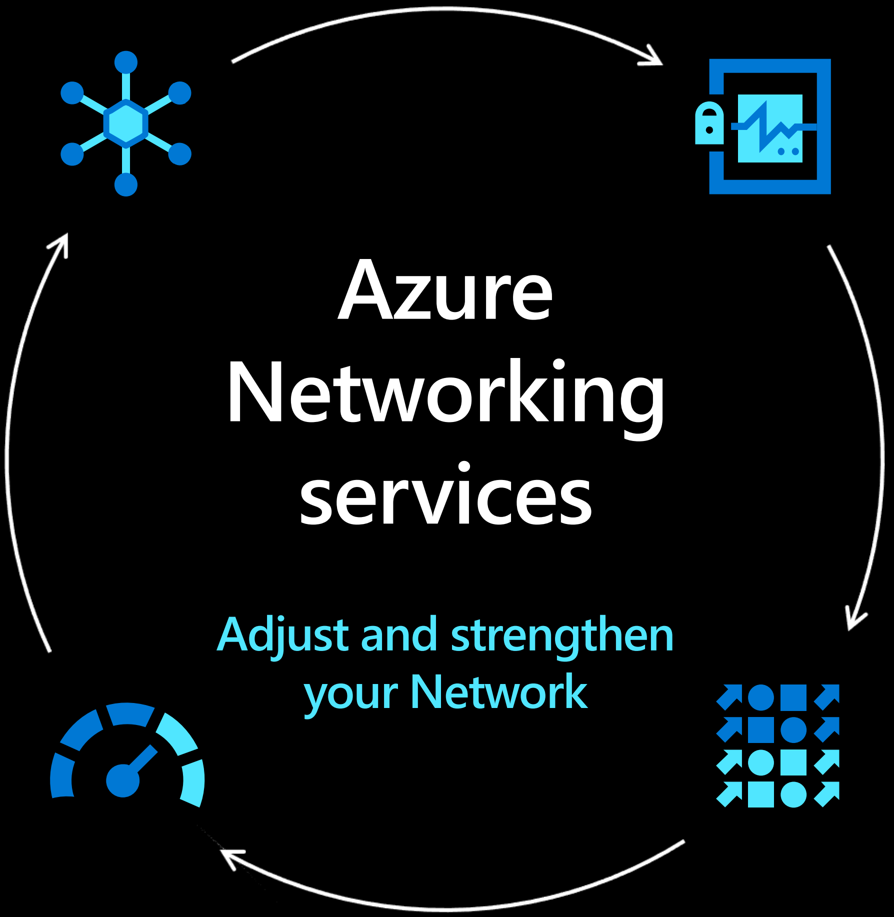
Microsoft Azure

WorkshopPLUS- Networking Essentials

Module # 3
Protect



Azure Networking services

Adjust and strengthen your Network

CONNECT & EXTEND

Virtual Networks

Routing/NSGs

ExpressRoute/VPN

Virtual WAN

PROTECT

Bastion

Azure Firewall

DDoS Protection

Web Application Firewall

PrivateLink/Private Endpoints

DELIVER

DNS, Azure Load Balancer

Traffic Manager

Application Gateway

CDN/Azure Front Door

MONITOR

Azure Monitor

Azure Network Watcher

Azure Bastion

Azure Bastion

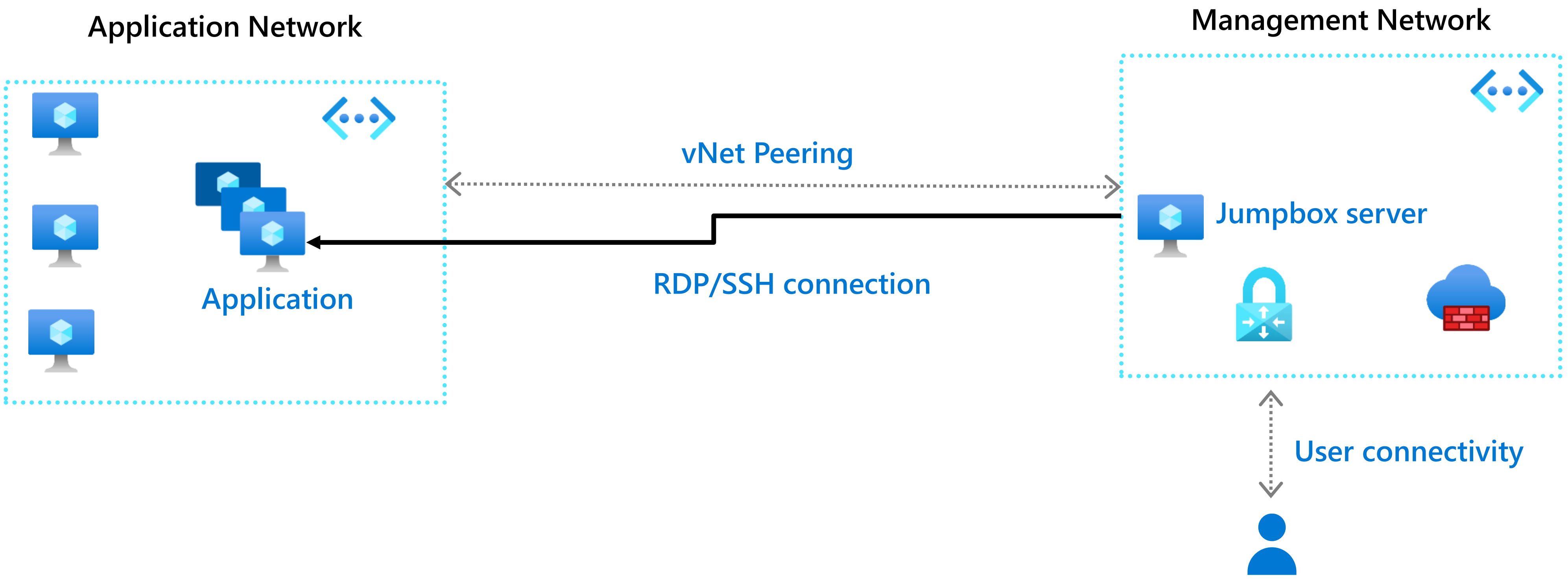
Connect to your remote workloads directly in a browser

Security handled by the Bastion service

Only need to expose port 443 on the public IP(s) of Bastion

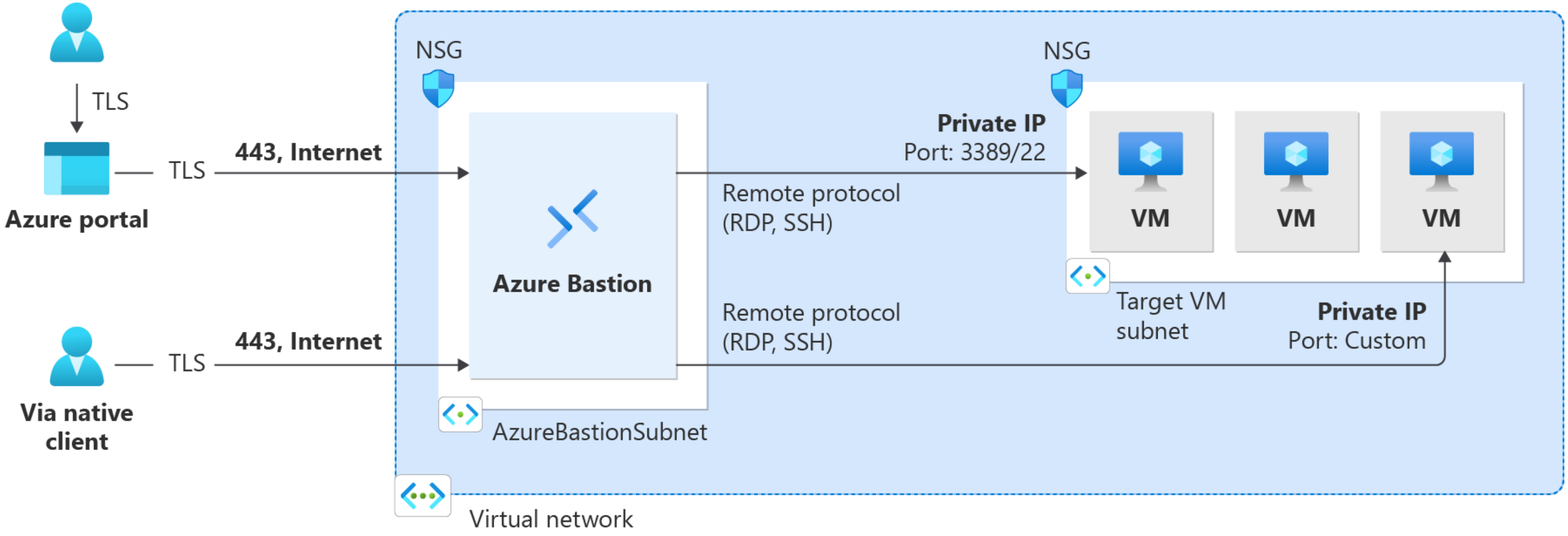
Traditional Jumpbox Solutions

Deploy remote connectivity solution to a semi-trusted management network

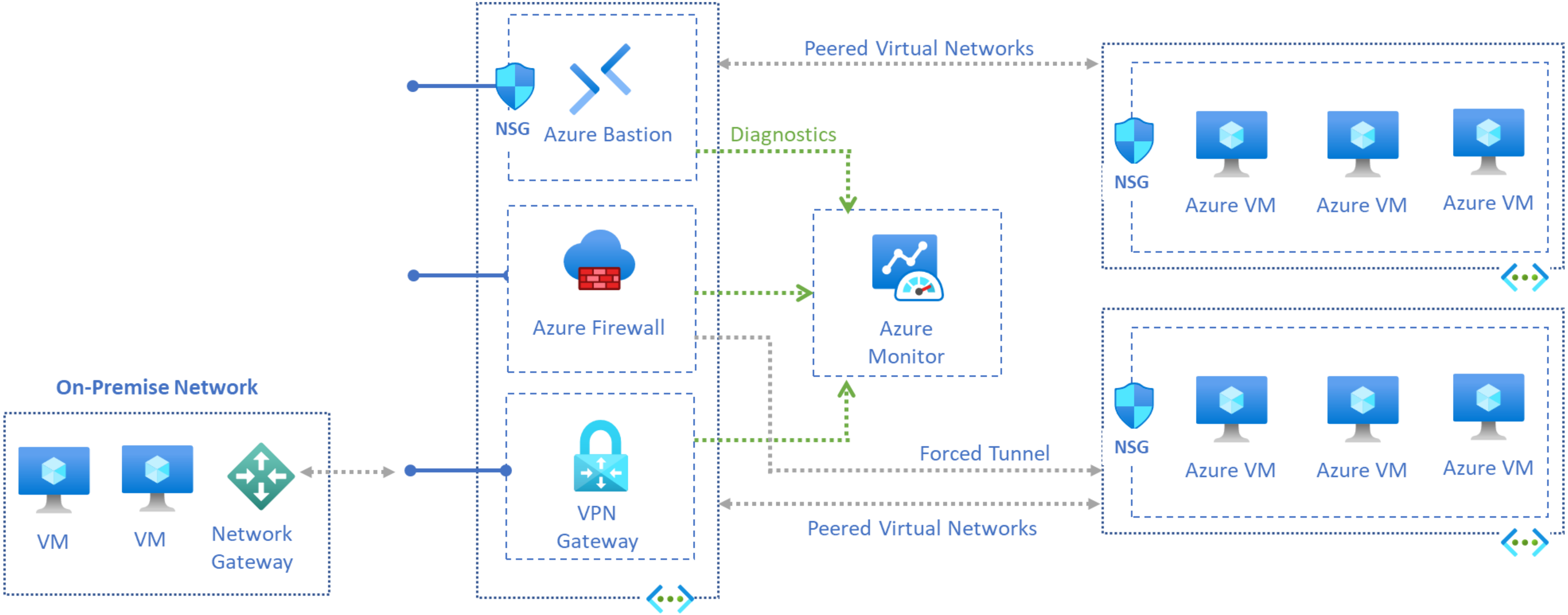


Azure Bastion

Fully managed jumpbox-as-a-service that provides secure RDP and SSH connectivity to Azure VMs



