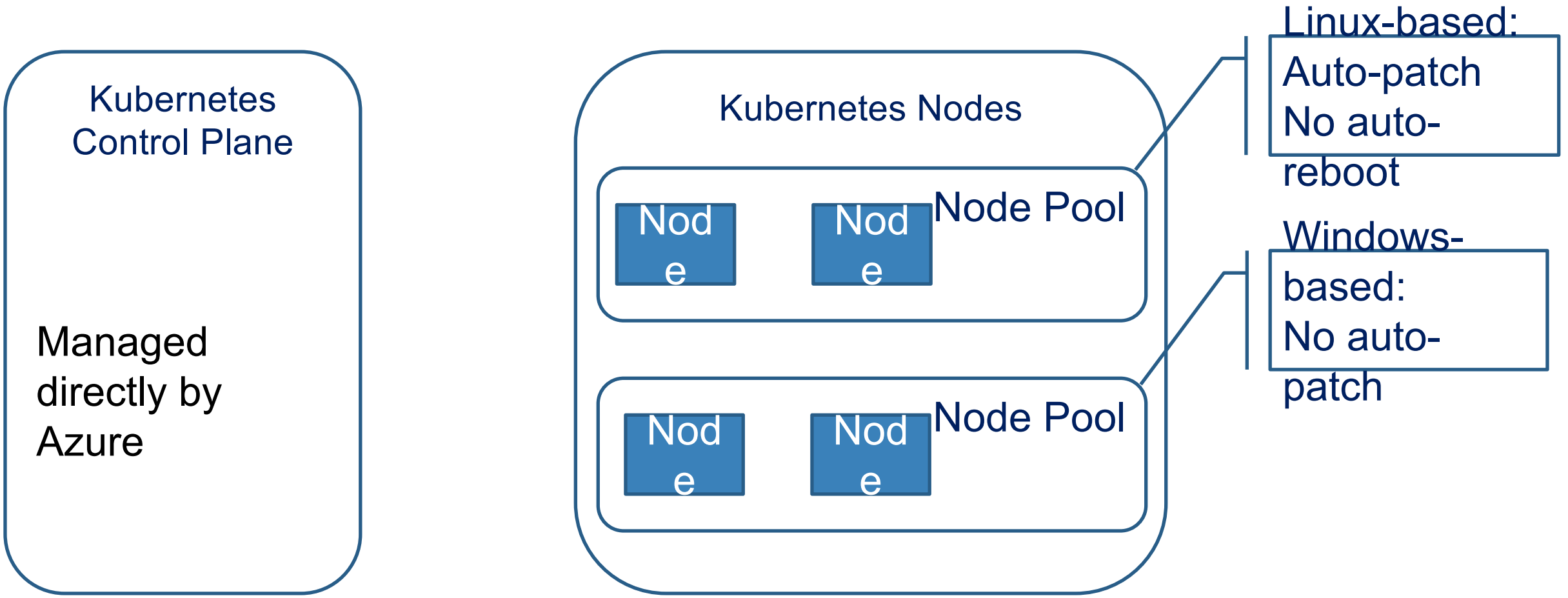


RBAC and Azure AD for Kubernetes

- Create Azure AD Applications
  - Server – access Azure AD, publish API
  - Client – access server API
- Deploy the cluster
  - az aks create --resource-group --name --generate-ssh-keys --aad-server-app-id --aad-server-app-secret --aad-client-app-id --aad-tenant-id
- Create an RBAC binding
- Access the cluster with Azure AD

