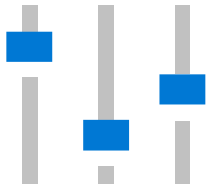
Microsoft

Azure Network Security

Binal Shah
Principal Cloud Solution Architect
binal.shah@microsoft.com

Zero Trust Network Security Maturity Model



Segmentation

Segment networks to prevent lateral movement and data exfiltration

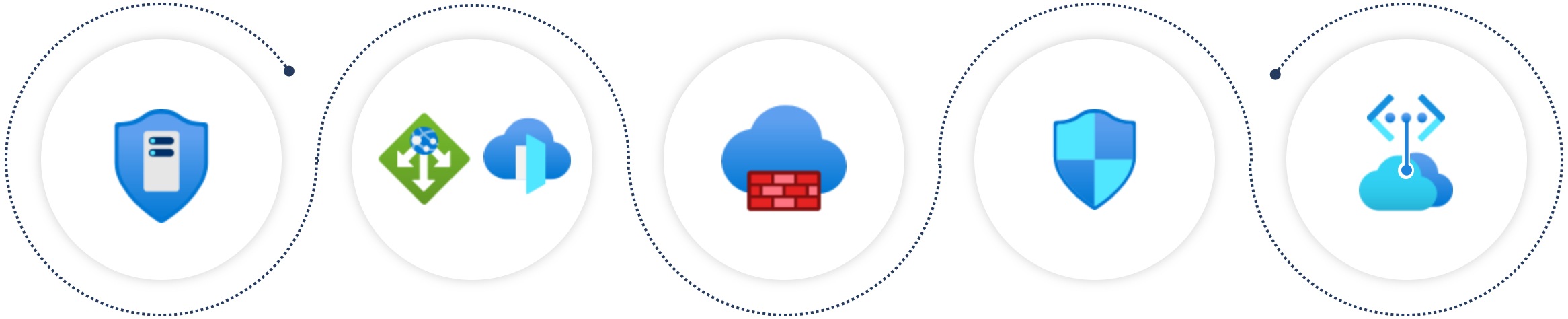
Threat Protection

Real-time threat protection to detect and respond to threats on networks

Encryption

Protect data and end-to-end traffic flow with strong encryption standards

Protection services enabling zero trust



DDoS protection

DDOS protection tuned to your application traffic patterns

Web Application Firewall

Centralized inbound web application protection from common exploits and vulnerabilities

Azure Firewall

Advanced Network and Application threat protection for Azure cloud Infrastructure.

Network Security Groups

Distributed inbound & outbound network (L3-L4) traffic filtering on VM, Container or subnet

VNET Integration

Restrict access to Azure service resources (PaaS) to only your Virtual Network using VNET Injection, Private Link and Service Endpoints

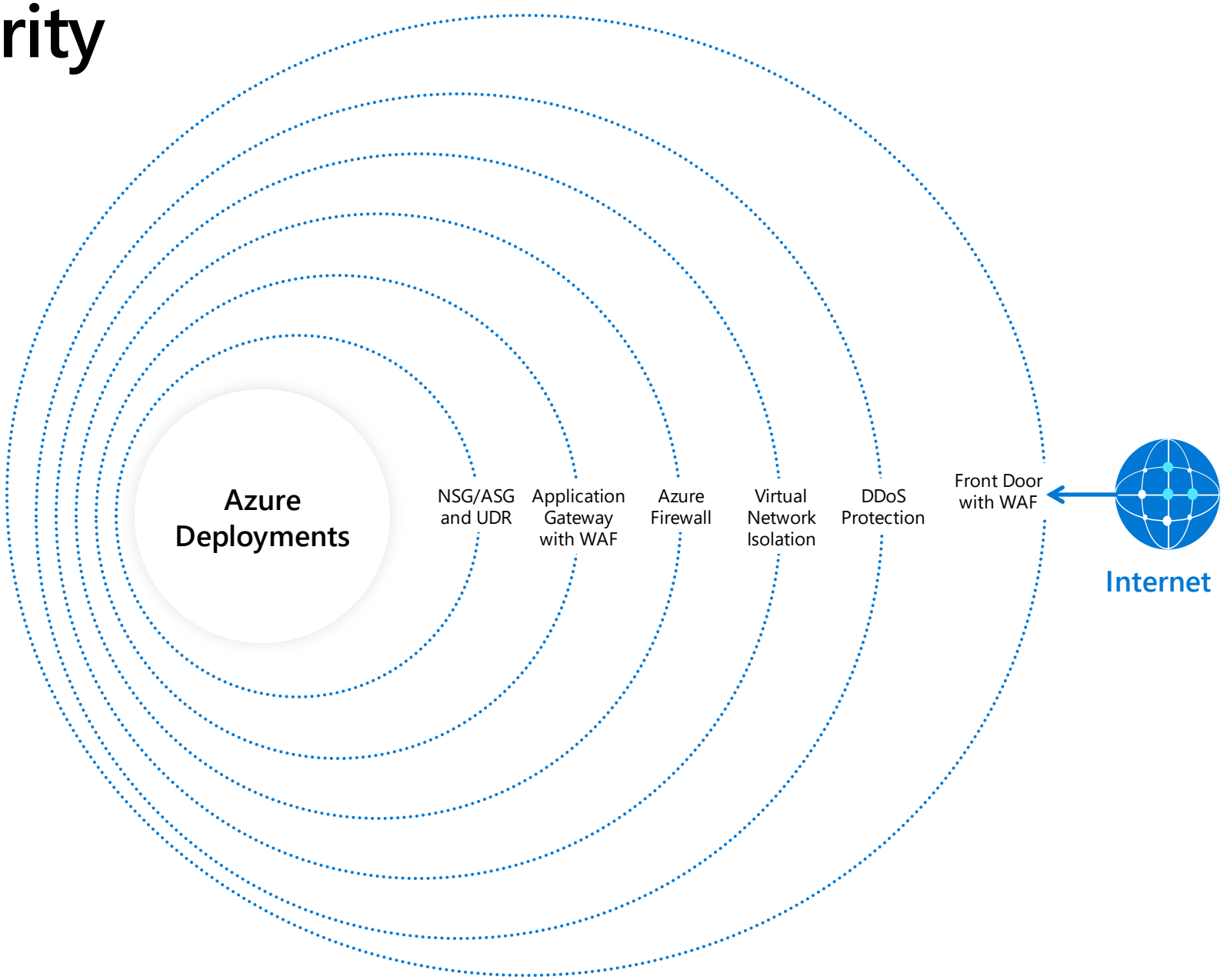
Application protection

Segmentation

Azure network security

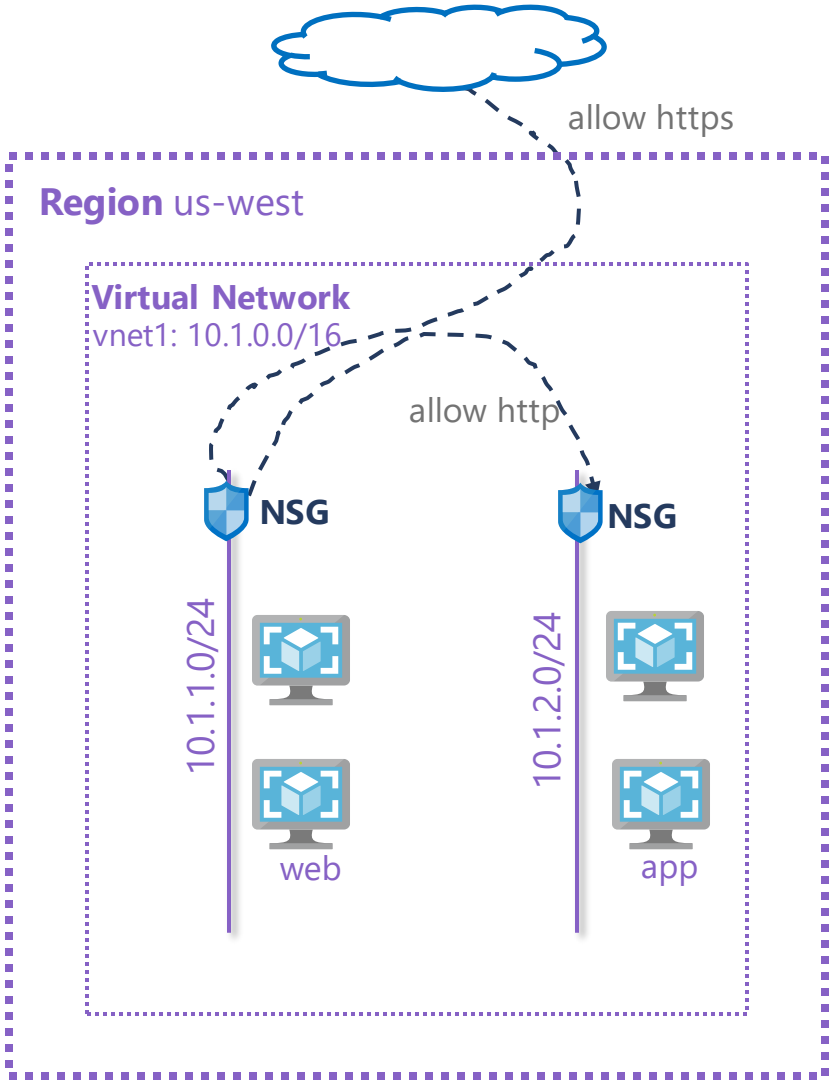
Layered defense approach with cloud native services

- A Zero Trust approach
- Stop attacks at Network edge
- Use virtual network for network segmentation
- Control routing behavior
- Use Service Endpoints to restrict access to PaaS resources
- Use Private Link to enable private access to your PaaS services
- Use Private Link Service to provide private access to your provider service



Network Security Group

- Protects workloads with distributed ACLs
- Applied on subnets or NICs
- Supports application security groups to enable micro-segmentation
- Supports service tags for Azure service IP addresses



Action	Name	Source	Destination	Port
Allow	Webrule	Internet	10.1.1.0/24	443
Allow	Webtoapp	web	app	80
Deny	DenyAll	Any	Any	Any

Network Security Group

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	•••
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalan...	Any	Allow	•••
65500	DenyAllInBound	Any	Any	Any	Any	Deny	•••

Outbound security rules

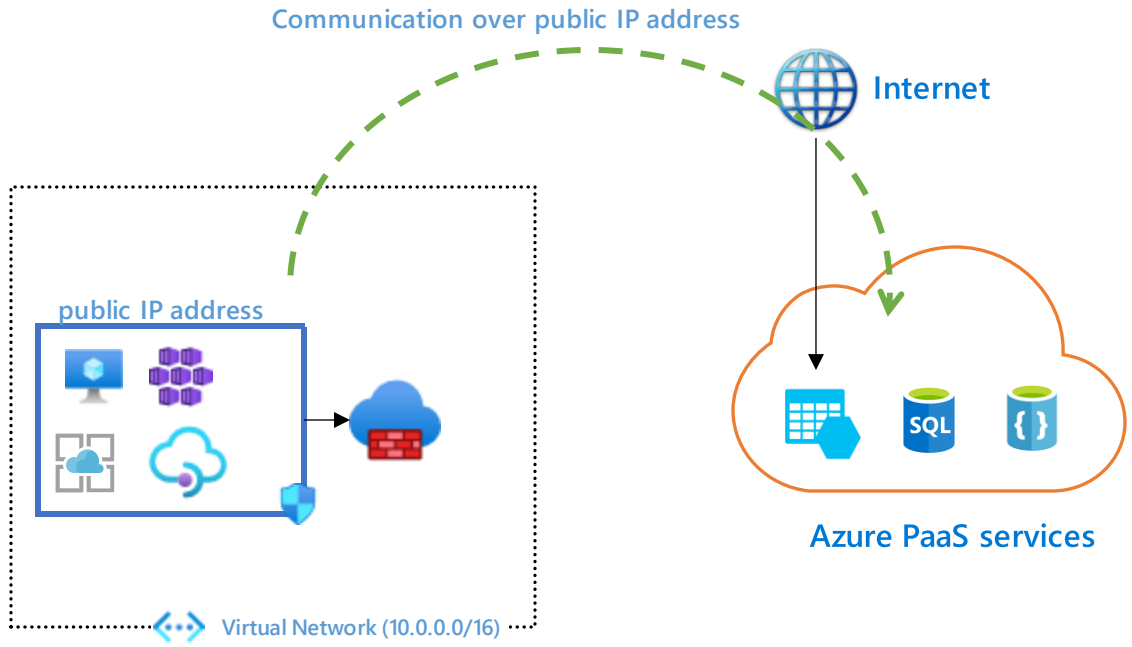
Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	•••
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow	•••
65500	DenyAllOutBound	Any	Any	Any	Any	Deny	•••

Microsoft

Azure Private Link

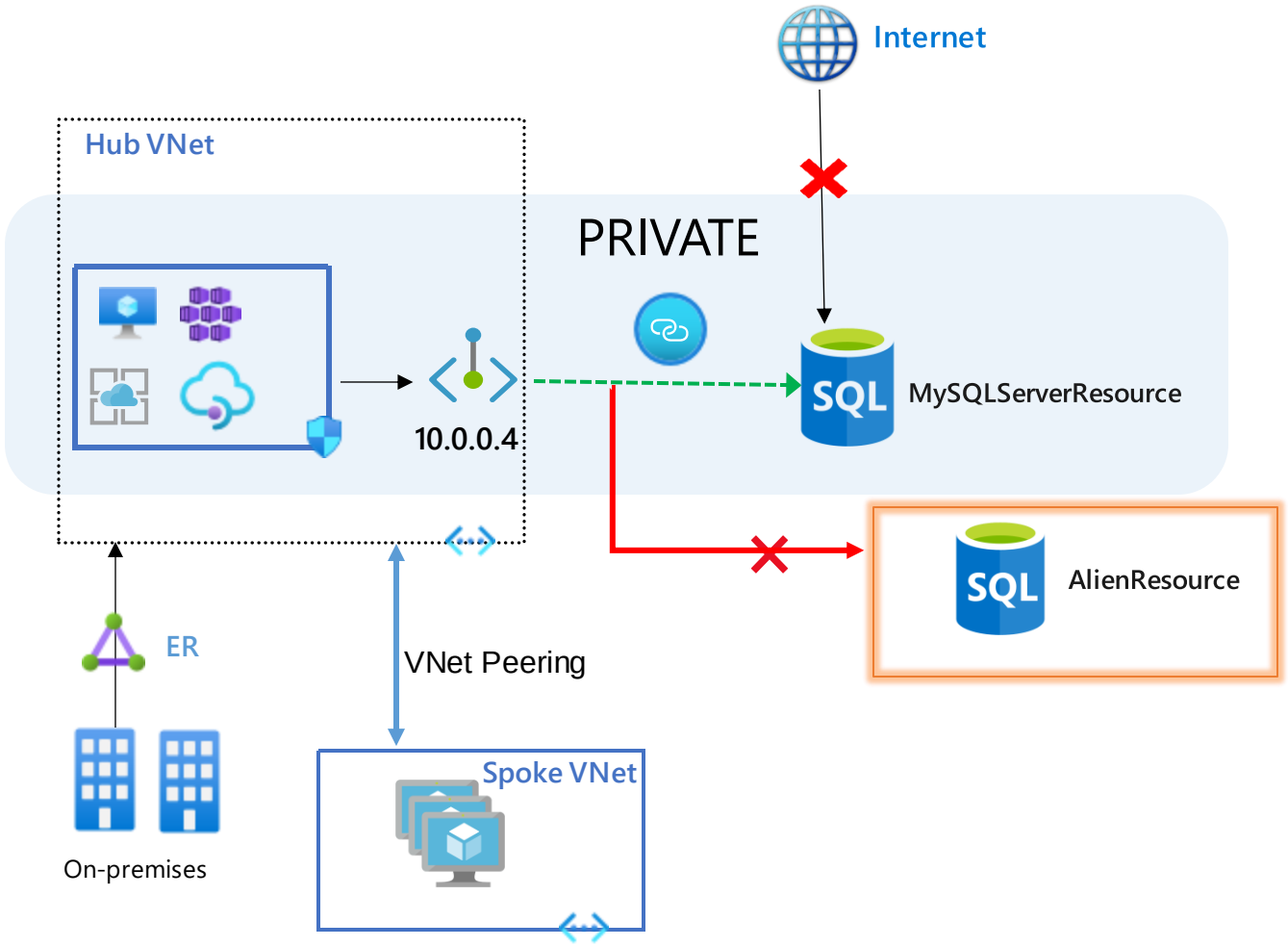
Access to Azure PaaS services

- PaaS service ranges are public IP ranges
- Workloads need a public IP address to reach the services.
- Firewall needs rules to allow this traffic.



Private Link

- Private connectivity to your **specific PaaS resource**
- Traffic stays on Microsoft backbone
- No firewall rules for public IP ranges
- Private access from on-premises
- Private access across vnet peers
- Data exfiltration protection



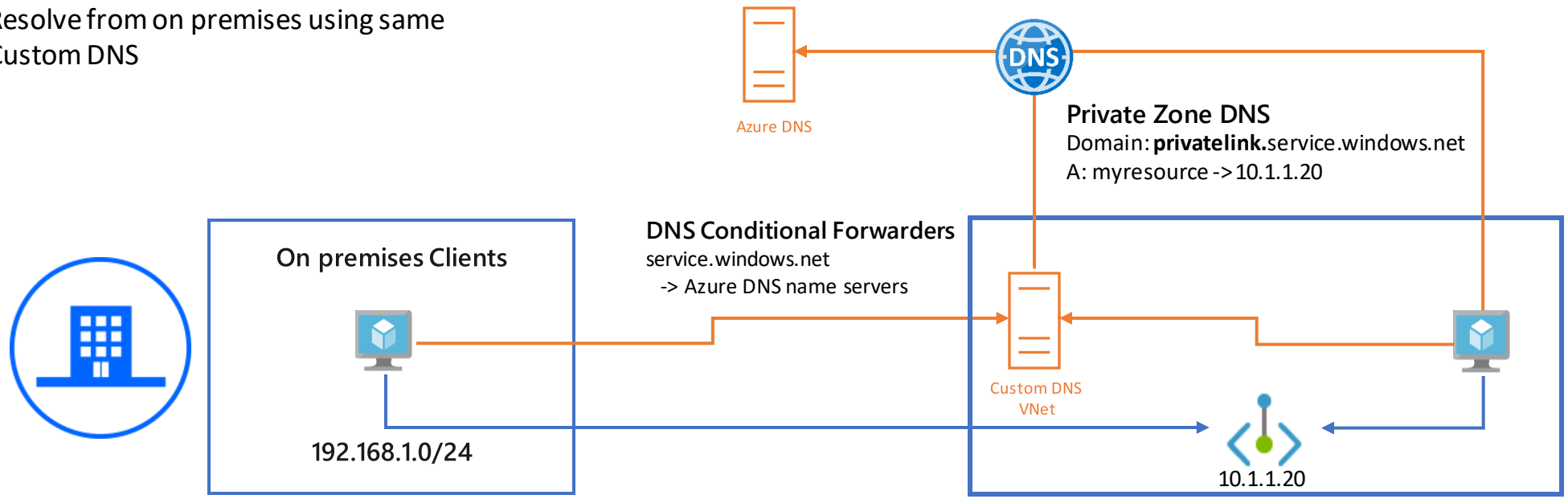
Private Endpoint: DNS Integration

Using Custom DNS on Azure

- ✓ Resolving on Custom DNS on Azure with conditional forwarding for Azure DNS
- ✓ Integrate Private Zone DNS with private record for VNet
- ✓ Resolve from on premises using same Custom DNS

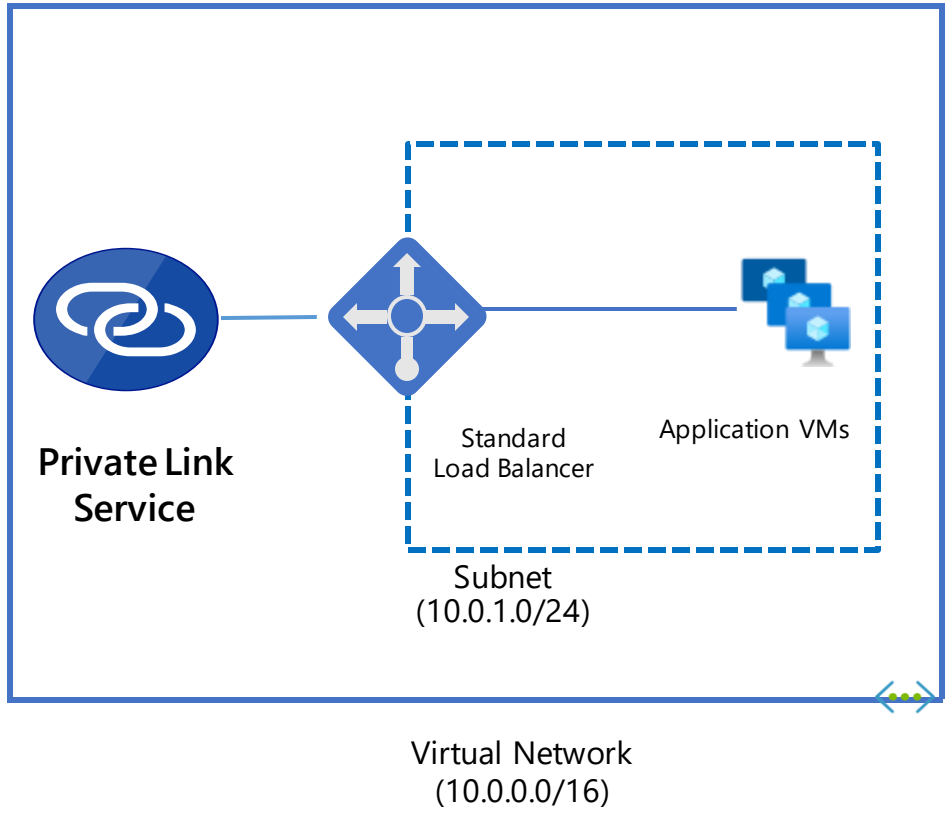
Using Private Zone DNS

- ✓ Same connection URL, no change required on Applications
- ✓ Easy to configure DNS server to resolve from VNet
- ✓ Internet remains resolving to Public IP address

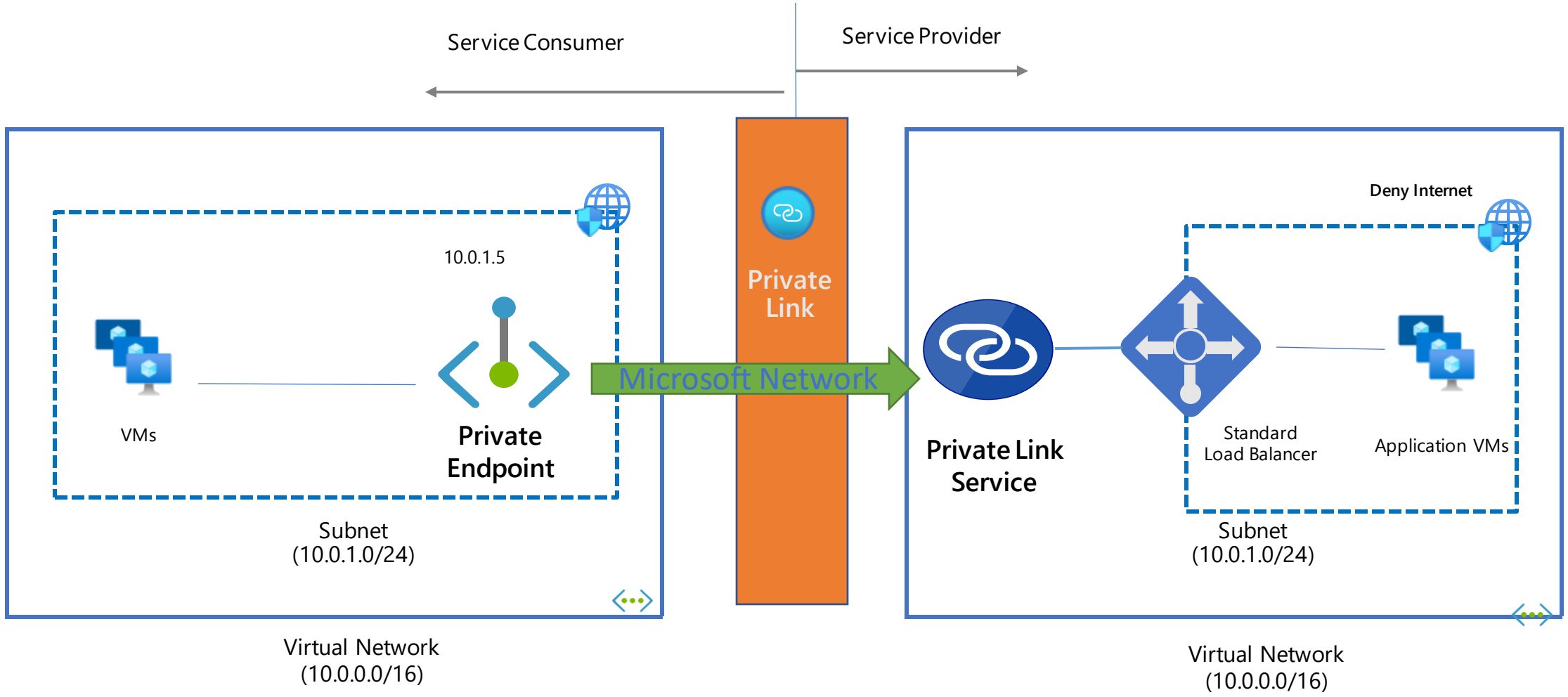


Private Link Service

- Application running behind Standard Load Balancer
- Private Link Service tied to Frontend IP configuration of Standard Load Balancer
- Frontend IP Configuration can be either Public or Private



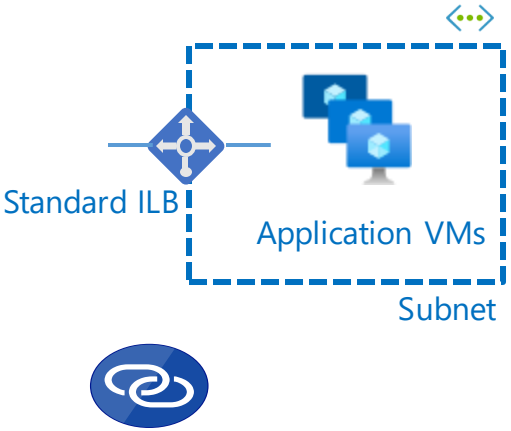
Private Link Service



Approval Workflow

Service Consumer

Service Provider



1. Create your application behind a standard Load Balancer.
2. Create a Private Link Service attached to SLB FE IP.
3. Share the private link service ID (Alias/ARM URI) with consumers. You can either do it offline or advertise publicly.

<ServiceName>.<GUID>.<region>.azure.privatelinkservice

A request will be sent to provider for approval

6. Act on the request – Accept/Reject It.

Decision sent to consumer

4. Create a Private endpoint in any subnet by specifying a private Link service URI/Alias.
5. Configure your DNS record for easy access using the private IP address (CA).
7. Connection Succeeded/Rejected.