Hub and Spoke Connectivity

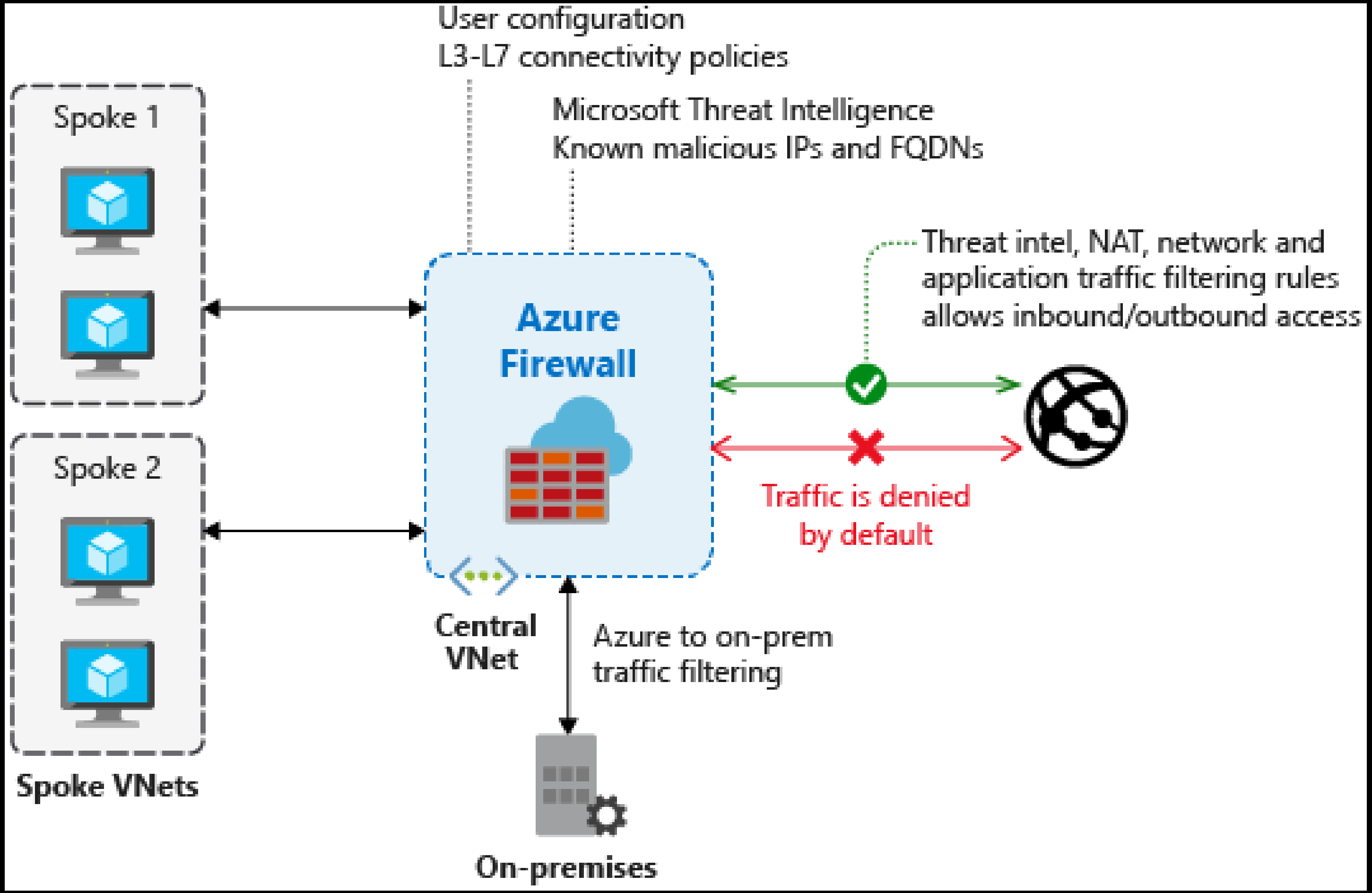


Azure Firewall

Connect and Secure critical Azure Services using Azure Firewall

What is the Azure Firewall?

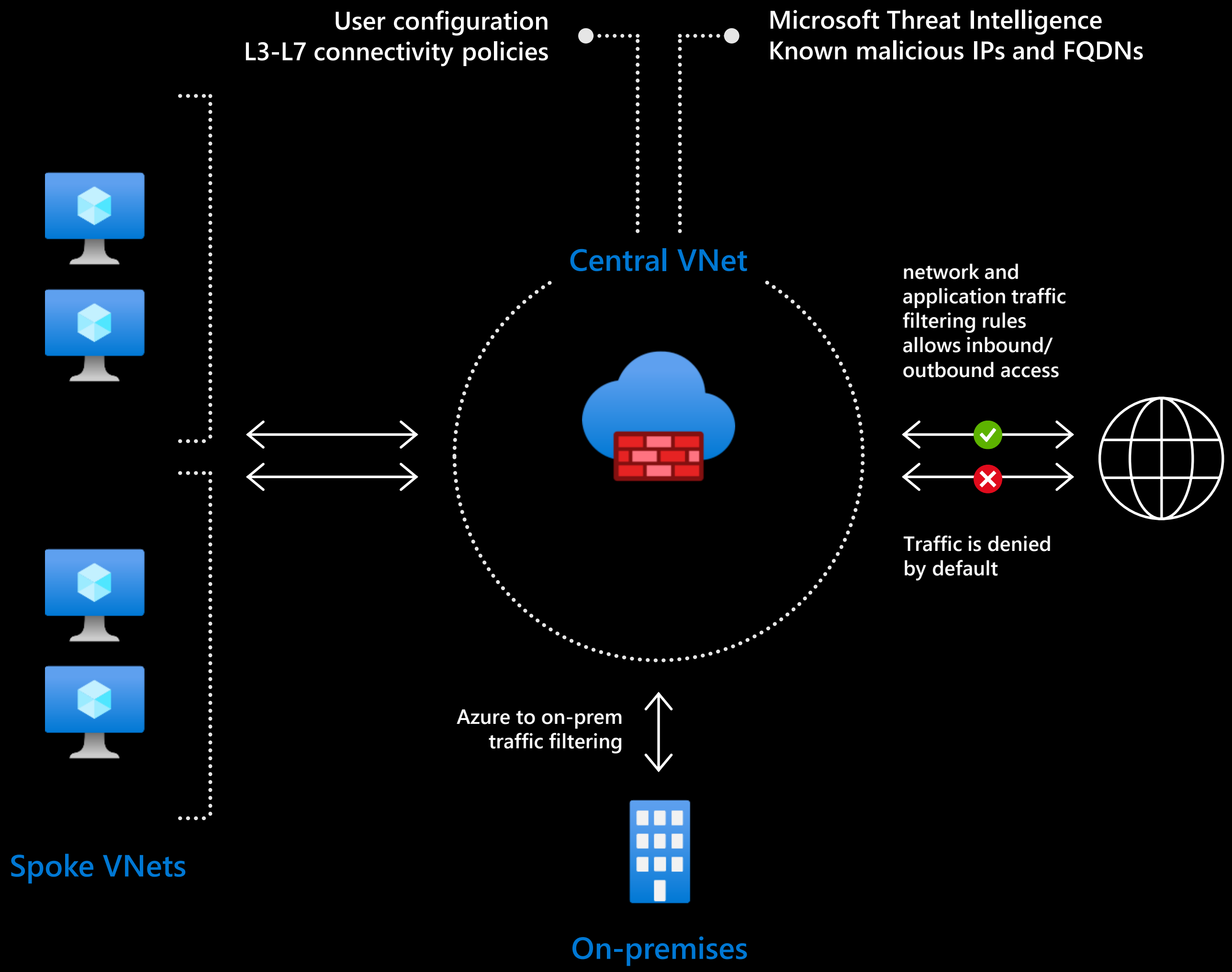
Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.


User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Spoke 1
Spoke 2
Spoke VNets
Azure Firewall
Threat intel, NAT, network and application traffic filtering rules allows inbound/outbound access
Traffic is denied by default
Central VNet
Azure to on-prem traffic filtering
On-premises

Azure Firewall

Cloud native stateful Firewall as a service

- A first among public cloud providers
- **Central governance of all traffic flows**
- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions
- **Complete VNET protection**
- Filter Outbound, Inbound, Spoke-Spoke and Hybrid Connections traffic (VPN and ExpressRoute)
- **Centralized logging**
- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice
- **Best for Azure**
- DevOps integration, integration with Sentinel and ASC, FQDN Tags, Service Tags, Integration with ASE, Backup and other Azure services

