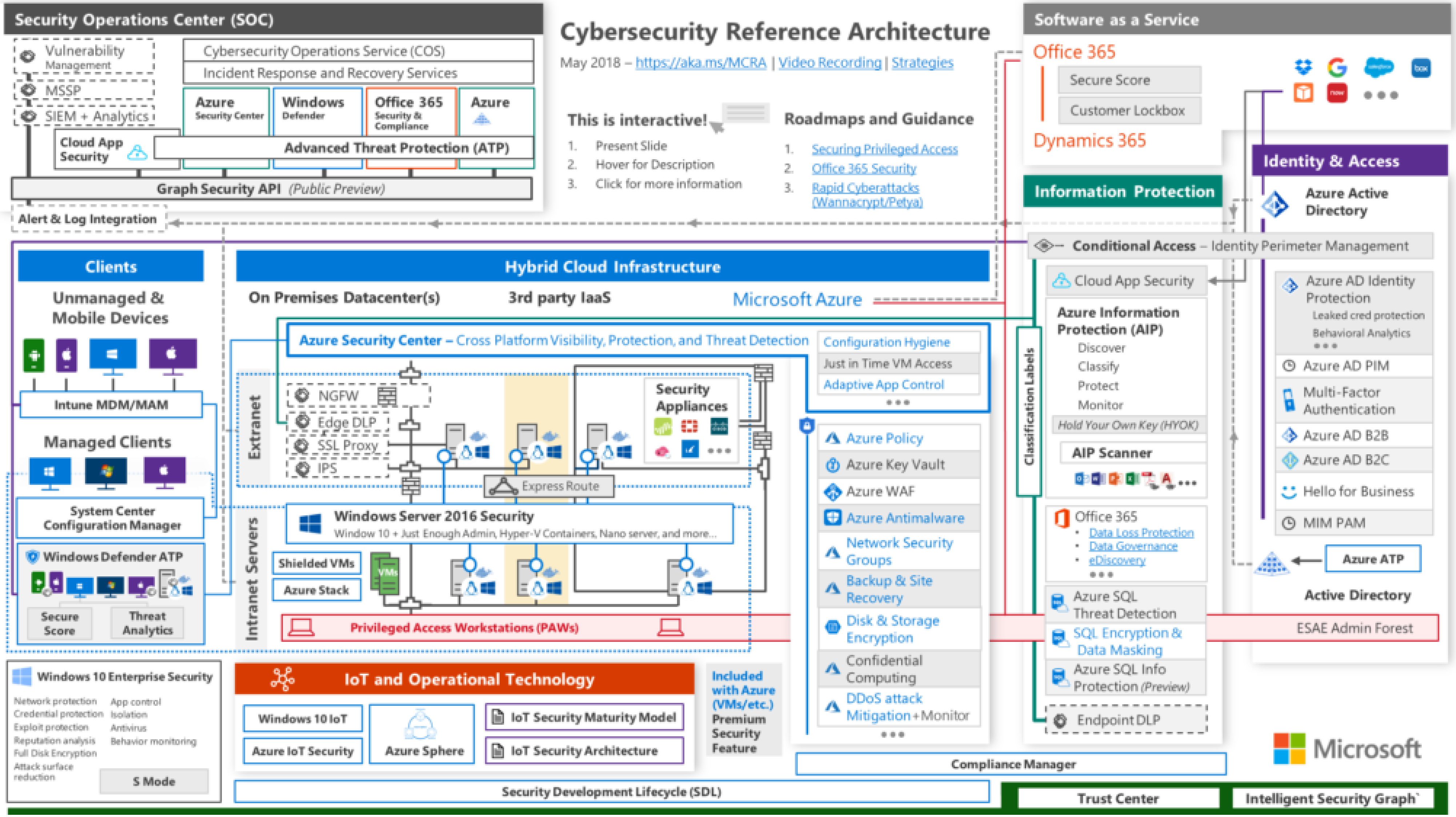
Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies



Security Operations Center (SOC)

Vulnerability Management

MSSP

SIEM + Analytics

Cybersecurity Operations Service (COS)

Incident Response and Recovery Services

Azure Security Center

Windows Defender

Office 365 Security & Compliance

Azure

Cloud App Security

Advanced Threat Protection (ATP)

Graph Security API *(Public Preview)*

Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Windows Defender ATP

Secure Score

Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

Extranet

NGFW

Edge DLP

SSL Proxy

IPS

Security Appliances

Express Route

Intranet Servers

Windows Server 2016 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

Azure Stack

VMs

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation + Monitor

Included with Azure (VMs/etc.)

Premium Security Feature

Information Protection

Classification Labels

Cloud App Security

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection *(Preview)*

Endpoint DLP

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Windows 10 Enterprise Security

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Compliance Manager

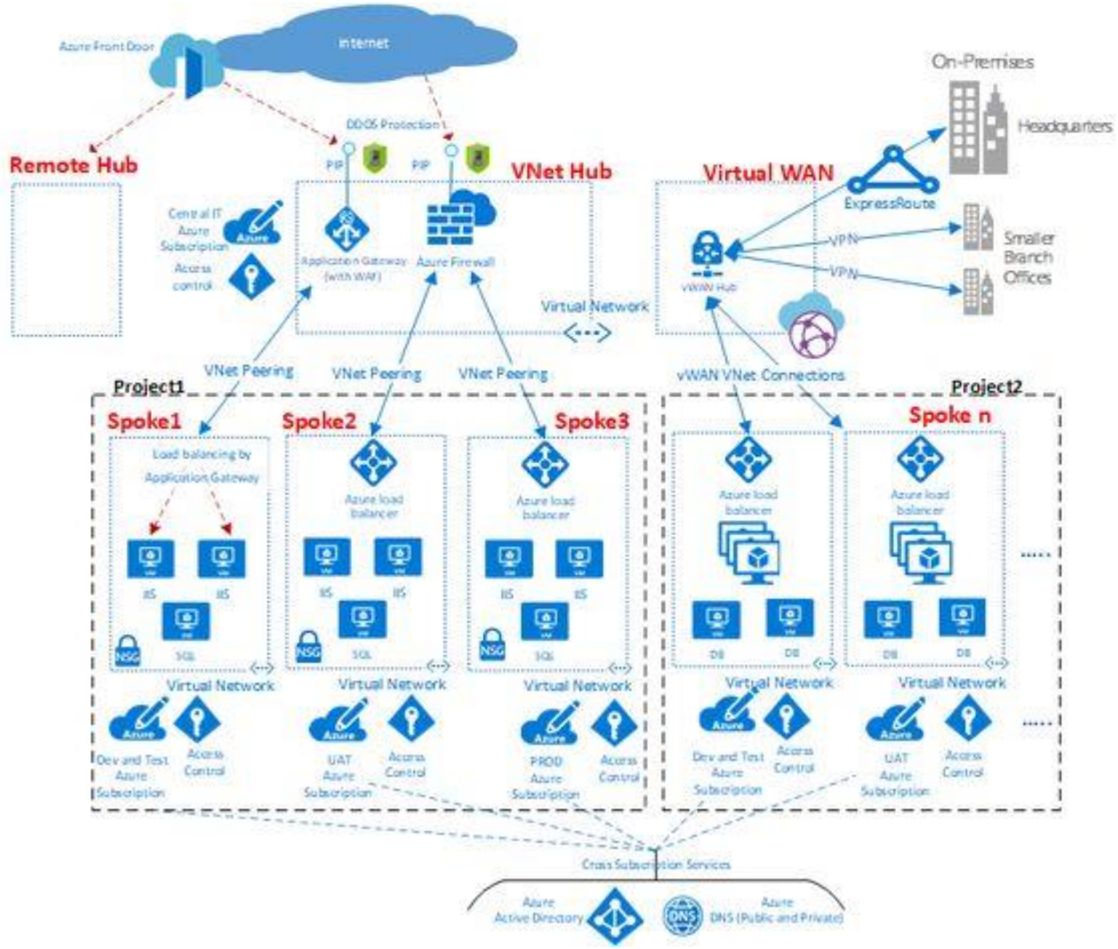
Security Development Lifecycle (SDL)