Microsoft

Azure Firewall

Azure Firewall

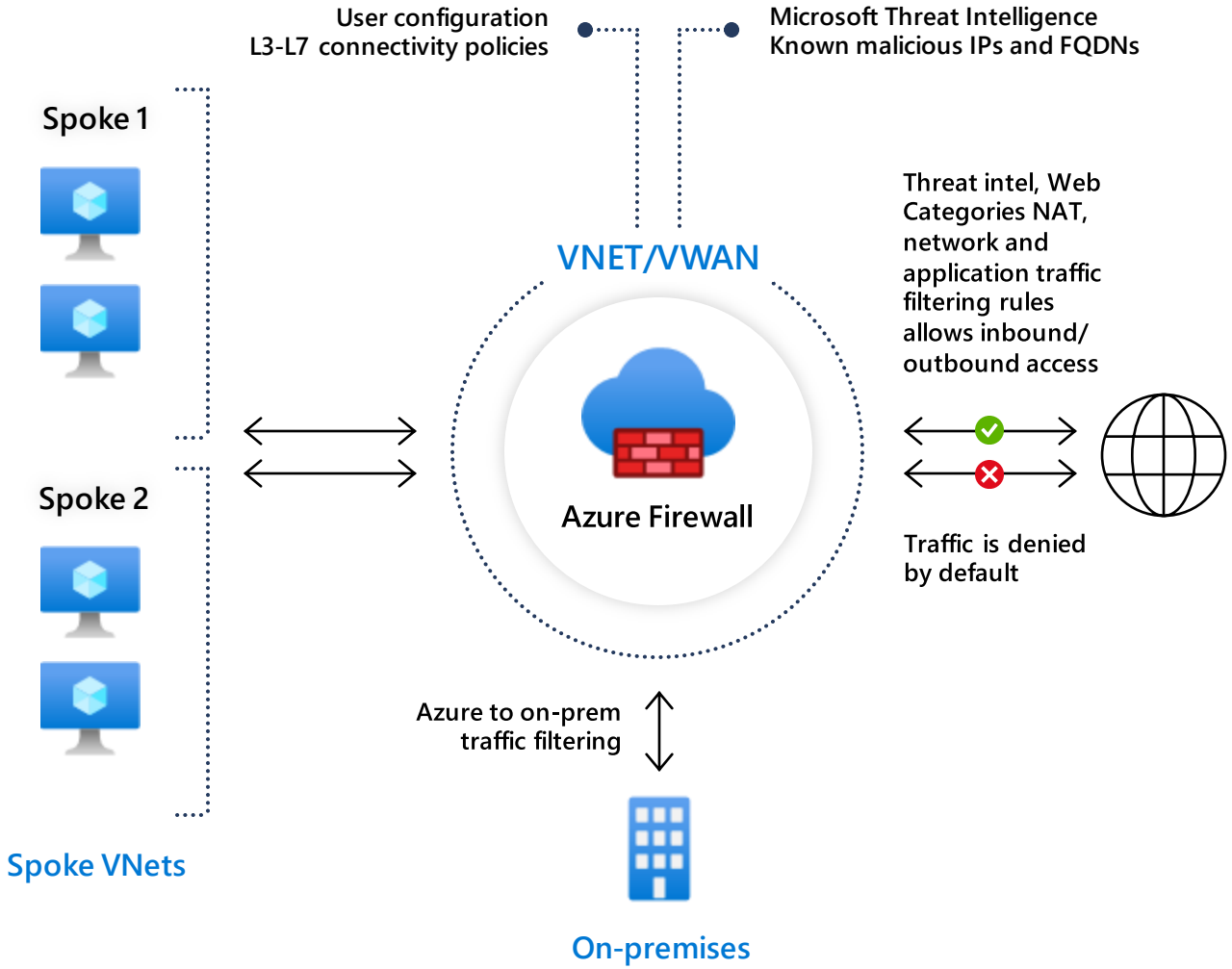
- Secures digital assets using cloud-native firewall capabilities with built-in high availability, auto-scalability, and zero maintenance.

- **Key Benefits**

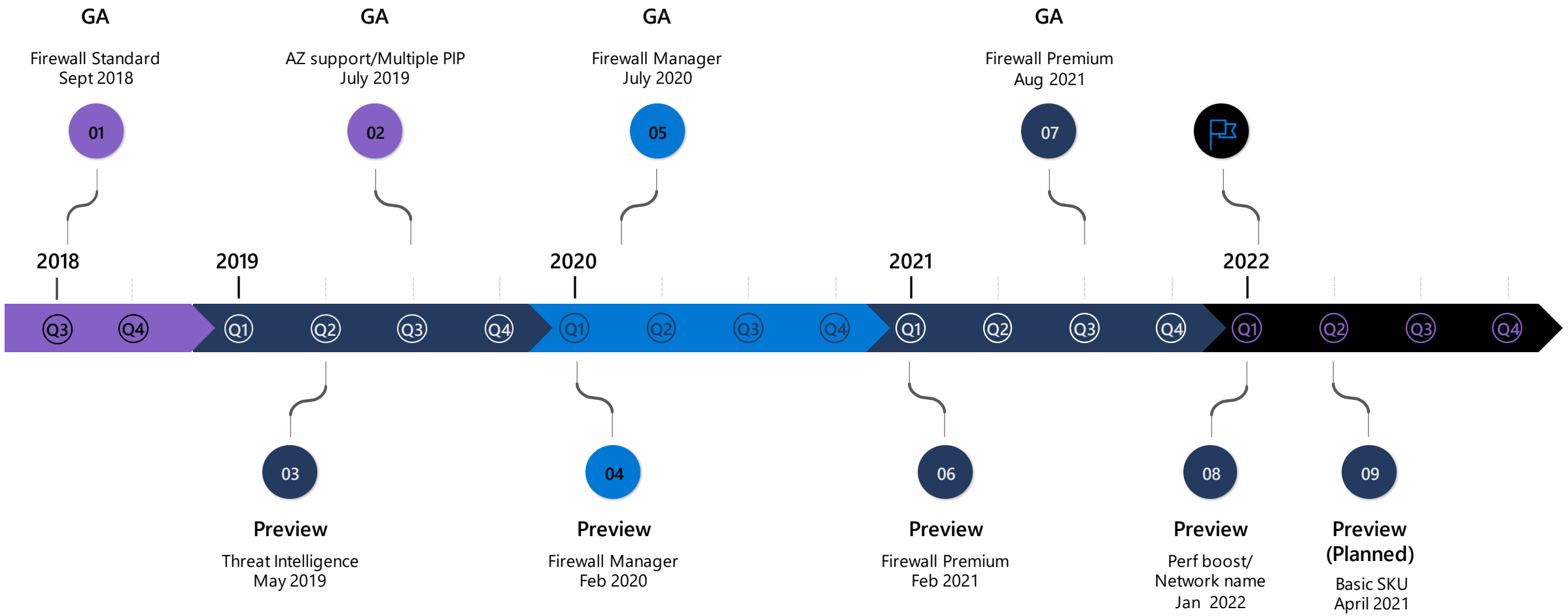
- Network and Application traffic filtering
- Built-in Threat intelligence
- Deploys and scale in minutes
- Supports E-W and N-S traffic filtering

- **Supported SKUs**

- Basic SKU for SMB segment (preview)
- Standard SKU for enterprise & government organizations
- Premium SKU for high-security environments



Our History


GA
Firewall Standard
Sept 2018
01
GA
AZ support/Multiple PIP
July 2019
02
GA
Firewall Manager
July 2020
05
GA
Firewall Premium
Aug 2021
07
2018
2019
2020
2021
2022
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
03
Preview
Threat Intelligence
May 2019
04
Preview
Firewall Manager
Feb 2020
06
Preview
Firewall Premium
Feb 2021
08
Preview
Perf boost/
Network name
Jan 2022
09
Preview
(Planned)
Basic SKU
April 2021

Azure Firewall

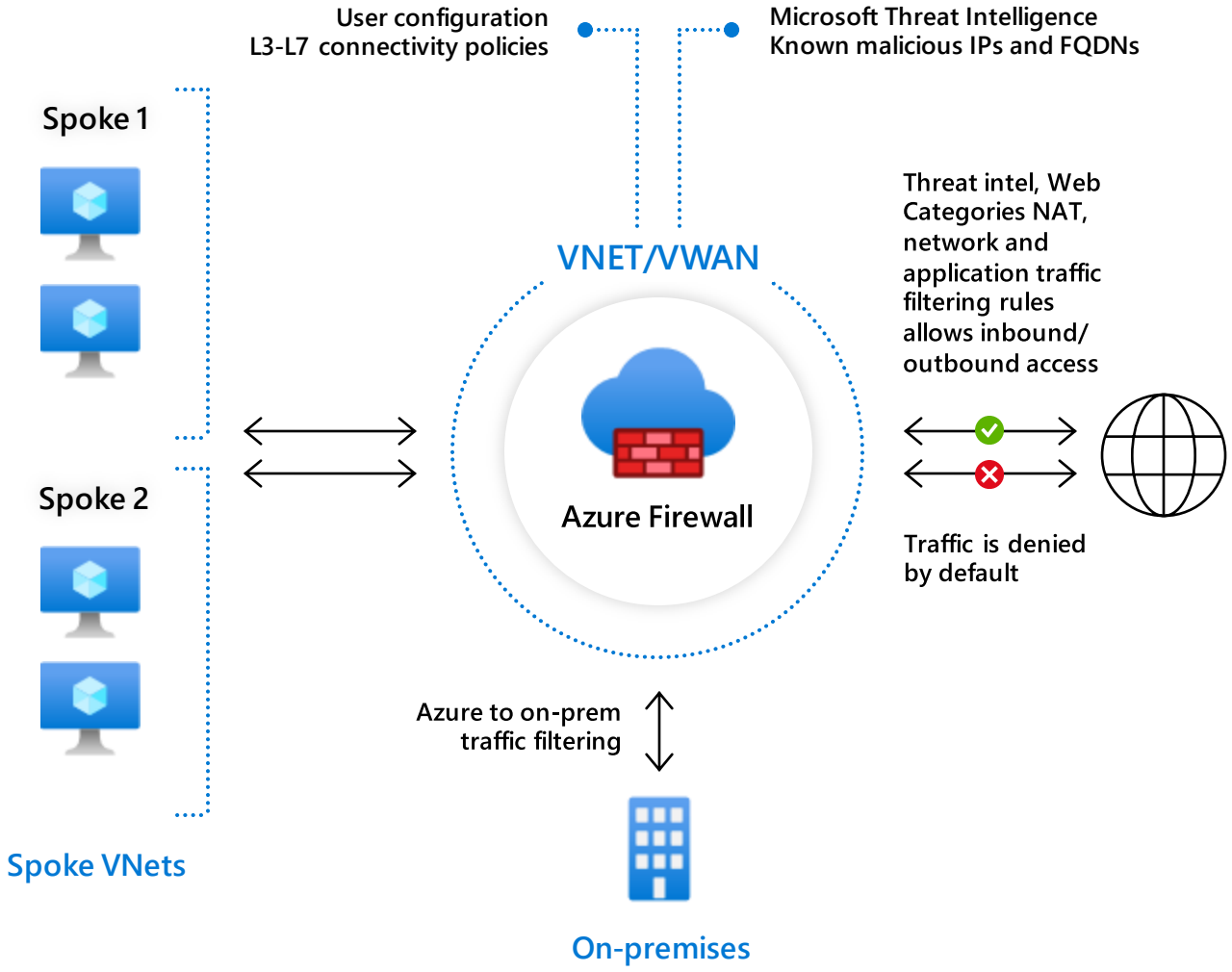
Secures digital assets using cloud-native firewall capabilities with built-in high availability, auto-scalability, and zero maintenance.

Key Benefits

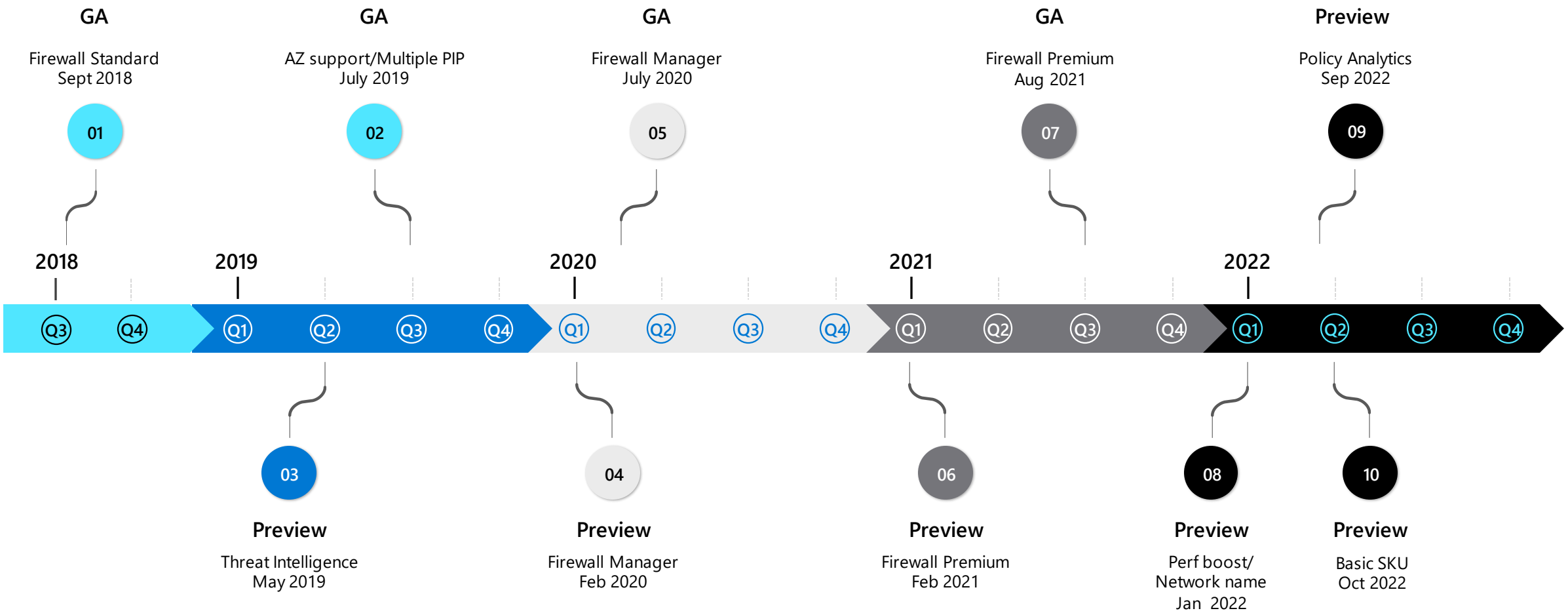
- Network and Application traffic filtering
- Built-in Threat intelligence
- Deploys and scale in minutes
- Supports E-W and N-S traffic filtering

Supported SKUs

- Basic SKU for SMB segment (Public Preview)
- Standard SKU for enterprise & government organizations
- Premium SKU for high-security environments



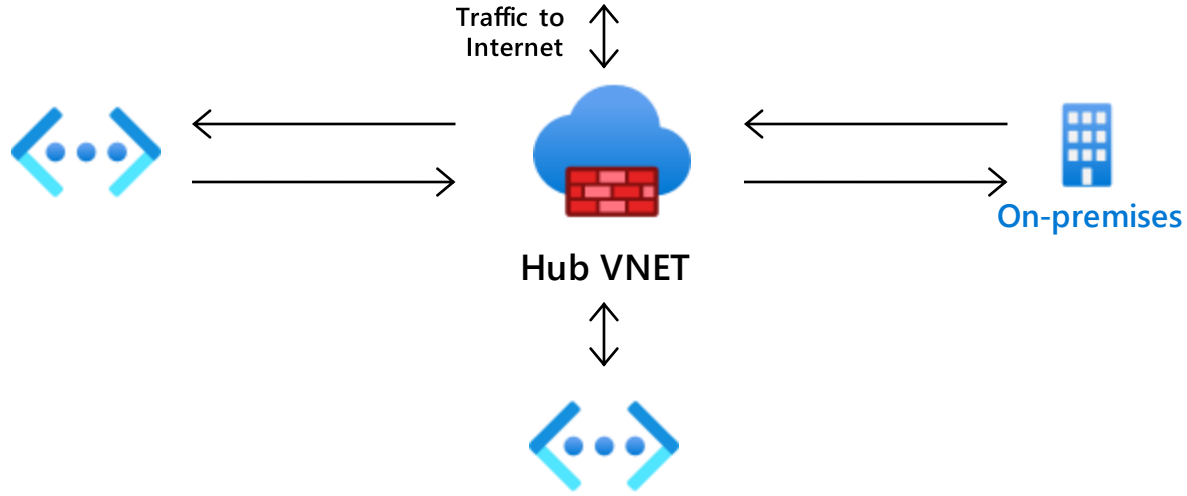
Our History



Firewall Use Cases

VNET deployment

- Firewall is in a Hub VNET.
- Secure traffic between spoke VNETs, subnets within VNETs and traffic to the internet.
- Optionally secure traffic to Branch offices via ER/VPN Gateway.

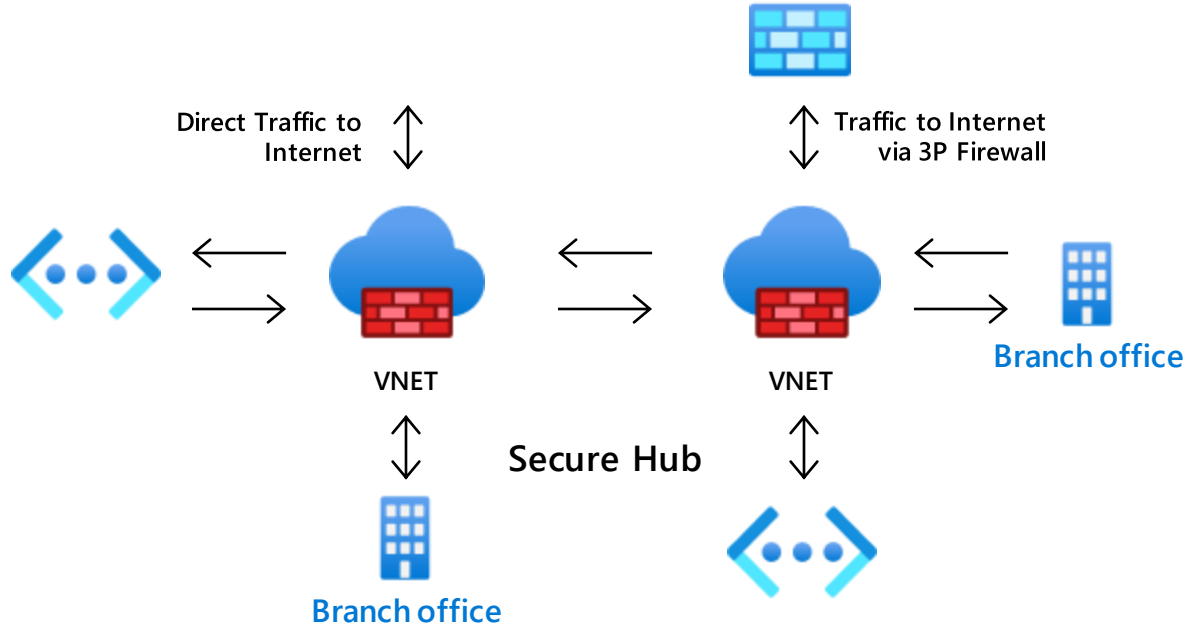


Virtual WAN (aka Secure Hub)

- Firewall is inside a Virtual WAN hub.
- Secure traffic between VNETs, Branch offices and cross hub.
- Automate route configuration to easily attract traffic to the firewall.

Forced Tunnel mode

- Internet breakout is via a 3rd party firewall deployed on-premise or elsewhere.
- Forced tunnel to on-premise firewalls is supported in VNET environments. Virtual WAN environments supports 3P security partner provider for breakout to the internet via CheckPoint & ZScaler.



Azure Firewall Basic

Enterprise-grade security for small and medium businesses

Comprehensive, cloud-native network firewall security

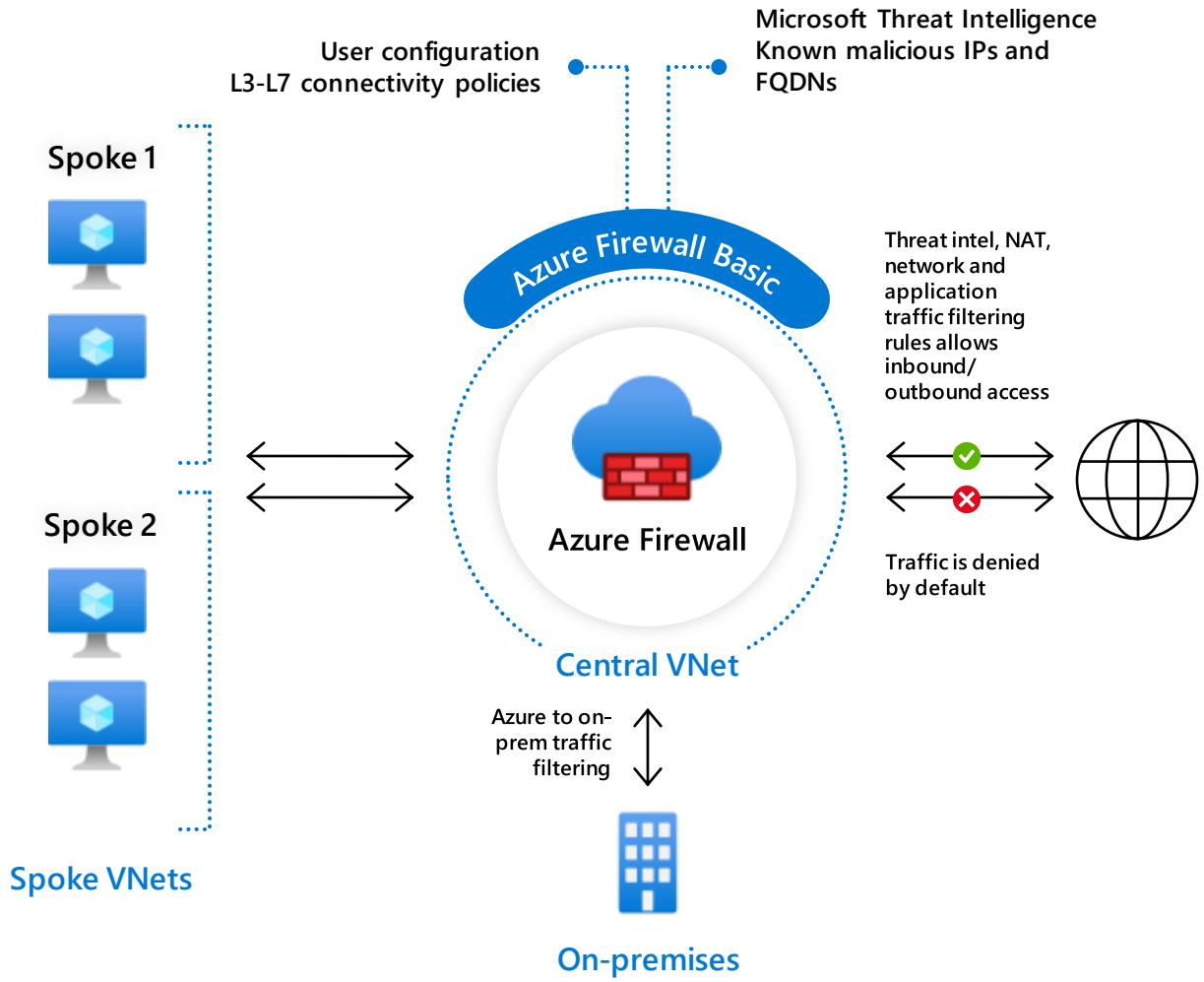
- Network and application traffic filtering
- Threat intelligence to alert on malicious traffic
- Built-in high availability
- Seamless integration with other Azure security services

Simple setup and easy-to-use

- Setup in just a few minutes
- Automate deployment (deploy as code)
- Zero maintenance with automatic updates
- Central management via Azure Firewall Manager

Cost-effective

Designed to deliver essential protection at a price point that meets your needs



Azure Firewall Standard

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

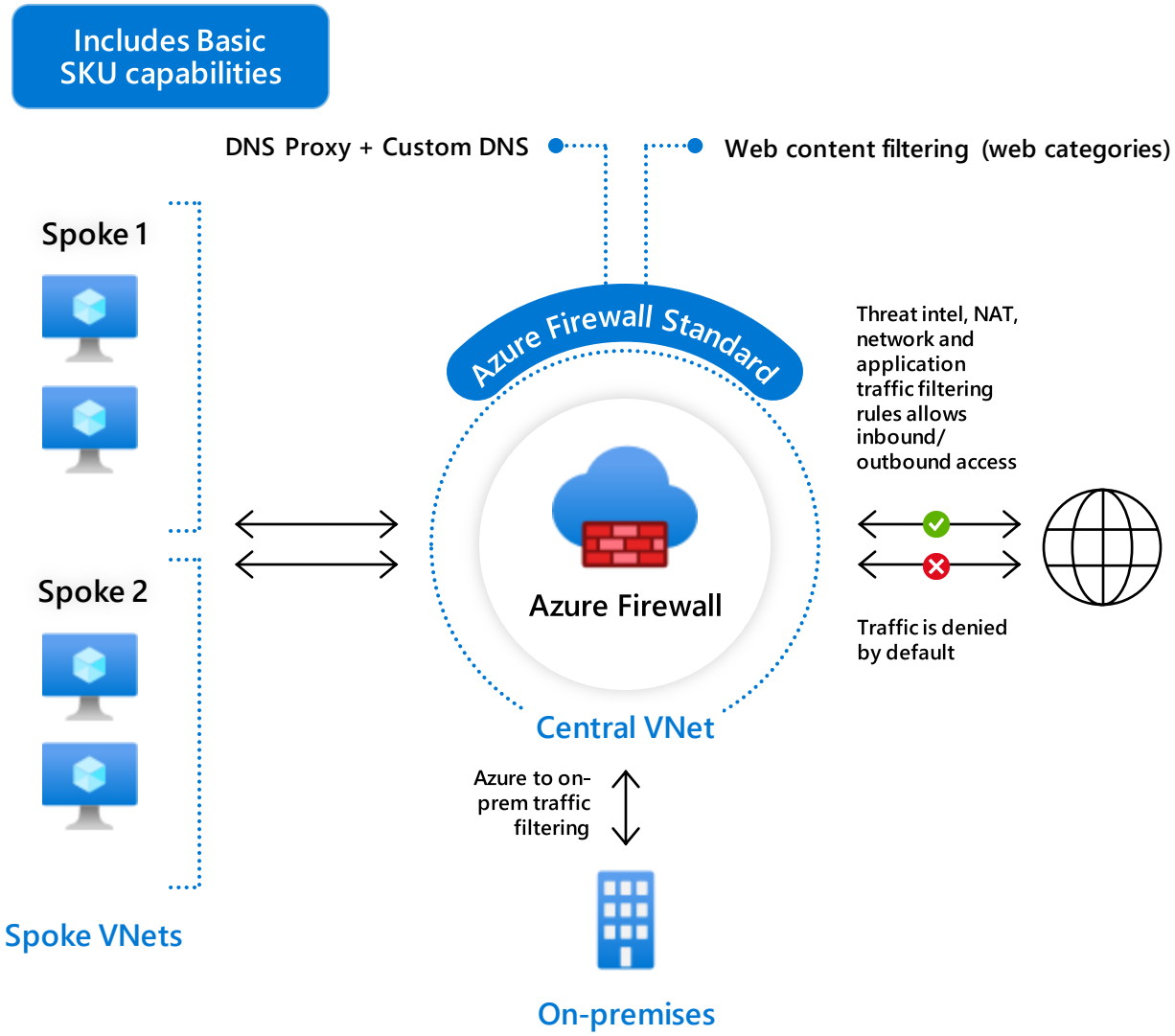
Filter Outbound, Inbound, Spoke-Spoke and Hybrid Connections traffic (VPN and ExpressRoute)

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.