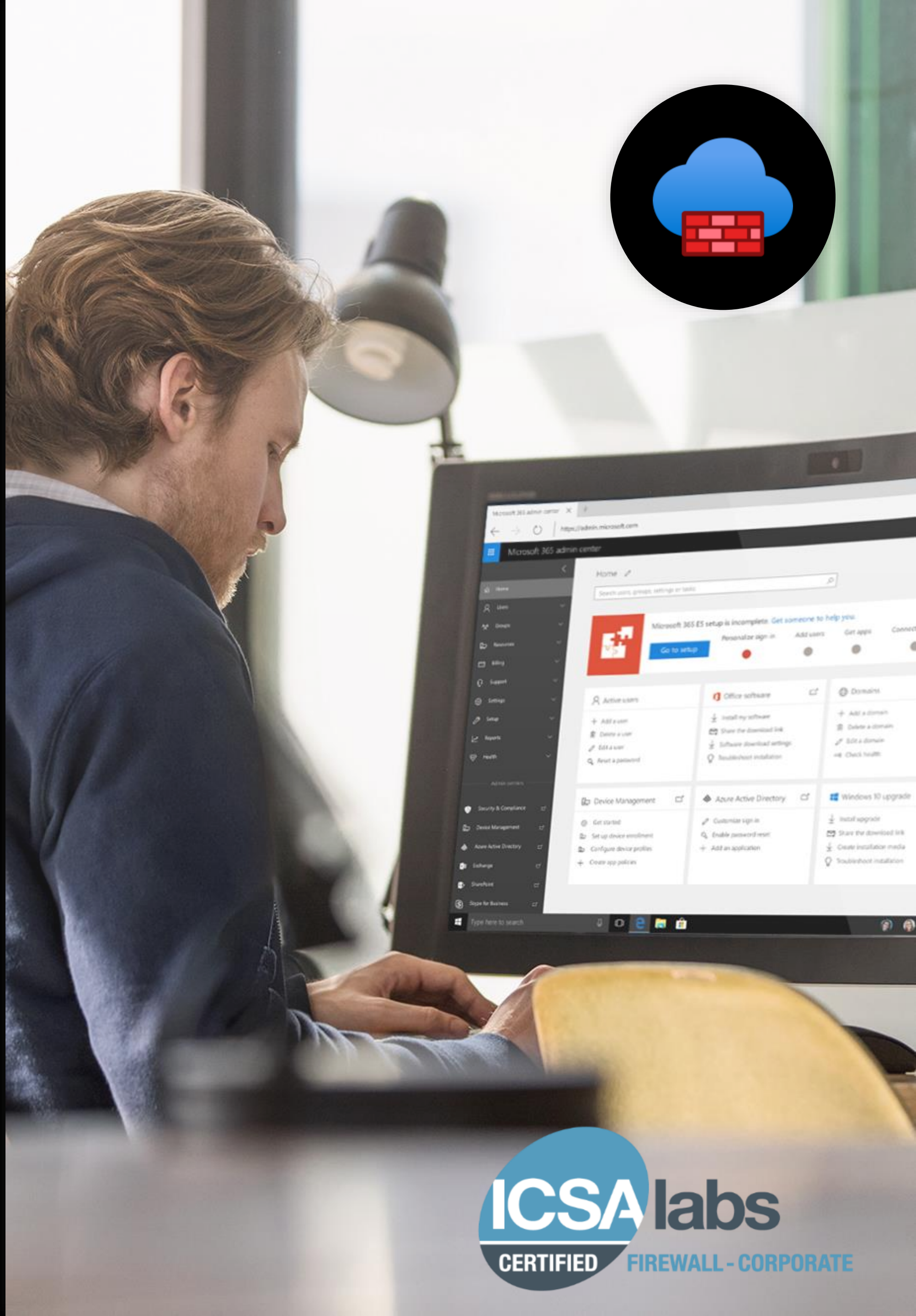

User configuration
L3-L7 connectivity policies
Microsoft Threat Intelligence
Known malicious IPs and FQDNs
Central VNet
network and application traffic filtering rules allows inbound/ outbound access
Traffic is denied by default
Azure to on-prem traffic filtering
Spoke VNets
On-premises

Standard Features

- Built-in high availability
- Availability Zones
- Unrestricted cloud scalability
- Application FQDN filtering rules
- Network traffic filtering rules
- FQDN tags
- Service tags
- Threat intelligence
- DNS proxy
- Custom DNS
- FQDN in network rules
- Deployment without public IP address in Forced Tunnel Mode
- Outbound SNAT support
- Inbound DNAT support
- Multiple public IP addresses
- Azure Monitor logging
- Forced tunneling
- Web categories

Premium Features

- TLS Inspection
- URL filtering
- IDPS (*Intrusion Detection and Prevention*)
- Web Categories (extended capabilities)



Fixed Cost

$1.25/standard firewall/hour

$1.75/premium firewall/hour

Variable Cost

$0.016/GB processed by the firewall

Most customers save 30%–50% in comparison to NVAs

When comparing with NVAs, consider the full TCO including
licensing, multiple VMs and 2 standard load balancers (traffic + rules charge)

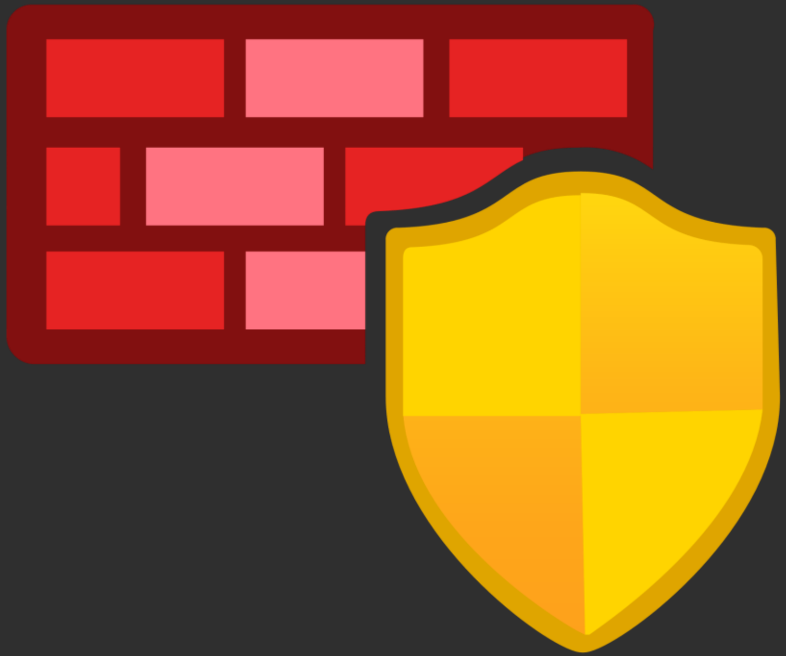
Throughput limit 30 Gbps

Assume at least one firewall per region

Azure Firewall versus Network Virtual Appliances – Cost comparison

Cost	Azure Firewall	NVAs
Compute	**$1.25** /standard firewall/hour **$1.75** /premium firewall/hour **$0.016** /GB processed (30%-50% cost saving)	Two plus VMs to meet peak requirements
Licensing		Per NVA vendor billing model
Standard Public Load Balancer		First five rules: $0.025/hour Additional rules: $0.01/rule/hour $0.005 per GB processed
Standard Internal Load Balancer		First five rules: $0.025/hour Additional rules: $0.01/rule/hour $0.005 per GB processed
Ongoing/Maintenance	Included	Customer responsibility
Support	Included in your Azure Support plan	Per NVA vendor billing model

Azure Firewall Manager



Azure Firewall Manager Overview

- Centralized Firewall Management & Administration
  - Create policy and apply across multiple firewalls
  - Supports DevOps model - Hierarchical policy & governance
  - Works across regions/subscription/deployments
- Support Two Deployment Architectures
  - Hub Virtual Network - a standard Azure virtual network with security (and routing in future) policies
  - Secured Virtual Hub - an Azure Virtual WAN Hub with security and routing policies
- Roadmap
  - Extend support to additional cloud native network security services

Azure Firewall Manager

Key features

Hub Virtual Networks

Brings centralized firewall management goodness to VNETs

Secure existing hub-and-spoke VNET deployments seamlessly

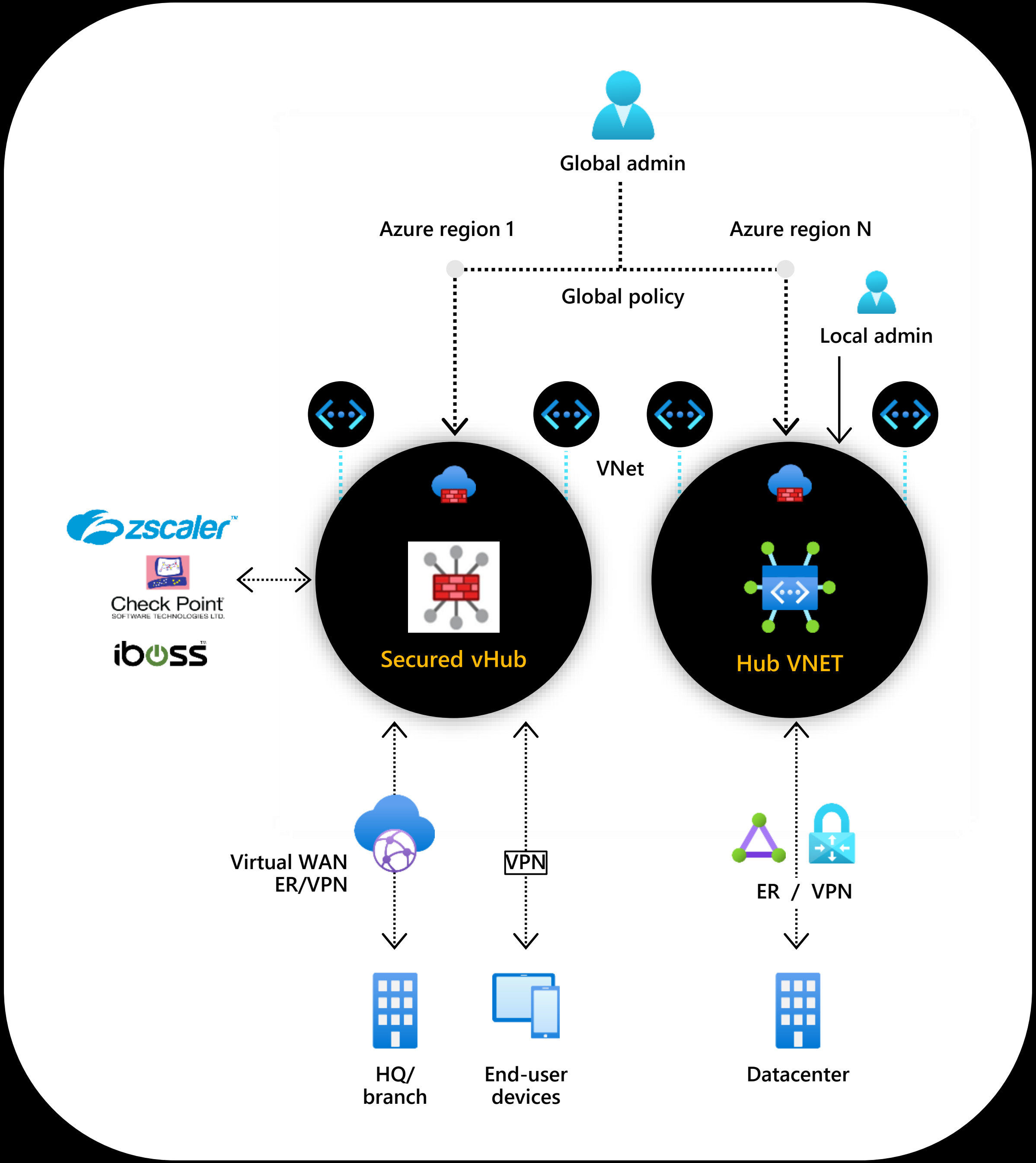
Update configuration across multiple firewall instances