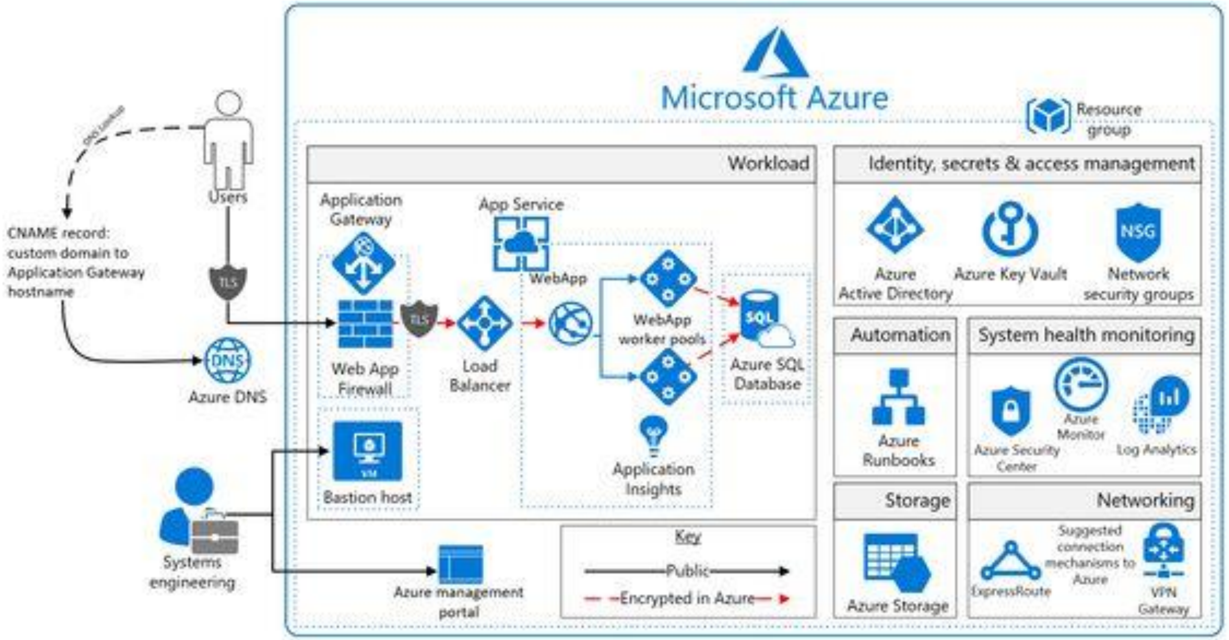
Trust Center

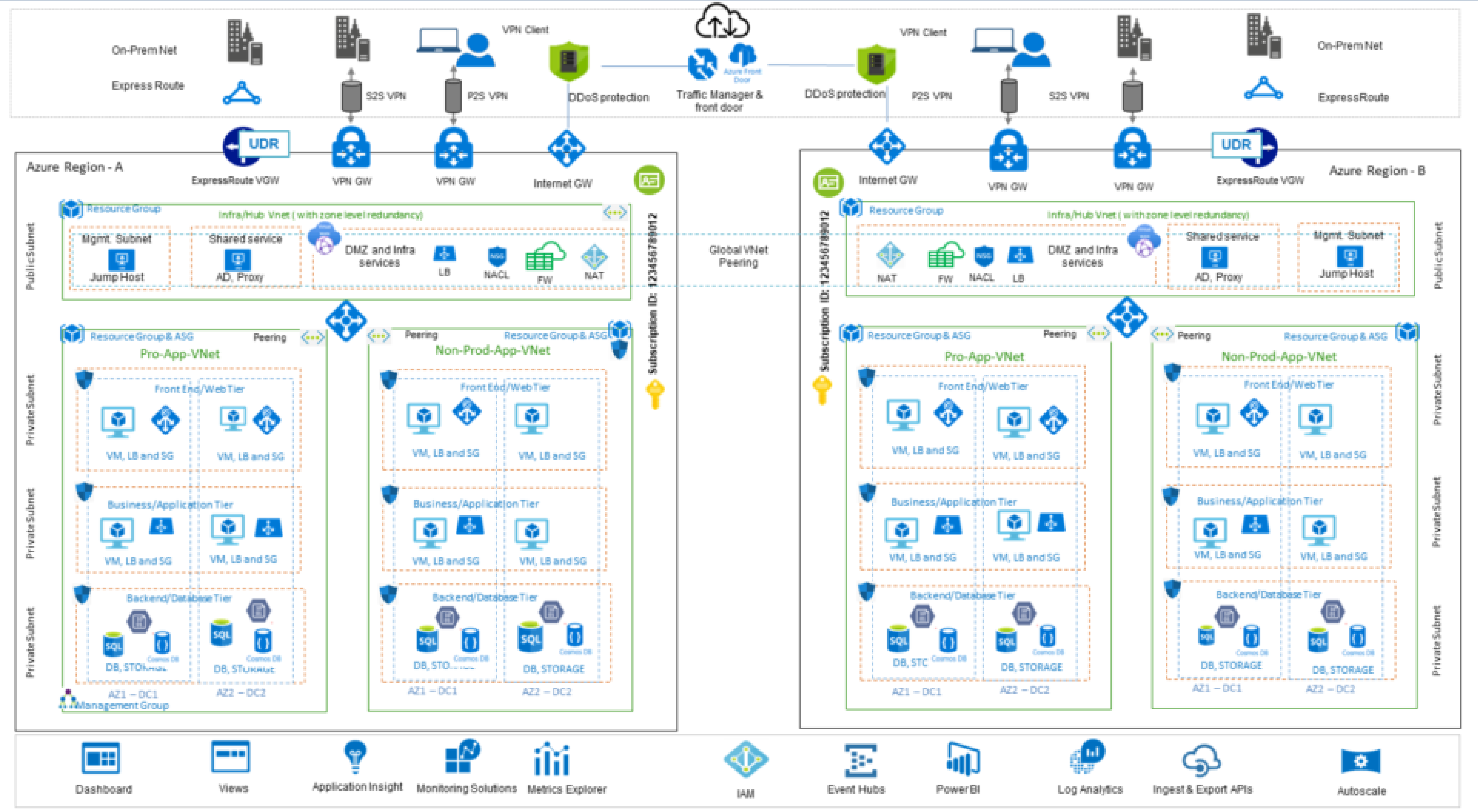
Intelligent Security Graph

Microsoft

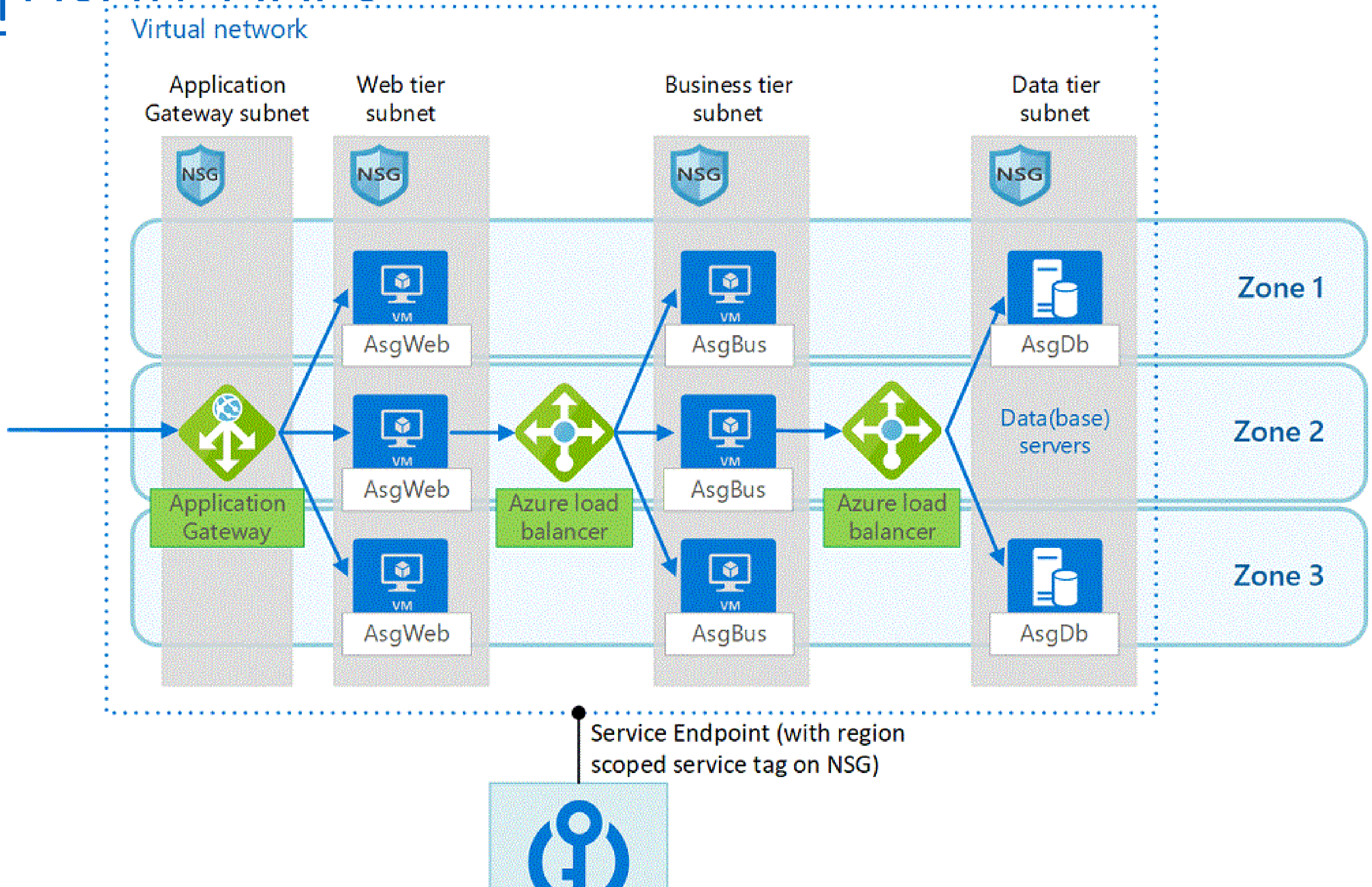
Azure Network connectivity product



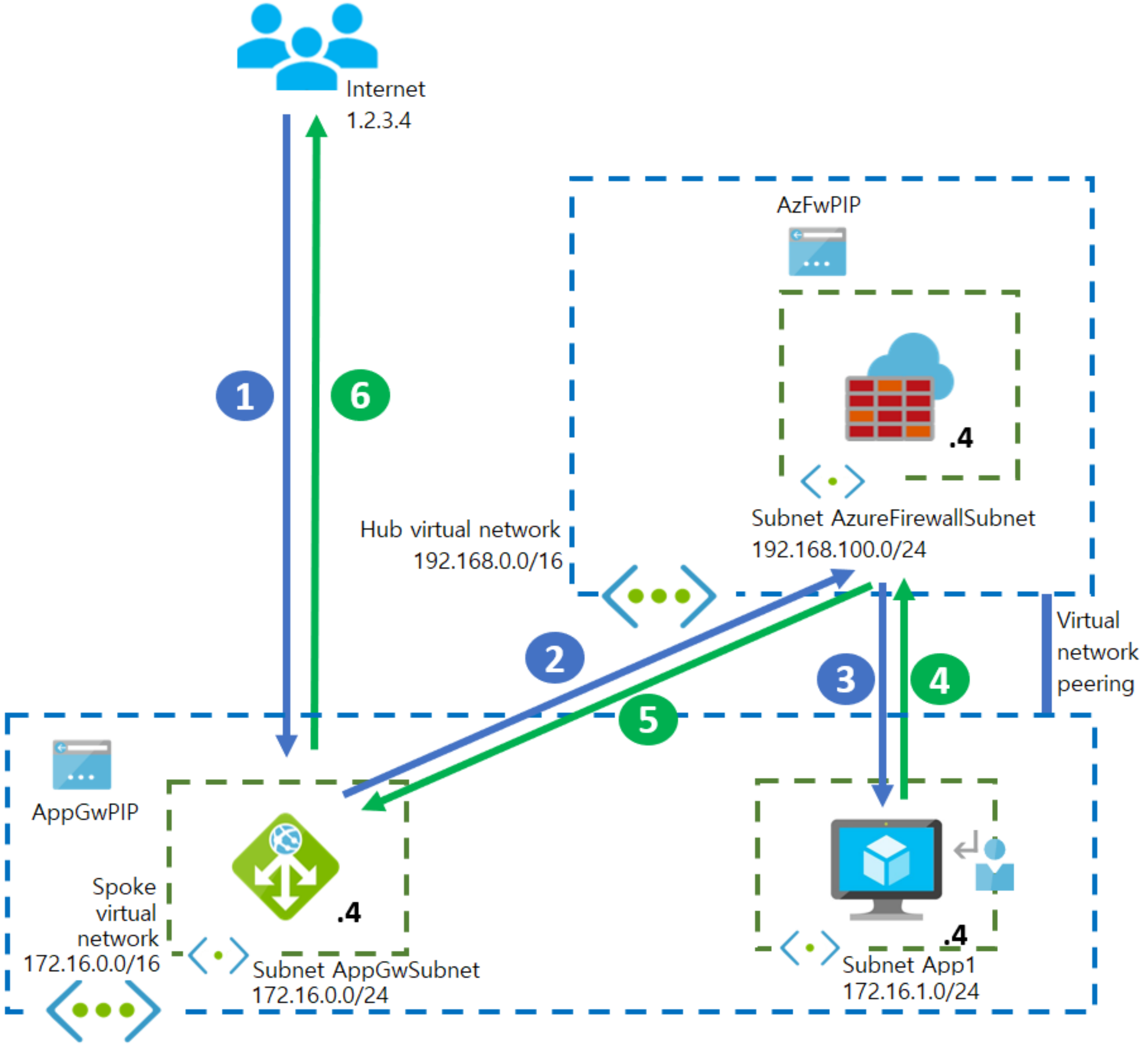

Microsoft Azure
Resource group
DNS Lookup
Users
CNAME record: custom domain to Application Gateway hostname
TLS
Azure DNS
Workload
Application Gateway
App Service
WebApp
Web App Firewall
TLS
Load Balancer
WebApp worker pools
SQL
Azure SQL Database
Application Insights
VM
Bastion host
Systems engineering
Azure management portal
Key
Public
Encrypted in Azure
Identity, secrets & access management
Azure Active Directory
Azure Key Vault
NSG
Network security groups
Automation
Azure Runbooks
System health monitoring
Azure Security Center
Azure Monitor
Log Analytics
Storage
Azure Storage
Networking
ExpressRoute
Suggested connection mechanisms to Azure
VPN Gateway