Azure Firewall Premium

Cloud native Next-Gen Firewall as a service

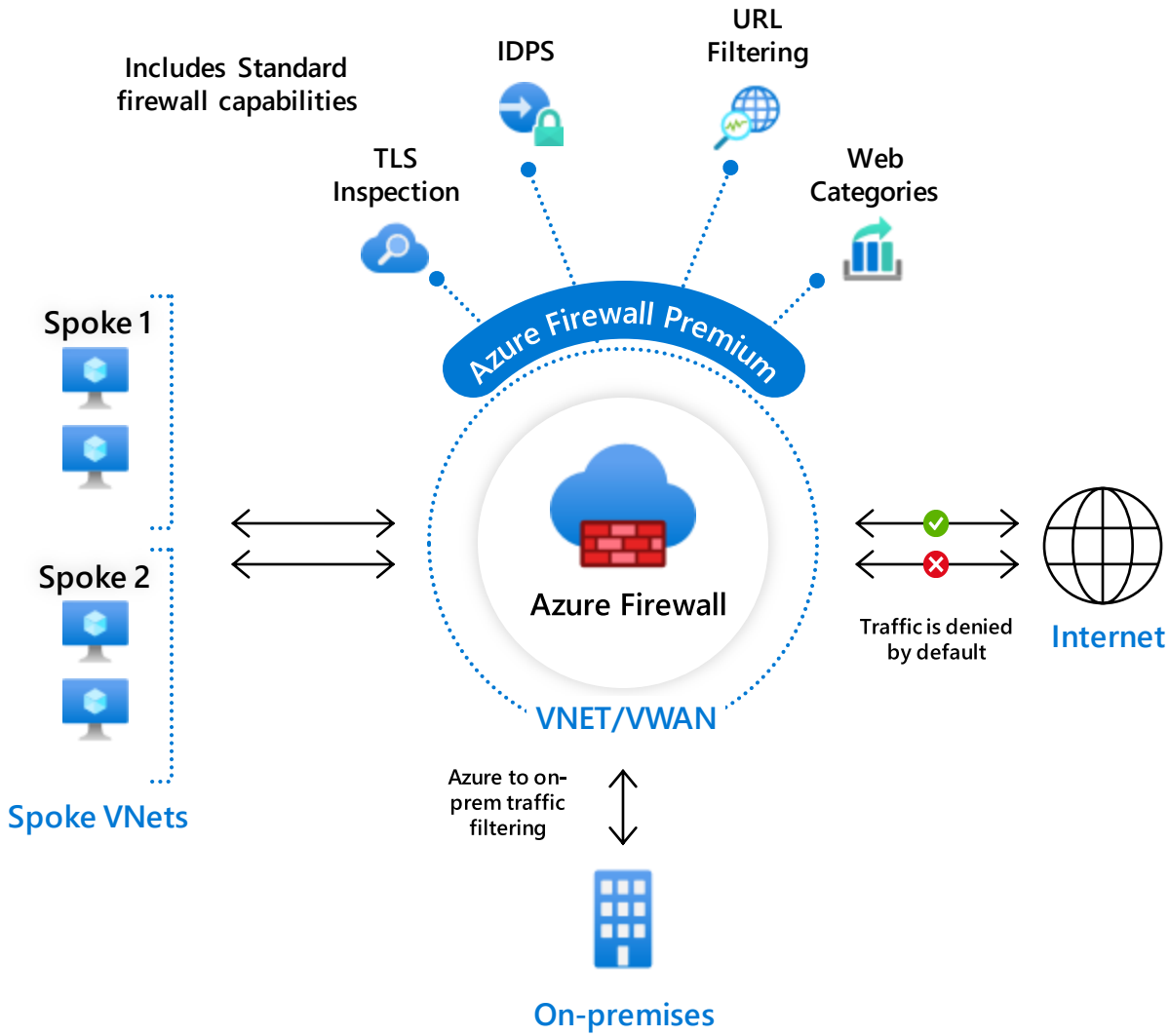
TLS Inspection
- Built-in TLS Inspection for Outbound and East-West traffic
- Inbound TLS termination is supported with Azure Application Gateway
- Customer provided key pair via Azure Key Vault integration

Intrusion Detection Prevention System (IDPS)
- Detect alert and block inbound/outbound malicious traffic
- Supported for both encrypted and plain text protocols
- Signature-based detection that is continuously updated

URL Filtering
- Restrict user access to HTTP/HTTPS Web content
- Support for URL wildcards

Web Categories
- Allow or deny user access to website categories such as gambling, social media and others
- Web categories maintained and continuously updated
- URL based category matching

Azure Firewall Standard
- Including all standard firewall capabilities



Feature Category	Feature	Firewall Basic *Public Preview*	Firewall Standard	Firewall Premium
L3-L7 Filtering	Application level FQDN filtering (SNI based) for HTTPS/SQL	✓	✓	✓
	Network level FQDN filtering – all ports and protocols		✓	✓
	Stateful firewall (5 tuple rules)	✓	✓	✓
	Network Address Translation (SNAT+DNAT)	✓	✓	✓
Reliability & Performance	Availability zones	✓	✓	✓
	Built-in HA	✓	✓	✓
	Cloud scalability (auto-scale as traffic grows)	Up to 250 Mbps	Up to 30 Gbps	Up to 100 Gbps
	Fat Flow support	N/A	1 Gbps	10 Gbps
Ease of Management	Central management via Firewall Manager	✓	✓	✓
	Policy Analytics (Rule Management over time)	✓	✓	✓
Enterprise Integration	Full logging including SIEM integration	✓	✓	✓
	Service Tags and FQDN Tags for easy policy management	✓	✓	✓
	Easy DevOps integration using REST/PS/CLI/Templates/ Terraform	✓	✓	✓
	Web content filtering (web categories)		✓	✓
	DNS Proxy + Custom DNS		✓	✓
Advanced Threat Protection	Threat intelligence-based filtering (known malicious IP address/ domains)	Alert	✓	✓
	Inbound TLS termination (TLS reverse proxy)			Using App GW
	Outbound TLS termination (TLS forward proxy)			✓
	Fully managed IDPS			✓
	URL filtering (full path - incl. SSL termination)			✓

Azure Firewall

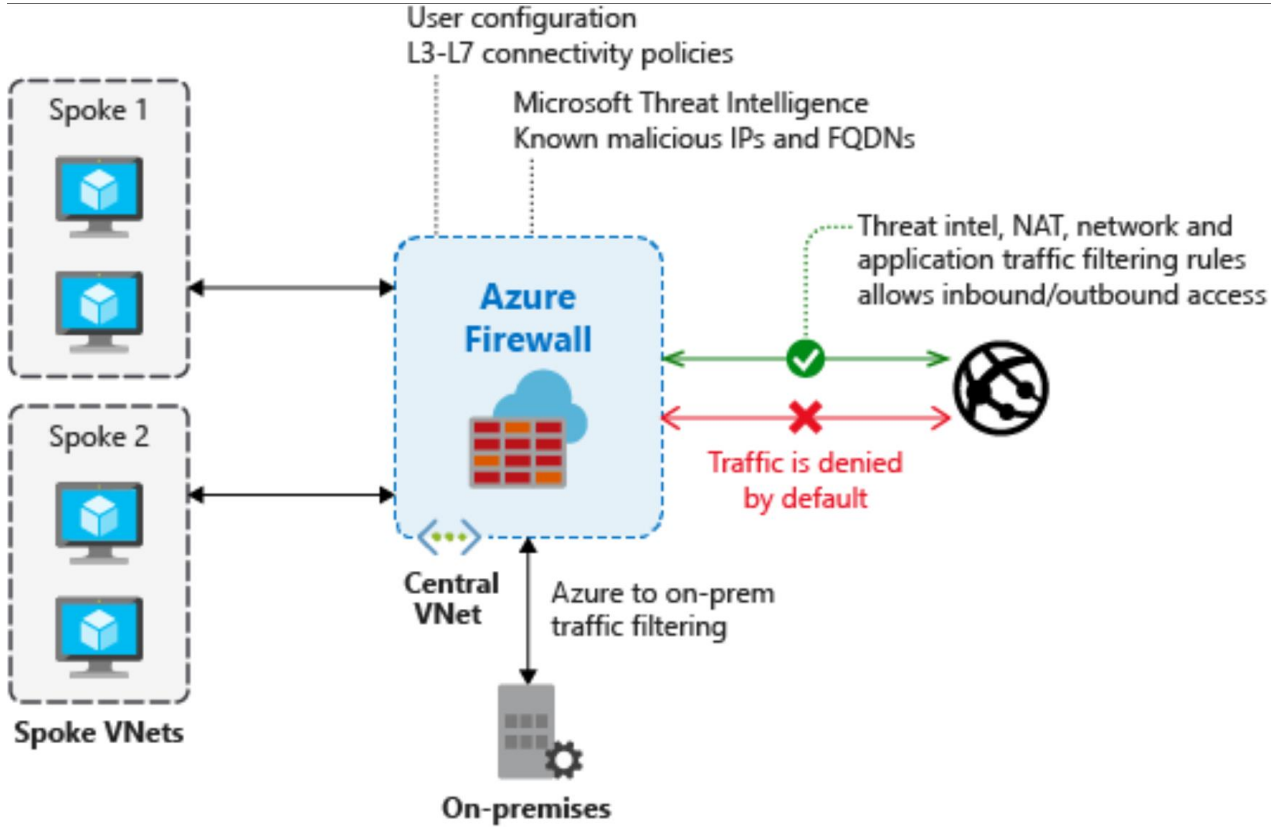
Rules Processing Logic

Threat Intelligence

NAT Rules

Network Rules

Application Rules



Policy Analytics (preview)

Manage Azure Firewall rules over time

Policy Insights

- Highlights key information of the Firewall policy such as Policy limits, Duplicate rules, Wildcard in rules and more.

Policy Recommendations

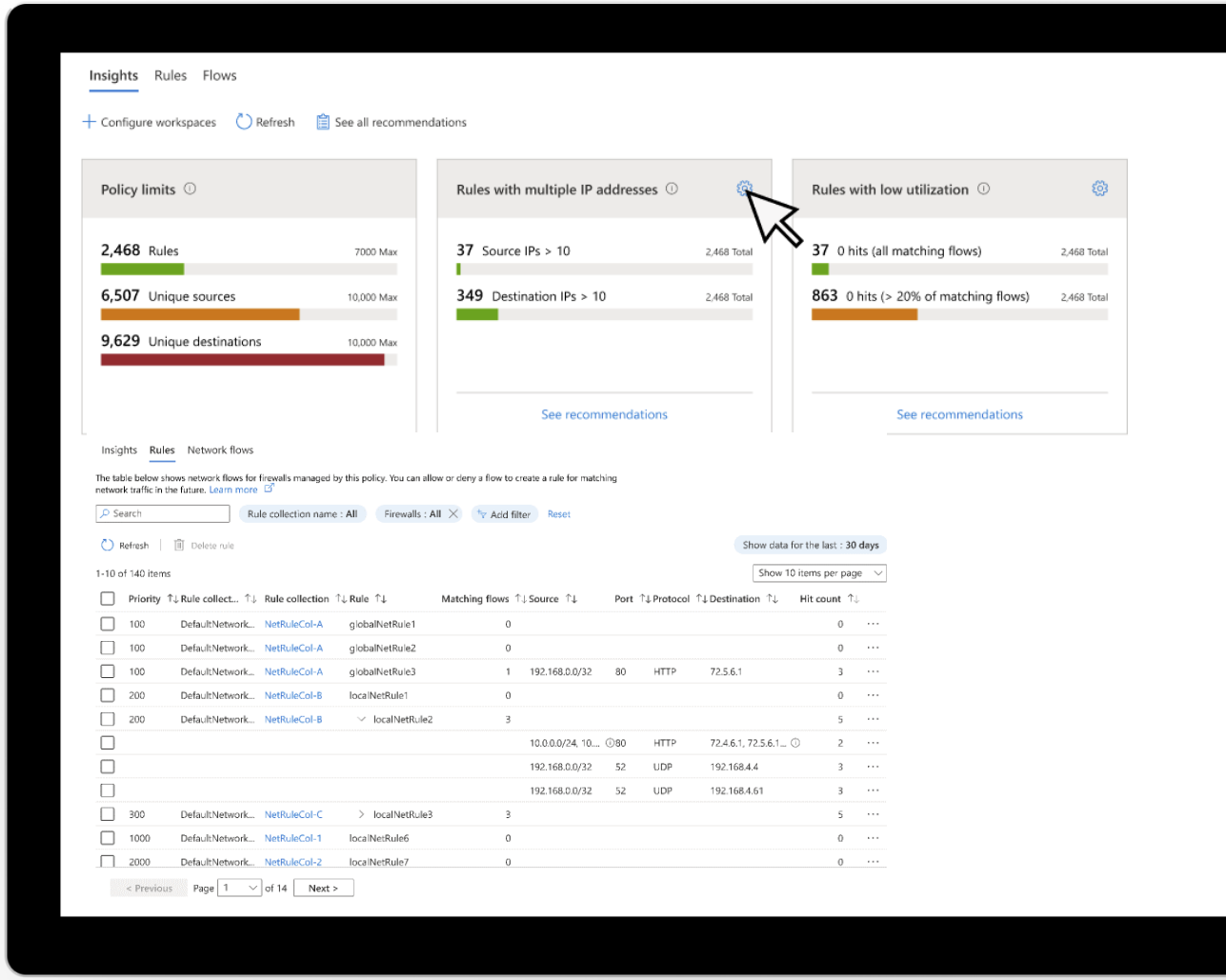
- Recommendations to improve the Rules in the policy including rules with low/no hits, overly permissive rules, potentially malicious sources.

Rule Analytics

- Visibility into the traffic flows of the rules over time
- Rule hit count for Application, Network and DNAT rules

Single Rule Analysis

- Refine the rules permissions
- Inspect the flows hit per a specific rule



Azure

Azure Firewall Workbook and Sentinel Integration

Azure Firewall Data Connector for Azure Sentinel can be used to ingest logs to visualize data in the Firewall Workbook available in Sentinel.

- The workbook can also be downloaded from our GitHub repo (https://aka.ms/AzNetSec) and used with a Log Analytics workspace.

Optimize security with Azure Firewall solution for Microsoft Sentinel (public preview)

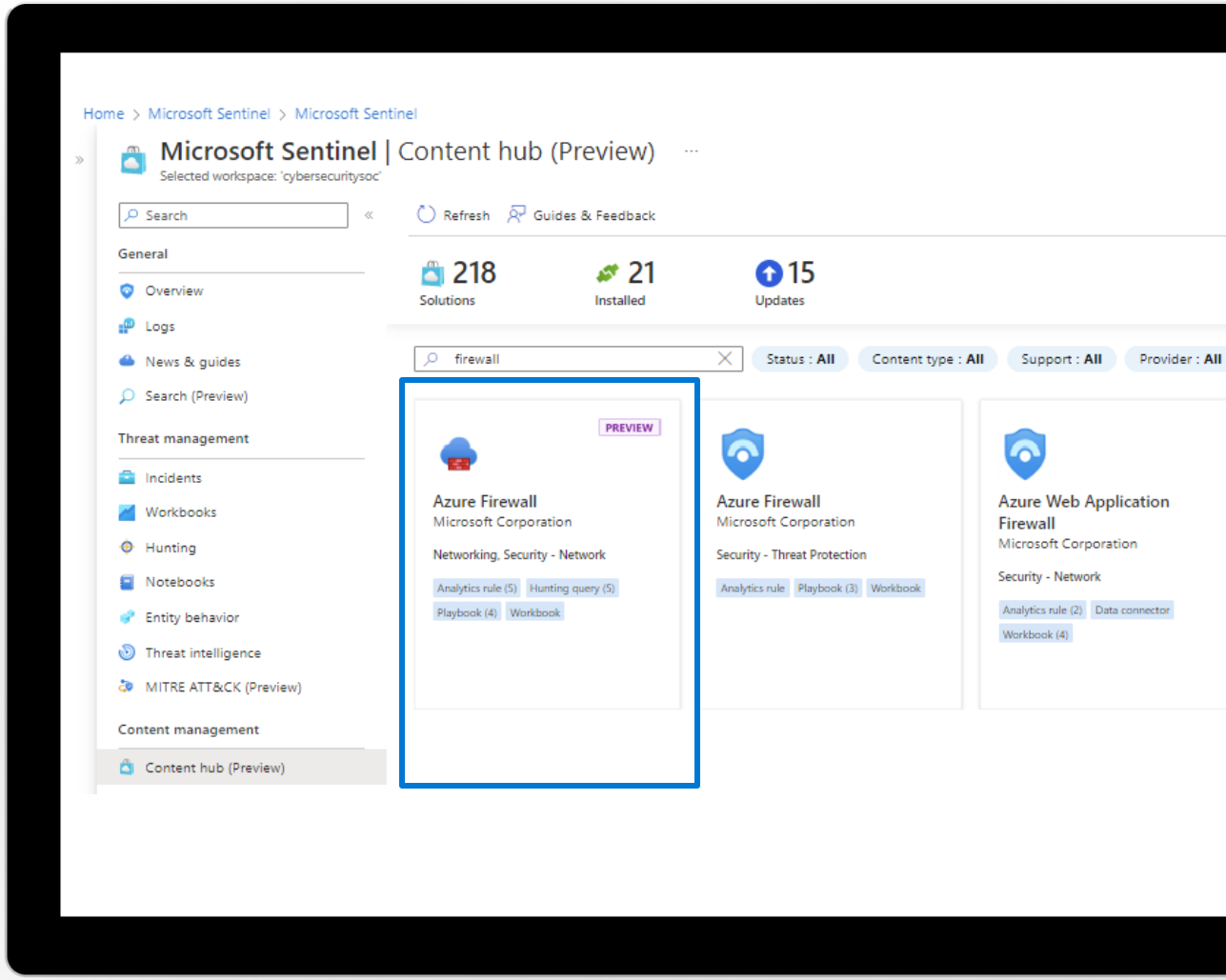
Built-in Threat Detection

- Port scan
- Port sweep
- Abnormal deny rate for source IP
- Abnormal Port to protocol
- Multiple sources affected by the same TI destination

Hunting queries

- First time a source IP connects to destination port
- First time source IP connects to a destination
- Source IP abnormally connects to multiple destinations
- Uncommon port for the organization
- Uncommon port connection to destination IP

Automating response and correlation



Response Automation

Azure Firewall Custom Connector

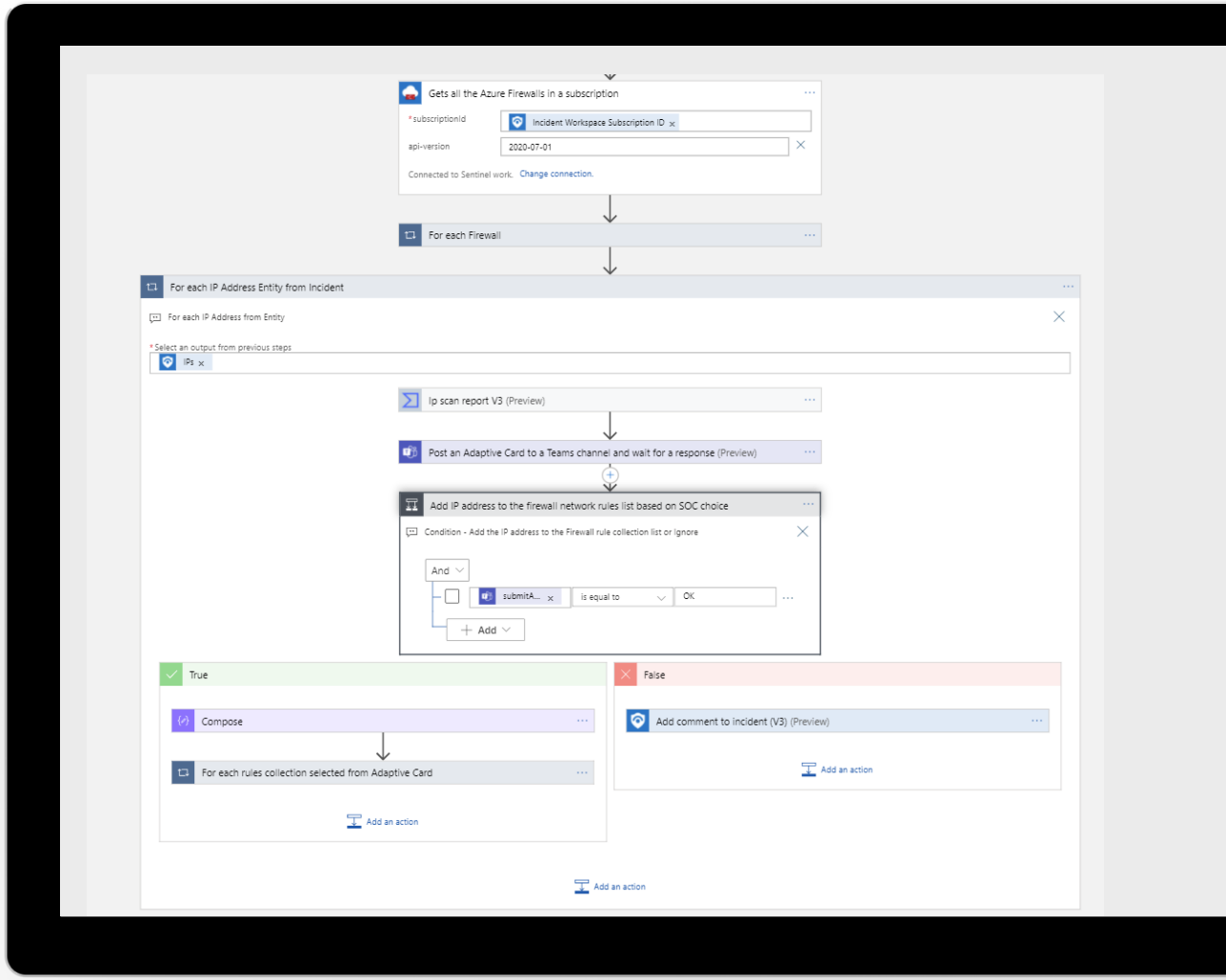
Take different actions against Azure Firewall, Firewall Policy, and IP Groups using Playbooks.

Playbooks

- Add IP to IP Group
- Add IP to Threat Intel Allow List
- Add new rule to block IP

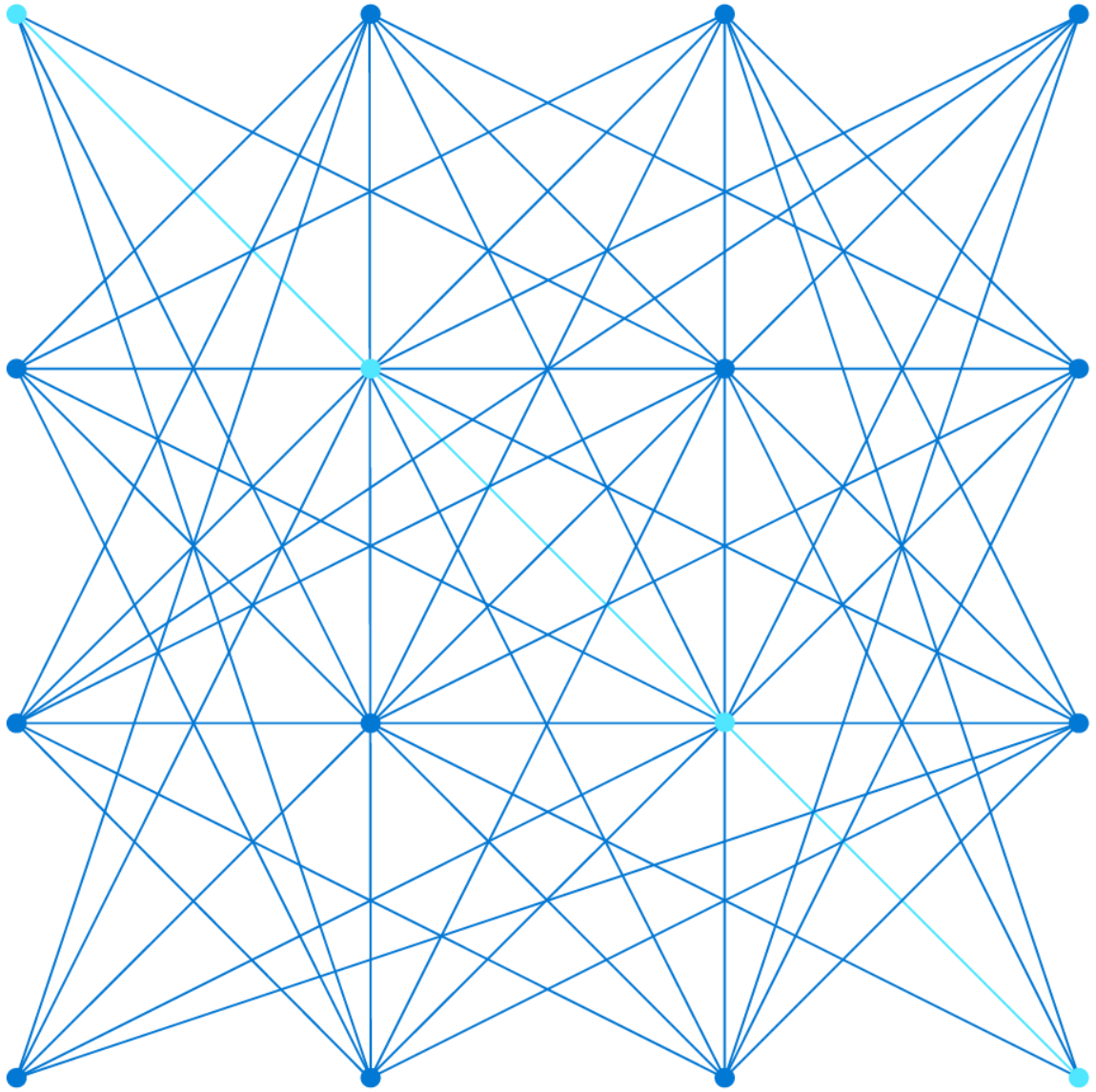
Playbook support for the Classic rules, Standard and Premium policy:

Playbook Name	Premium Policy	Standard Policy	Classic Rules
AzureFirewall-BlockIP-addToIPGroup	Yes	Yes	Yes
AzureFirewall-AddIPtoTIAllowList	No	Yes	No
AzureFirewall-BlockIP-addNewRule	No	No	Yes



Microsoft Azure

Azure Firewall Manager



Enterprise challenges

Complex network architecture and constantly changing threat environment

Need complete visibility into the network	Centralized management and administration
Enforcing consistent security policies across multiple firewalls	Simplify rule management across multiple firewall
Compliance using a zero-trust security model	Networks are automatically secured and protected
Respond to internet attacks	Rapidly push firewall protection policy to respond to new threats

Azure Firewall Manager

Single Pane of glass to manage Azure Firewall, DDoS & WAF across Azure Tenant

Azure Firewall Management

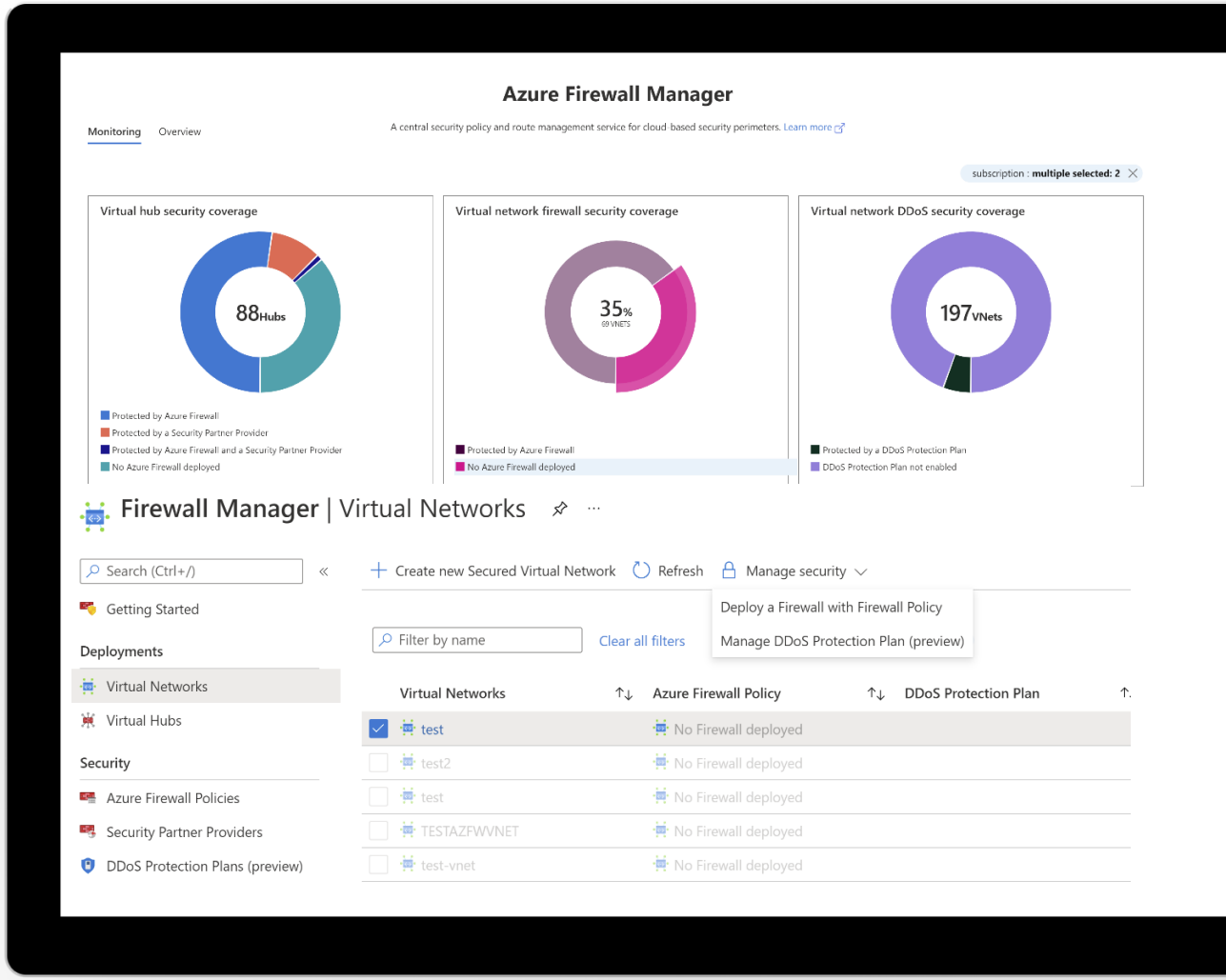
- Deploy Azure Firewall across both VNET and VWAN deployments
- Associate Azure Firewall Policy to one or more Firewalls
- View and modify Azure Firewall Policy
- Gain insights into Firewall Traffic with Policy Insights *Preview*