Secure Virtual Hub

Centralized security for virtual WAN hubs

Automated routing - secures V2I, B2I, V2V, B2V with just few clicks

Advanced security with 3rd party SECSaaS partners



Central security and policy management

Deploy and configure multiple Azure Firewall instances

- Span different Azure regions and subscriptions from a single pane of glass

Enforce consistent configuration across Azure Firewall

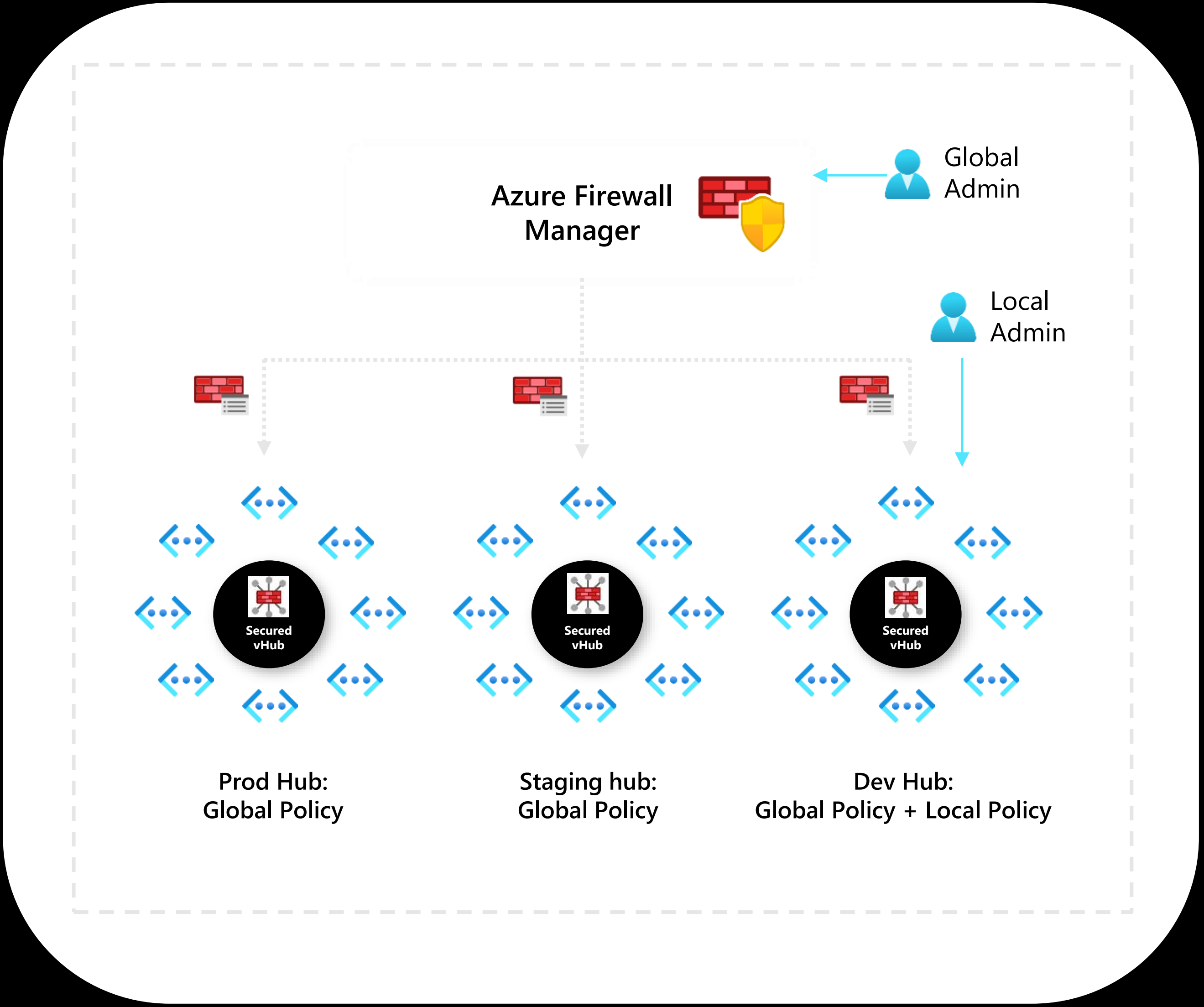
- Manage Network address translation (NAT), network, and application rule collections, as well as threat intelligence and DNS settings.

DevOps optimized hierarchical Azure Firewall policies

- Global firewall policies authored by Central IT with local derived firewall policies for DevOps self-service for better agility

Manage Azure Firewall Policy independent of Azure Firewall

- Azure Firewall Policy is a top-level resource with independent access control and activity tracking.



Azure Firewall synergies and recommendations

Application Gateway WAF

- Provides inbound protection for web applications (L7)
- Azure Firewall provides network level protection(L3) for all ports and protocols and application level protection (L7) for outbound HTTP/S. Azure Firewall should be deployed alongside Azure WAF
- Azure Firewall can be combined with 3rd party WAF/DDoS solutions

Network Security Groups (NSG)

- NSG and Azure Firewall are complementary, with both you have defense and in-depth
- NSGs provides host based, distributed network layer traffic filtering to limit traffic to resources within virtual networks
- Azure Firewall is a fully stateful centralized network firewall as-a-service, providing network and application level protection across virtual networks and subscriptions

Service endpoints

- Recommended for secure access to Azure PaaS services
- Can be leveraged with Azure Firewall for central logging for all traffic by enabling service endpoints in the Azure Firewall subnet and disabling it on the connected spoke VNETs

Web Application Firewall

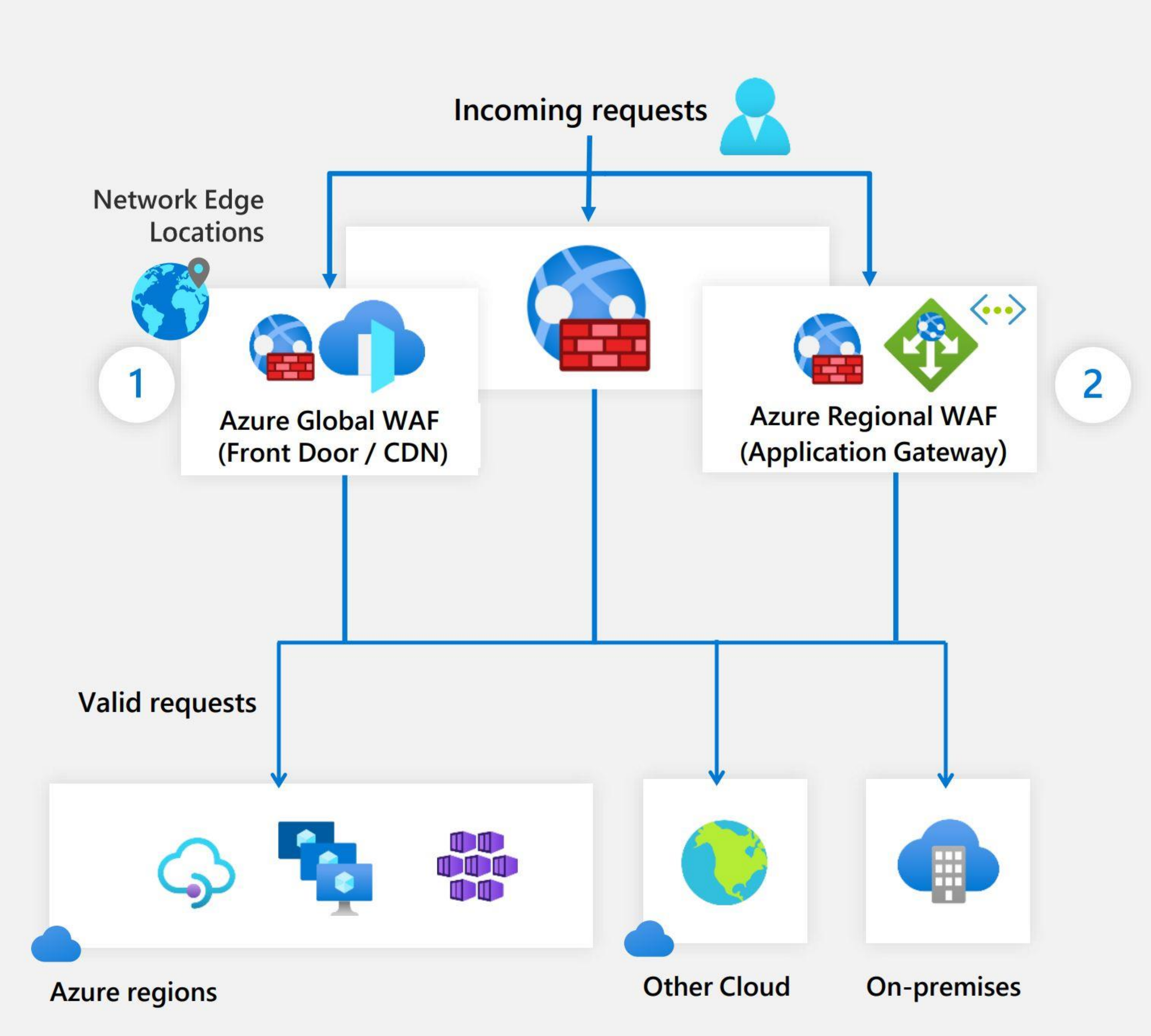
A cloud-native web application firewall (WAF) service that provides powerful protection for web apps

Web Application Firewall (WAF)

Securing PaaS Services

Key Benefits

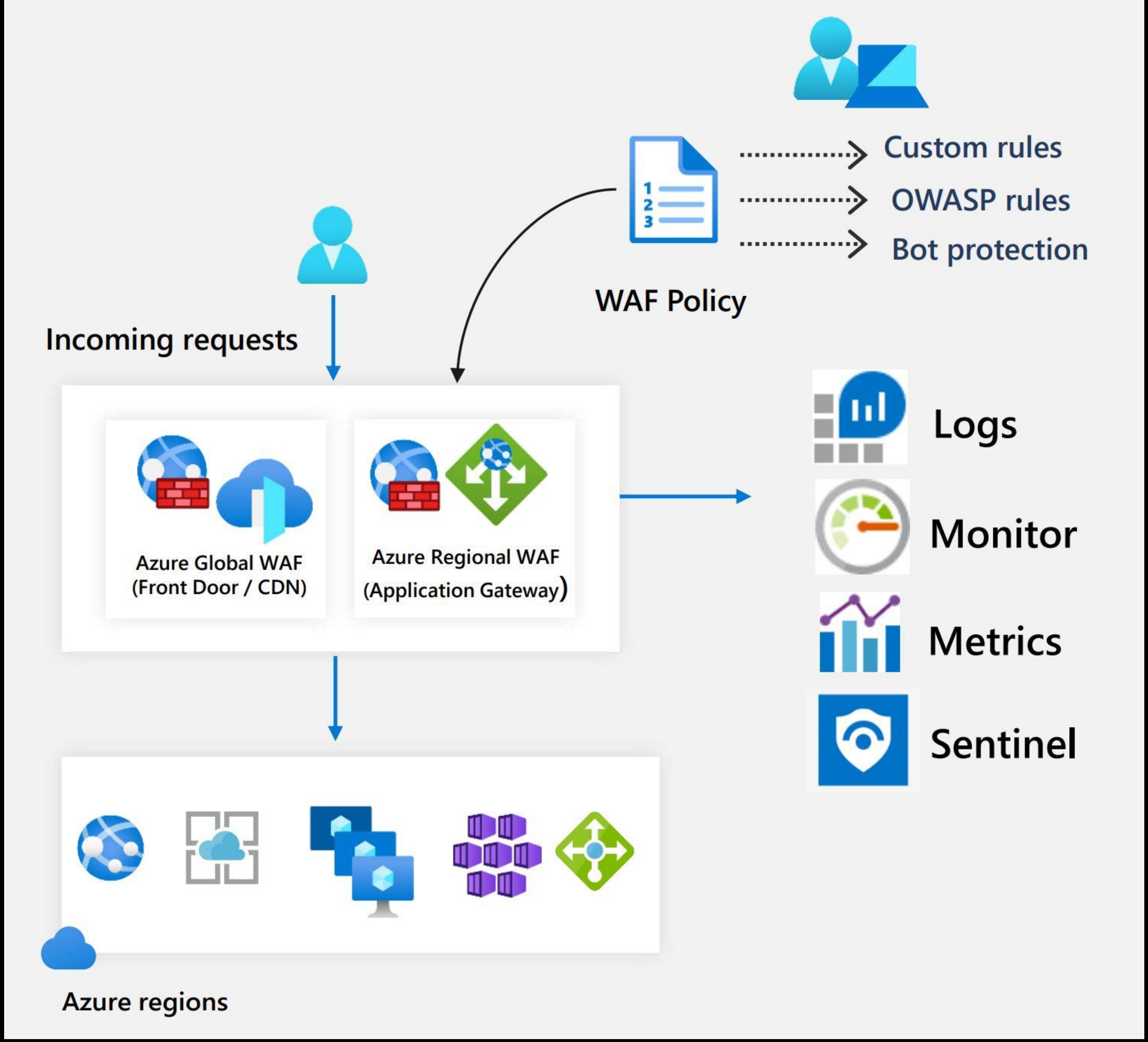
- Strong Layer 7 defenses
- Provides centralized protection of web applications from common attacks, such as SQL injection and cross-site scripting.
- Helps make security management much simpler and gives application administrators better assurance of protection against threats and intrusions.
- 1) **Integrated with Azure Front Door, and Azure Content Delivery Network (CDN)** at network edge, combine application acceleration, caching, and protection
- 2) **Integrated with Application Gateway**, dedicated protection for both public and private web sites