https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration

Kubernetes Updates and Patches



Demo: Azure AD for Kubernetes

Configure AKS Security
Part II

Configure AKS Security

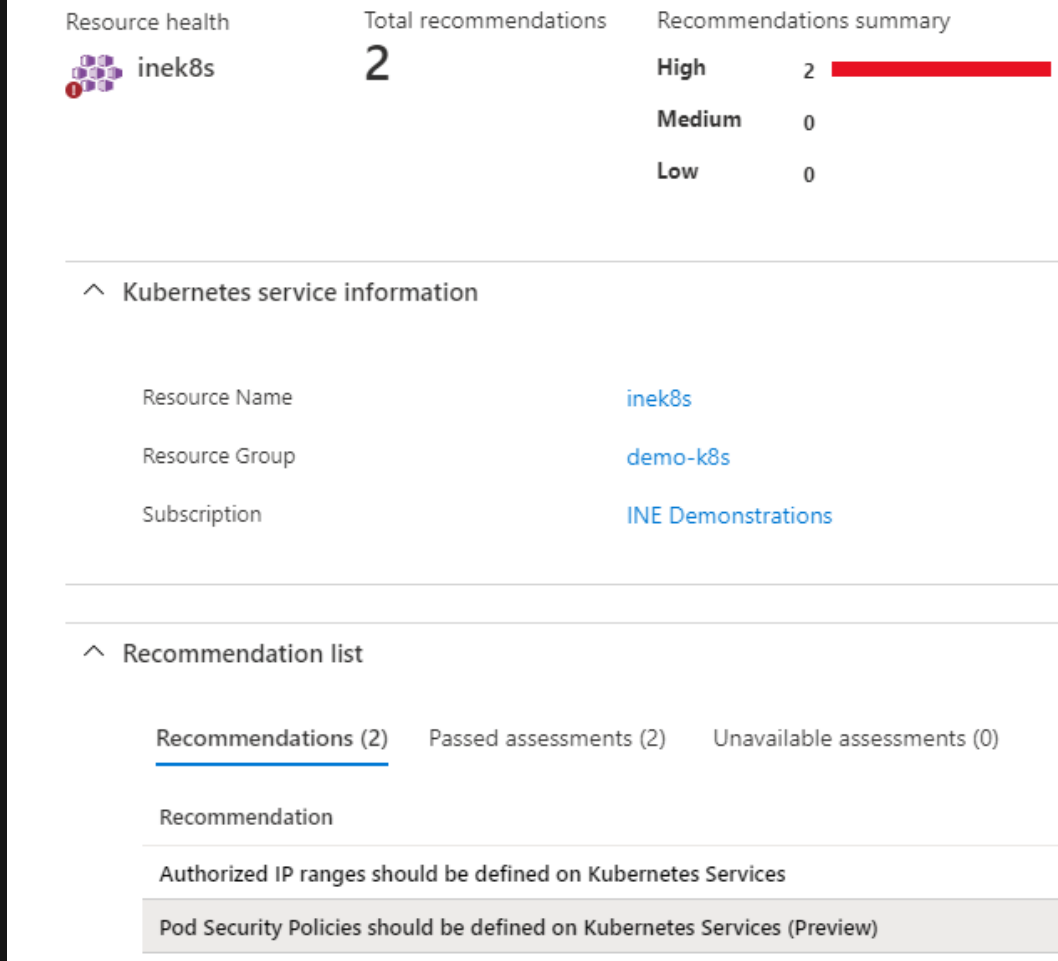
- Kubernetes Certificates and Secrets
- Azure Kubernetes Service Security
- Kubernetes Networking
- Demo: Kubernetes Security and Networking

Kubernetes Certificates and Secrets

- Certificates used for internal Kubernetes communication
  - Cluster CA created on API server
  - Kubelets (Kubernetes processes) Certificate Signing request
  - Etcd key value store
    - Certificate from cluster CA
    - Creates CA for data replication
  - API aggregator - certificates for API communication
  - Service account token for each node
  - Client certificate
- Secrets
  - Used for sensitive pod data (credentials)
  - Created via Kubernetes API
  - Stored in tmpfs