On-Prem Net
Express Route
S2S VPN
P2S VPN
VPN Client
DDoS protection
Azure Front Door
Traffic Manager & front door
DDoS protection
VPN Client
P2S VPN
S2S VPN
On-Prem Net
ExpressRoute
UDR
ExpressRoute VGW
VPN GW
VPN GW
Internet GW
Internet GW
VPN GW
VPN GW
UDR
ExpressRoute VGW
Azure Region - A
Azure Region - B
Resource Group
Infra/Hub Vnet (with zone level redundancy)
Mgmt. Subnet
Jump Host
Shared service
AD, Proxy
DMZ and Infra services
LB
NACL
FW
NAT
Public Subnet
Subscription ID: 123456789012
Global VNet Peering
Subscription ID: 123456789012
Resource Group
Infra/Hub Vnet (with zone level redundancy)
NAT
FW
NACL
LB
DMZ and Infra services
Shared service
AD, Proxy
Mgmt. Subnet
Jump Host
Public Subnet
Resource Group & ASG
Peering
Pro-App-VNet
Peering
Resource Group & ASG
Non-Prod-App-VNet
Private Subnet
Front End/Web Tier
VM, LB and SG
VM, LB and SG
Private Subnet
Business/Application Tier
VM, LB and SG
VM, LB and SG
Private Subnet
Backend/Database Tier
SQL
Cosmos DB
DB, STORAGE
AZ1 – DC1
AZ2 – DC2
Management Group
Resource Group & ASG
Peering
Pro-App-VNet
Peering
Resource Group & ASG
Non-Prod-App-VNet
Private Subnet
Private Subnet
Private Subnet
Dashboard
Views
Application Insight
Monitoring Solutions
Metrics Explorer
IAM
Event Hubs
Power BI
Log Analytics
Ingest & Export APIs
Autoscale

[Security considerations for highly sensitive IaaS apps in Azure - Azure Architecture Center | Microsoft Docs]



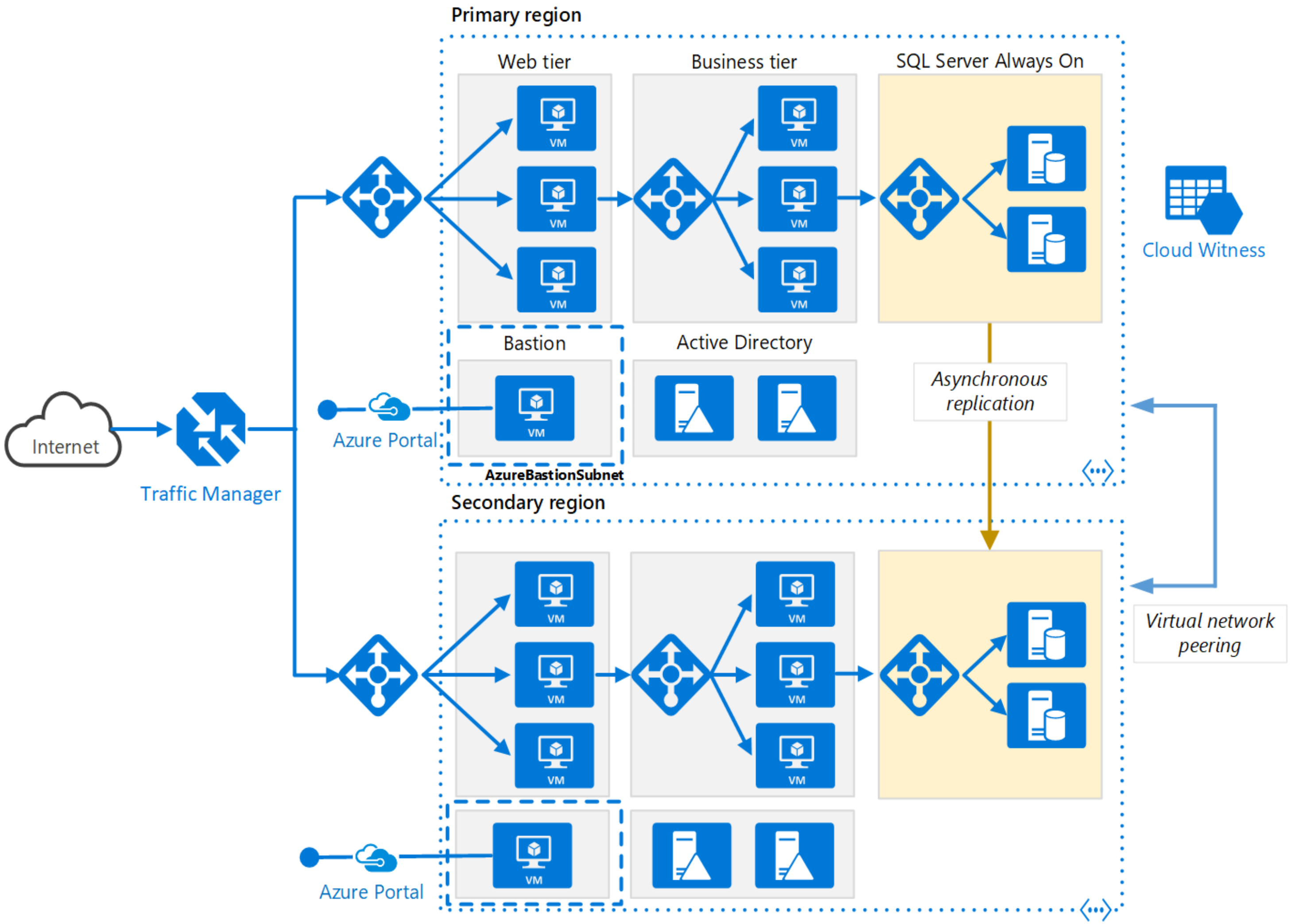
[Zero-trust network for web applications with Azure Firewall and Application Gateway - Azure Architecture Center | Microsoft Docs]



- Azure Firewall architecture overview - Azure Architecture Center | Microsoft Docs

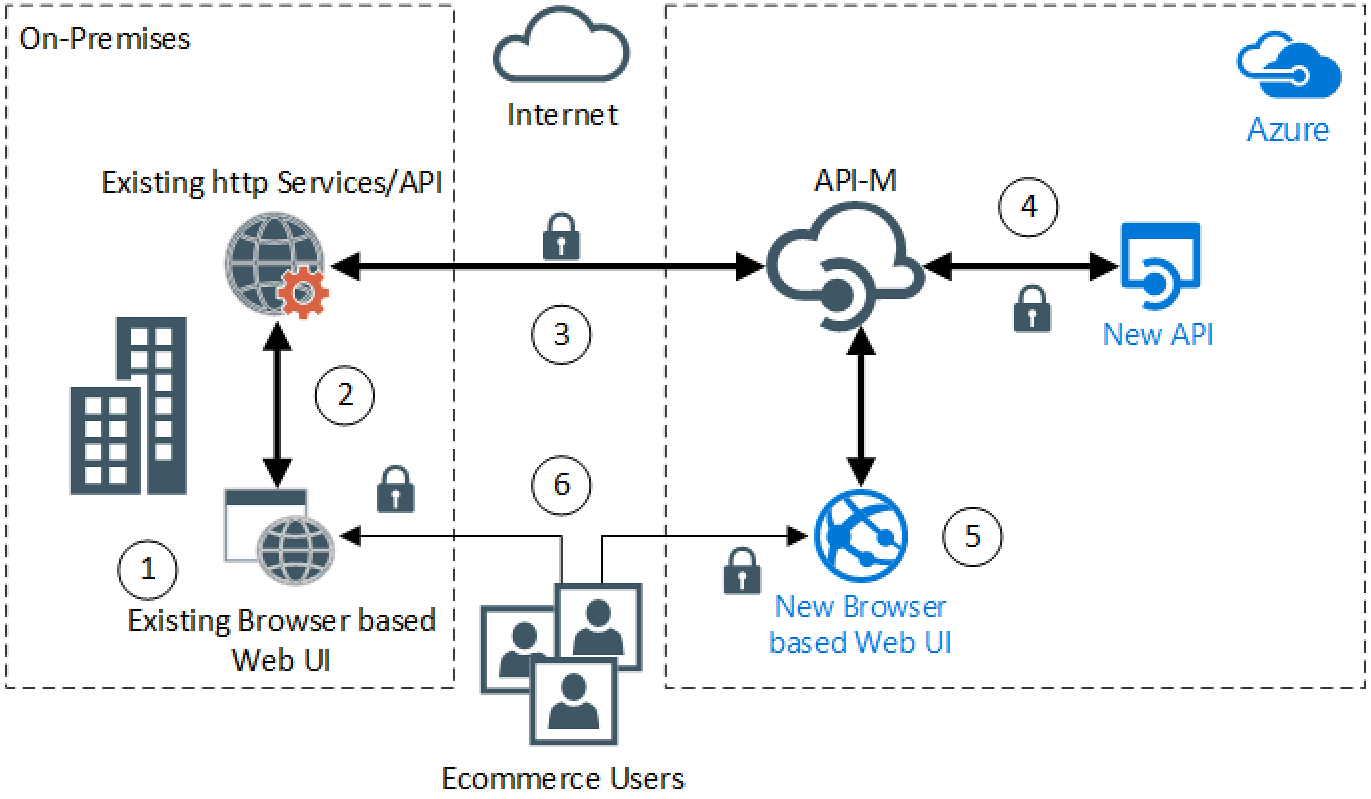
- Browse Azure Architectures - Azure Architecture Center | Microsoft Docs