Web Application Firewall (WAF)

Key Features

- ✓ Preconfigured OWASP top 10
- ✓ Bot protection integration with Microsoft Threat Intelligence
- ✓ Conditional rate limiting at Azure network edge
- ✓ Logs and Metrics for detection and alerts
  - Respond and remediate with Sentinel (SOAR) integration
- ✓ Powerful custom rules engine
  - Geo-filtering
  - IP Restriction
  - HTTP Parameter Filtering
  - Size Restriction
  - Preconfigured OWASP top 10



Microsoft

Azure WAF with Application Gateway

Protection from common application vulnerabilities

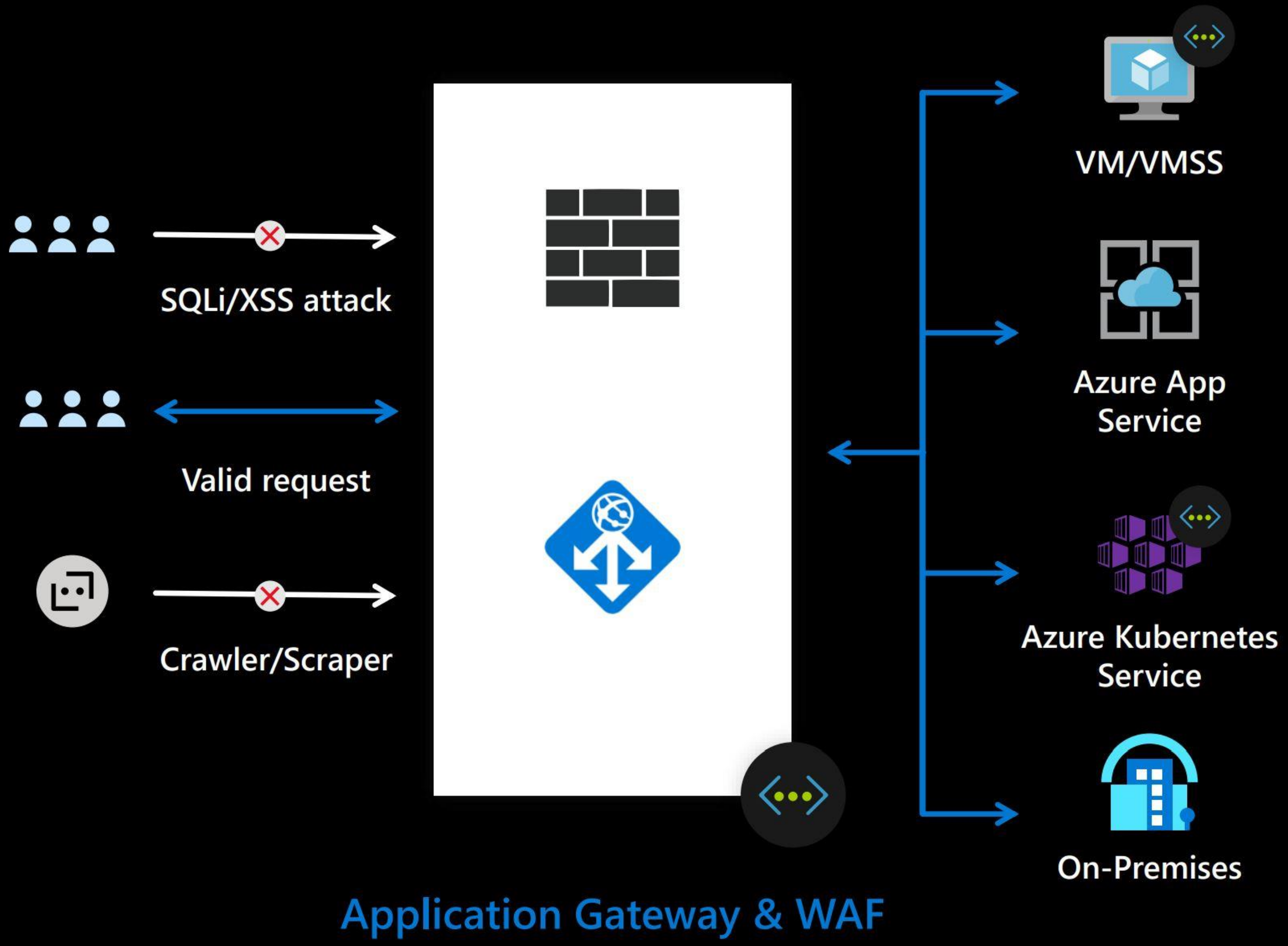
- OWASP top 10 out of box protection

  CRS 2.2.9, CRS 3.0, CRS 3.1, CRS 3.2 (public preview)

  Custom Rules supported

  BOT protection

- Rule configurability, exclusion lists, different rules sets, anomaly scoring
- Support public IP, private IPs, cross region, or on-premises backend pools
- Native in region and intra-VNet/hybrid integration
- Near real time monitoring/alerting with Azure Monitor, Azure Security Center integration, Azure Sentinel integration
- Highly available, autoscaling, fully platform managed

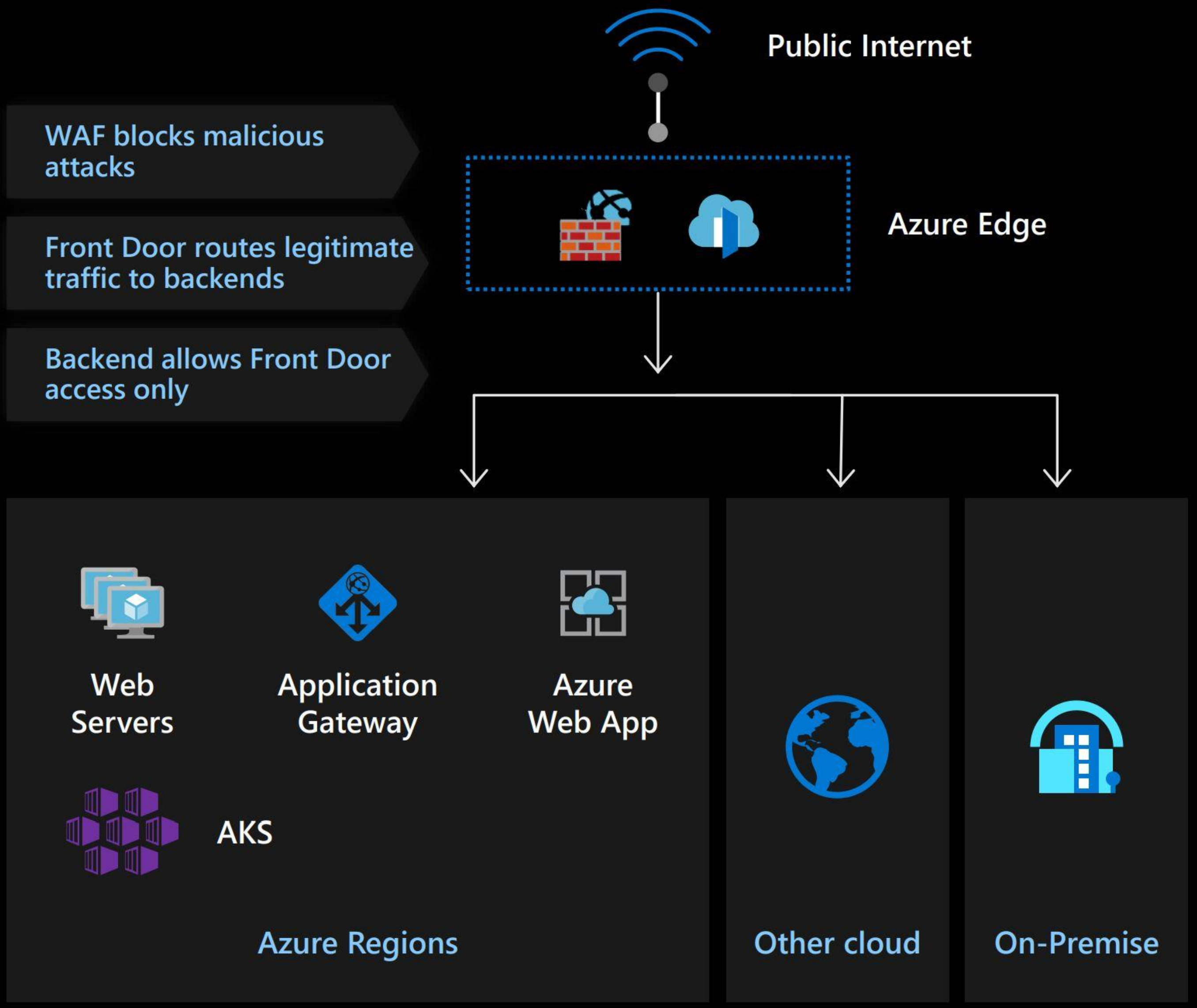


Microsoft

Azure WAF with Front Door

Web Application protection at network edge

- Easy setup with managed ruleset (OWASP TOP 10) and custom rules
- Bot protection using threat intelligence-based filtering
- Global insights
- Cost efficient: Pay as you go
- Scalable, highly available, low latency