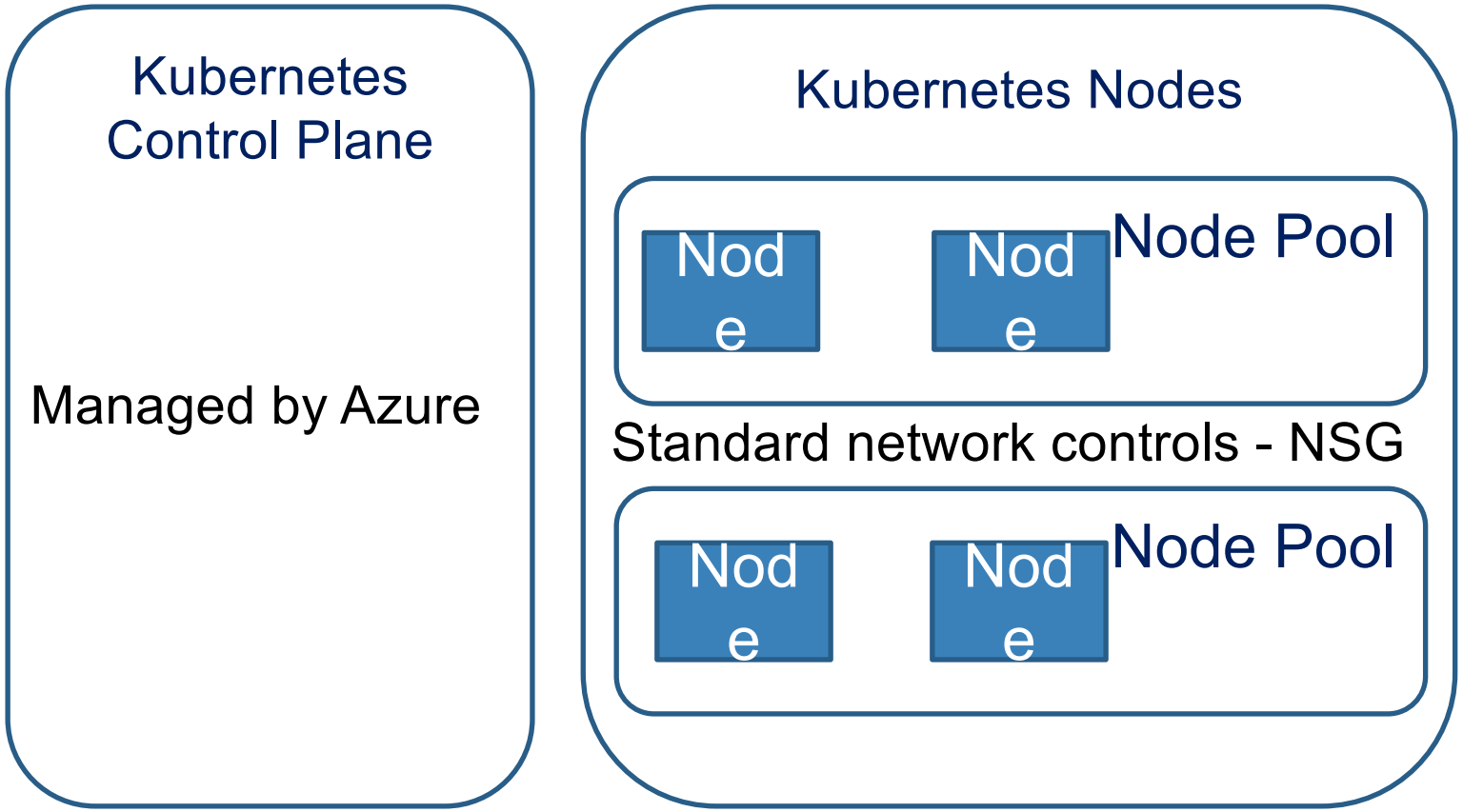
Azure Kubernetes Service Security

- + Security Center
- + Restricted Ips
- + Pod Policy



Azure Kubernetes Service Security

+ Security Center
+ Restricted Ips
+ Pod Policy



az aks update … --api-server-authorized-ip-ranges 40.117.0.0/16

Azure Kubernetes Service Security

- Security Center
- Restricted Ips
- Pod Policy

```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: psp-deny-privileged
spec:
  privileged: false
  seLinux:
    rule: RunAsAny
  supplementalGroups:
    rule: RunAsAny
  runAsUser:
    rule: RunAsAny
  fsGroup:
    rule: RunAsAny
  volumes:
  - '*'
```

In preview as of June 2020

https://docs.microsoft.com/en-us/azure/aks/use-pod-secu

Kubernetes Networking

- Kubernetes cluster is in a virtual network
  - NSGs and routing tables apply
  - Can use existing virtual network
  - Can peer other virtual networks
- Private Cluster
- Network policy
- Ingress control
  - HTTP application routing
  - Ingress controller

Demo: Kubernetes Security and Networking

Azure Container Registry

Azure Container Registry

- Container Registry Concepts
- ACR and DevOps
- Demonstration: Implement an Azure Container Registry

ACR and DevOps

- Push from CI/CD pipeline
- Pull from Azure Web App for Containers
- ACR Tasks – automated container build
- ACR Webhooks