Multi-region N-zones design

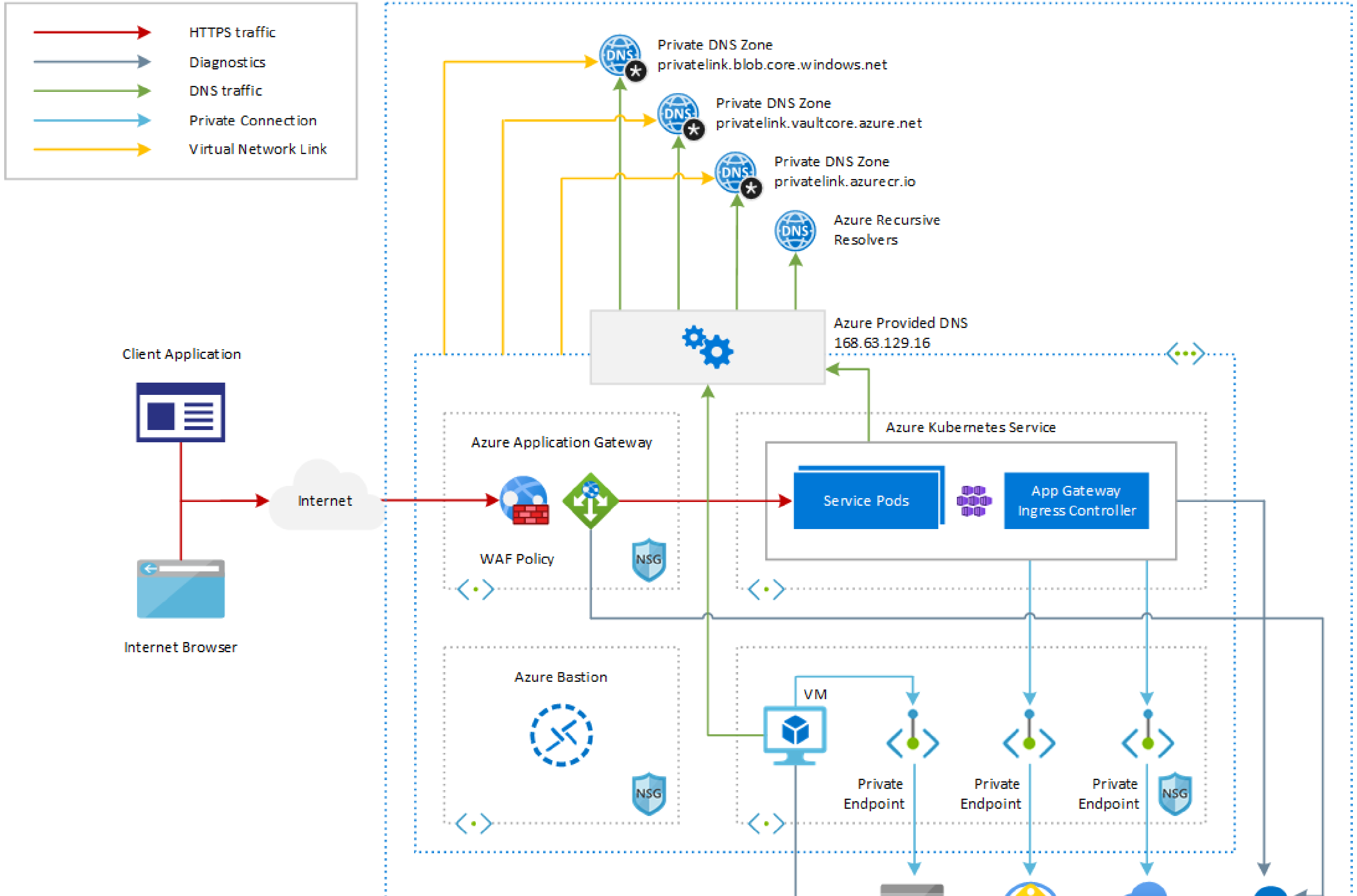


- 1. Primary and secondary regions. Use two regions to achieve higher availability. One is the primary region. The other region is for failover.
- 2. Azure Traffic Manager. Traffic Manager routes incoming requests to one of the regions. During normal operations, it routes requests to the primary region. If that region becomes unavailable, Traffic Manager fails over to the secondary region. For more information, see the section Traffic Manager configuration.
- 3. Resource groups. Create separate resource groups for the primary region, the secondary region, and for Traffic Manager. This gives you the flexibility to manage each region as a single collection of resources. For example, you could redeploy one region, without taking down the other one. Link the resource groups, so that you can run a query to list all the resources for the application.
- 4. Virtual networks. Create a separate virtual network for each region. Make sure the address spaces do not overlap.
- 5. SQL Server Always On Availability Group. If you are using SQL Server, we recommend SQL Always On Availability Groups for high availability. Create a single availability group that includes the SQL Server instances in both regions.

Migrate a web app using Azure APIM - Azure Architecture Center | Microsoft Docs



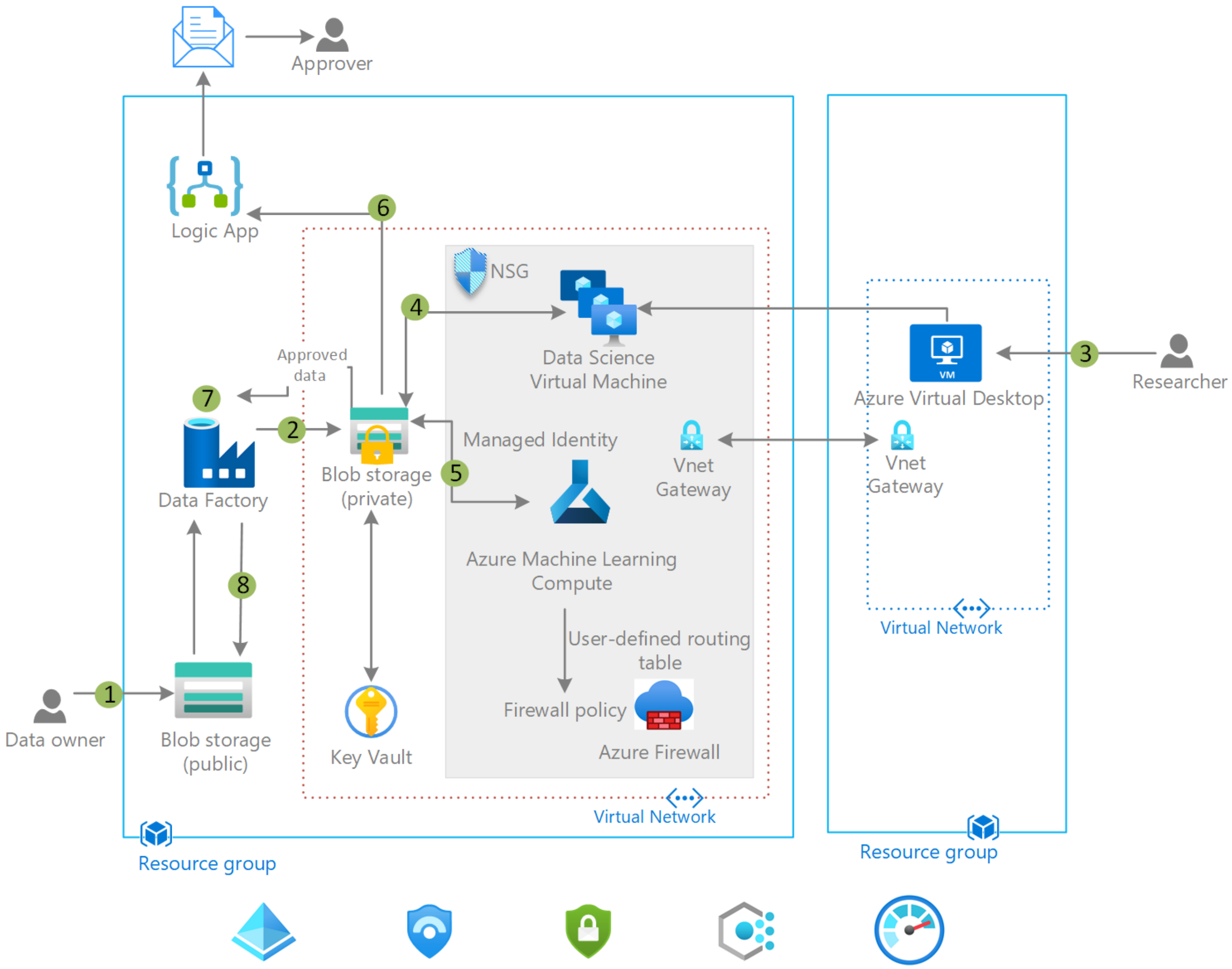
Use Application Gateway Ingress Controller (AGIC) with a multitenant Azure Kubernetes Service - Azure Architecture Center | Microsoft Docs



- Azure Application Gateway, has the layer 7 security application firewall + load balancing functions
- Layer 7 security functions include: SQL injection, across site scripting
- By using WAF policy
- Secure Sockets Layer (SSL/TLS) termination
- Autoscaling
- Zone redundancy
- Static VIP
- Web Application Firewall
- Ingress Controller for AKS
- URL-based routing
- Multiple-site hosting
- Redirection
- Session affinity
- WebSocket and HTTP/2 traffic
- Connection draining
- Custom error pages
- Rewrite HTTP headers
- Sizing

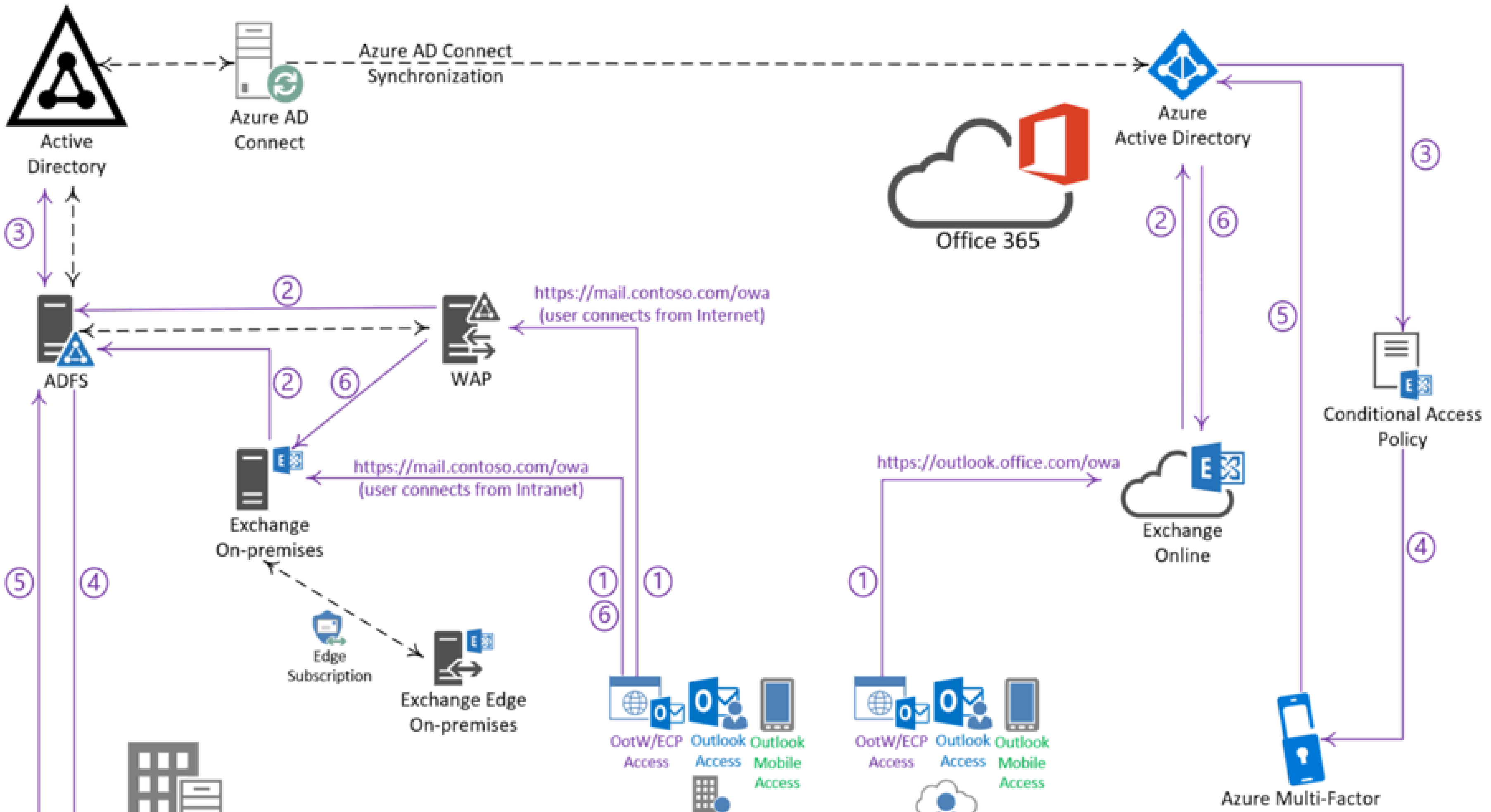
- Azure Traffic Manager - traffic routing methods | Microsoft Docs