DDOS management

- View and create DDoS Protection Plans
- Associate DDoS plans to VNETs

WAF management

- Deploy and configure WAF policies
- Upgrade from legacy WAF configuration to WAF policies on Azure Application Gateway



Central security and policy management

Deploy and configure Azure Firewall policies, Azure WAF policies, and Azure DDoS Protection plans

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

Enforce consistent configuration across Azure Firewall

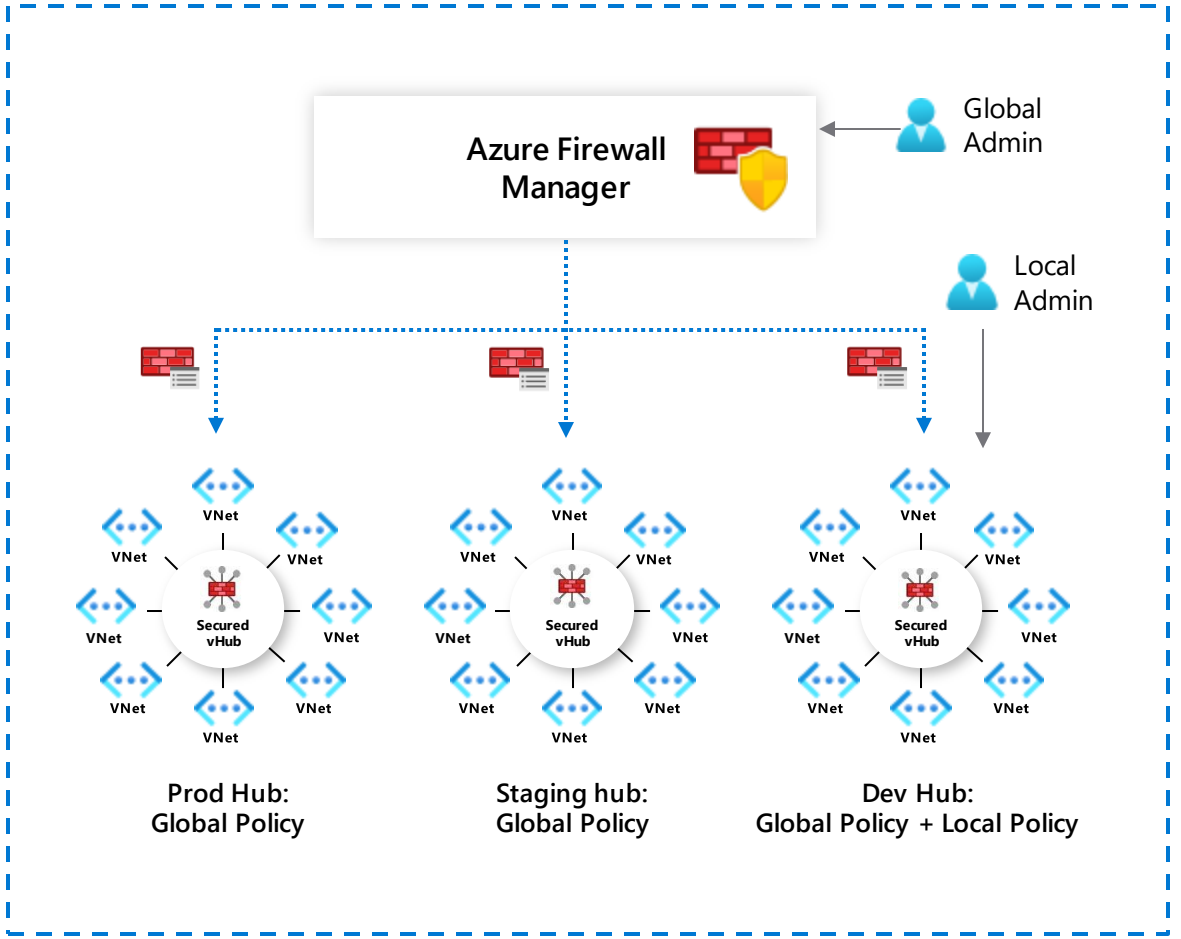
Manage Network address translation (NAT), network, and application rule collections, as well as threat intelligence and DNS settings.

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.



Multi security provider support (secure hub only)

Combine best of breed security

Azure Firewall for east-west (virtual network to virtual network/branch to virtual network) traffic filtering.

Security partner of your choice for north-south (virtual network to Internet/branch to Internet) traffic filtering.

Use Azure for Edge security

Avoids routing internet traffic to on-premise.

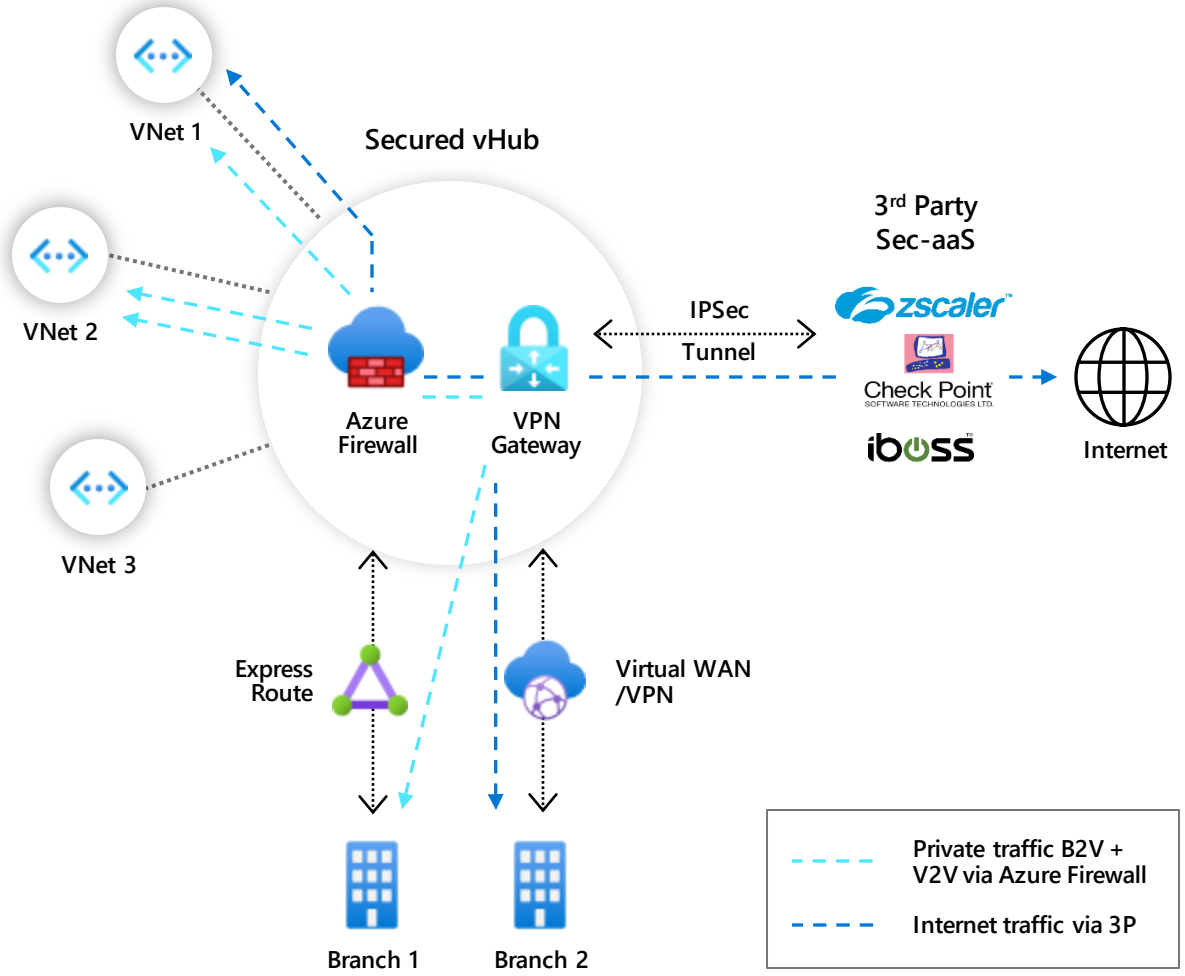
Route internet traffic directly from Azure.

Partners

- **Zscaler (currently runs on ZIA cloud, roadmap to run on Azure)**
- **Check Point (runs on Azure)**
- **iboss (runs on Azure)**

Simplifies connectivity and security

Easily attract traffic to your secured virtual hub for filtering and logging without manipulating User Defined Routes.



Azure Firewall pricing page

Firewall Pricing

Fixed Cost

$0.395/Basic firewall/hour

$1.25/Standard firewall/hour

$1.75/Premium firewall/hour

Variable Cost

$0.065/GB processed by the firewall (Basic)

$0.016/GB processed by the firewall (Standard & Premium)

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 Manager pricing page

Firewall Manager GA Pricing

Azure Firewall in Secured Virtual Hubs

Fixed fee: $1.25/firewall/hour

Variable fee: $0.016/GB processed by the firewall

Azure Firewall Manager policies

Fixed fee: $100/Policy/Region

Policies that are associated with a single hub are free of charge

Policy Analytics

Azure Firewall Manager 3rd party integration

Fixed fee: $0.4/Secured hub/hour

Virtual WAN VPN GA charges apply

Microsoft

Azure Firewall Premium

Azure Firewall Premium

Cloud native next-gen Firewall as a service

TLS Inspection

Built-in TLS Inspection for Outbound and East-West traffic

Inbound TLS termination is supported with Azure Application Gateway

Customer provided key pair via Azure Key Vault integration

Intrusion Detection Prevention System (IDPS)

Detect alert and block inbound/outbound malicious traffic

Supported for both encrypted and plain text protocols

Signature-based detection that is continuously updated

URL Filtering

Restrict user access to HTTP/HTTPS Web content

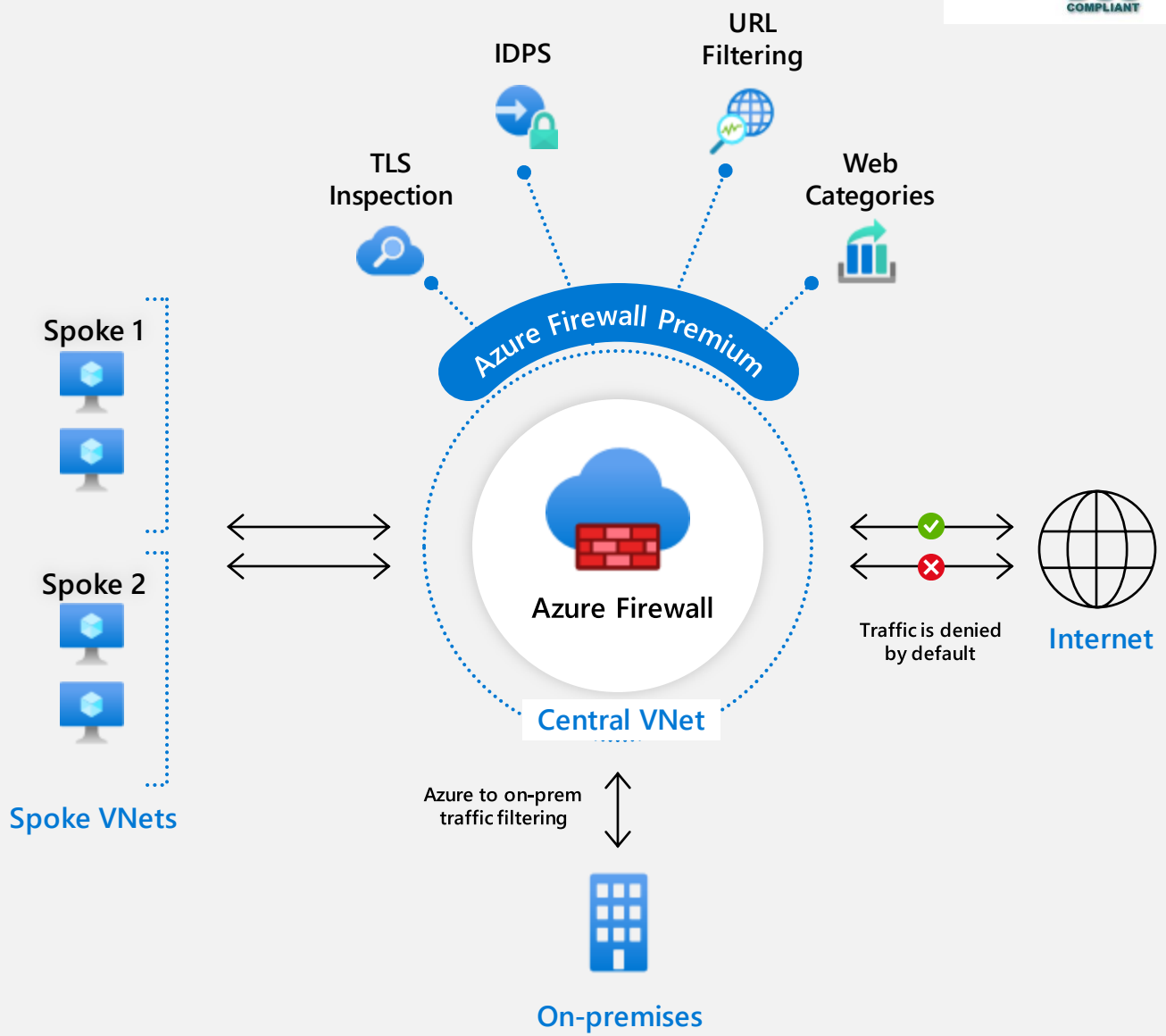
Support for URL wildcards

Web Categories

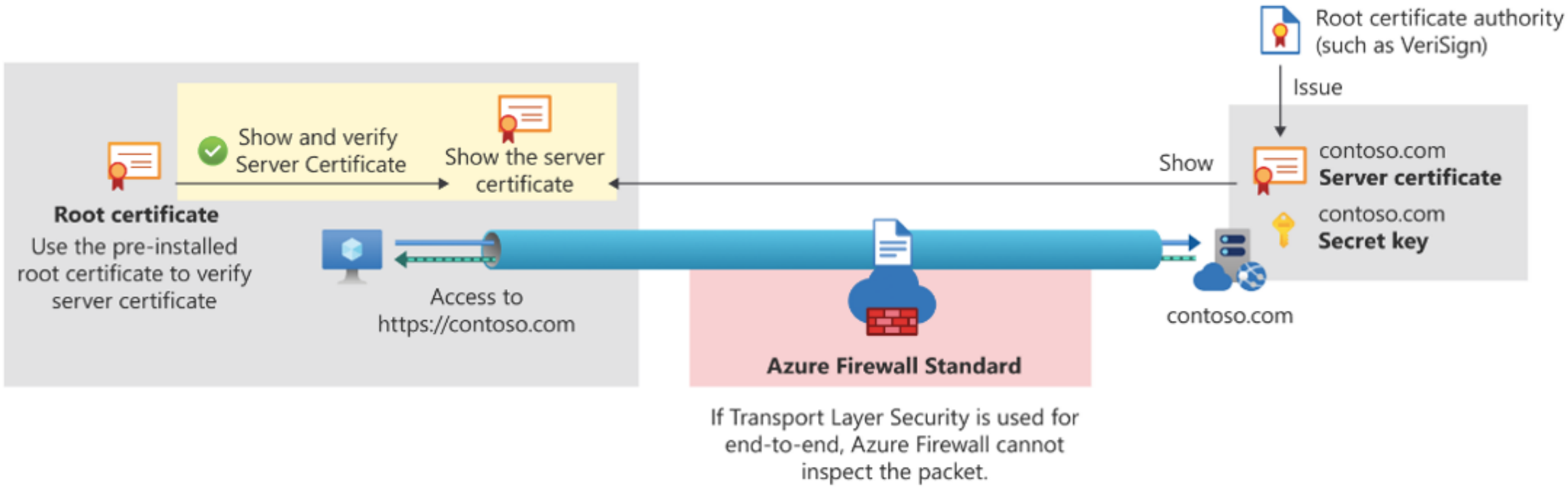
Allow or deny user access to website categories such as gambling, social media and others

Web categories maintained and continuously updated

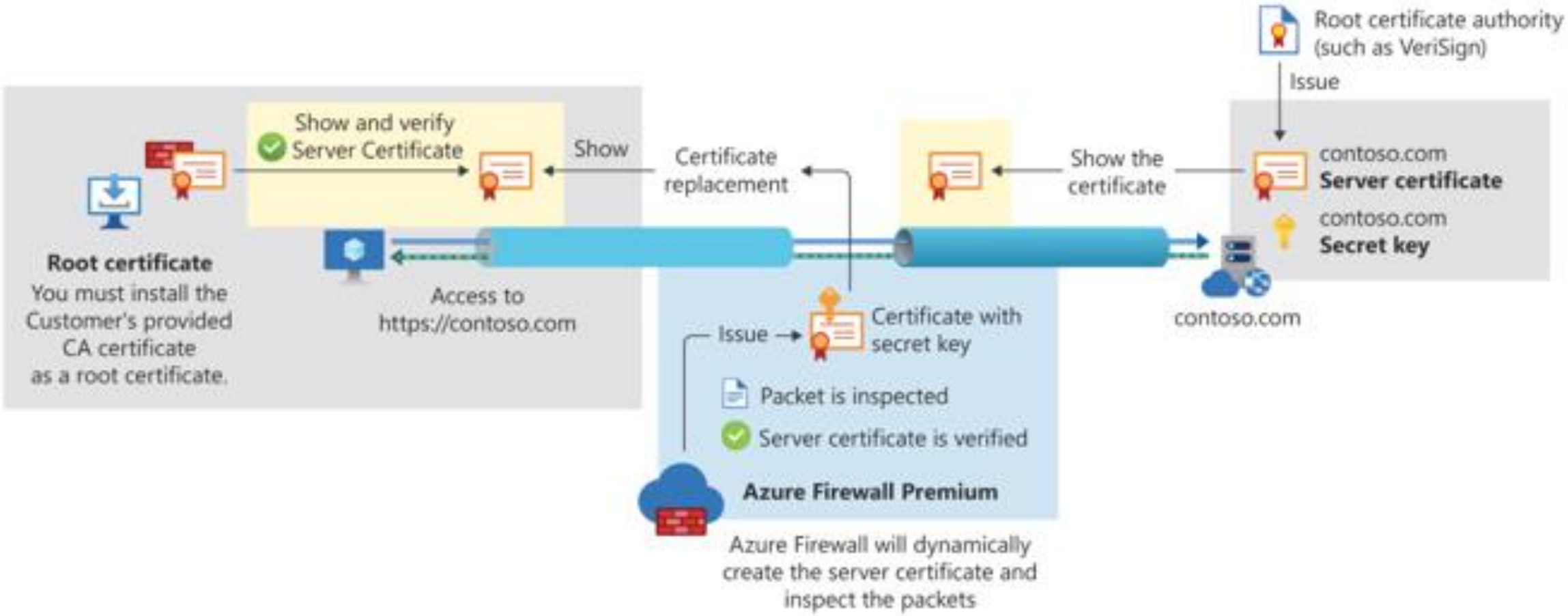
URL based category matching



Azure Firewall Premium – without TLS Inspection

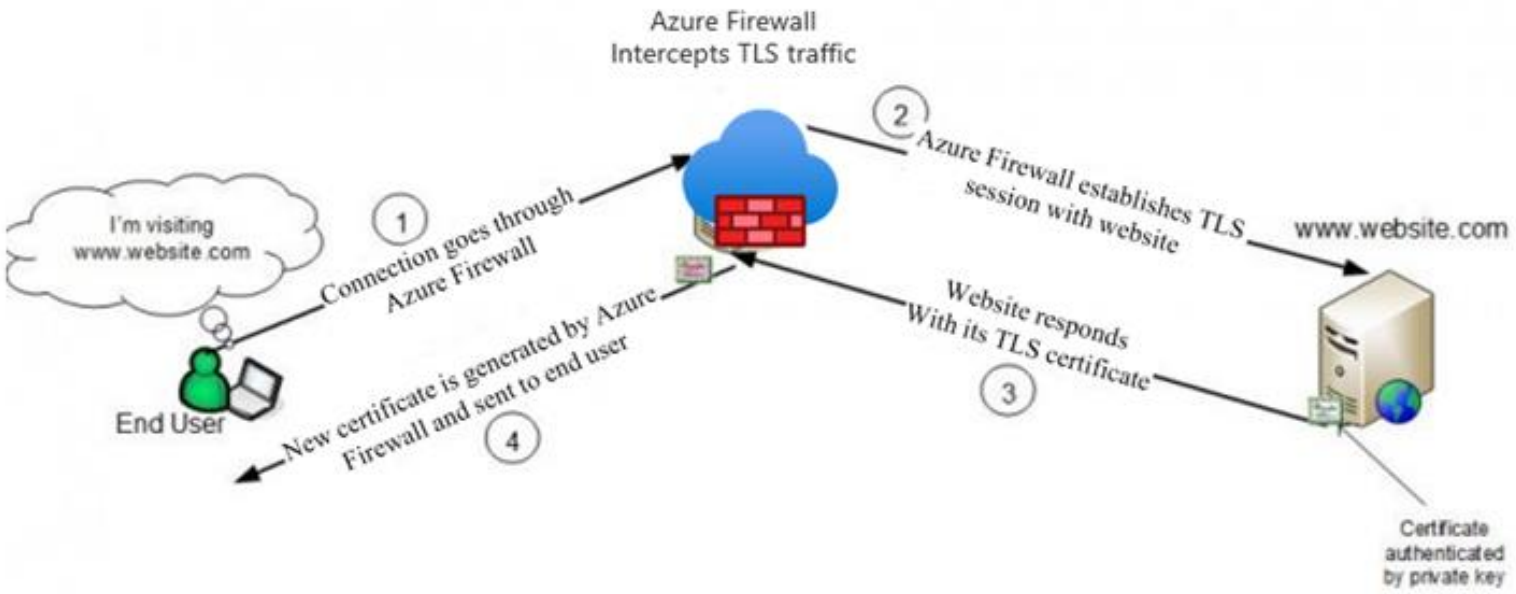


Azure Firewall Premium – TLS Inspection

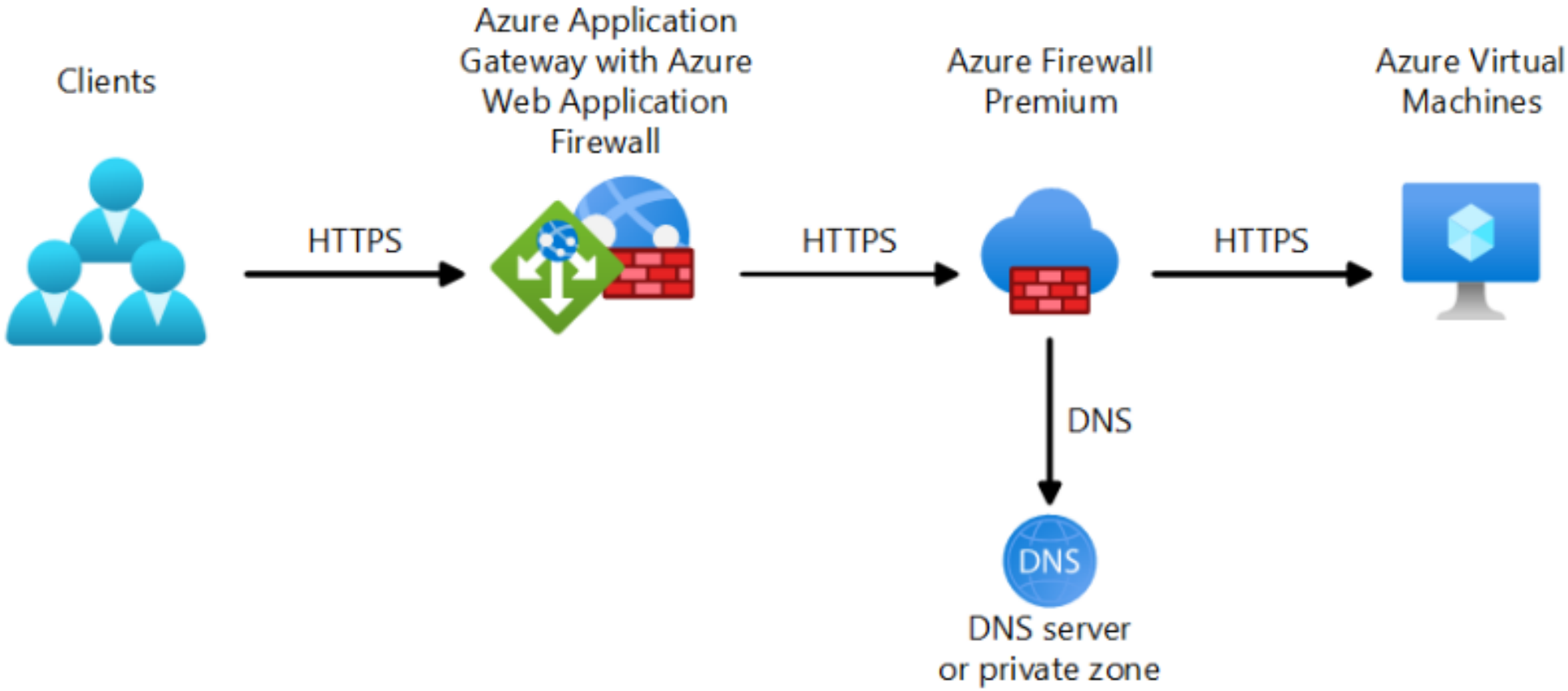


Azure Firewall Premium – TLS Inspection

- Azure Firewall intercepts outbound traffic for inspection
- Intermediary certificate should be uploaded to the Firewall to verify server certificate.