Role-Based Access Control

Role-Based Access Control

- Role-Based Access Control (RBAC) Concepts
- Role Definition

Role-Based Access Control Concepts

Role-Based Access Control Concepts

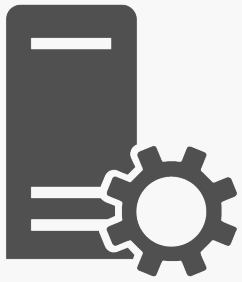
- Define role
  - Level – subscription*
  - Permission - Microsoft.Authorization/roleDefinitions/write (read)
  - Elements – Name, Description, Actions, NotActions, DataActions, NotDataActions, AssignableScopes
- Assign role
  - Level – management group, subscription, resource group, resource
  - Permission - Microsoft.Authorization/roleAssignments/*
- Effective permissions
  - Azure RBAC is additive
  - Deny assignments – blueprints and managed apps

Role Definition


```
{
        "Name": "Website Contributor",
        "Id": "de139f84-1756-47ae-9be6-808fbbe84772",
        "IsCustom": false,
        "Description": "Lets you manage websites (not web plans), but not access to them.",
        "Actions": [
                "Microsoft.Authorization/*/read",
                "Microsoft.Insights/alertRules/*",
                "Microsoft.Insights/components/*",
                …
                "Microsoft.Web/sites/*“
         ] …
```

Role Definition

```
…
        "NotActions": [],
        "DataActions": [],
        "NotDataActions": [],
        "AssignableScopes": ["/"]
}
```



RBAC In Action

RBAC in Action

- Demonstration: RBAC
- Troubleshoot RBAC

Troubleshoot RBAC

- Role definition or assignment rights
- Custom role limit - 5000 custom roles per tenant
- Migrate a subscription between tenants
- RBAC changes can take 30 minutes
- Obscure permissions
  - Web apps
  - Virtual machines

Policies and Initiatives

Policies and Initiatives

- Policies and Initiatives
- Policy Definition
- Policy and RBAC

Policies and Initiatives

- Use Cases
  - Deny
  - Monitor
  - Audit
  - Correct
- Components
  - Filter
  - Action
  - Parameters
- Initiative
  - Shared set of policies
  - Parameter control

Policy Definition

```
"Properties": {
        "displayName": "Allowed virtual machine SKUs",
        "policyType": "BuiltIn",  "mode": "Indexed",
        "description": "This policy enables you to ....",
        "metadata": {"category": "Compute"},
        "parameters": {"listOfAllowedSKUs": "@{type=Array; metadata=}"},
        "policyRule": {
                "if": "@{allOf=System.Object[]}",
                "then": "@{effect=Deny}"
        }
},
```

Policy and RBAC

- RBAC focuses on permissions
- Policy focuses on resource properties
- RBAC defaults to deny
- Policy defaults to allow
- Policy and RBAC should be used together
  - VM Contributor
  - VM Sku policy