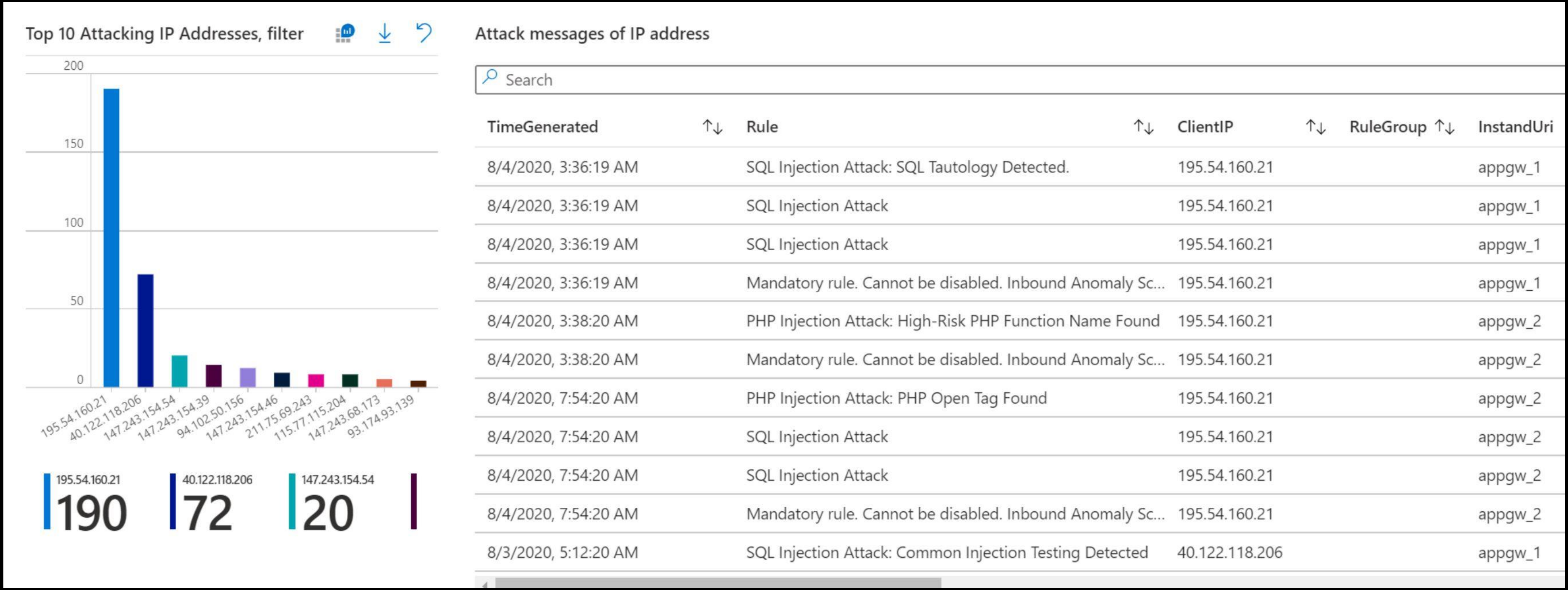

Public Internet
WAF blocks malicious attacks
Front Door routes legitimate traffic to backends
Backend allows Front Door access only
Azure Edge
Web Servers
Application Gateway
Azure Web App
AKS
Azure Regions
Other cloud
On-Premise

Metrics and Insights

Integration with Azure Monitor

Log analytics for access and WAF logs

Sentinel connector and workbook



Attack messages of IP address

TimeGenerated ↑↓	Rule ↑↓	ClientIP ↑↓	RuleGroup ↑↓	InstandUri
8/4/2020, 3:36:19 AM	SQL Injection Attack: SQL Tautology Detected.	195.54.160.21		appgw_1
8/4/2020, 3:36:19 AM	SQL Injection Attack	195.54.160.21		appgw_1
8/4/2020, 3:36:19 AM	SQL Injection Attack	195.54.160.21		appgw_1
8/4/2020, 3:36:19 AM	Mandatory rule. Cannot be disabled. Inbound Anomaly Sc...	195.54.160.21		appgw_1
8/4/2020, 3:38:20 AM	PHP Injection Attack: High-Risk PHP Function Name Found	195.54.160.21		appgw_2
8/4/2020, 3:38:20 AM	Mandatory rule. Cannot be disabled. Inbound Anomaly Sc...	195.54.160.21		appgw_2
8/4/2020, 7:54:20 AM	PHP Injection Attack: PHP Open Tag Found	195.54.160.21		appgw_2
8/4/2020, 7:54:20 AM	SQL Injection Attack	195.54.160.21		appgw_2
8/4/2020, 7:54:20 AM	SQL Injection Attack	195.54.160.21		appgw_2
8/4/2020, 7:54:20 AM	Mandatory rule. Cannot be disabled. Inbound Anomaly Sc...	195.54.160.21		appgw_2
8/3/2020, 5:12:20 AM	SQL Injection Attack: Common Injection Testing Detected	40.122.118.206		appgw_1

Azure DDoS Protection

What are DDoS attacks?

Distributed denial of service attacks

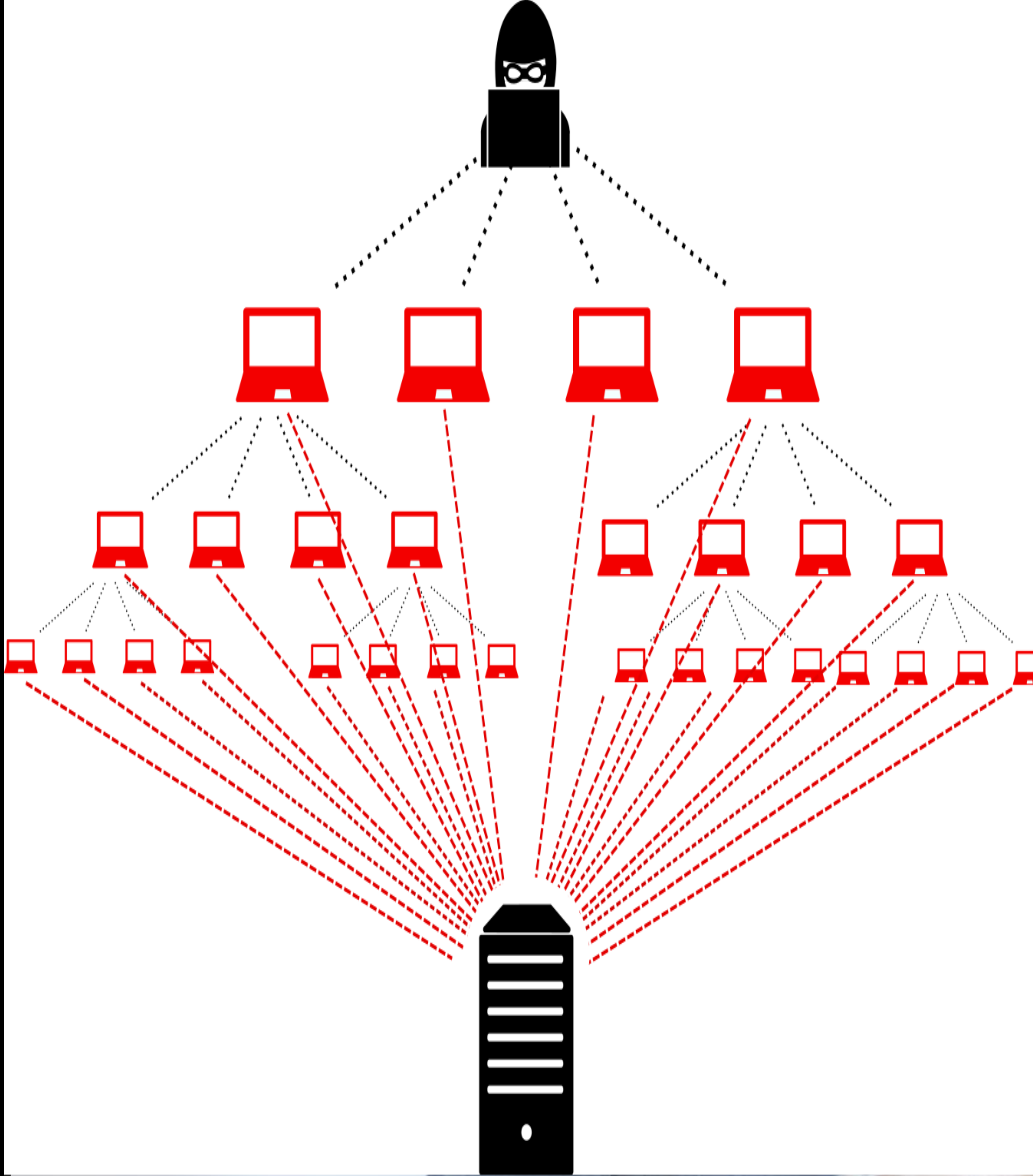
Bad actors generate malicious traffic to take down the network or application (public) by either impacting the availability or the performance of the network or application.

Why should I care?

Any public IP receiving traffic from the internet is susceptible to DDoS attacks.

Top cause of availability issue for large enterprises.