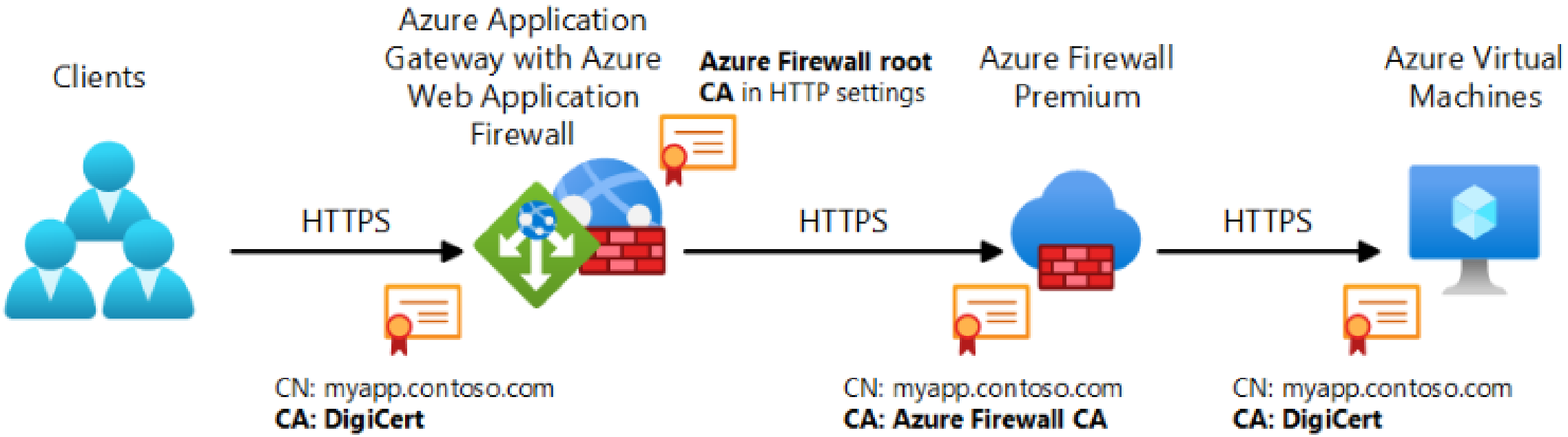


Azure Firewall with web applications



Microsoft Azure

Azure Firewall with web applications

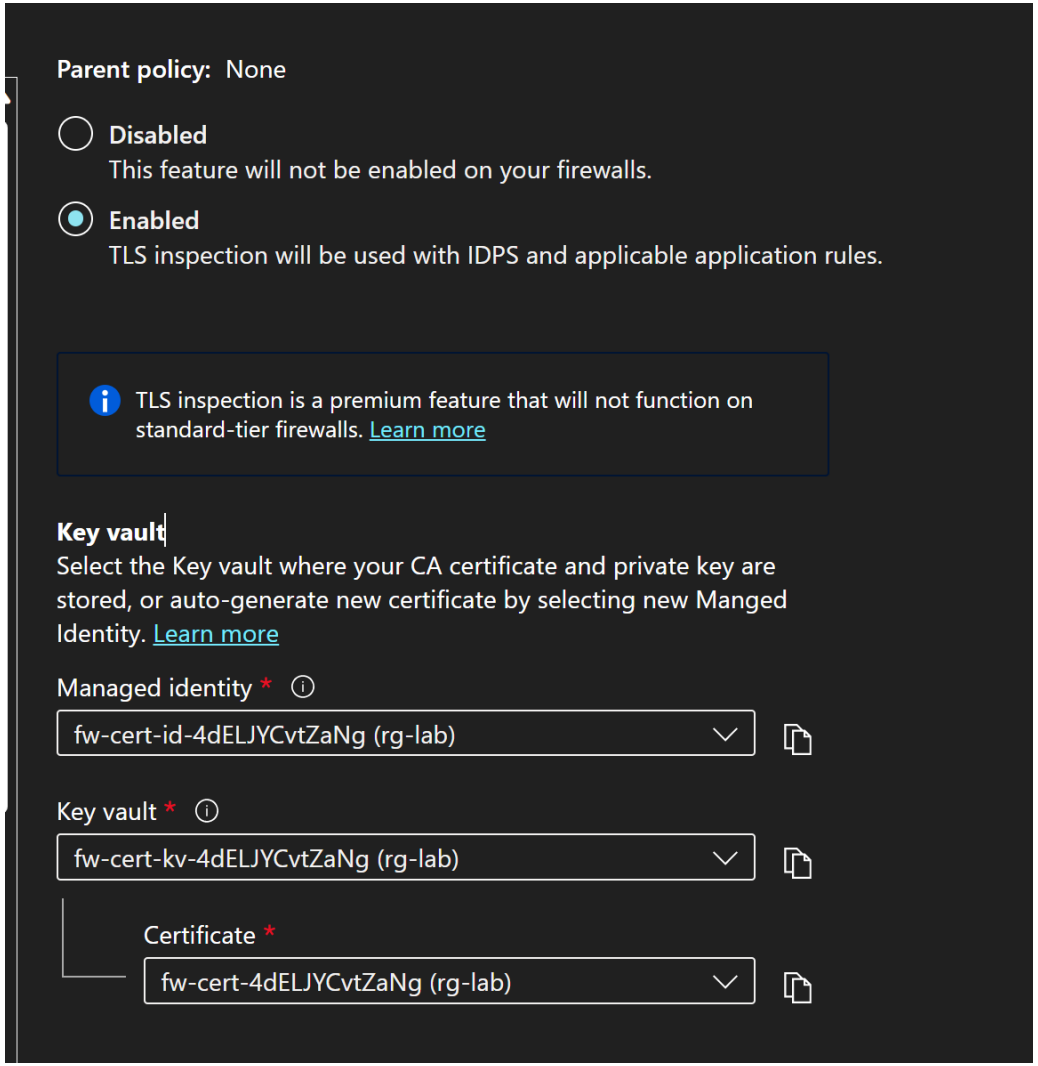


Microsoft Azure

Azure Firewall Premium – TLS Inspection

Enable TLS Inspection in Firewall Policy

Key Vault Integration



Azure Firewall Premium

Cloud native next-gen Firewall as a service

Intrusion Detection Prevention System (IDPS)

Detect alert and block inbound/outbound malicious traffic

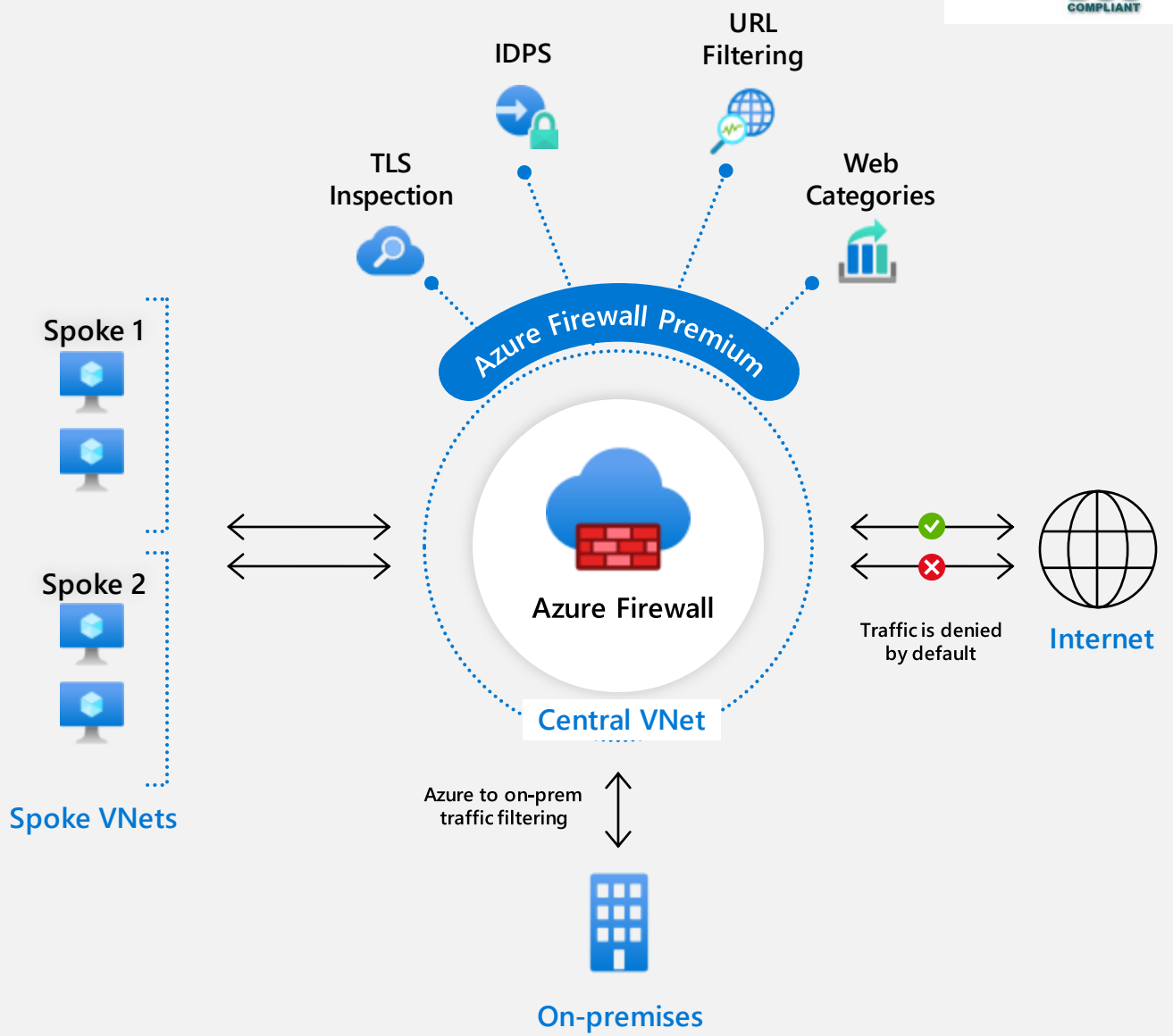
Signature-based detection that is continuously updated

Over 58,000 rules in over 50 categories

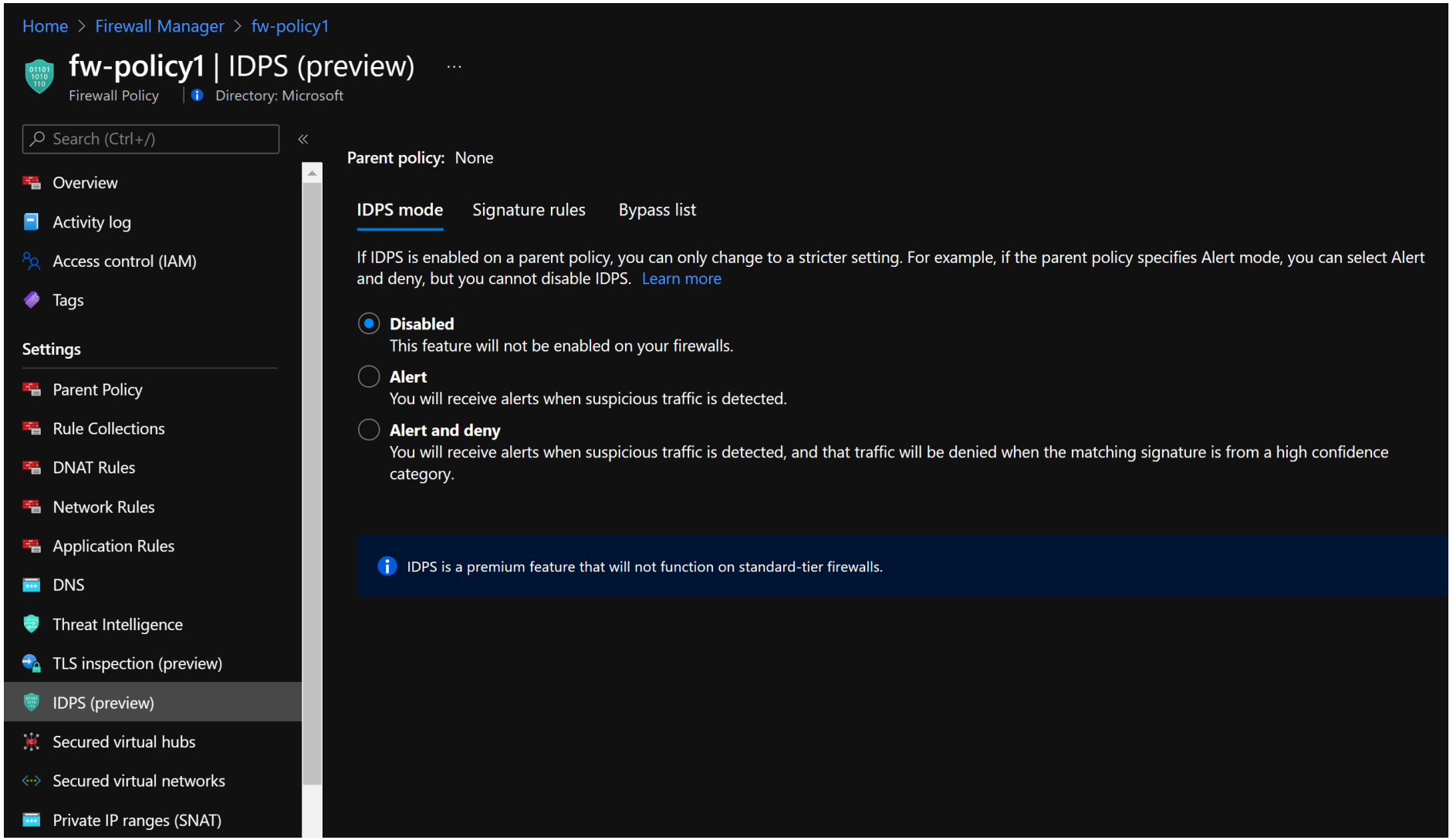
Detection and Prevention mode

IDPS Bypass List

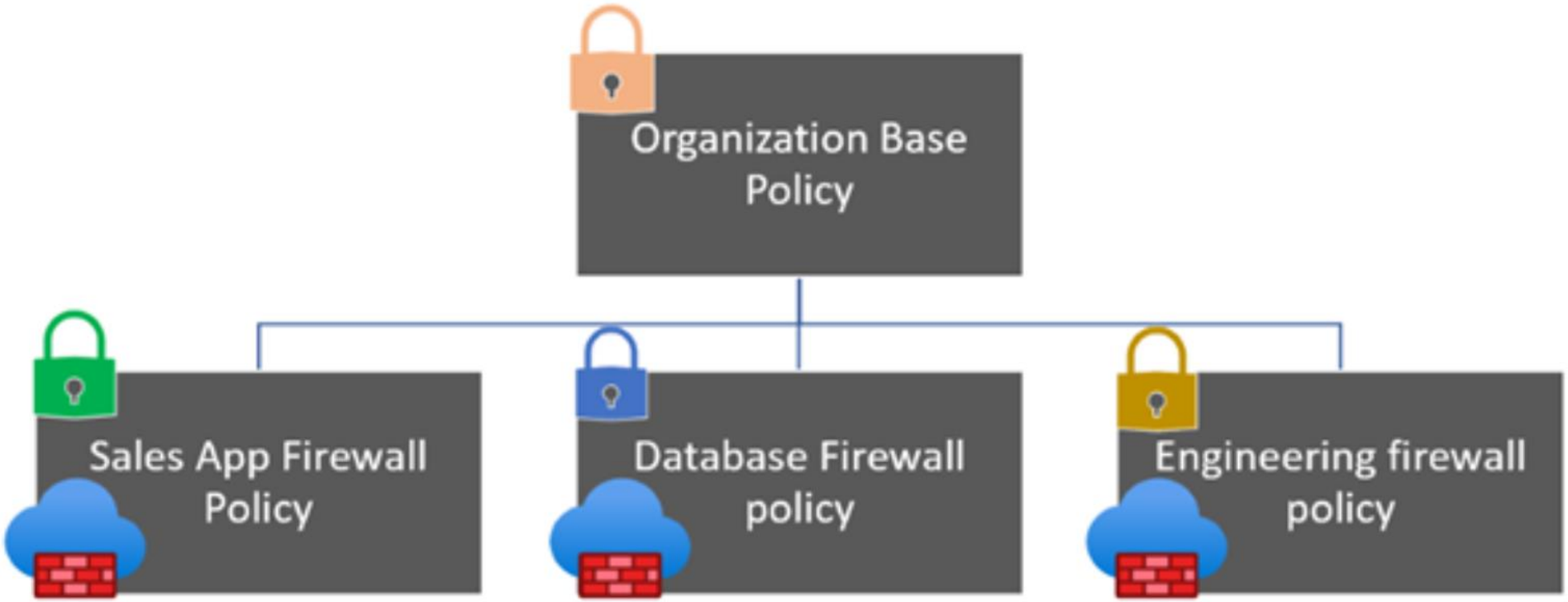
IDPS Private IP ranges (preview)



Azure Firewall Premium Configuration

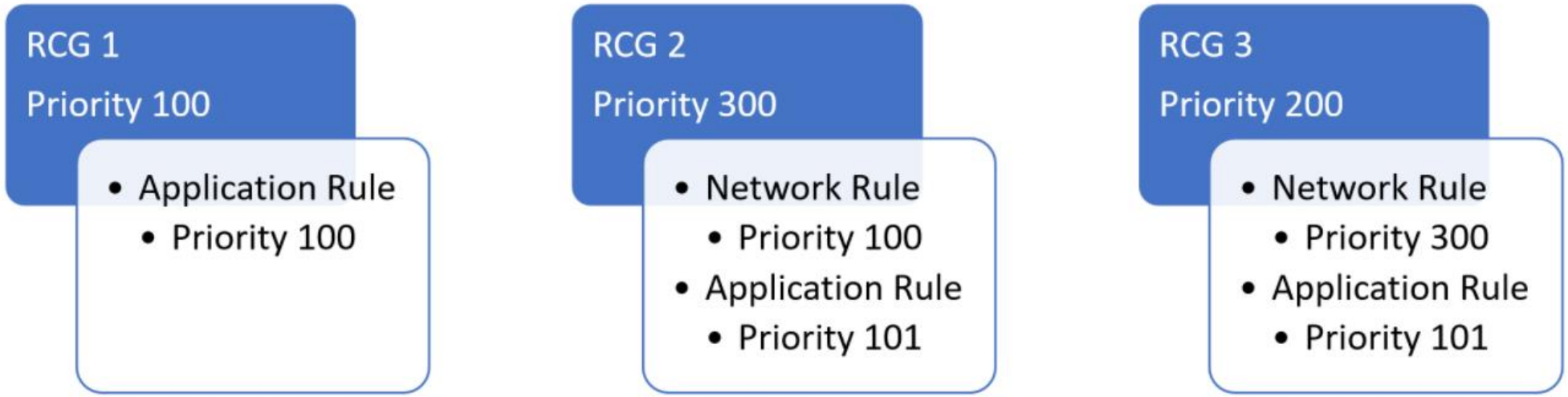


Azure Firewall Policy



Azure Firewall

Rules Processing Logic



Execution order:

Policy Analytics Preview

Manage Azure Firewall rules over time

Policy Insights

- Highlights key information of the Firewall policy such as Policy limits, Duplicate rules, Wildcard in rules and more.

Policy Recommendations

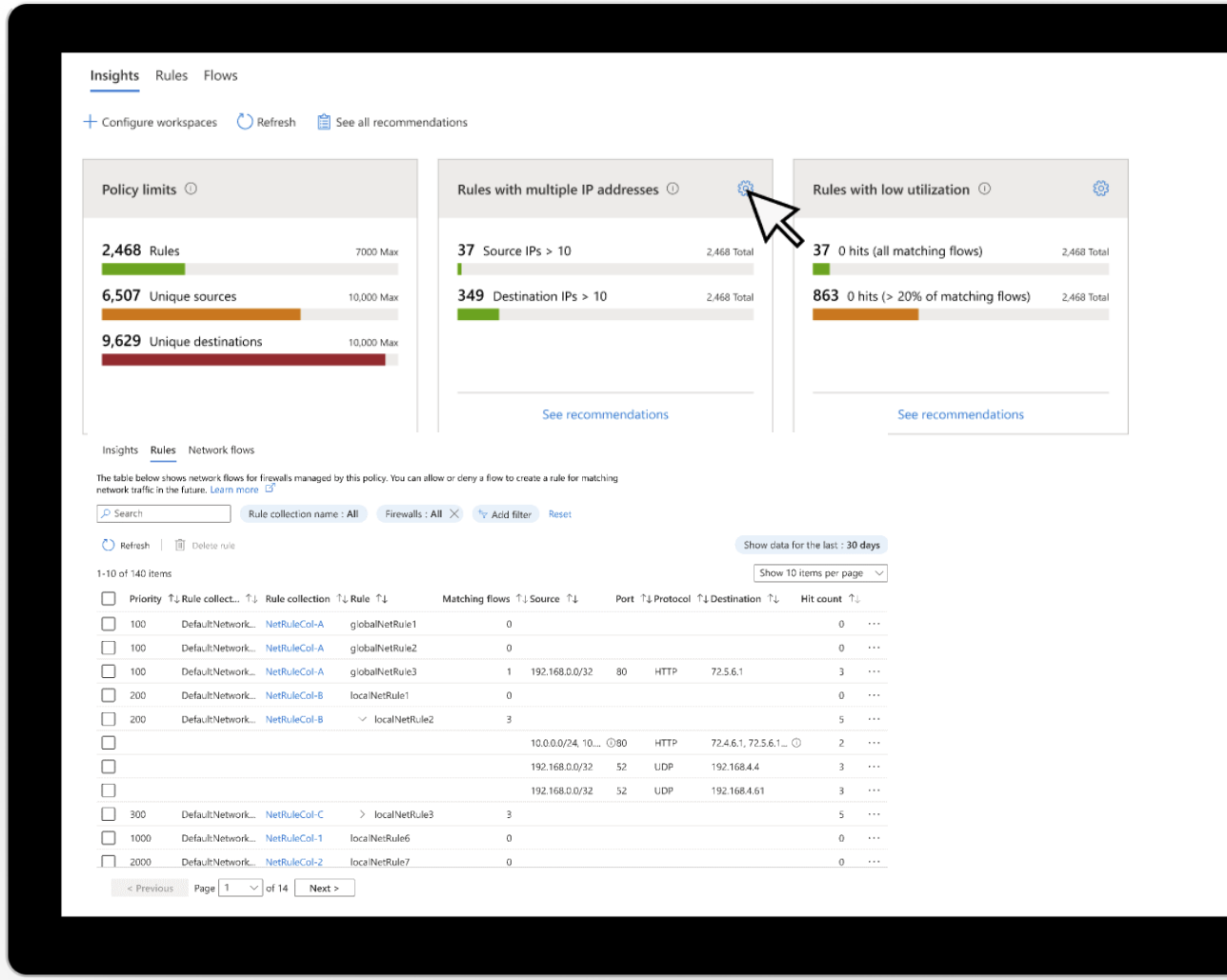
- Recommendations to improve the Rules in the policy including rules with low/no hits, overly permissive rules, potentially malicious sources.

Rule Analytics

- Visibility into the traffic flows of the rules over time
- Rule hit count for Application, Network and DNAT rules

Single Rule Analysis

- Refine the rules permissions
- Inspect the flows hit per a specific rule



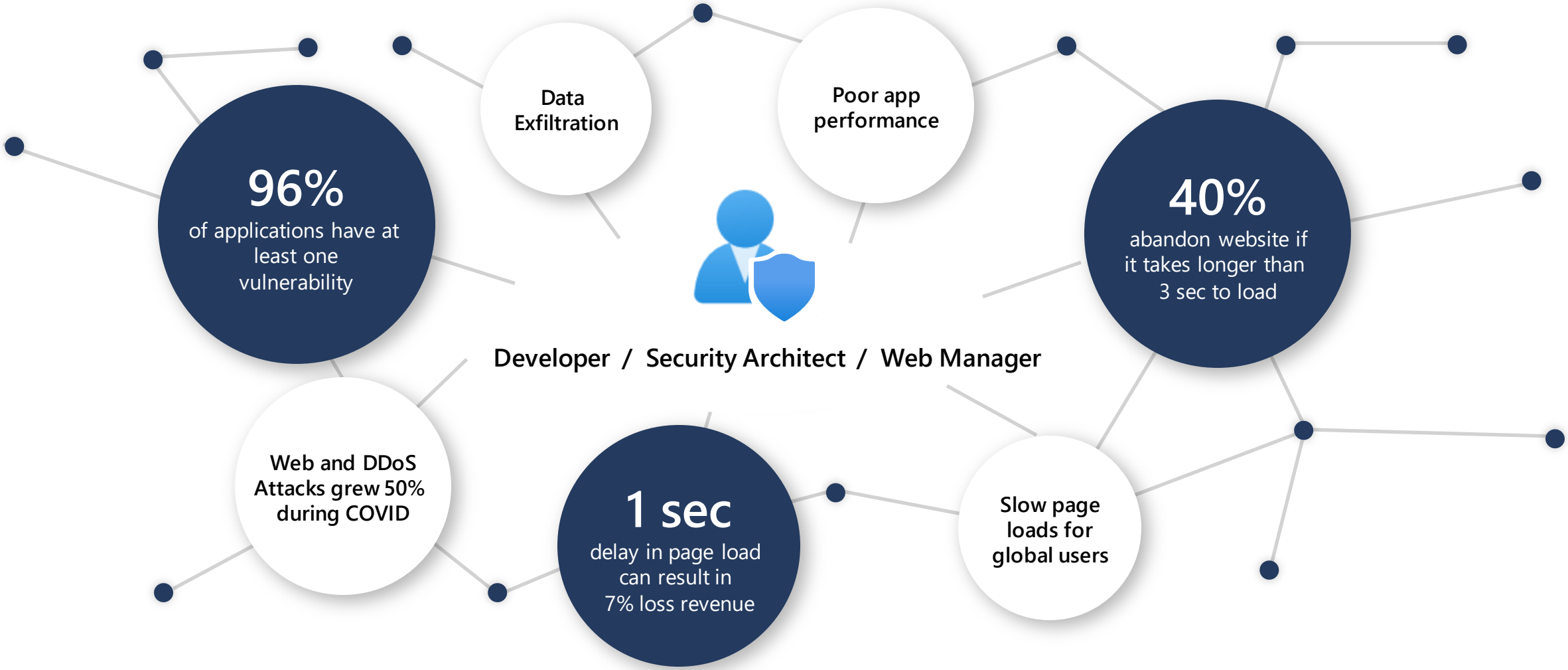
Microsoft

Azure Firewall Demo

Microsoft

Azure Web Application Firewall

Digital transformation brings about new challenges



Enterprises need a modern cloud CDN to protect, optimize and scale their applications

Azure web application protection

DDoS attacks

Web Application attacks

Malicious Bots

Global

Global footprint with non-HTTP/S traffic filtering

Azure Network Edges

Protects against common L7 web attacks

Azure WAF on Front Door

Legitimate traffic is allowed through

Azure Web Application Firewall combined with the global scale of Azure Network Edges provides protection from multiple attack types

Regional

L3/L4 DDoS Mitigation Tuned to App Traffic Patterns

Azure DDoS Standard

Protects against common L7 web attacks

Azure WAF on Application Gateway

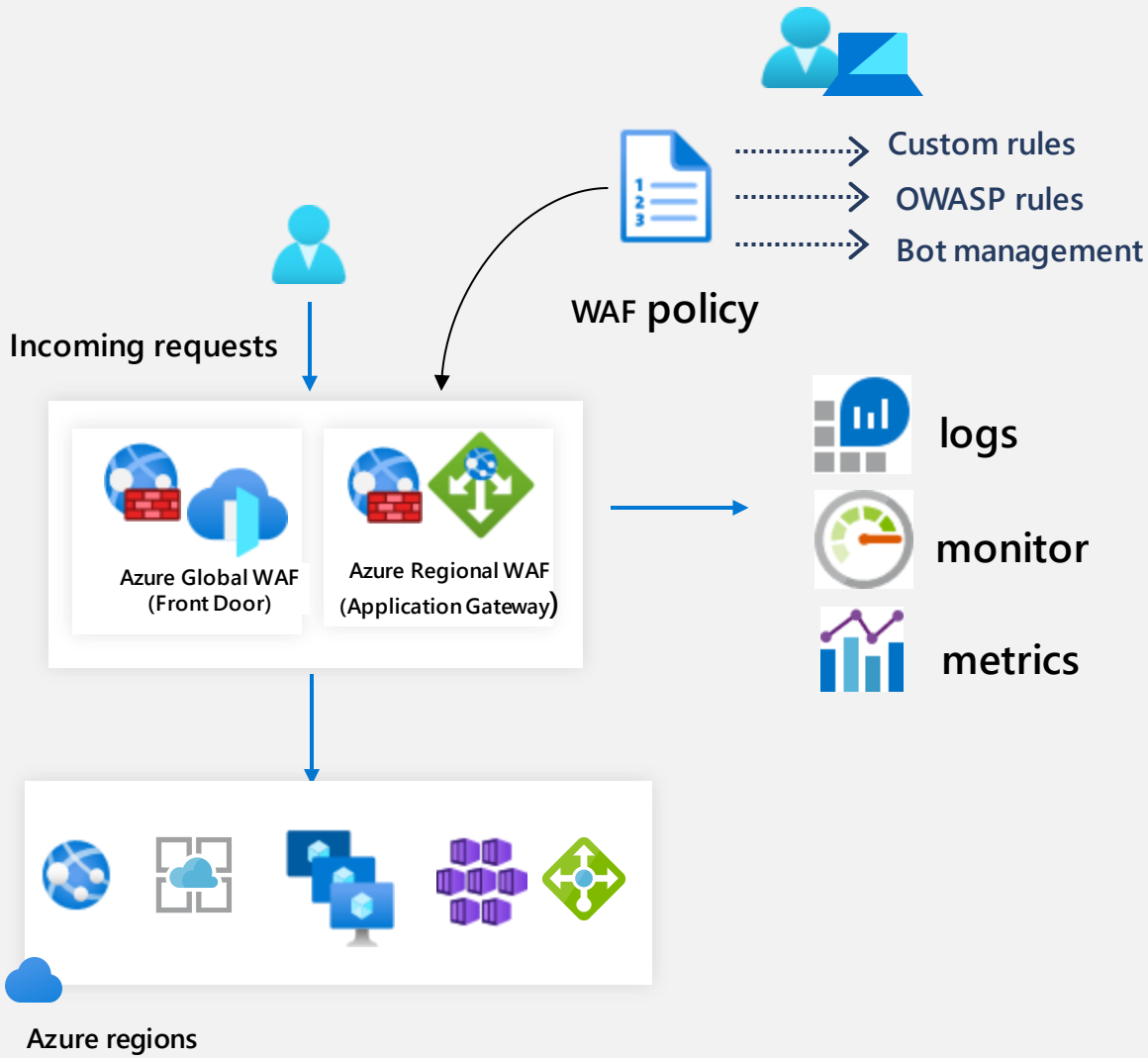
Legitimate traffic is allowed through

Azure DDoS Protection Standard combined with Azure Web Application Firewall provides adaptive protection from multiple attack types