Policies and Initiatives in Action

Policies and Initiatives in Action

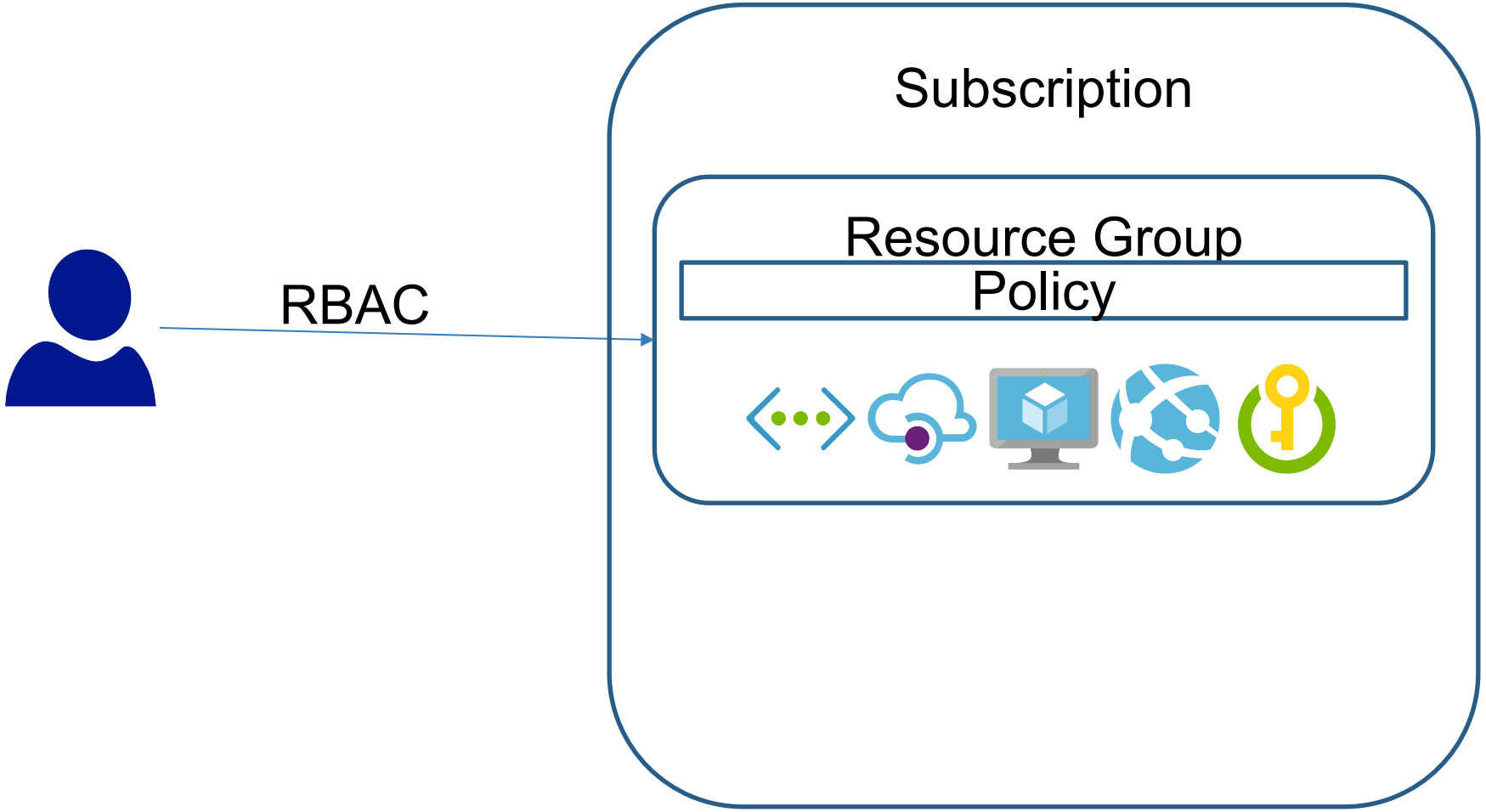
- Demonstration: Apply a Custom Policy
- Demonstration: Apply a Custom Initiative