Secure research environment for regulated data - Azure Architecture Center | Microsoft Docs

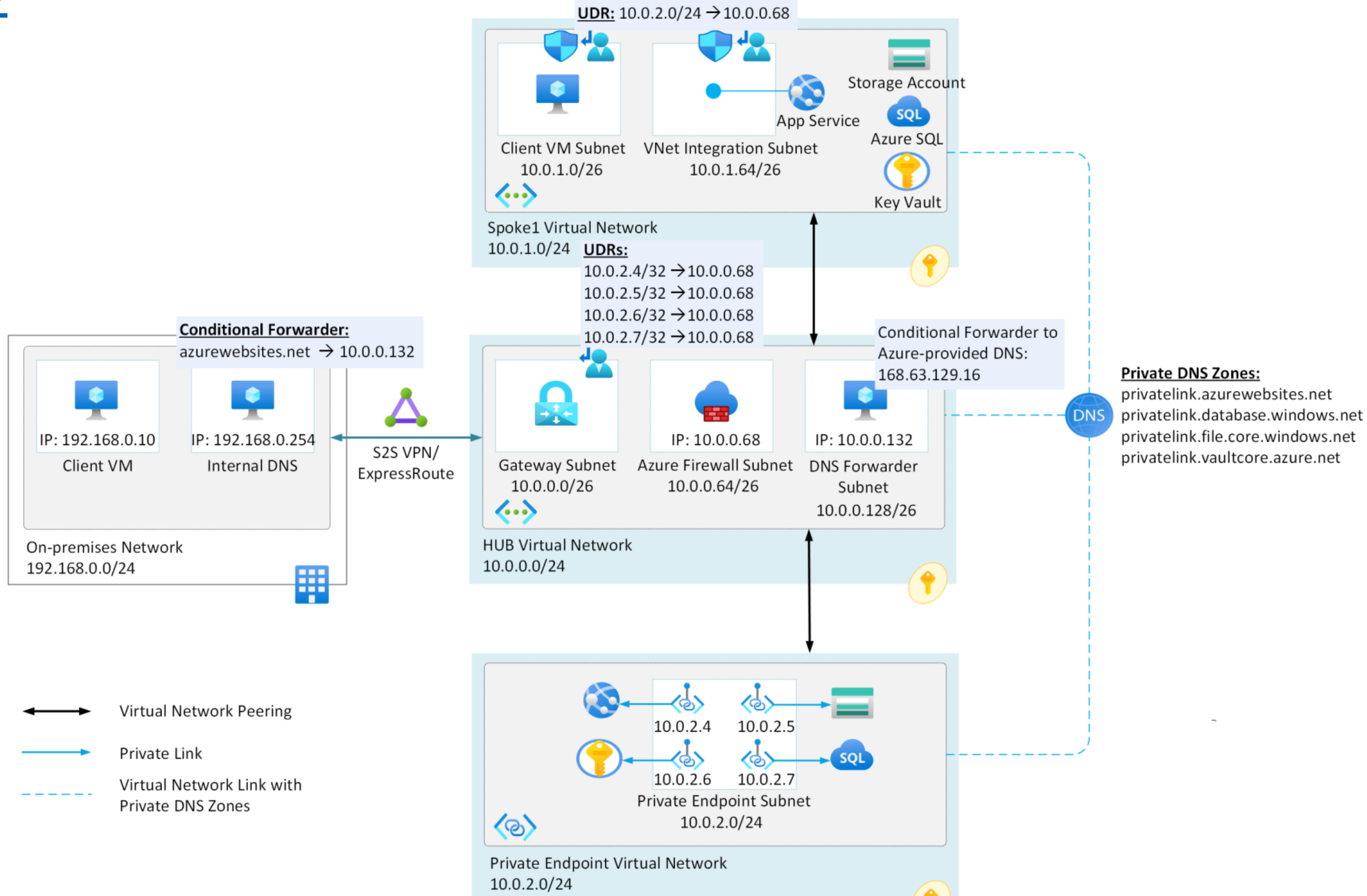


- GitHub - Azure-Samples/aks-agic: This sample shows how to deploy an AKS cluster with Application Gateway, Application Gateway Ingress Controller, Azure Container Registry, Log Analytics and Key Vault.

Enhanced-security hybrid messaging — web access - Azure Example Scenarios | Microsoft Docs



Improved-security access to multitenant web apps from an on-premises network - Azure Example Scenarios | Microsoft Docs



UDR: 10.0.2.0/24 → 10.0.0.68

Client VM Subnet
10.0.1.0/26

VNet Integration Subnet
10.0.1.64/26

App Service

Storage Account

Azure SQL

Key Vault

Spoke1 Virtual Network
10.0.1.0/24

UDRs:
10.0.2.4/32 → 10.0.0.68
10.0.2.5/32 → 10.0.0.68
10.0.2.6/32 → 10.0.0.68
10.0.2.7/32 → 10.0.0.68

Conditional Forwarder:
azurewebsites.net → 10.0.0.132

IP: 192.168.0.10
Client VM

IP: 192.168.0.254
Internal DNS

On-premises Network
192.168.0.0/24

S2S VPN/
ExpressRoute

Gateway Subnet
10.0.0.0/26

IP: 10.0.0.68
Azure Firewall Subnet
10.0.0.64/26

IP: 10.0.0.132
DNS Forwarder Subnet
10.0.0.128/26

Conditional Forwarder to
Azure-provided DNS:
168.63.129.16

HUB Virtual Network
10.0.0.0/24

DNS

Private DNS Zones:
privatelink.azurewebsites.net
privatelink.database.windows.net
privatelink.file.core.windows.net
privatelink.vaultcore.azure.net

10.0.2.4
10.0.2.5
10.0.2.6
10.0.2.7

SQL

Private Endpoint Subnet
10.0.2.0/24

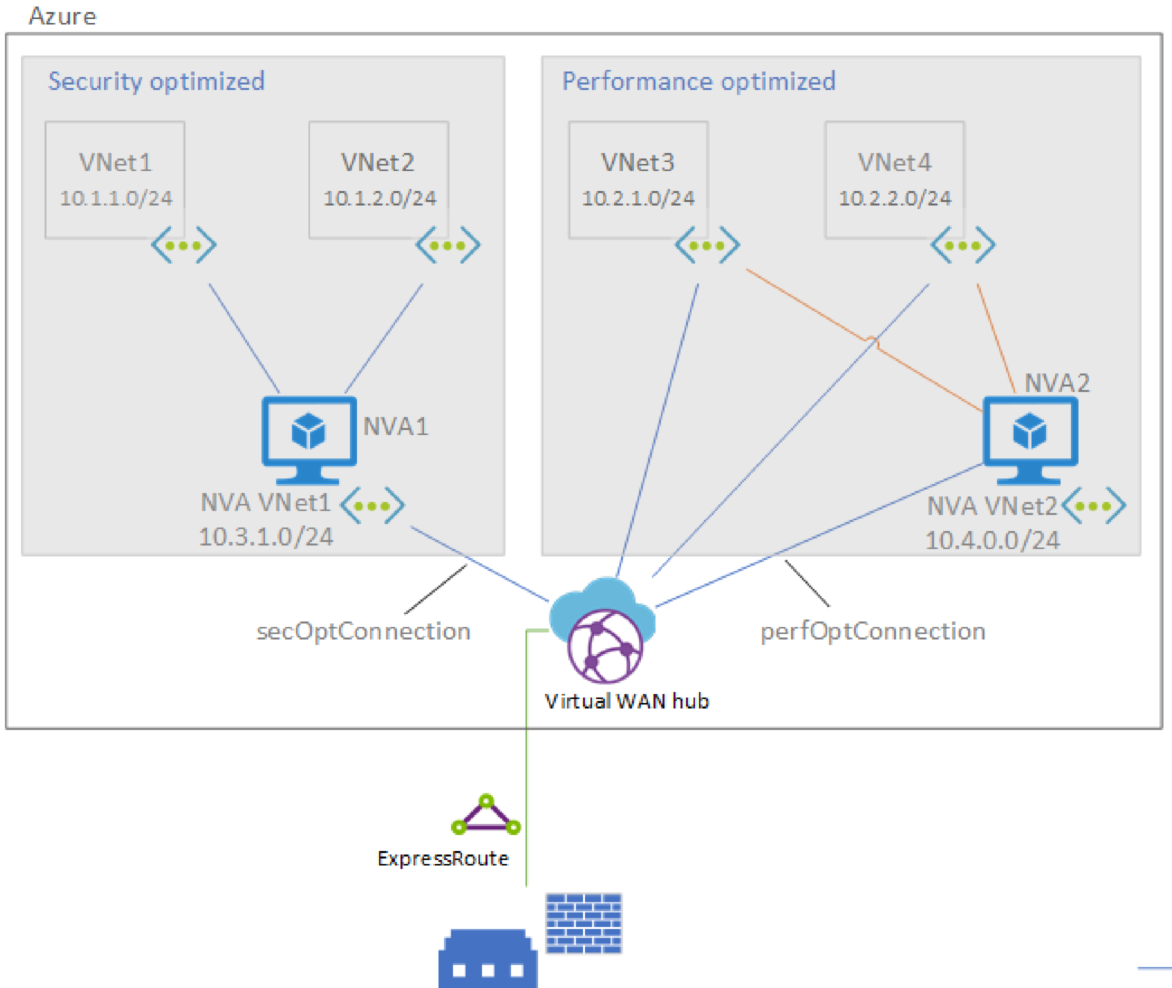
Private Endpoint Virtual Network
10.0.2.0/24