Azure Web Application Firewall

Intelligent application protection

- ✓ Managed rulesets powered by Microsoft Threat Intelligence to protect against OWASP top 10
- ✓ Powerful custom rules engine
  - Geo-filtering
  - IP restriction
  - http parameters filtering
  - size restriction
- ✓ Bot protection with Microsoft Threat Intelligence
- ✓ Conditional rate limiting at Azure network edge
- ✓ Built-in DDoS Protection
- ✓ Easy configuration: Portal, API, PS, Cli, Terraform



Azure Front Door

Modern cloud CDN that delivers optimized experiences to users anywhere

Modern Architecture

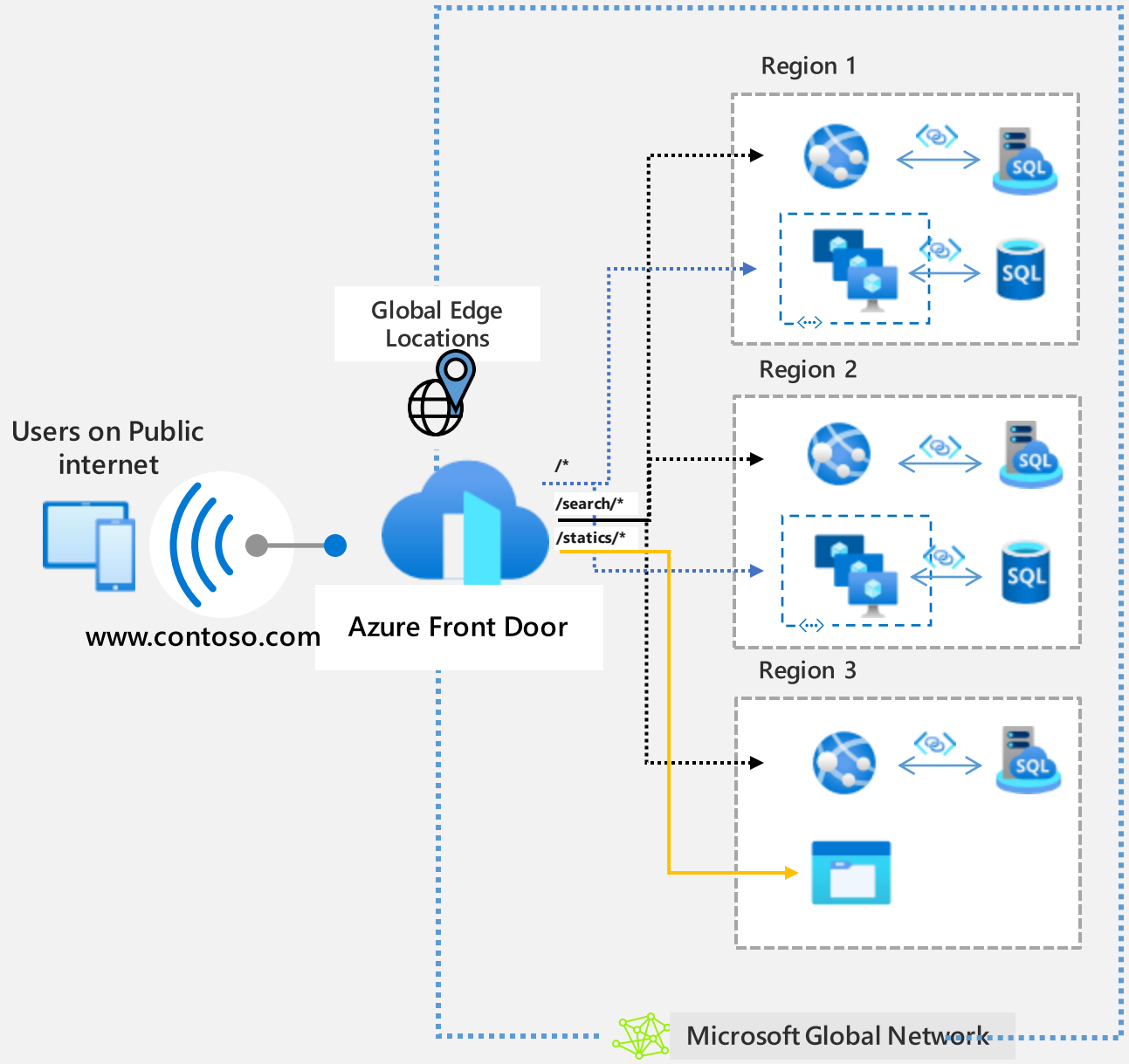
- Fully REST API driven to automate and streamline deployment
- Tight integration with Azure services including App Service, Storage, API Manager, App Gateway and Azure Sentinel
- Customizable rules for advanced routing
- Advanced analytics to monitor traffic and security in real time

Fast Global Delivery

- Low latency, high throughput content delivery from cloud or on-prem to global users
- Built on Microsoft massively-scaled private global network
- Supports static/dynamic content caching, file, OTT and video on-demand
- SSL offload and dynamic app acceleration at the edge close to user
- Simplified cost model with fewer meters to plan for

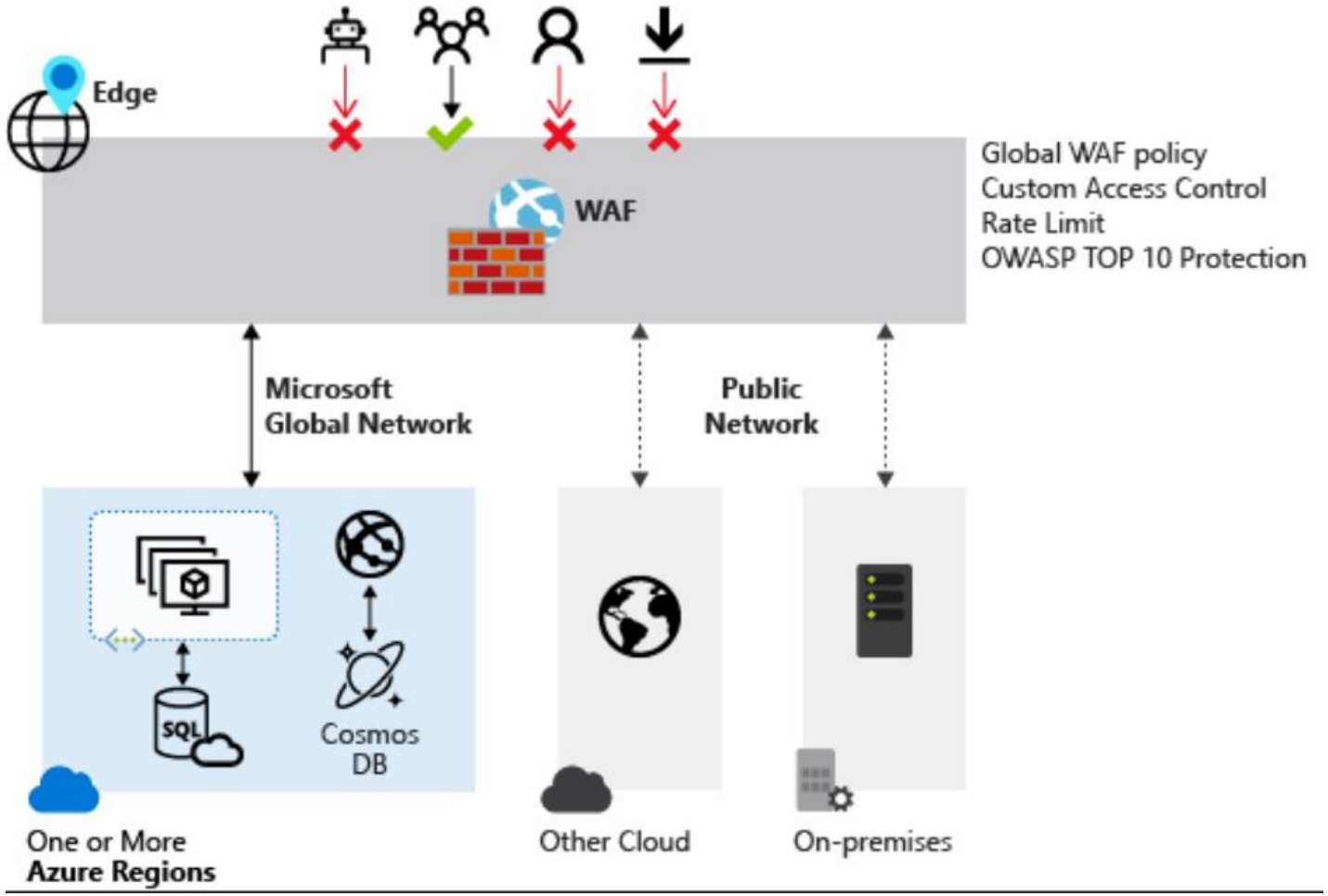
Intelligent Security

- WAF, DDoS and Bot Manager protection
- Azure Private Link support to access resources securely
- Powered by Microsoft Threat Intelligence



Azure Front Door WAF

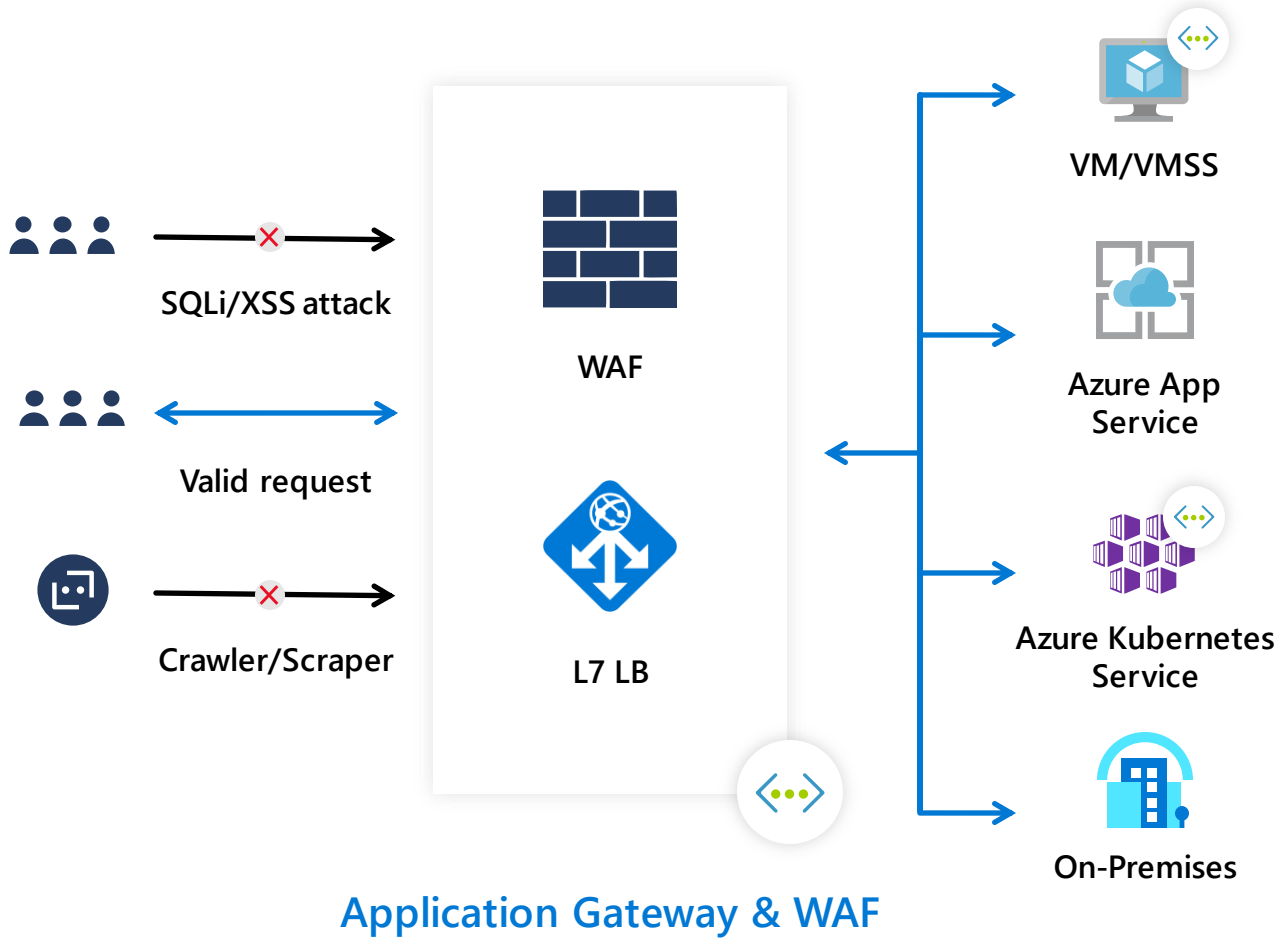
1. Global and centralized WAF
2. Prevents malicious attacks close to the attack sources
3. Custom and managed rules
4. Fully Integrated with the Premium SKU. Standard SKU limited to custom rules.
5. Rate limiting
6. BLOCK, ALLOW, LOG, REDIRECT Actions
6. Bot Protection



Azure WAF with Application Gateway

Protect from common application vulnerabilities

1. Highly available, autoscaling, fully platform managed
2. Native in region and intra-VNet/hybrid integration
3. Support public IP, private IPs, cross region, or on-premises backend pools
4. OWASP top 10 out of box protection
   CRS 3.0, CRS 3.1 , CRS 3.2
   Custom Rules supported
5. Rule configurability, exclusion lists, different rules sets, anomaly scoring
6. Near real time monitoring/alerting with Azure Monitor, Azure Security Center integration, Azure Sentinel integration



Azure Web Application Firewall

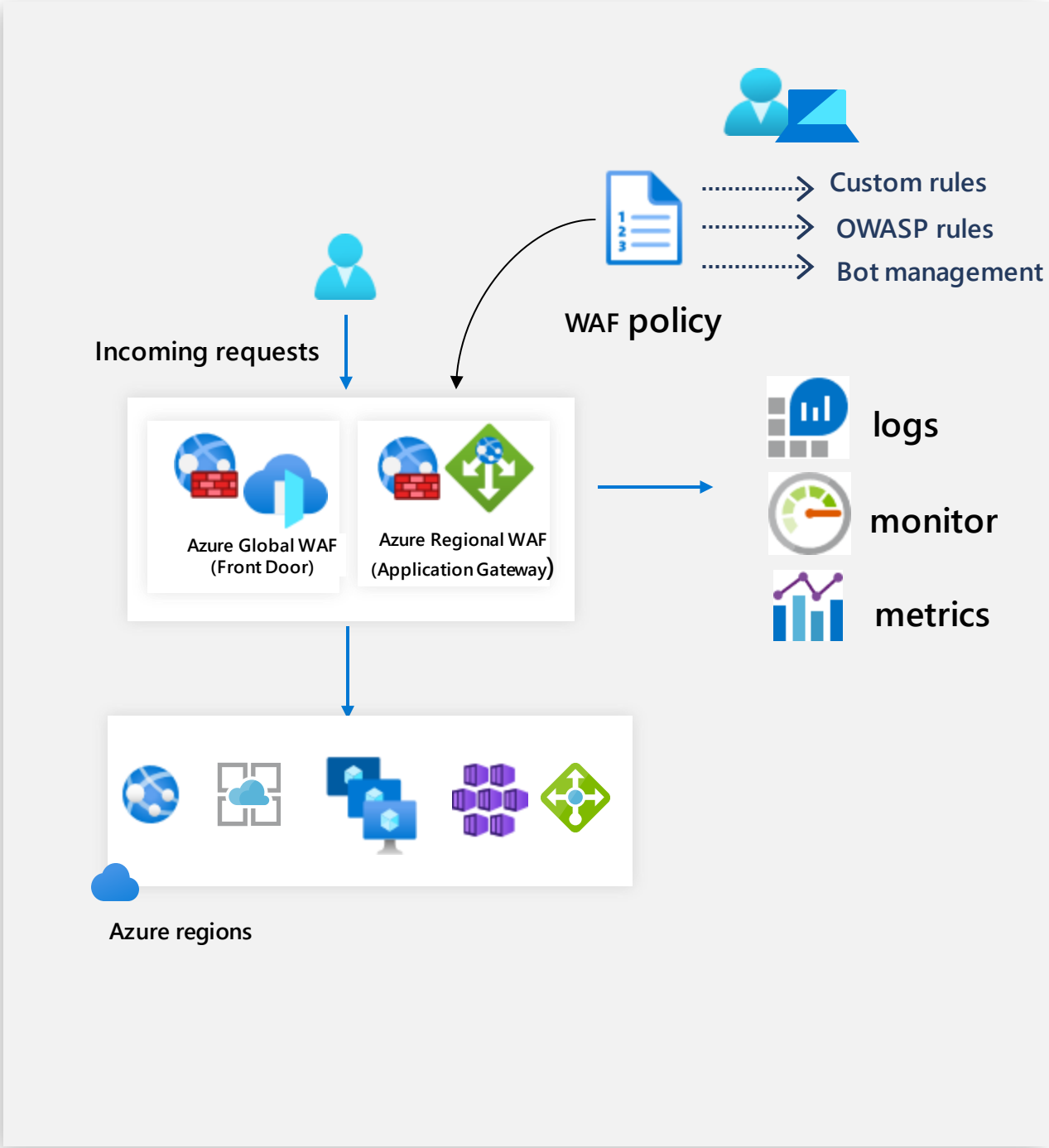
WAF modes

Detection mode

- Monitors and logs all threat alerts
- Does not block incoming requests
- Turn on Diagnostics and WAF logs

Prevention mode

- Blocks attacks identified by the rules
- “403 Unauthorized access” error



Different WAF Policy Categories

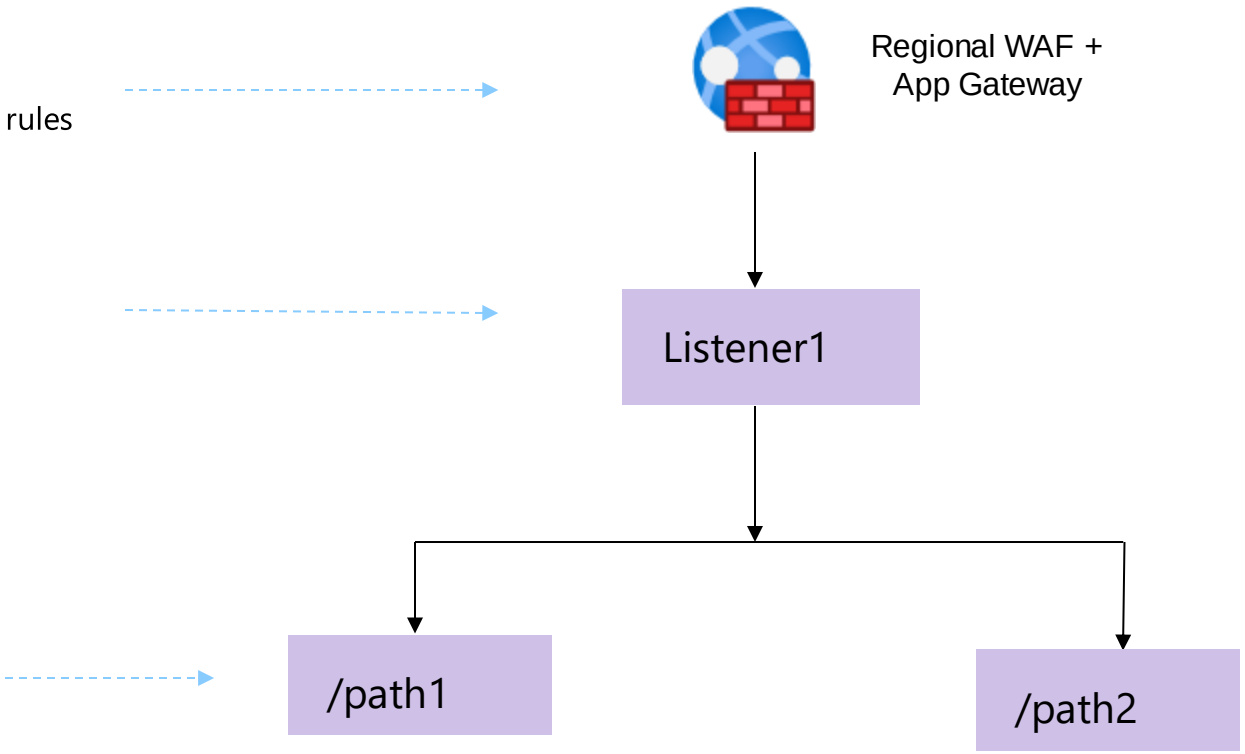
- Global WAF Policy
  - All sites in Application Gateway are protected with the same policy
- Per-Site WAF Policy
  - Each listener is protected by a WAF policy with unique custom rules, exclusions etc.
- Per-URI WAF Policy
  - URI level specific WAF configuration using Path Based Rule to manage access to resource

WAF Policies Demo

Global WAF Policy
Enable Managed Rules and Bot rules

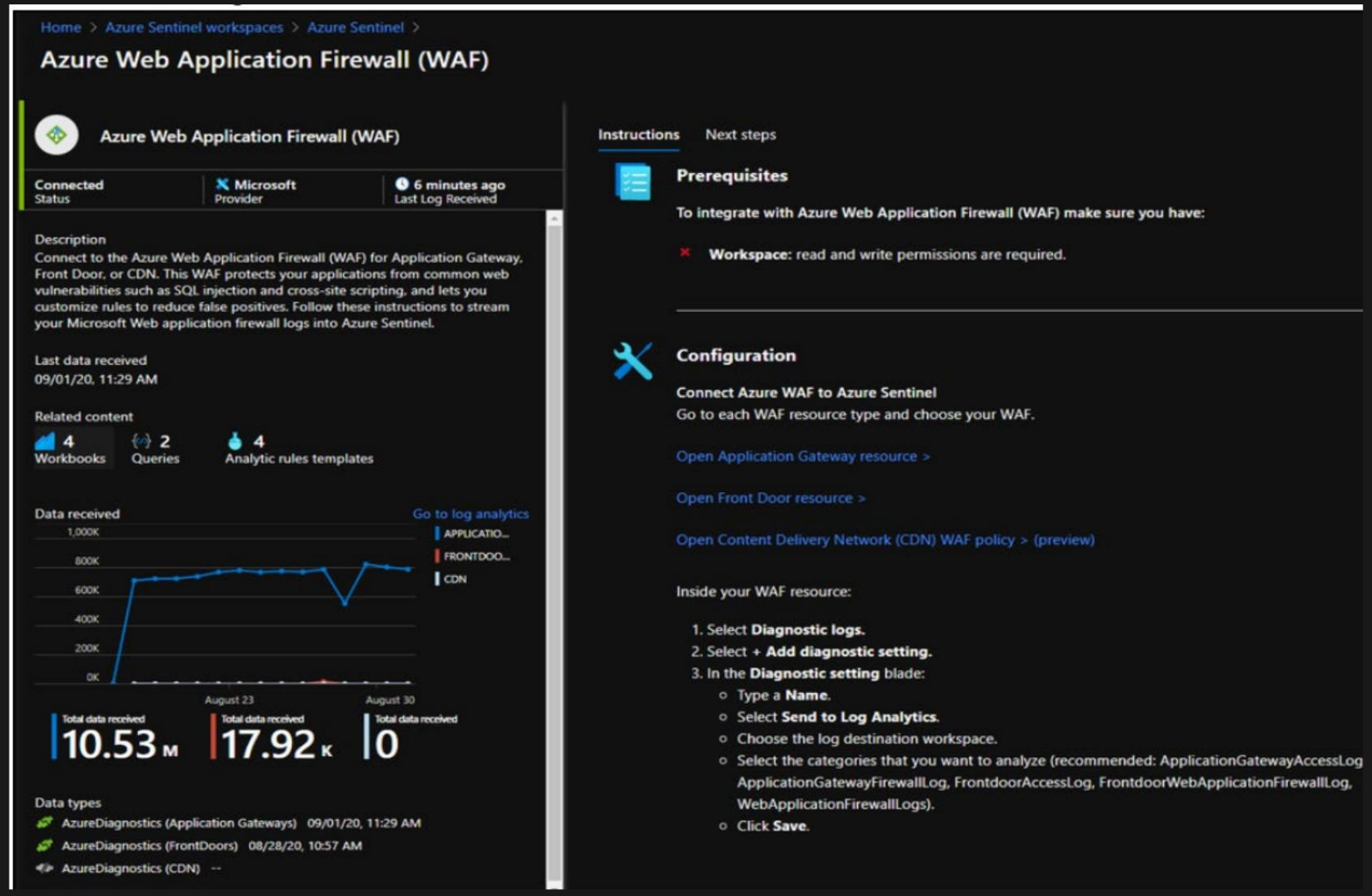
Per-site WAF Policy
Allow only US traffic

Per-URI WAF Policy
Allow specific IPs



WAF Integration

- Send WAF Data to Azure Sentinel
- Hunting Using WAF Data
- Generate Incidents using Azure
- Azure Sentinel Analytics
- Respond to Incidents with Playbooks
- Visualize with Azure Monitor Workbooks



Azure WAF Pricing with Application Gateway v2

	Web Application Firewall Application Gateway
Fixed	**$0.443** per gateway-hour
Capacity Unit[1]	**$0.0144** per capacity unit-hour

Microsoft Azure

Azure DDoS Protection

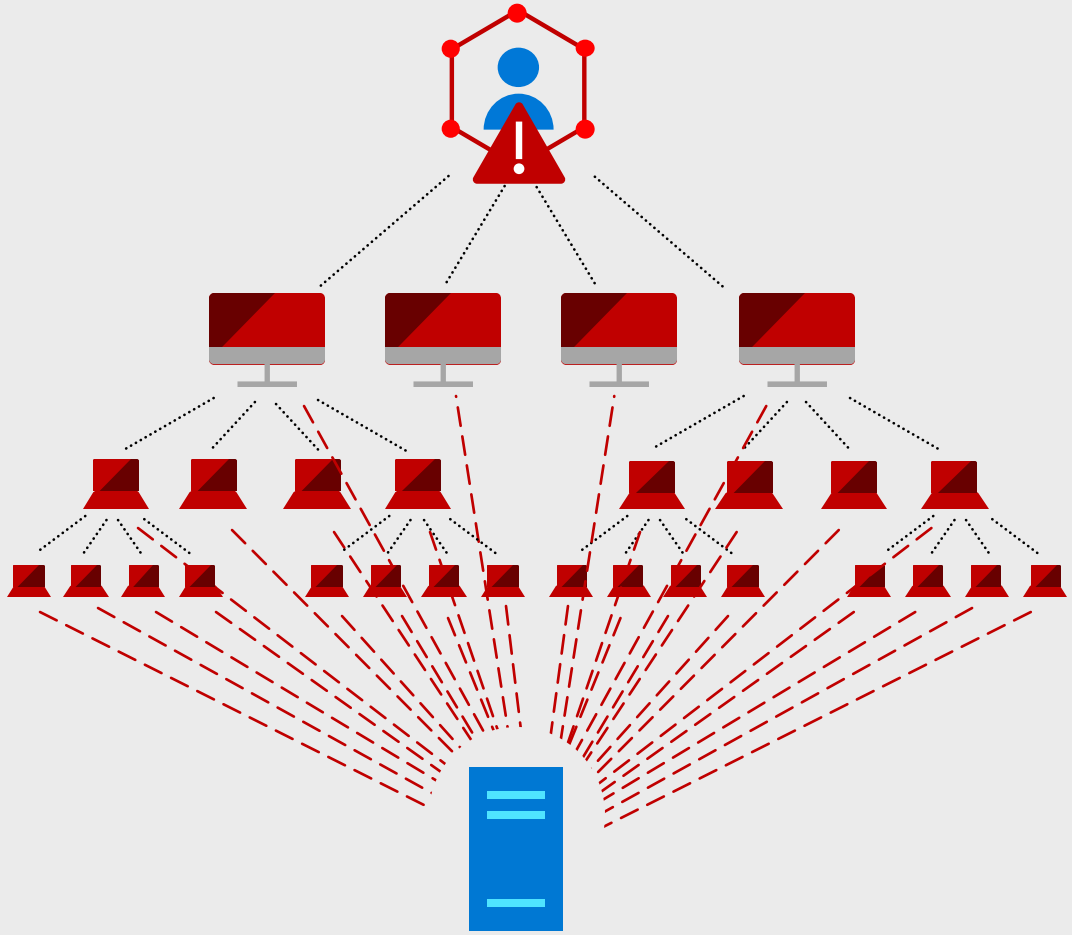
What are DDoS attacks?