Azure Blueprints

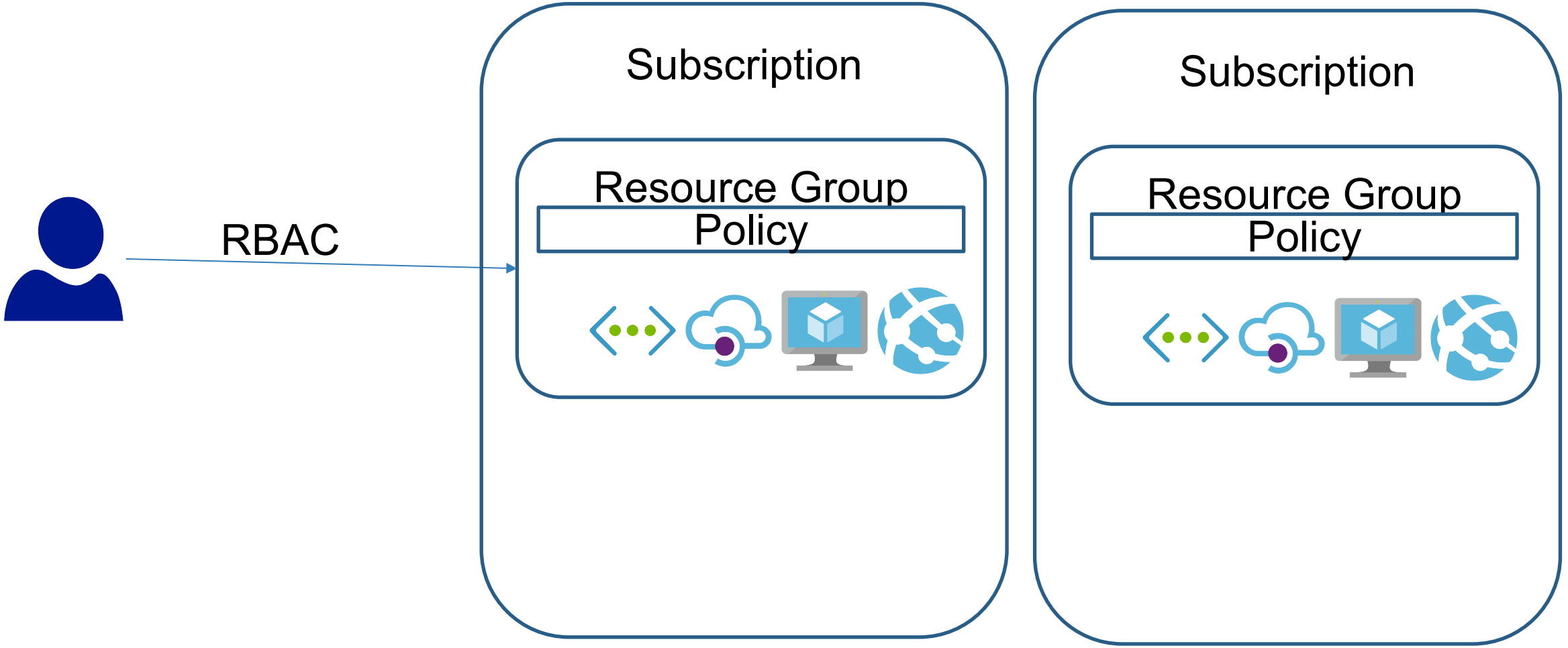
Azure Blueprints

- Managing Governance at Scale
- Azure Blueprints
- Demo: Azure Blueprints

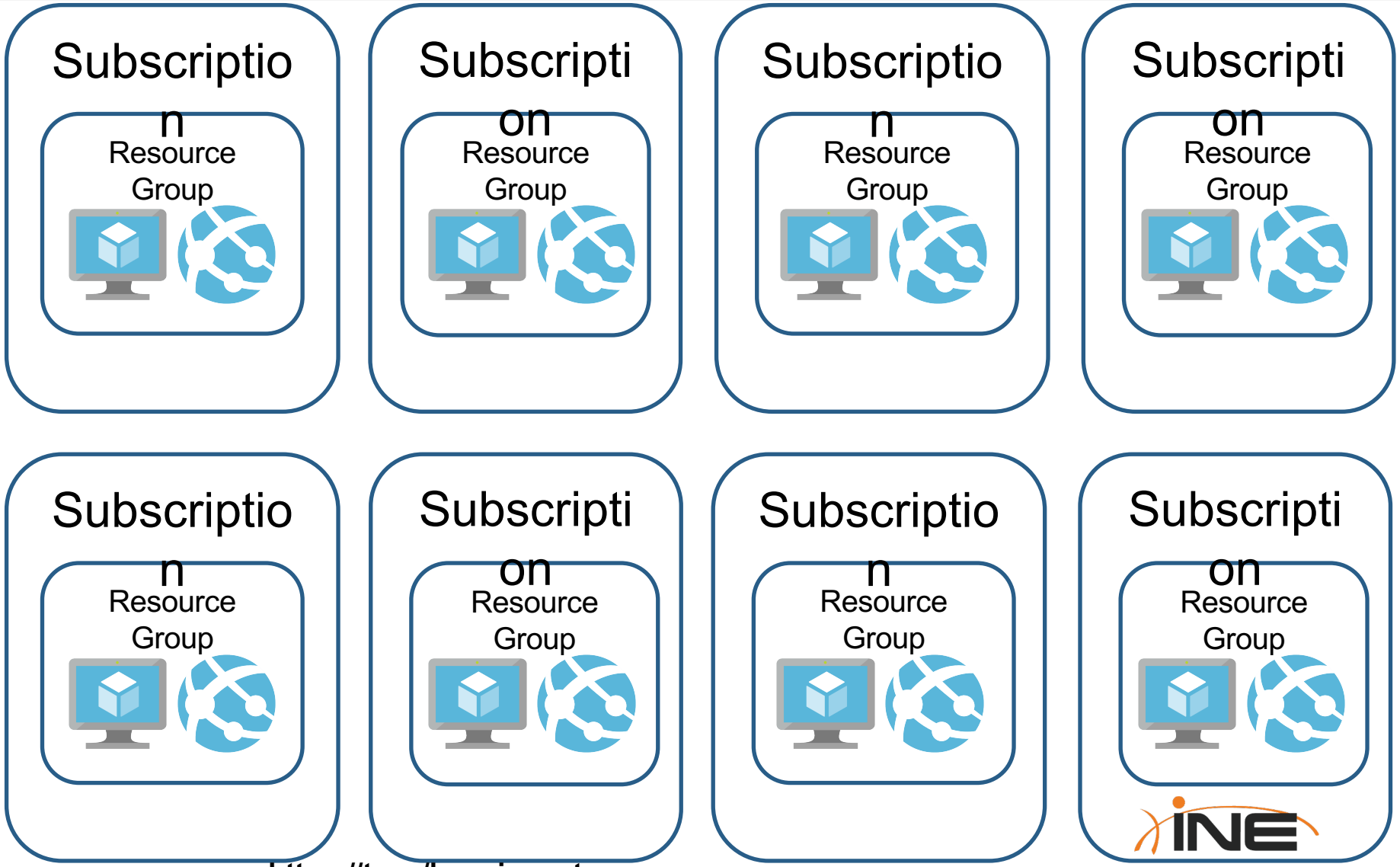
Managing Governance at Scale



Managing Governance at Scale

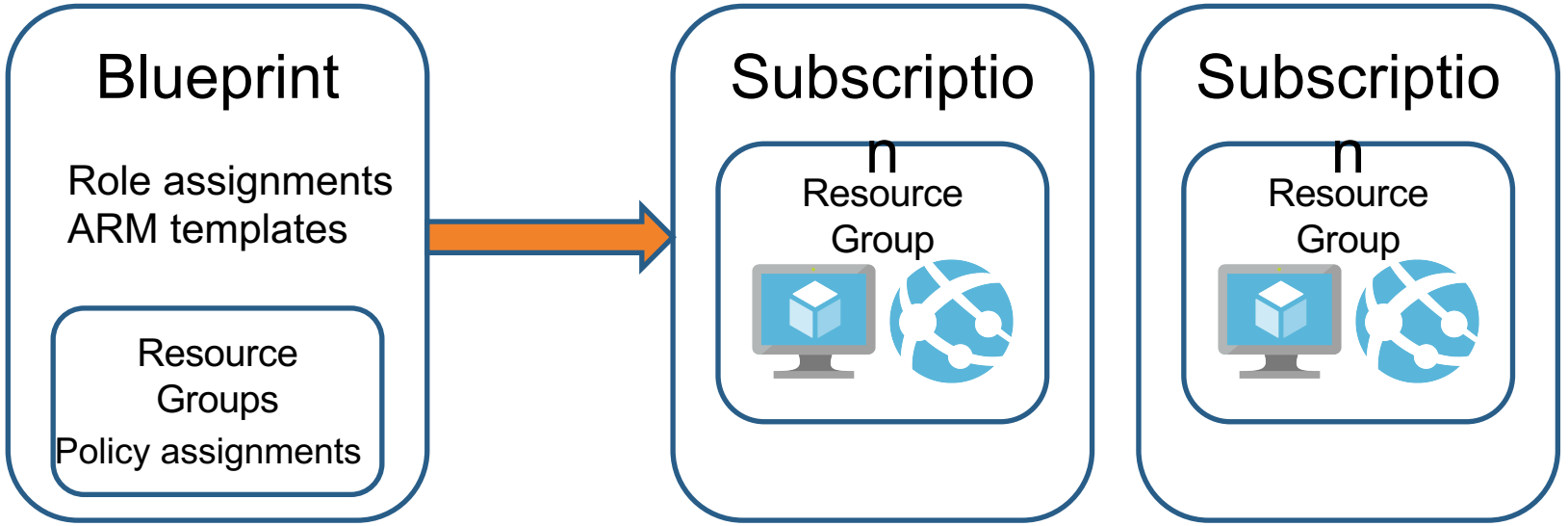


Managing Governance at Scale



Azure Blueprints

- Role Assignments
- Policy Assignments
- Azure Resource Manager Templates
- Resource Groups



Demo: Azure Blueprints

Resource Locks

Resource Locks

- Resource Locks
- Demo: Resource Locks

Resource Locks

- Protect resources
- Delete or Read-only
- Apply to resource groups and resources
- Active in the management plane

Production VM

```
Remove-AzVM -Name Production
```

Remove-AzVM : The scope '…/virtualMachines/Production' cannot perform delete operation because following scope(s) are locked: '…/resourceGroups/production'. Please remove the lock and try again.

Demo: Resource Locks