Virtual Network Peering

Private Link

Virtual Network Link with
Private DNS Zones

Virtual WAN architecture optimized for department-specific requirements - Azure Example Scenarios | Microsoft Docs



UDR route table for all subnets in VNet1 and VNet2

Name	Address prefix	Next hop type	Next hop IP address
rt-to-secOptimized	10.1.0.0/16	Virtual appliance	<ip address NVA1>

UDR route table for all subnets in VNet3 and VNet4

Name	Address prefix	Next hop type	Next hop IP address
rt-to-internet	0.0.0.0/0	Virtual appliance	<ip address NVA2>
vnet-to-vnet	10.2.0.0/16	Virtual appliance	<ip address NVA2>

Static routes on secOptConnection

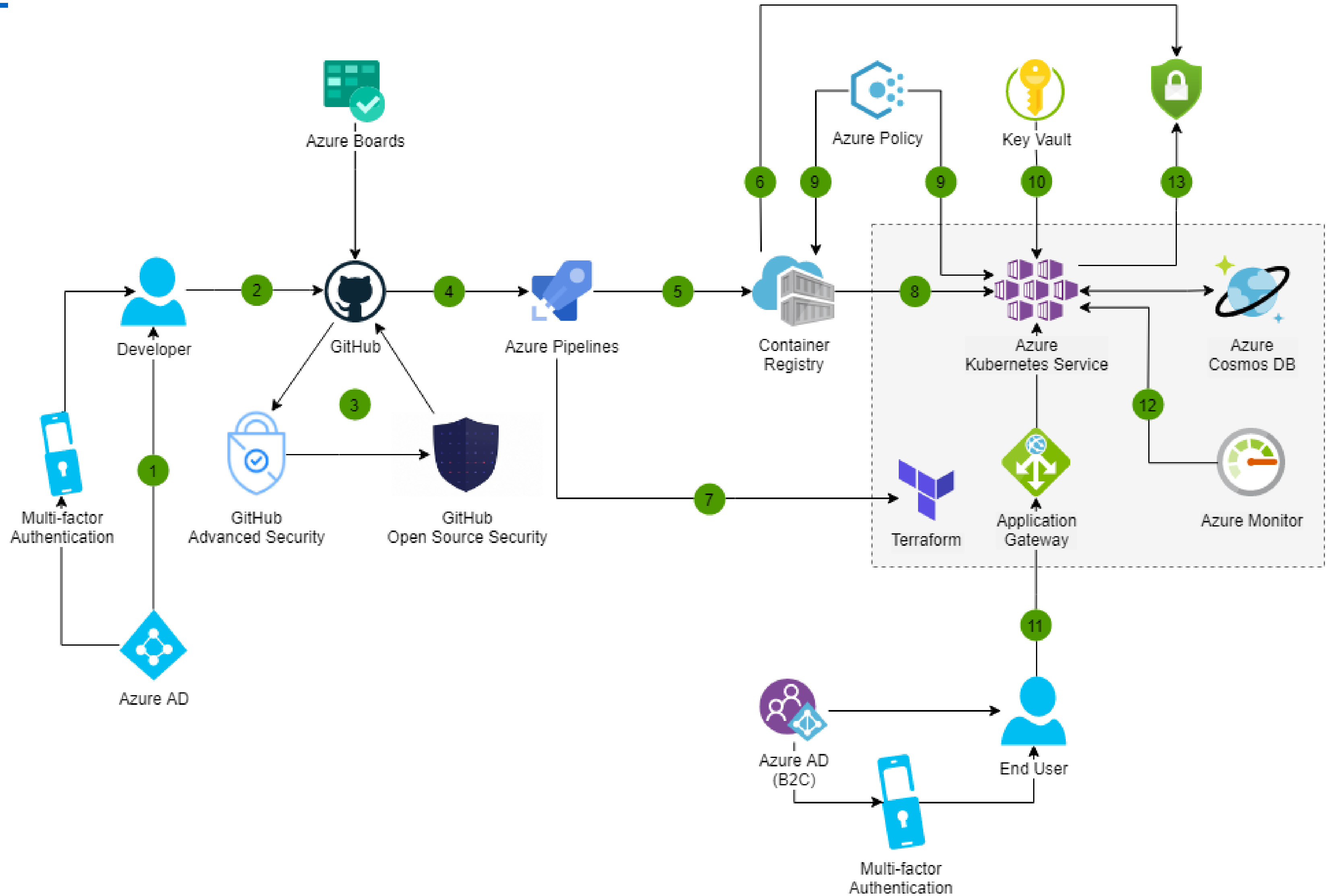
Name	Address prefix	Next hop type	Next hop IP address
rt-to-secOptimized	10.1.0.0/16	Virtual appliance	<ip address NVA1>

Static routes on perfOptConnection

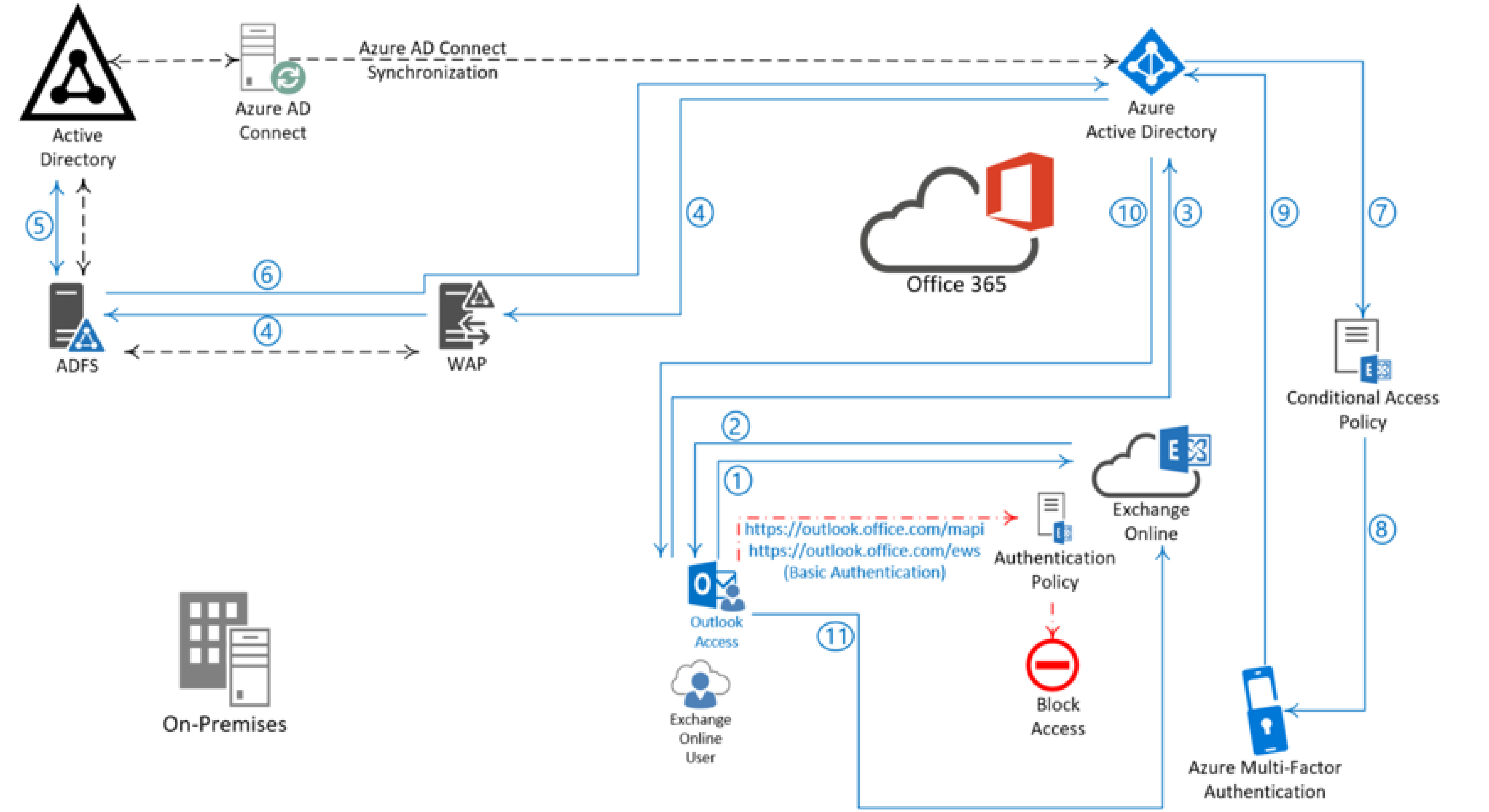
None

—— Hub virtual network connection

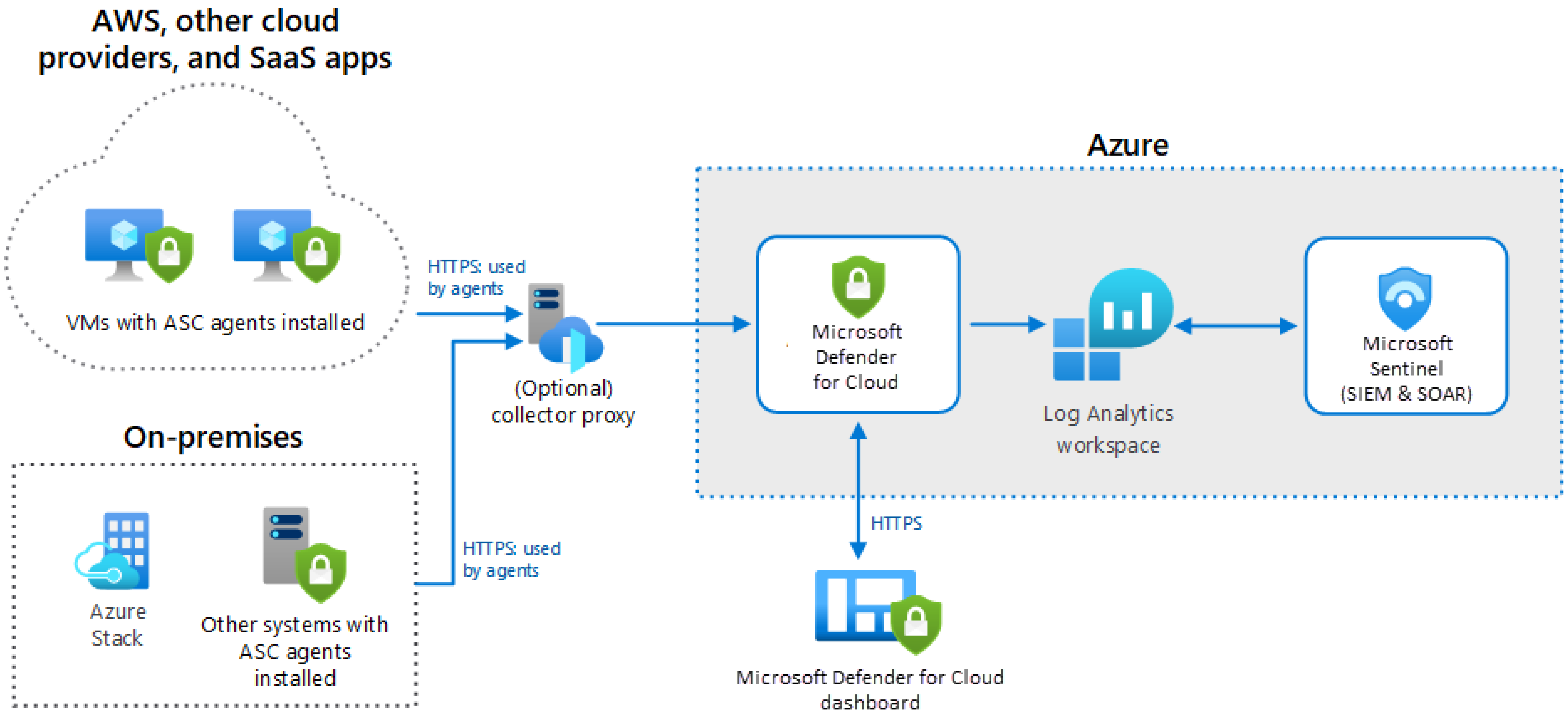
DevSecOps in Azure - Azure Solution Ideas | Microsoft Docs