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.

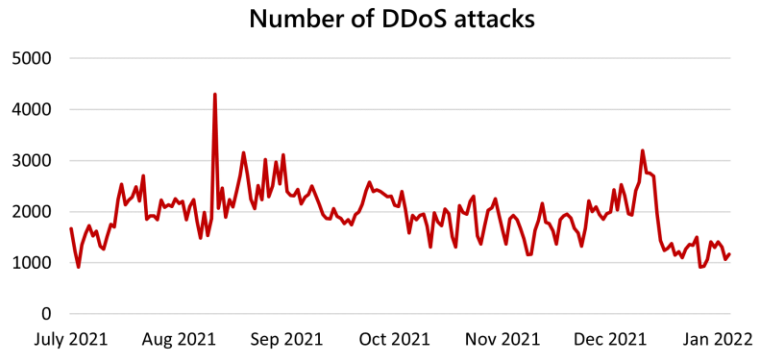
Top cause of availability issue for large enterprises.



How real are they?

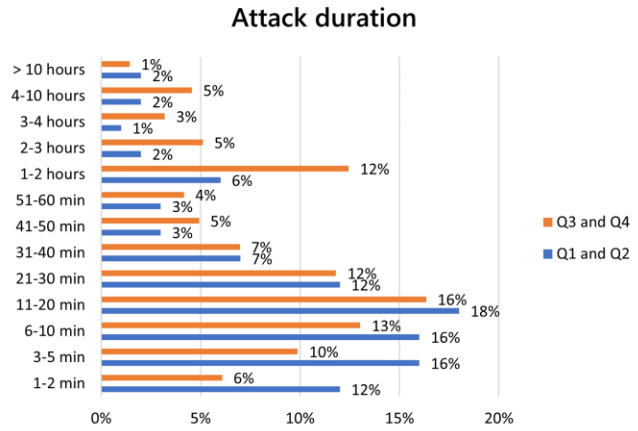
01

DDoS attacks increased by 43% in H2 of 2021



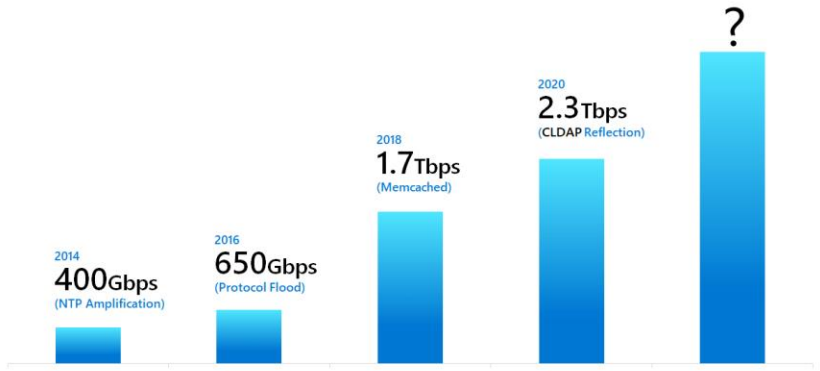
03

73% of DDoS attacks are under an hour



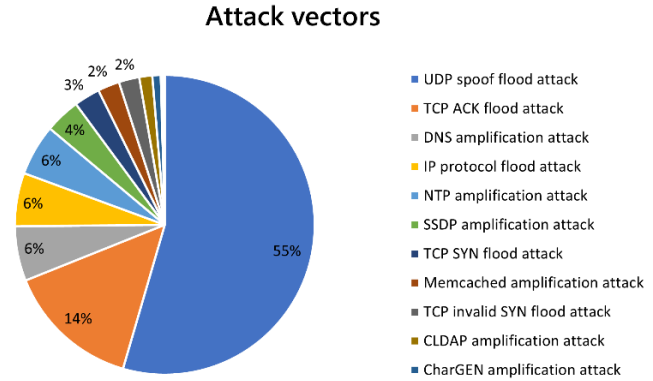
02

Attack bandwidth



04

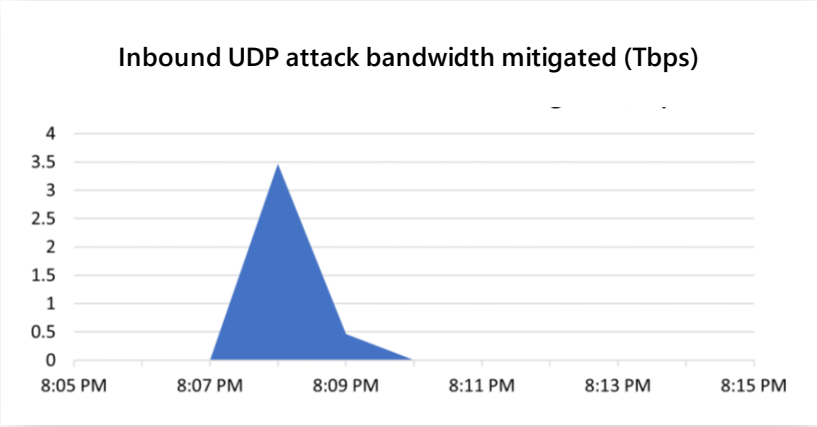
Attack vectors



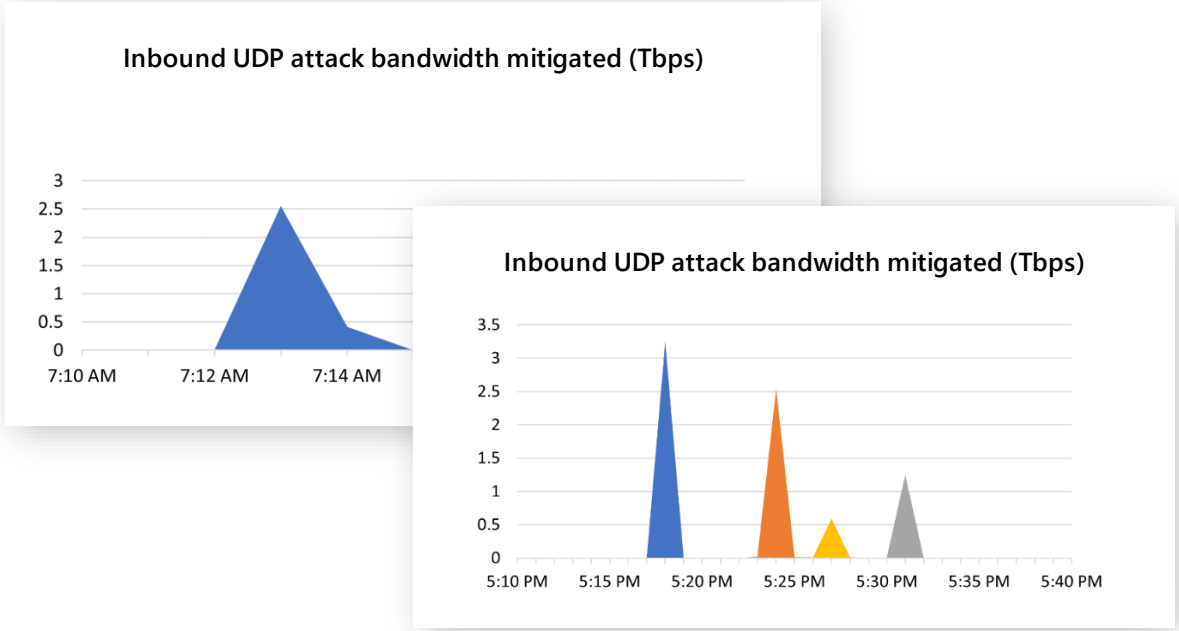
Source: Azure DDoS Protection—2021 Q3 and Q4 DDoS attack trends

CY2021 Holiday Season

On November 11, 2021, we mitigated a **3.47 Tbps (340M pps)** DDoS UDP attack in Azure, the largest attack ever reported in history!



In December, we mitigated two more attacks that surpassed 2.5 Tbps – one was a **3.25 Tbps** UDP attack, and the other attack was a **2.55 Tbps** UDP attack.



Azure DDoS Network Protection

Cloud scale DDoS protection for Virtual Networks in Azure

01 Azure global network

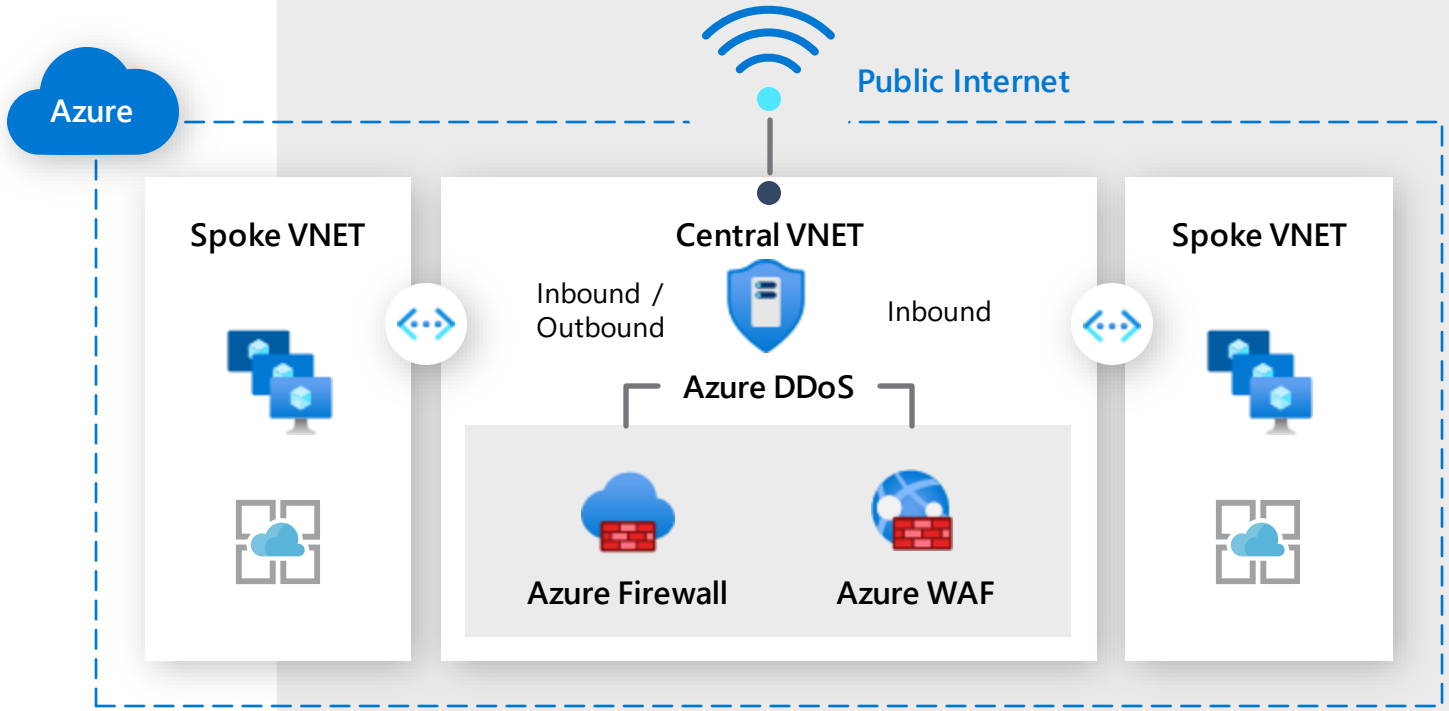
02 Adaptive tuning

03 Attack analytics & metrics

04 Integration with Microsoft Defender for Cloud & Sentinel

05 DDoS Rapid Response (DRR)

06 SLA guarantee and cost protection



Azure DDoS IP Protection (Preview)

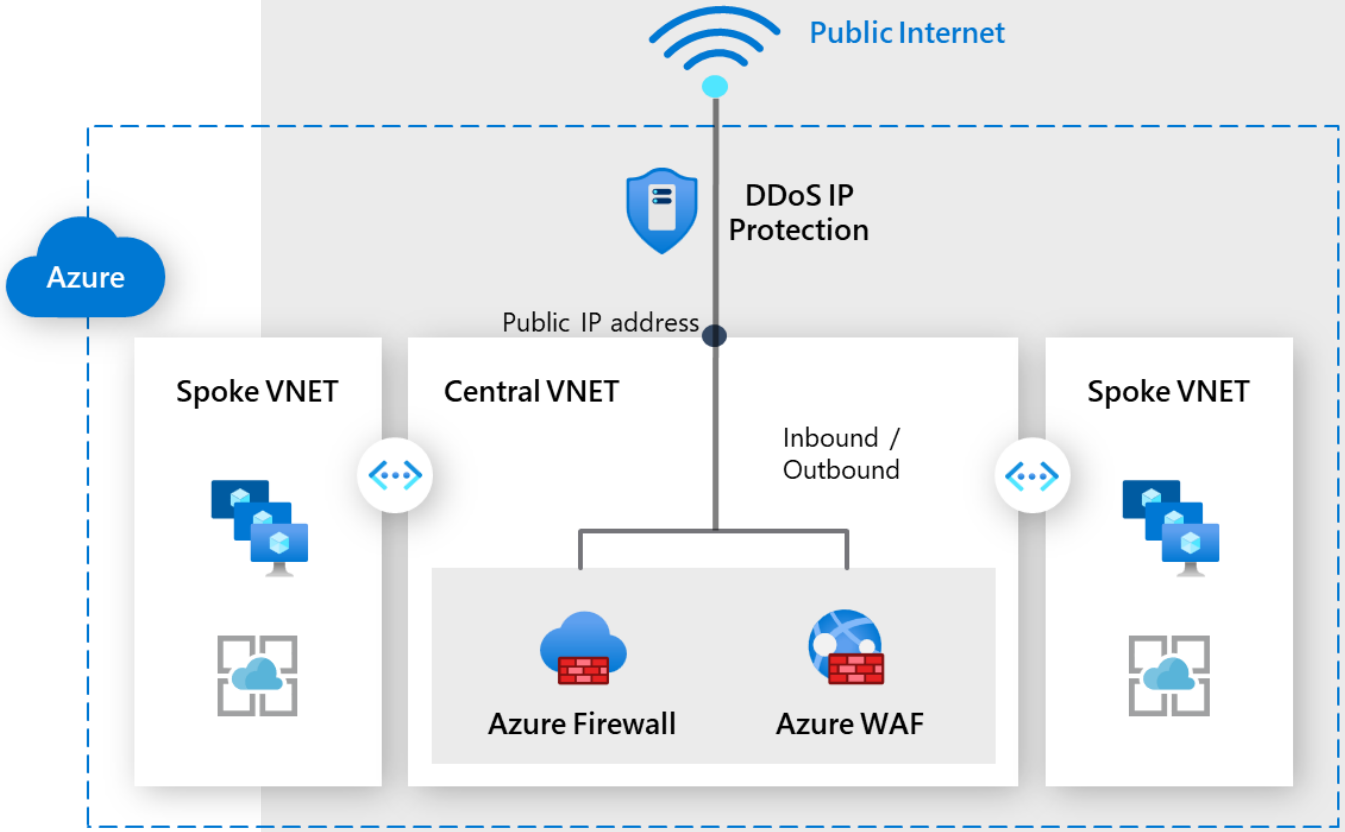
DDoS protection designed for small & medium businesses

01 Cost-effective, enterprise–grade DDoS protection

02 Flexibility to enable protection on an individual public IP resource

03 Easy to configure and monitor

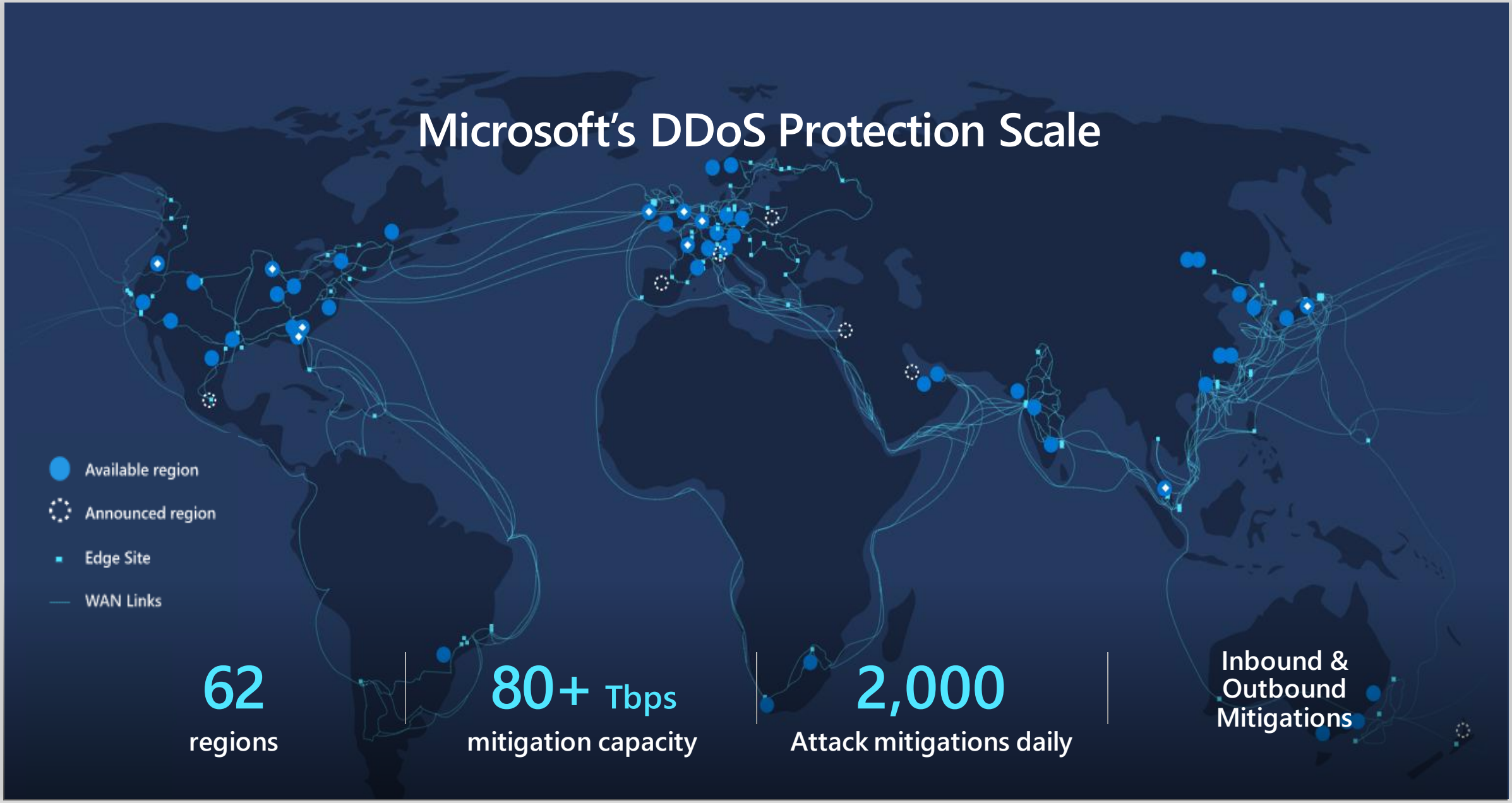
04 Integration with Microsoft Defender for Cloud & Sentinel



SKU comparison

Feature	DDoS IP Protection (Preview)	DDoS Network Protection
Active traffic monitoring & always on detection	✓	✓
L3/L4 Automatic attack mitigation	✓	✓
Automatic attack mitigation	✓	✓
Application based mitigation policies	✓	✓
Metrics & alerts	✓	✓
Mitigation reports	✓	✓
Mitigation flow logs	✓	✓
Mitigation policies tuned to customers application	✓	✓
Integration with Firewall Manager	✓	✓
Azure Sentinel data connector and workbook	✓	✓
DDoS rapid response support		✓
Cost protection		✓
WAF discount		✓

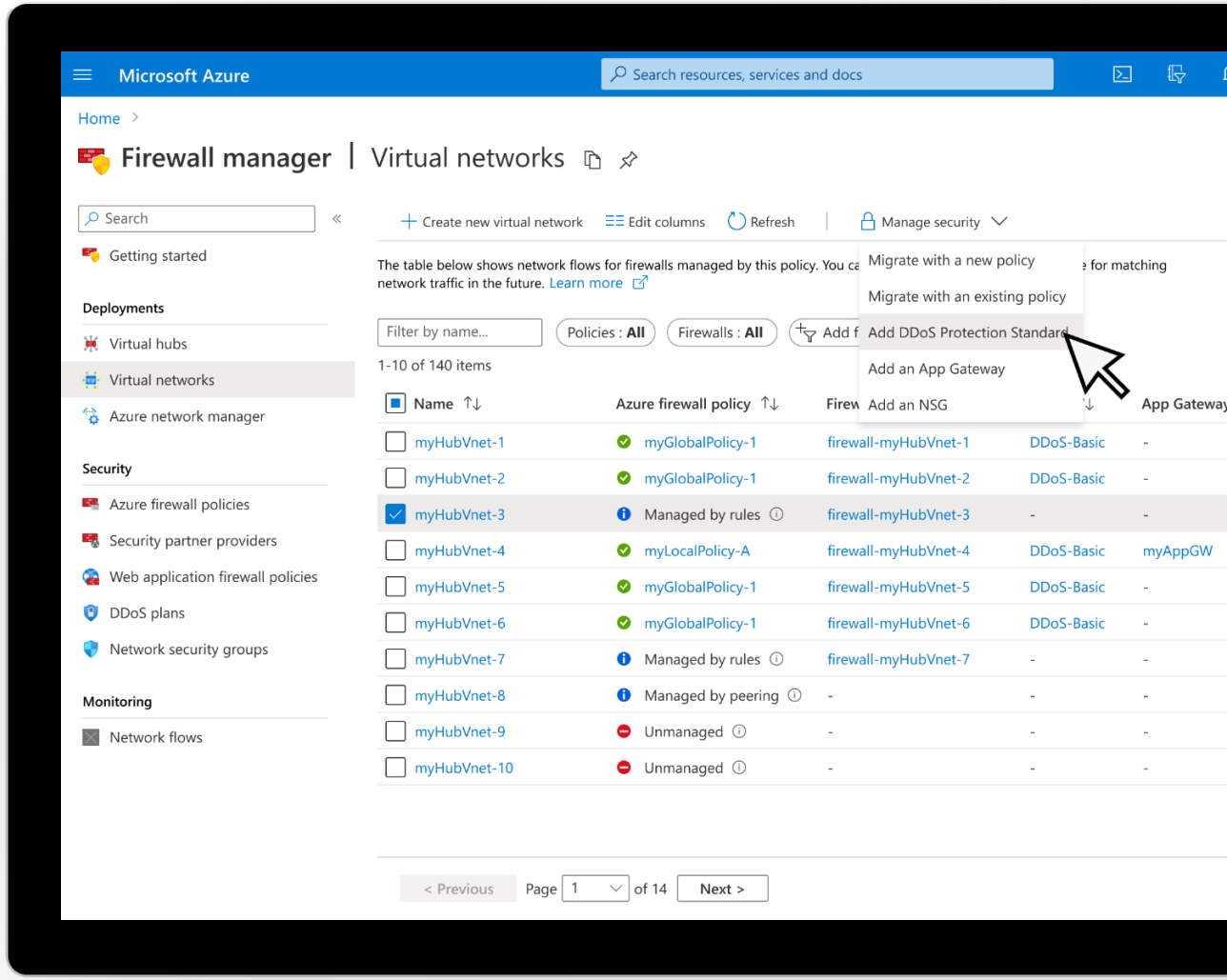
Microsoft's DDoS Protection Scale



Microsoft Azure

DDoS integration with Azure Firewall Manager

Take actions to protect unprotected virtual networks within Firewall Manager to improve network security posture.



Inline DDoS protection with Gateway LB and Partner NVAs

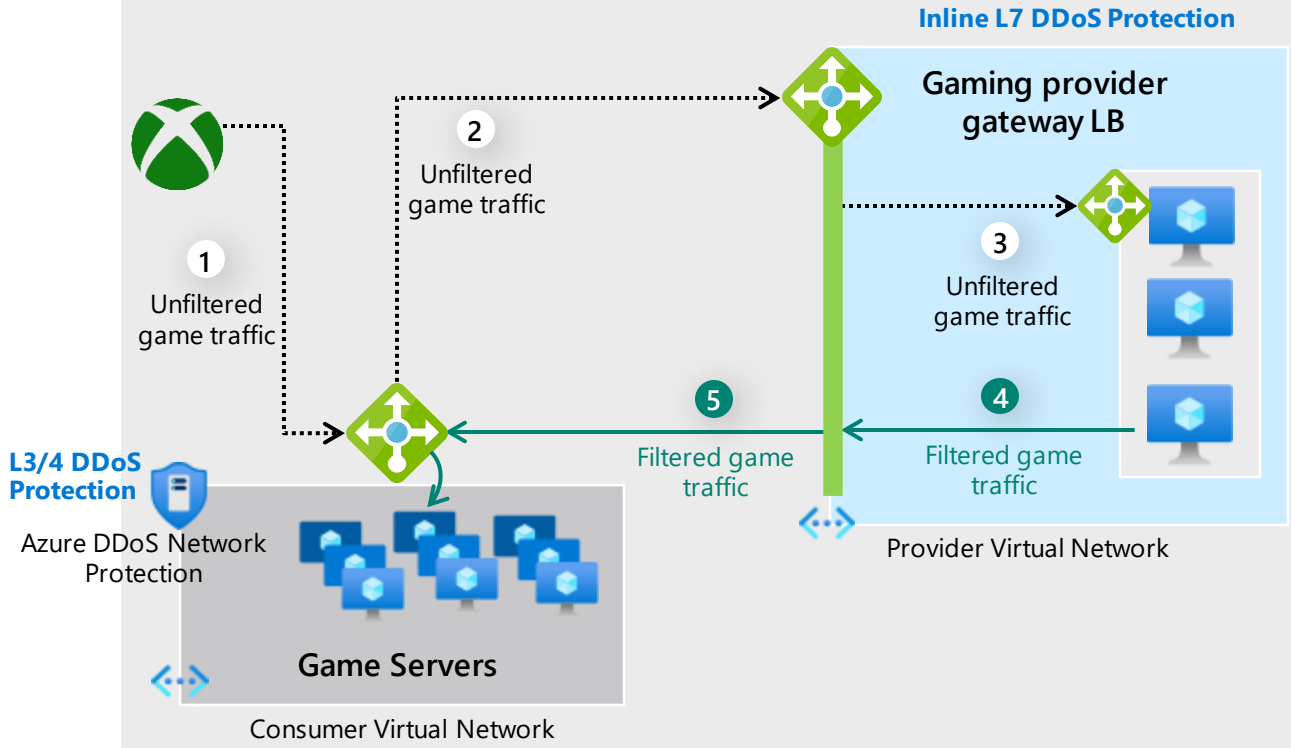
Public preview

DDoS attacks on game servers cause outages ranging from 2-10 seconds resulting in game disruption.

Existing solutions are focused to protect a load balanced, stateless, TCP service against attacks that last for minutes/hours.

These are ill-suited to protect against DDoS attacks on game servers.

Gateway LB enables protection of game servers via enabling gaming partners to create an inline DDoS solution.