ACR opportunity , $3k/month



Azure DDoS protection standard

Cloud scale DDoS protection for Virtual Networks in Azure

01 Azure global network

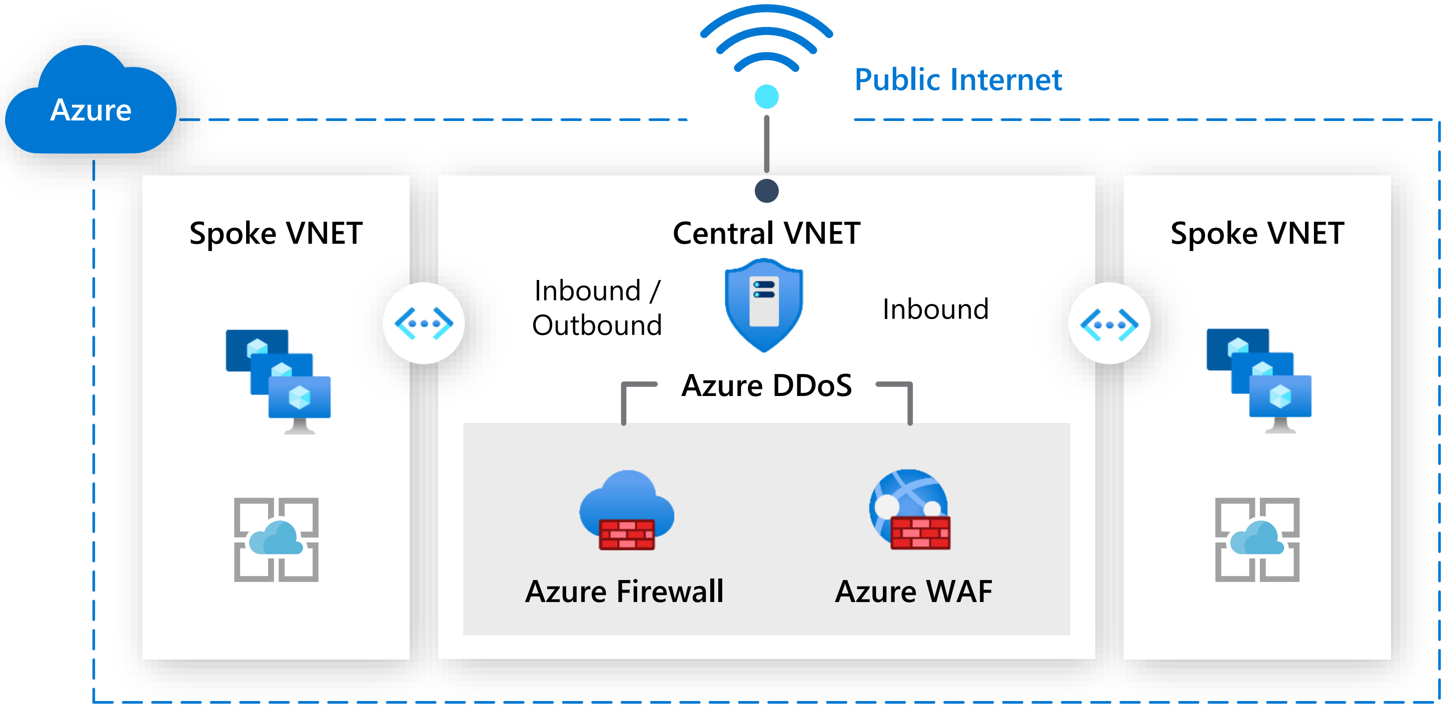
02 Adaptive tuning

03 Attack analytics & metrics

04 Integration with Azure Security Center and Sentinel

05 DDoS Rapid Response (DRR)

06 SLA guarantee and cost protection



Azure Service Endpoints

Service Endpoints

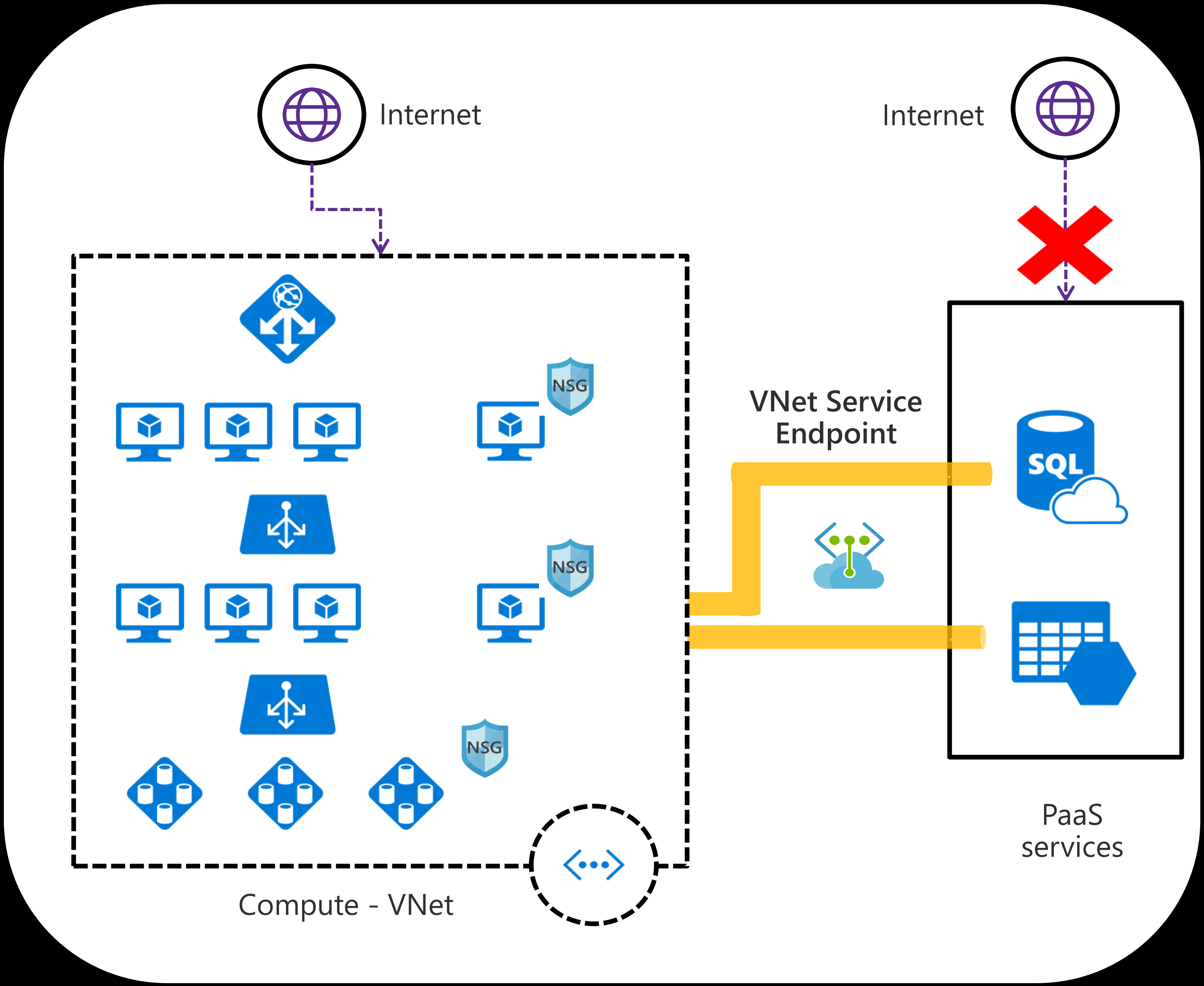
Securing PaaS Services

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
- Azure App Service

Public Preview:

- Azure Container Registry

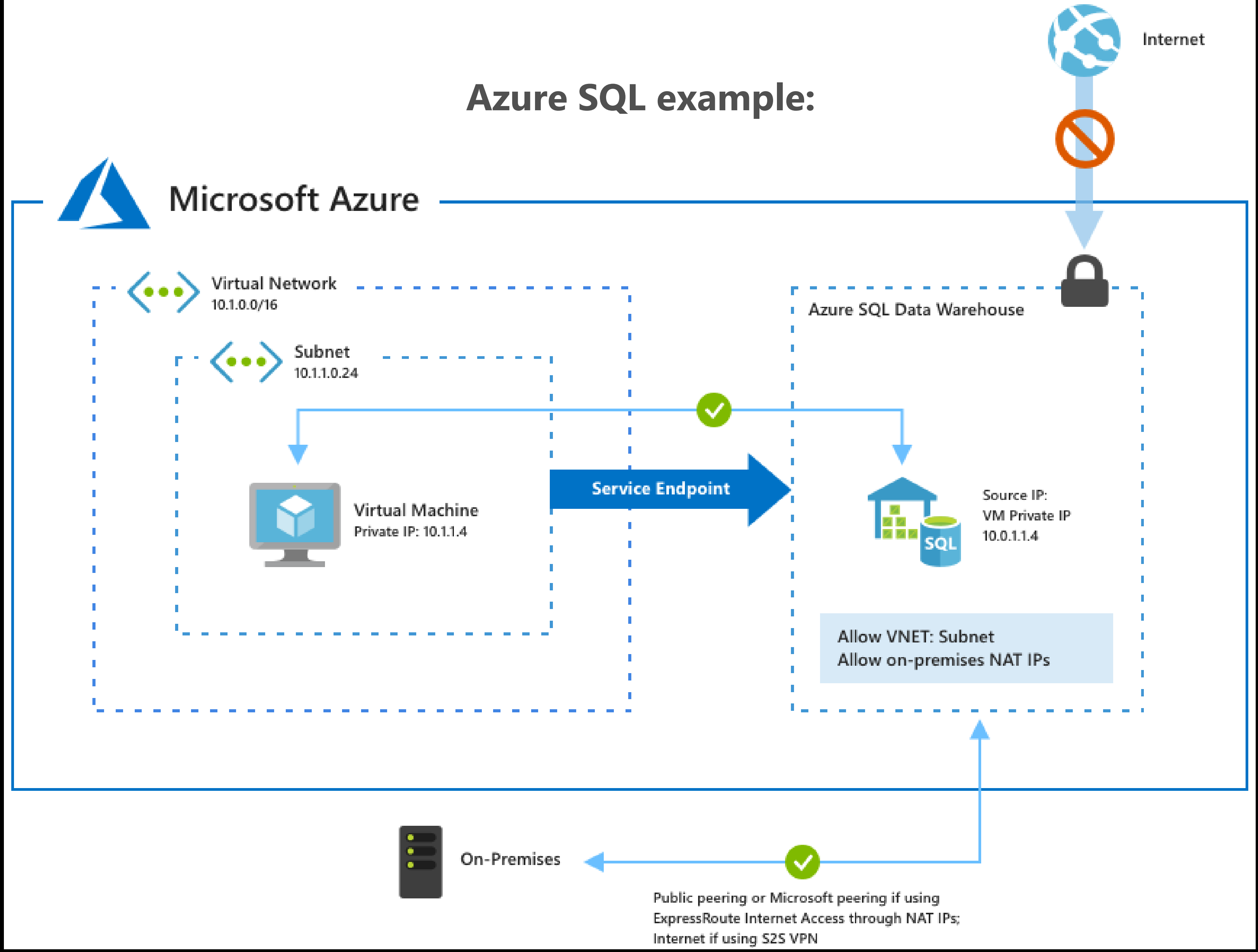


Service Endpoint

Securing PaaS Services

Key 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



Private Link and Private Endpoints

Private Link

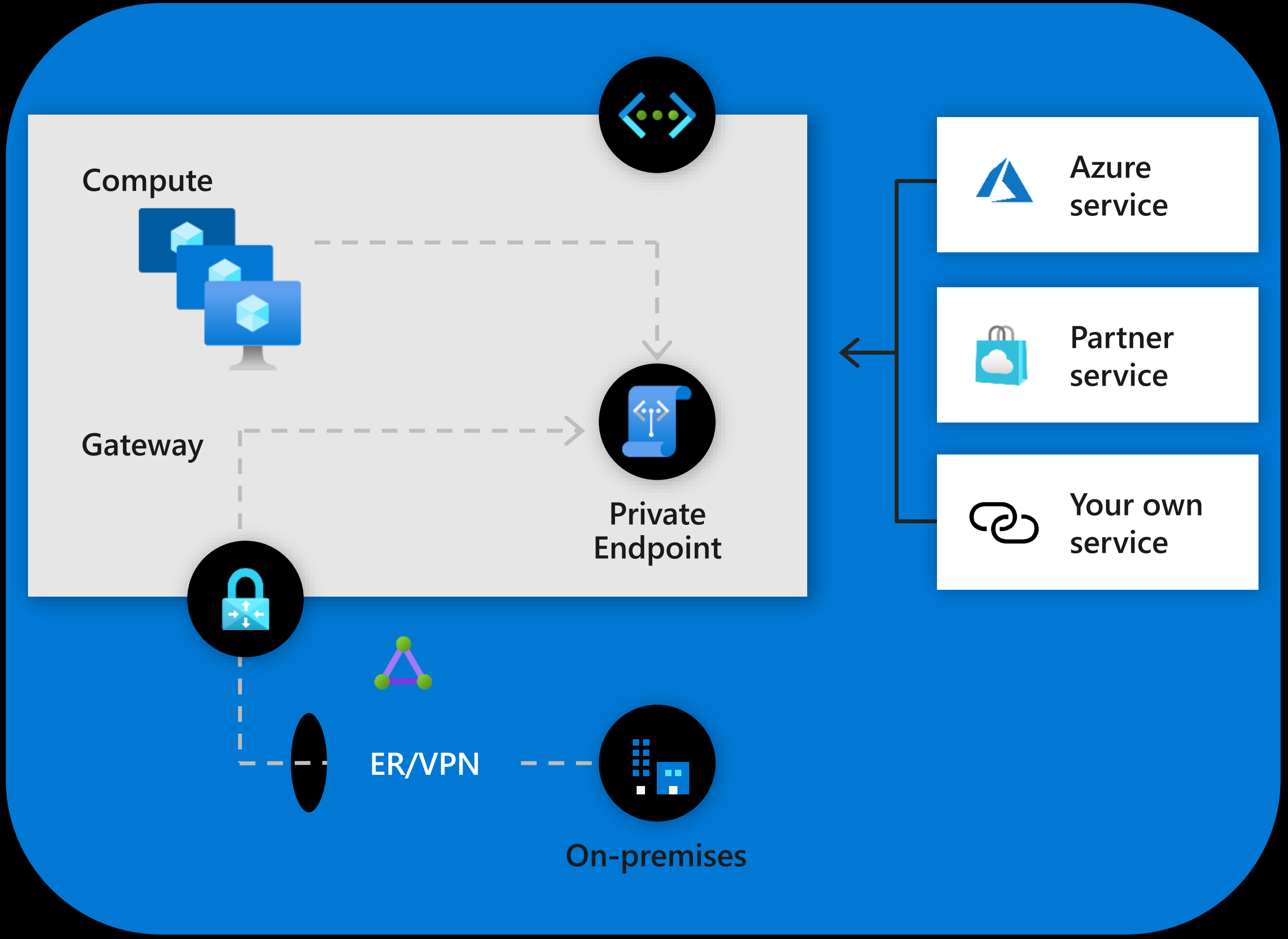
Highly secure and private connectivity solution for Azure Platform