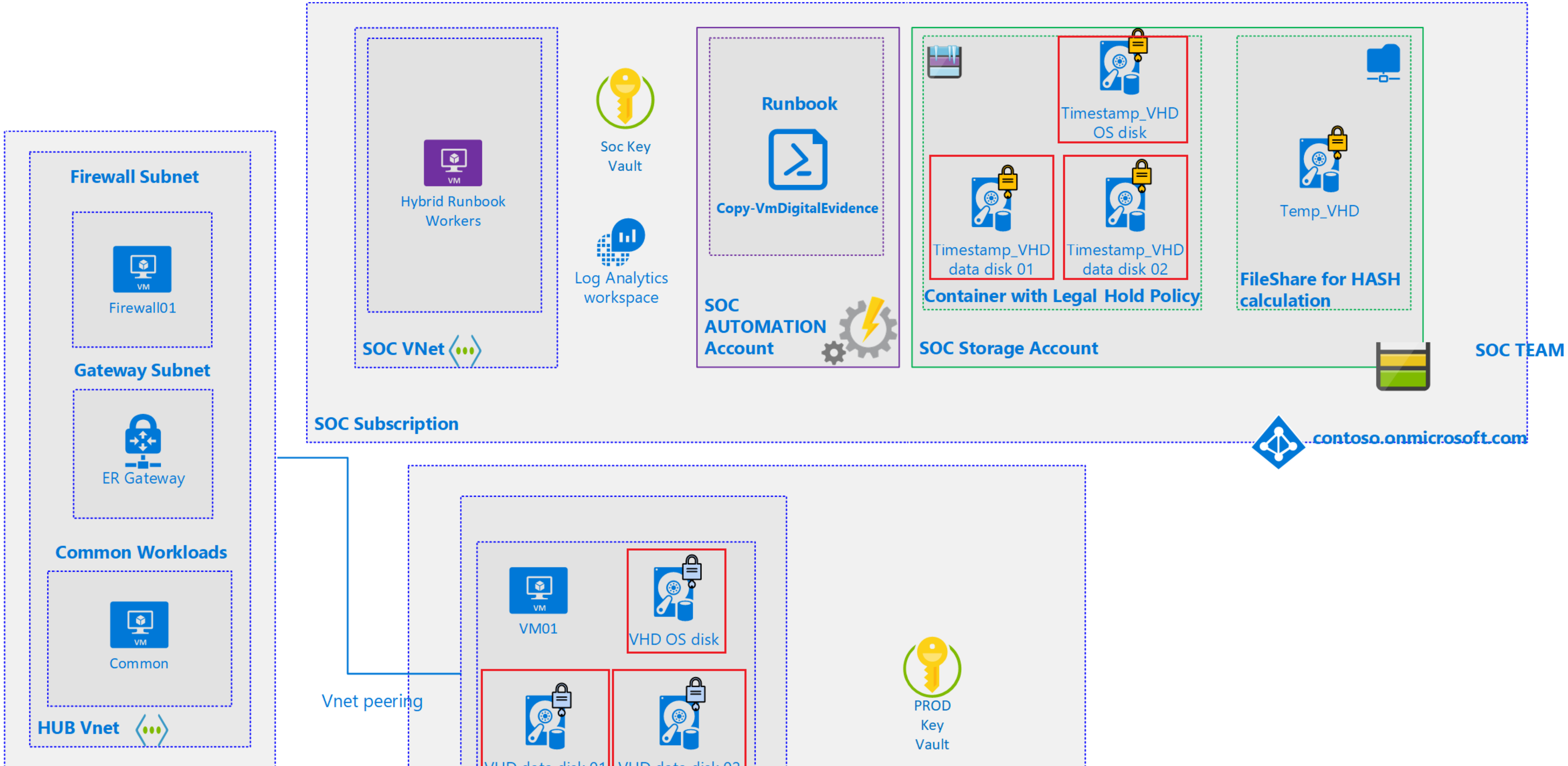
Enhanced-security hybrid messaging — client acce Docs



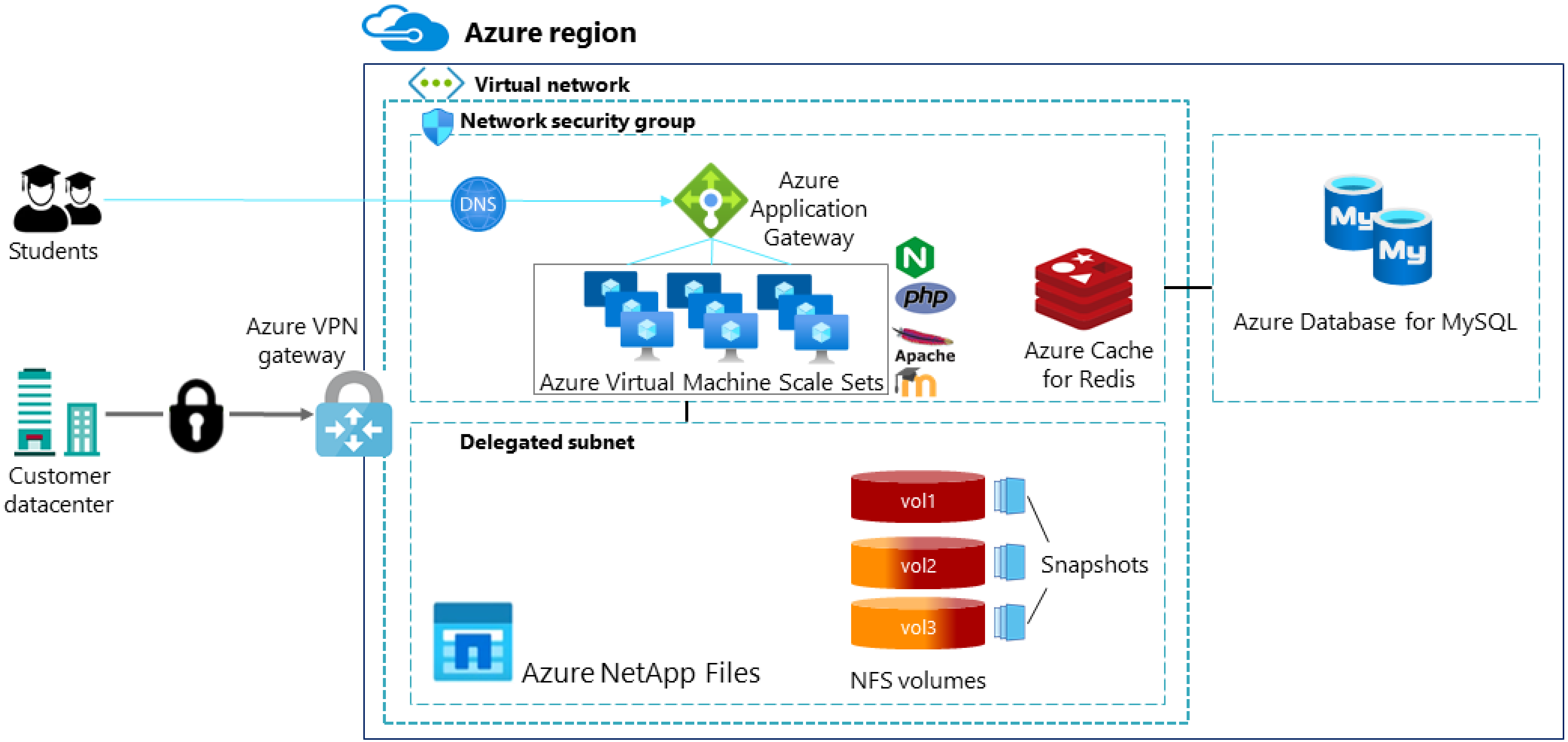
Hybrid security monitoring with Microsoft Sentinel - Azure Architecture Center | Microsoft Docs


AWS, other cloud providers, and SaaS apps
VMs with ASC agents installed
HTTPS: used by agents
(Optional) collector proxy
On-premises
Azure Stack
Other systems with ASC agents installed
HTTPS: used by agents
Azure
Microsoft Defender for Cloud
Log Analytics workspace
Microsoft Sentinel (SIEM & SOAR)
HTTPS
Microsoft Defender for Cloud dashboard