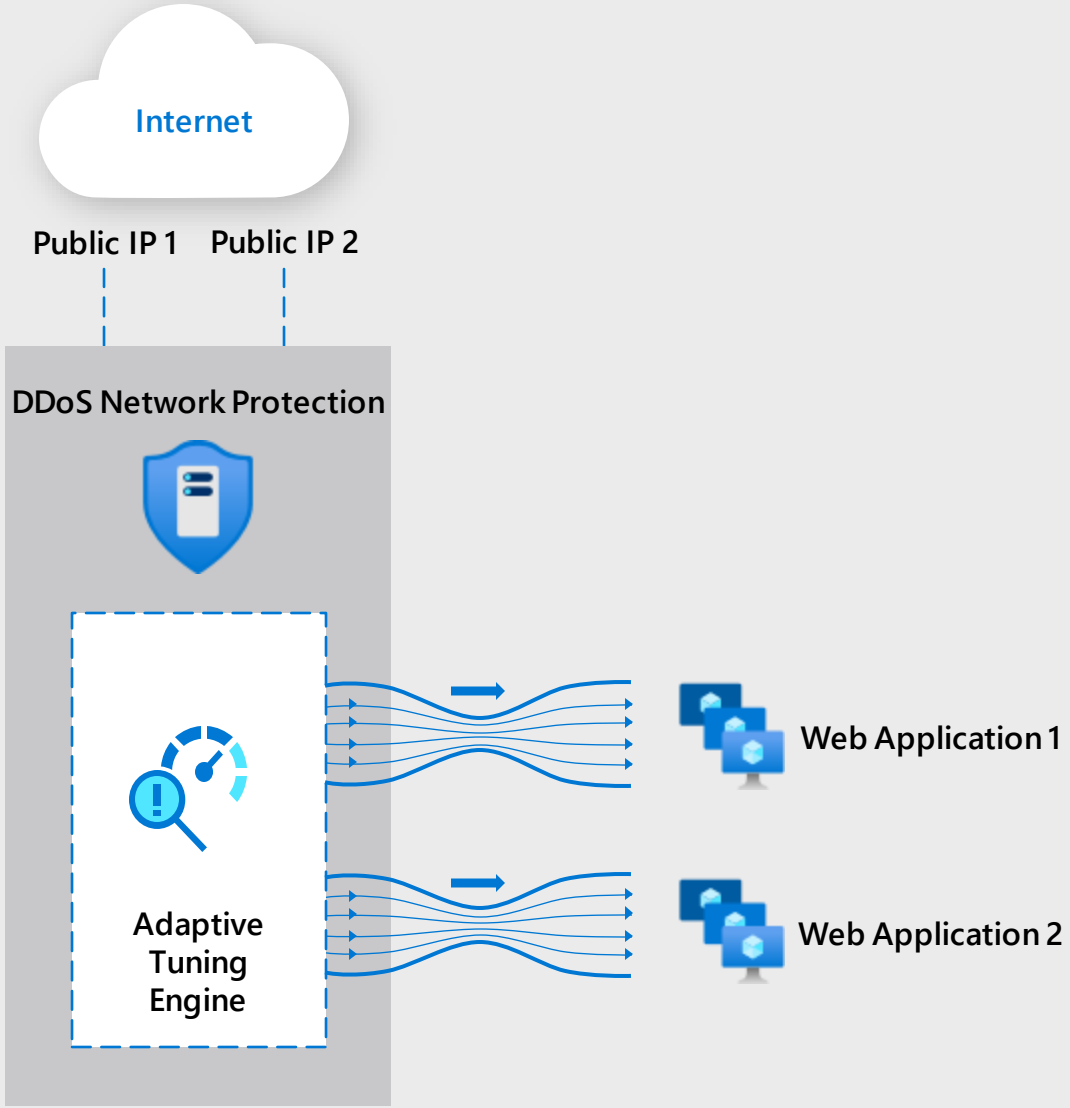
Adaptive tuning

Protection policies tuned to your application's traffic profile.

Continuously profiles normal Public IP traffic.

Utilizes machine learning algorithms for adaptive tuning and setting mitigation threshold.

Easy to setup with no user configuration is required.



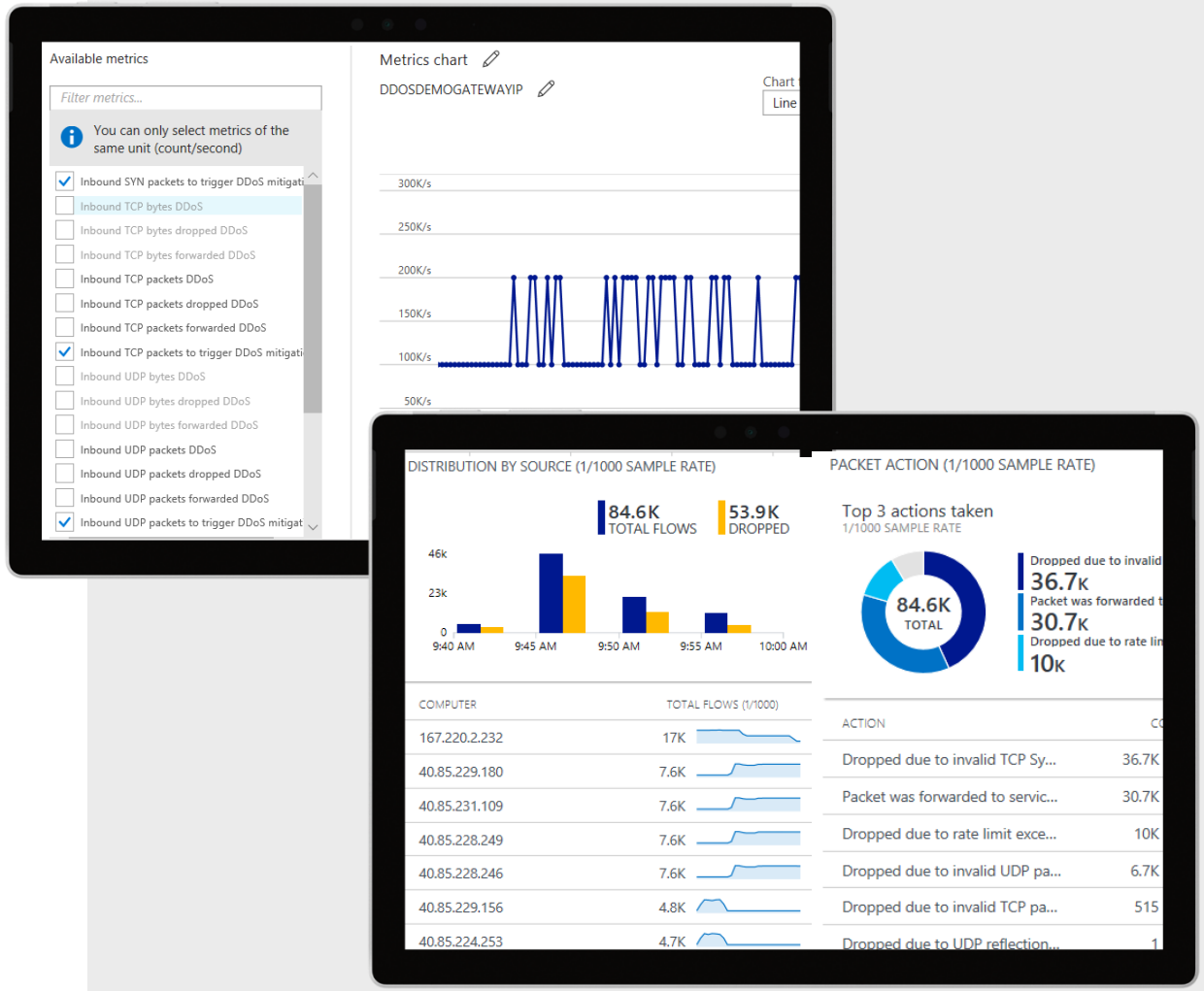
Attack analytics and metrics

Telemetry through Azure Monitor

Provides near real-time network attack mitigation flow logs

Attack data snapshots every 5 mins and full post attack summary

Logging can be integrated with Azure Sentinel, Splunk, OMS, and Azure Storage

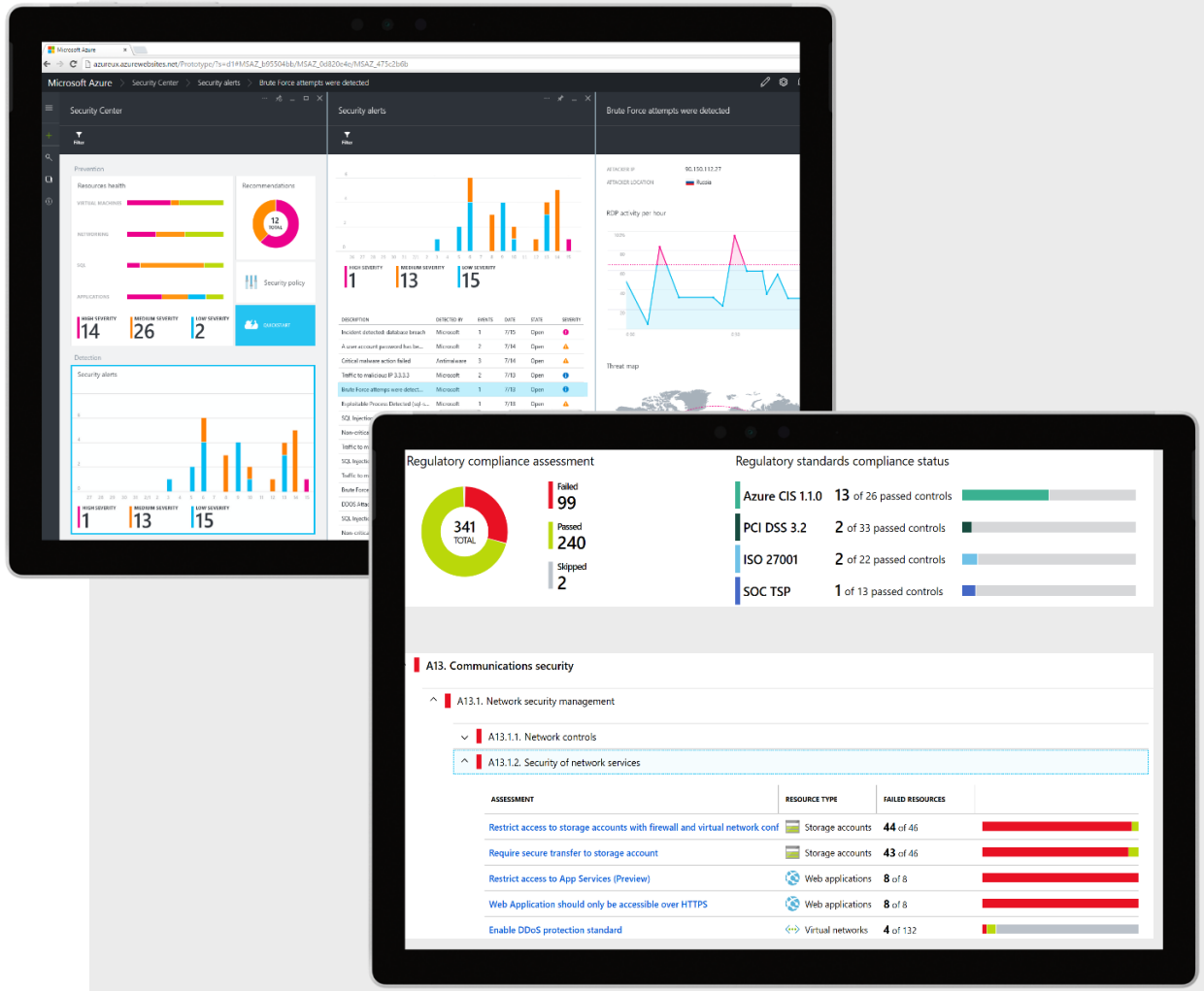


Microsoft Defender for Cloud Integration

Recommendations for unprotected public IPs

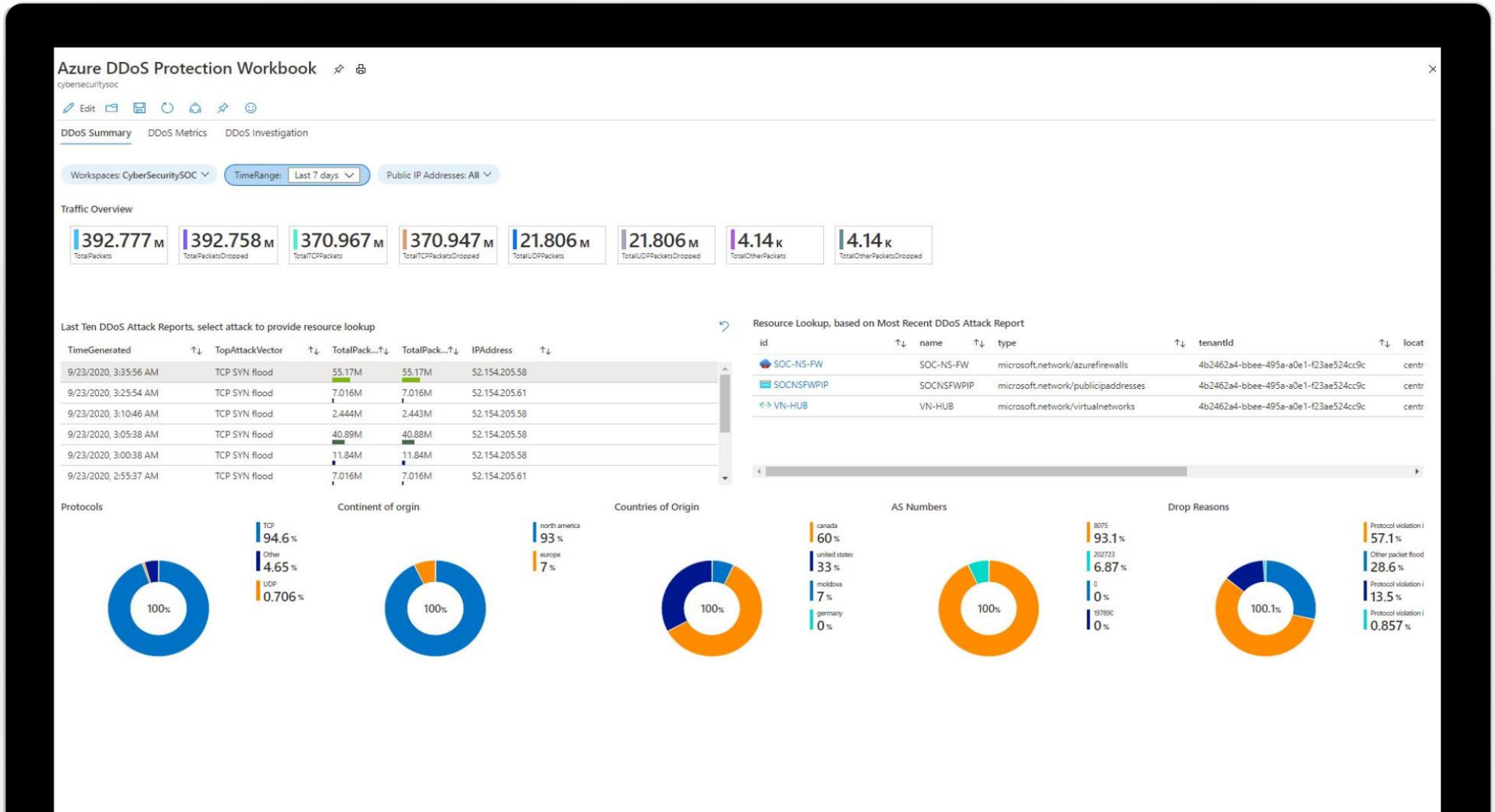
Alerts Integration into a single dashboard

Regulatory Compliance recommendations based on standards



Azure DDoS Protection

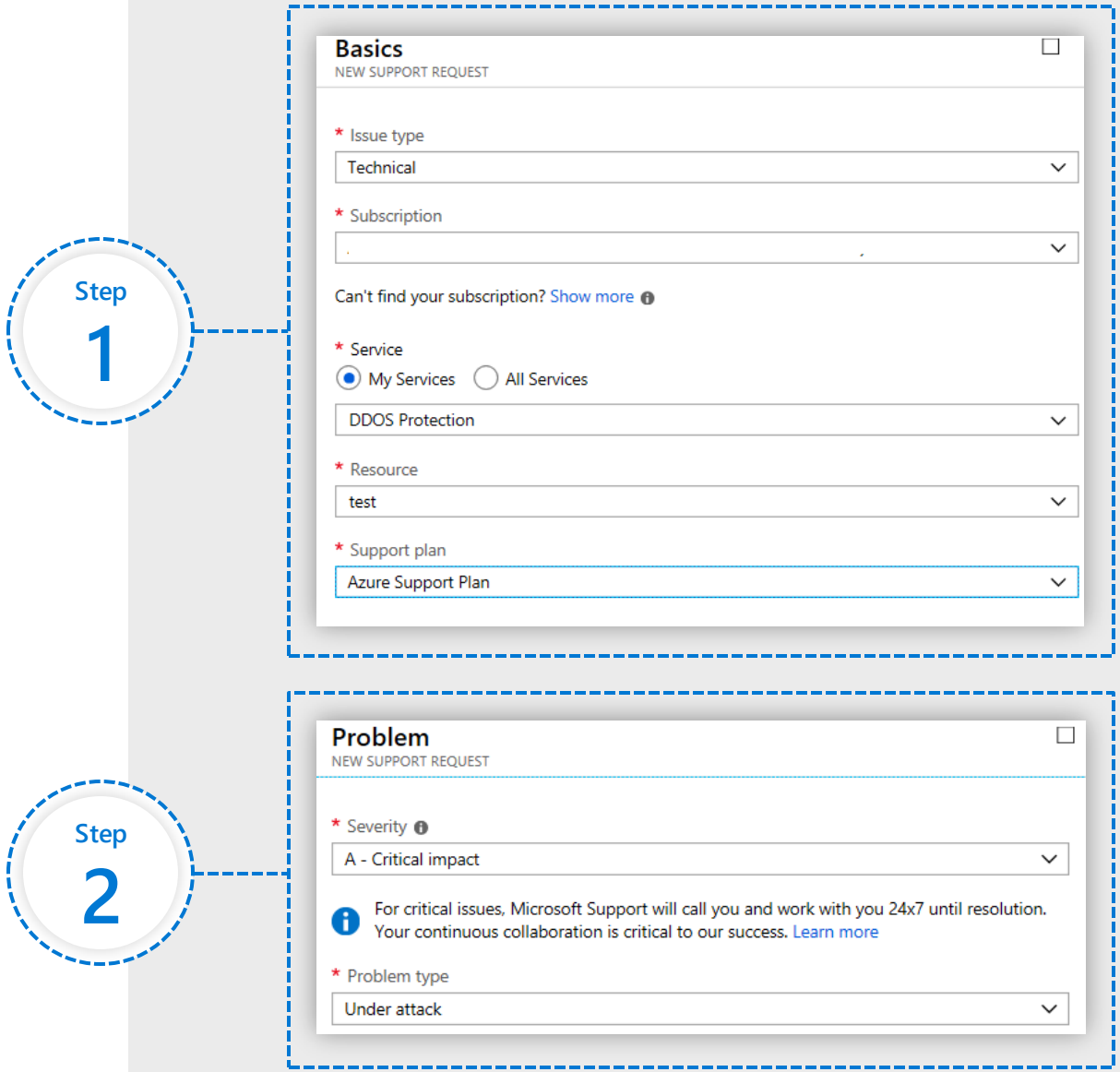
Attack analytics and Microsoft Sentinel integration



DDoS Rapid Response (DRR)

Specialized DDoS Rapid Response support during active attacks

Custom mitigation policy configuration



DDoS SLA Guarantee and Cost Protection

99.99% SLA guarantee for Azure DDoS Protection service

99.99% SLA guarantee that during attack the target resource will not be impacted

Receive 100% service credits for resource costs incurred as a result of a documented DDoS attack

Azure DDoS Network Protection - Pricing

Fixed Cost

$3K/month for the entire tenant (multiple subscriptions and VNETs)

$30/month for each IP above 100

Pricing includes

Cost protection against unforeseen scale out of resources

Access to rapid response support for DDoS cases without paying $75K/annum of ARR premium

Examples of resources protected under DDoS cost protection:

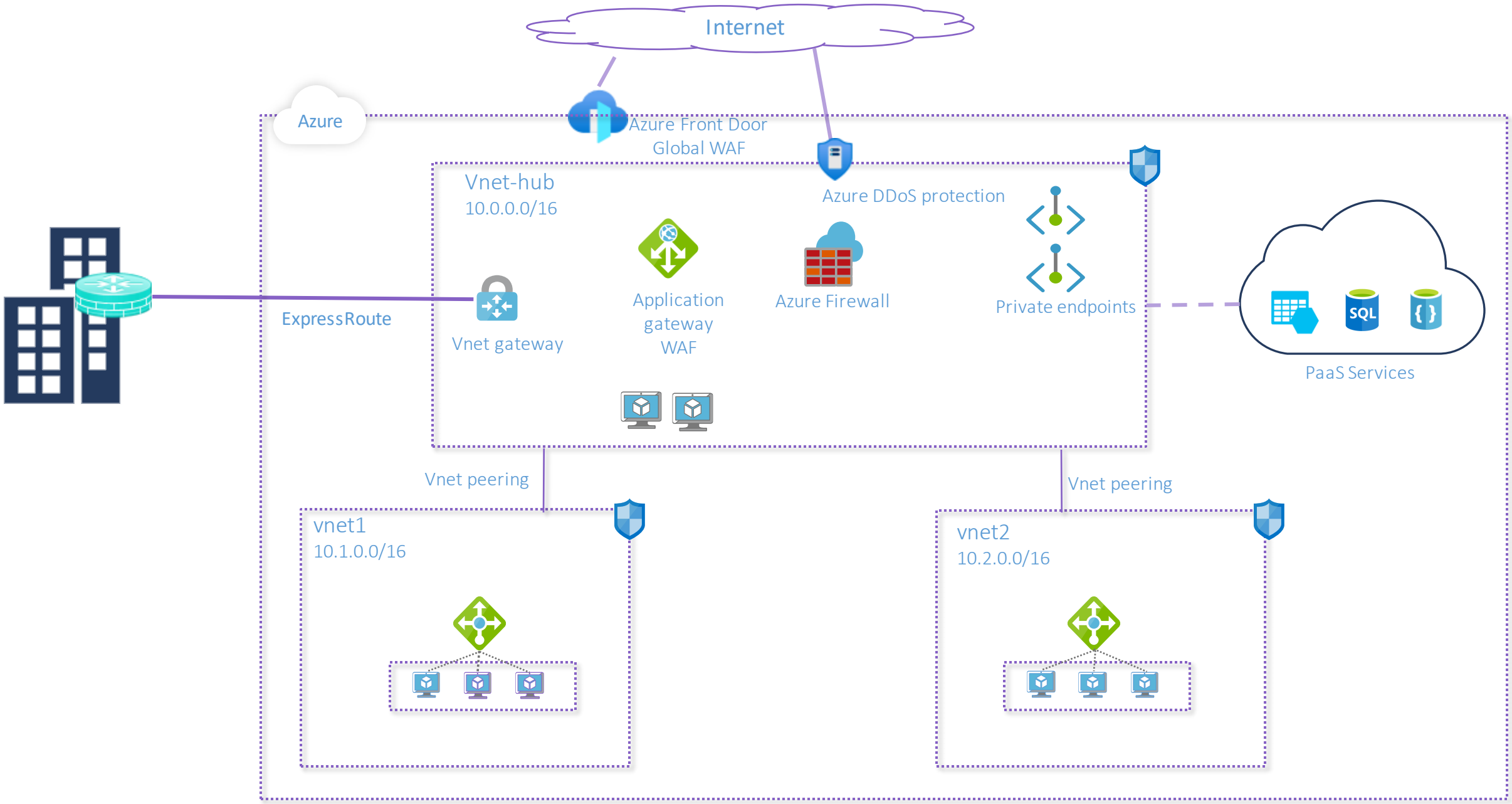
- Data process (ingress/egress) for Azure firewall, AppGW/WAF
  - **WAF is 100% discounted when DDoS Network Protection is enabled on the VNET; AppGW charges will apply**
- Scale out of VMs, AKS
- Data egress for network bandwidth-happens during an amplification attack when DDoS impacted app makes outbound connections.
- Scale out of backend PaaS resources like SQL, CosmosDB, Storage, App Services etc.

Azure DDoS Protection Pricing | Microsoft Azure

Azure DDoS IP Protection (Preview) - Pricing

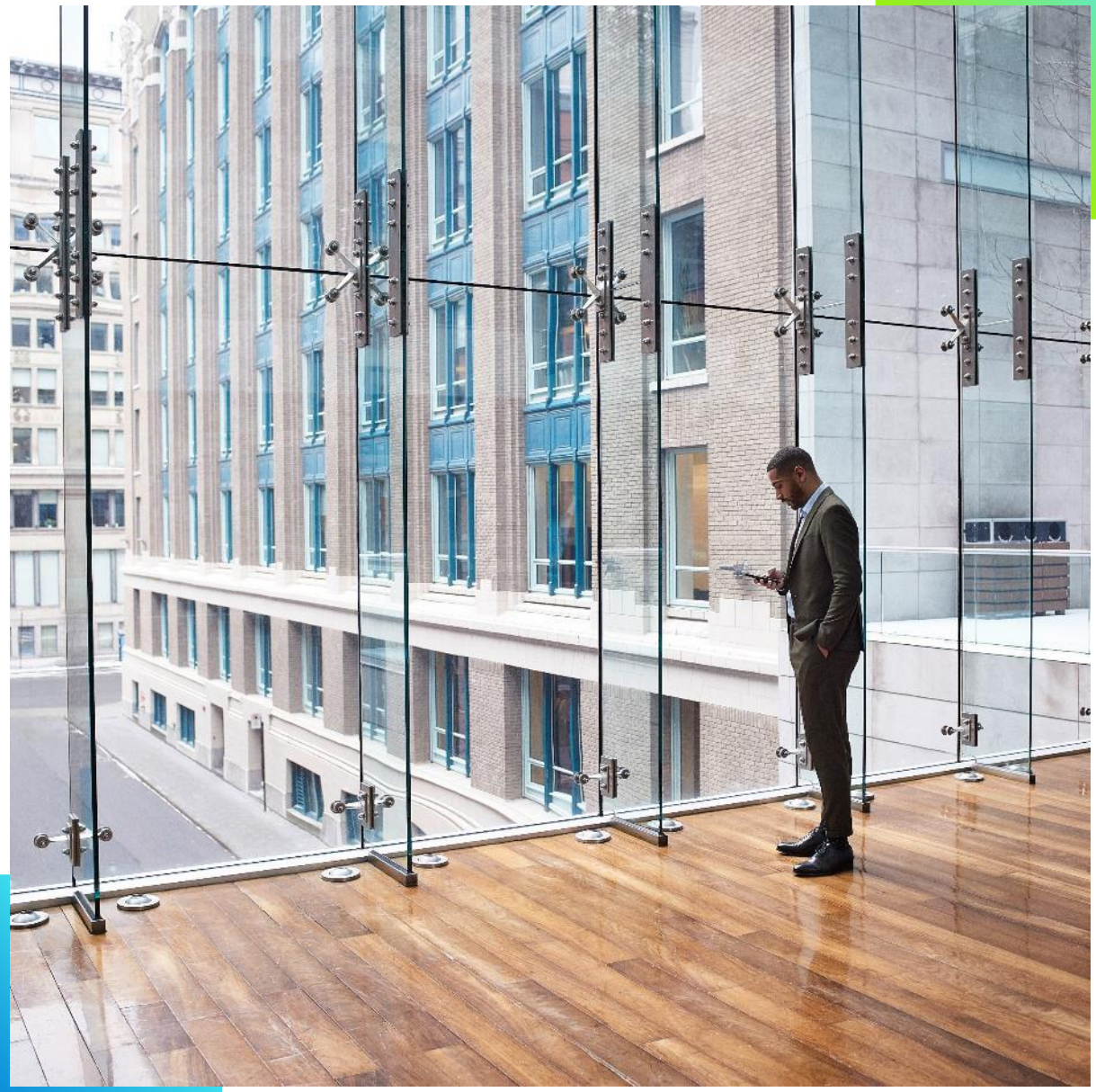
Azure DDoS Protection Pricing | Microsoft Azure

Azure Secure Hybrid Architecture



Key takeaways

- Complete your defense in depth security with best-in-class cloud native services
- Every Azure Virtual Network and Public IP should be protected by Firewall and DDoS
- Every Web/API/Mobile application should have WAF protection enabled
- Access to VMs should only be via Azure Bastion
- Enable Azure Private Link for the most secure way to access all PaaS services



Resources

- Network security strategies on Azure
- Best practices for network security
- Azure Private Link
- Azure Private Link service
- Azure Firewall Standard features
- Azure Firewall Premium features
- Azure Firewall preview features
- Azure Firewall Architecture with Application Gateways
- Azure Firewall to inspect traffic to Private Endpoints
- Integrate NAT gateway with Azure Firewall
- Azure Secured Virtual Hub (Azure Virtual WAN)
- Azure Web Application Firewall (WAF) policy
- Azure DDoS Protection
- Azure DDoS Protection SKU Comparison

Microsoft

Questions

Microsoft

Thank You