Consistent experience across Azure services, partner services and your own services

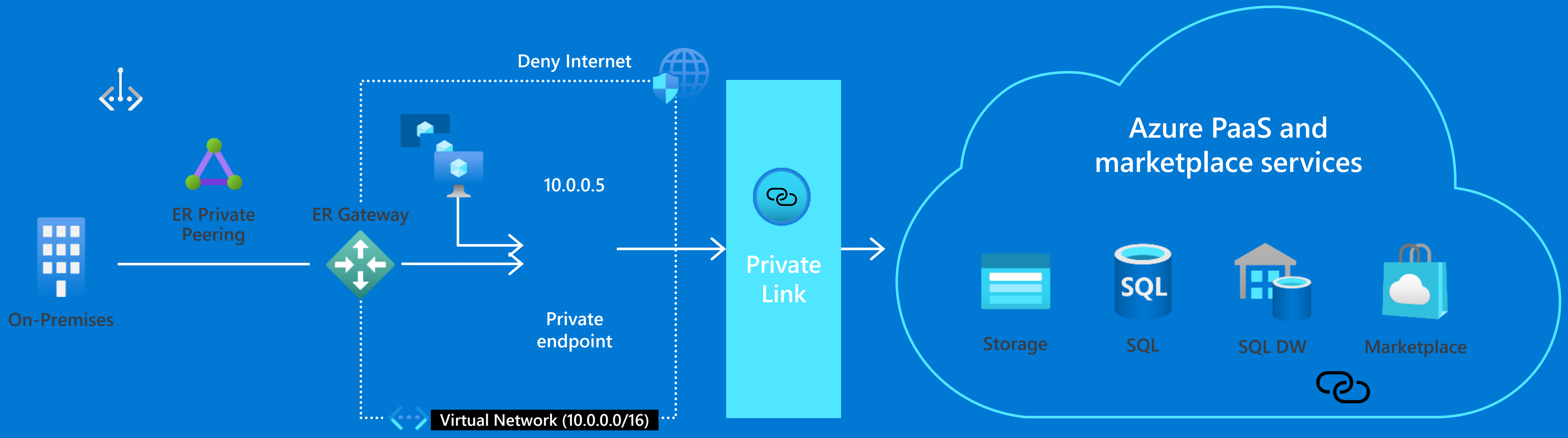
Simplified networking

- No Internet gateway, NAT devices, public IP, ER or VPN
- Predictable IP addresses for PaaS resources
- Access from peered and on-prem networks privately

Simplified security



Azure Private Link



Private Link for Azure Storage, SQL DB and customer own service

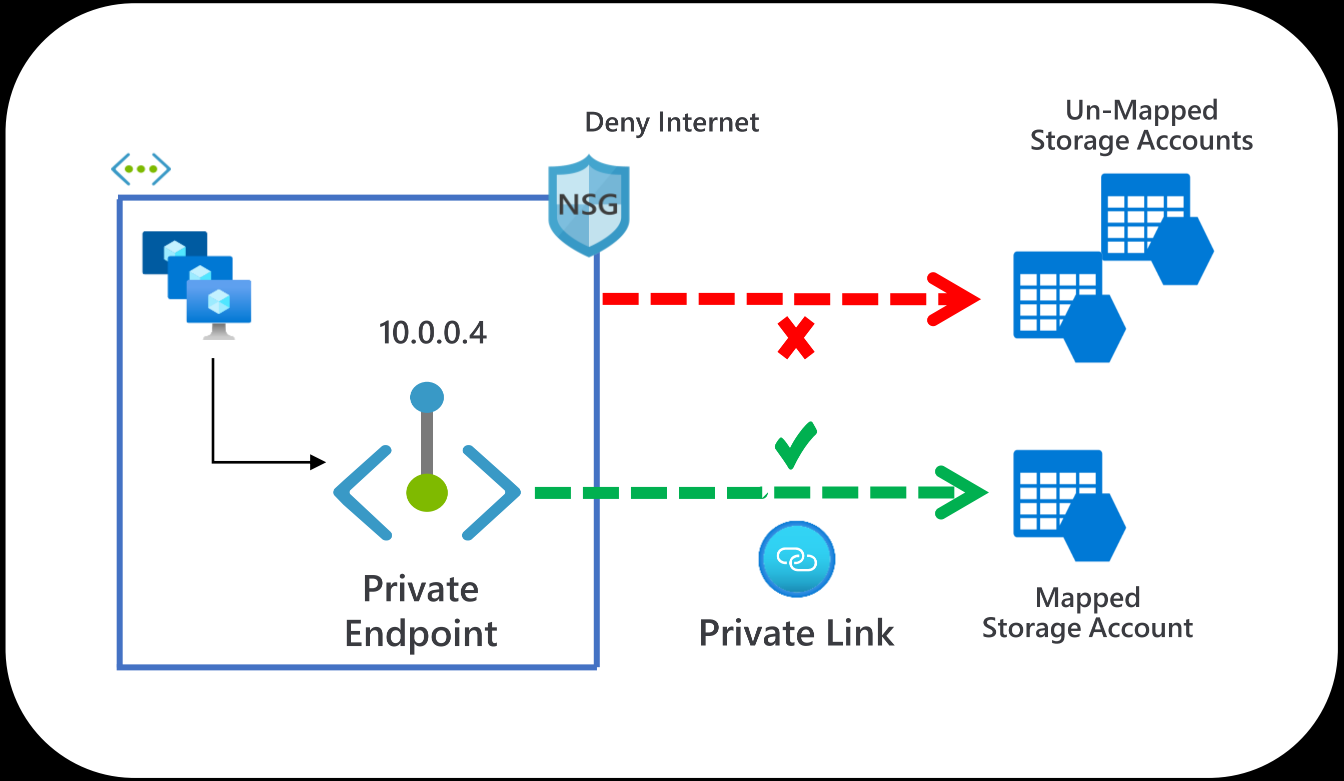
Private access from Virtual Network resources, peered networks and on-premise networks	In-built Data Exfiltration Protection	Predictable private IP addresses for PaaS resources	Unified experience across PaaS, Customer Owned and marketplace Services

Data Exfiltration Protection

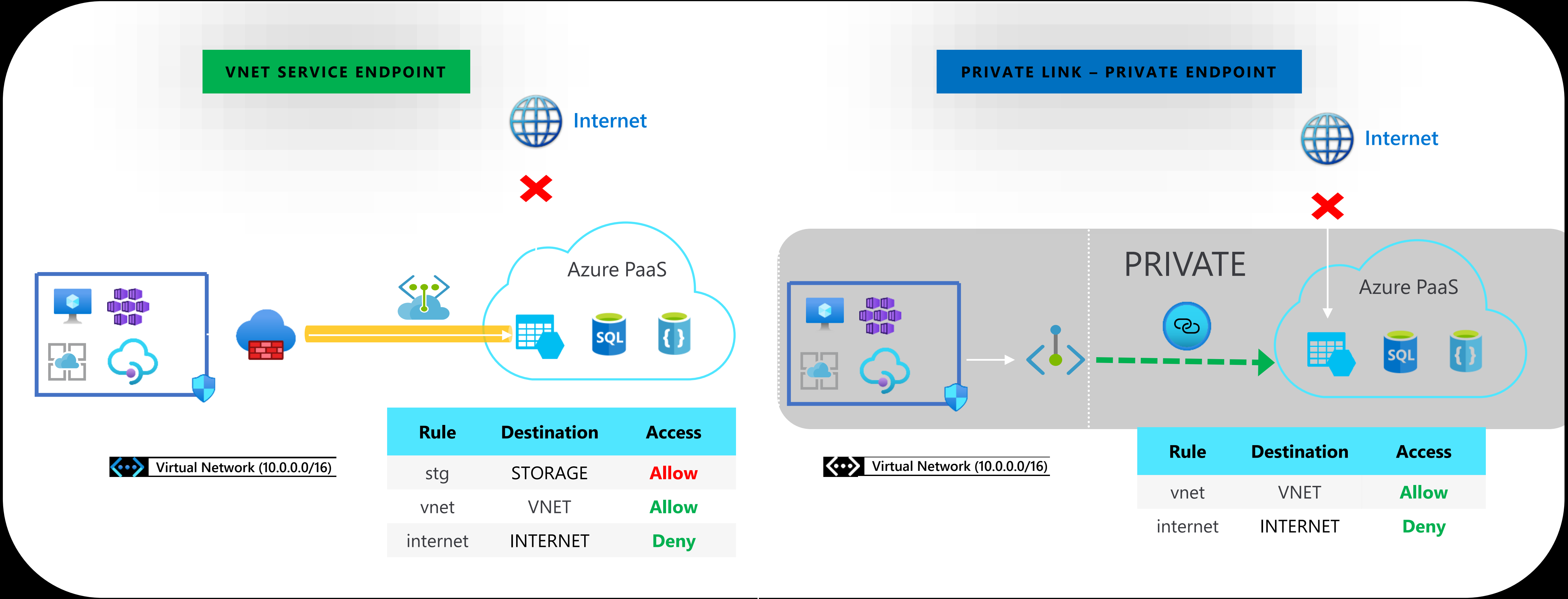
Private Endpoint maps specific PaaS resource to an IP address, not the entire service

Access only to mapped PaaS resource

Data exfiltration protection is in-built



Comparing Service Endpoint & Private Link


VNET SERVICE ENDPOINT
Internet
Azure PaaS
SQL
Virtual Network (10.0.0.0/16)
PRIVATE LINK – PRIVATE ENDPOINT
Internet
PRIVATE
Azure PaaS
SQL
Virtual Network (10.0.0.0/16)

Rule	Destination	Access
stg	STORAGE	Allow
vnet	VNET	Allow
internet	INTERNET	Deny

Rule	Destination	Access
vnet	VNET	Allow
internet	INTERNET	Deny

- VNet to PaaS service via the Microsoft backbone
- Destination is still a public IP address. NSG opened to Service Tags
- Need to pass NVA/Firewall for data exfiltration protection

- VNet PaaS via the Microsoft backbone
- PaaS resource mapped to Private IP Address. NSGs restricted to VNet space
- In-built data exfiltration protection

Your Own Private Link Service

- Create or Convert your existing services into Private Link Service
- VNet-VNet Connectivity without worrying about overlapping IP Space
- No regional, tenant, subscription or RBAC restrictions
- Easily Scale and manage your service

Private Link Service

Microsoft Education