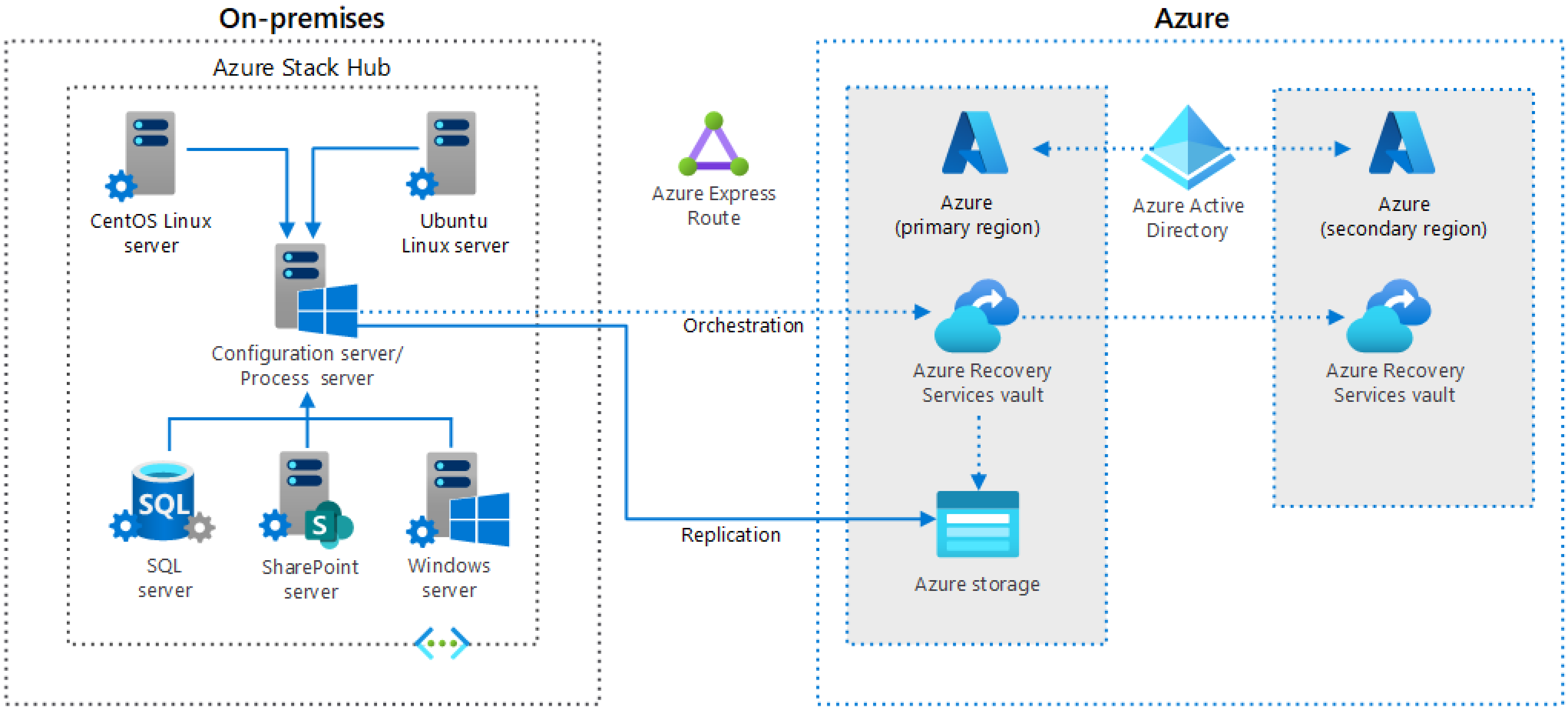
Computer forensics chain of custody in Azure - Azure Example Scenarios | Microsoft Docs



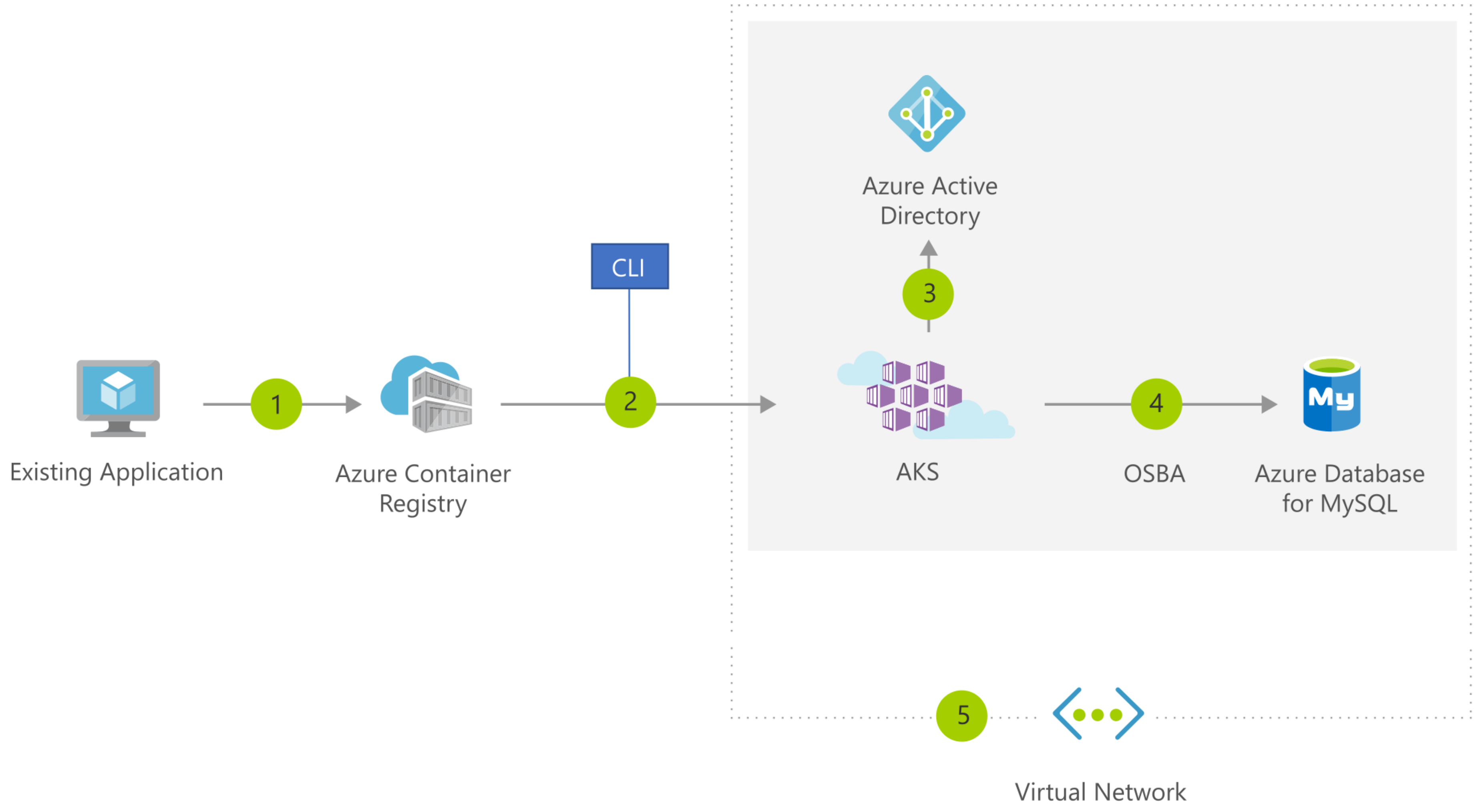
Moodle deployment with Azure NetApp Files - Azure Example Scenarios | Microsoft Docs



Disaster recovery for Azure Stack Hub VMs - Azure Architecture Center | Microsoft Docs



Lift and shift to containers with AKS - Azure Solution Ideas | Microsoft Docs



- Understanding Cybersecurity Risk Management – YouTube

Cyber security standards(HOMEWORK 1)

- Control frameworks

NIST 800-53

CIS Controls(CSC)

- program frameworks

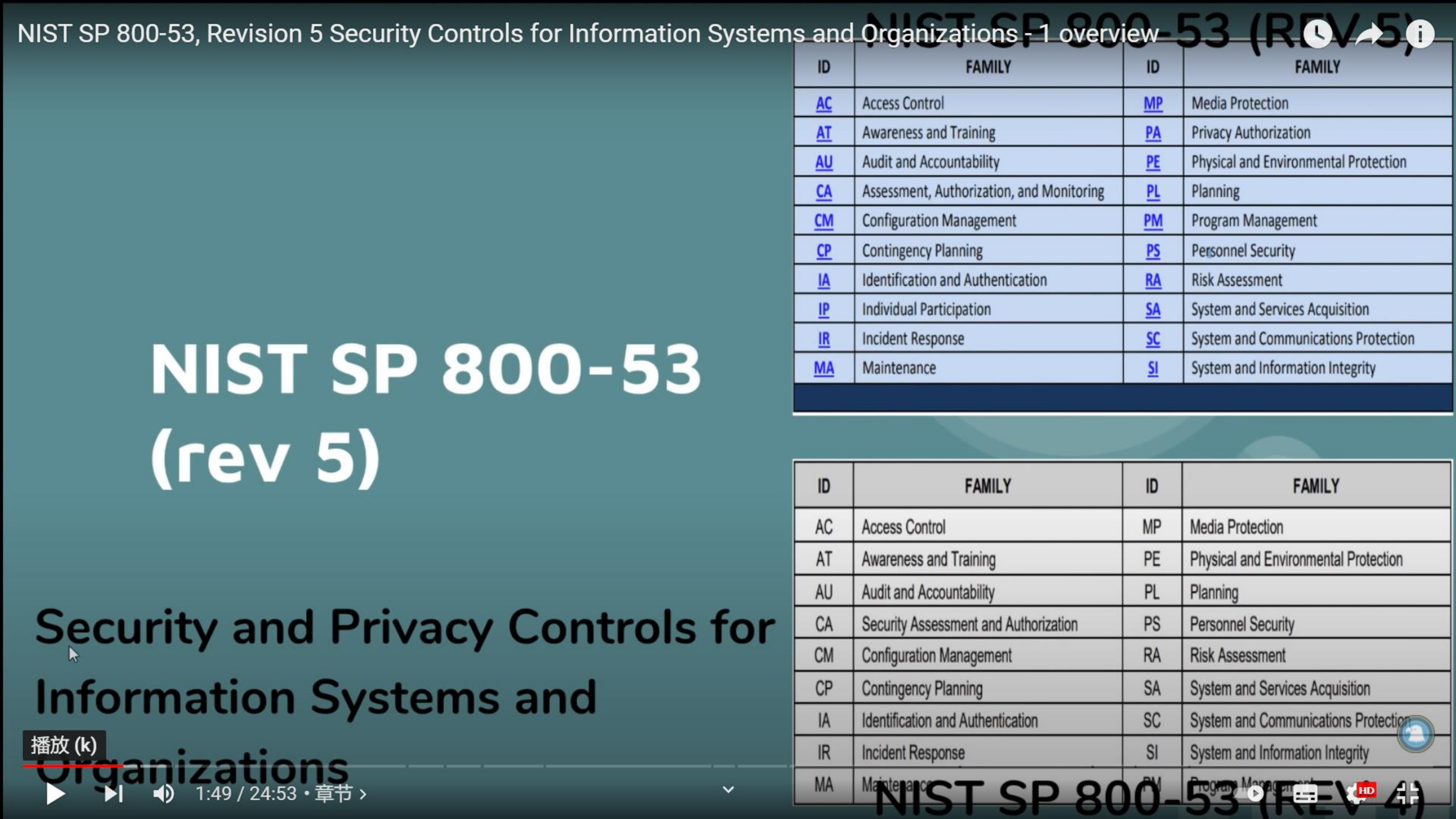
ISO 27000

NIST CSF

Risk frameworks NIST 800-39, 37, 30

- ISO 27005
- FAIR
- MITRE AttaCK

Home work complete 2 security frameworks (CSC and NIST 800-53, 27000)



NIST SP 800-53, Revision 5 Security Controls for Information Systems and Organizations - 1 overview
播放 (k)
1:49 / 24:53 • 章节 ›

NIST SP 800-53 (rev 5)

Security and Privacy Controls for Information Systems and Organizations

NIST SP 800-53 (REV 5)

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

NIST SP 800-53 (REV 4)

ASSET SECURITY (HOMEWORK 2)

- CISSP Asset Security Domain | CISSP Domain 2: Asset Security | CISSP Training | Simplilearn – YouTube

- COMPLETE THE KNOWLEDGE OF THIS CHAPTER ACCORING TO THE VIDEO