Azure Firewall

A fully managed, cloud-based firewall that protects your Azure resources

August, 9, 2021

Maheshk@microsoft.com

Microsoft Azure

Demo Setup: Aug/9

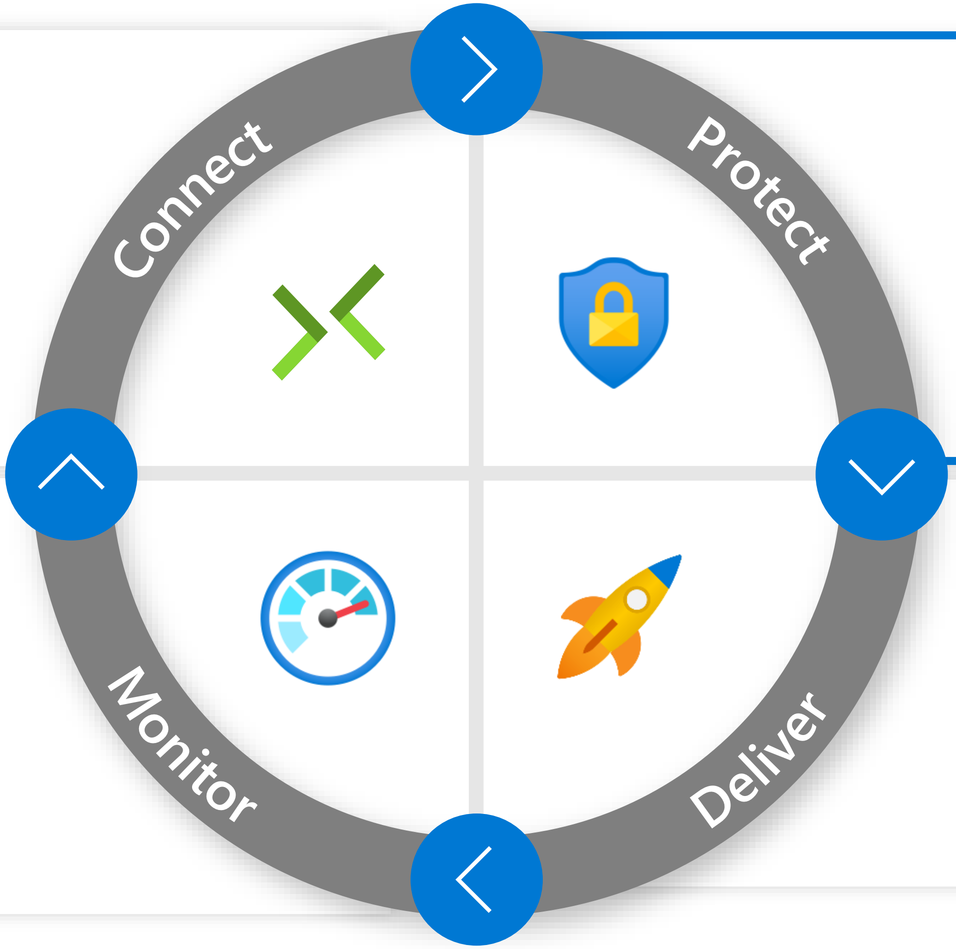
Tutorial: Deploy and configure Azure Firewall and policy using the Azure portal
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal-policy

Firewall and Application Gateway for virtual networks (Architecture recommendation)
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/firewall-application-gateway

Monitor Logs,
https://docs.microsoft.com/en-us/azure/firewall/firewall-workbook

Deep dive Video
https://www.youtube.com/watch?v=JiUerkqyW0g

Azure networking services



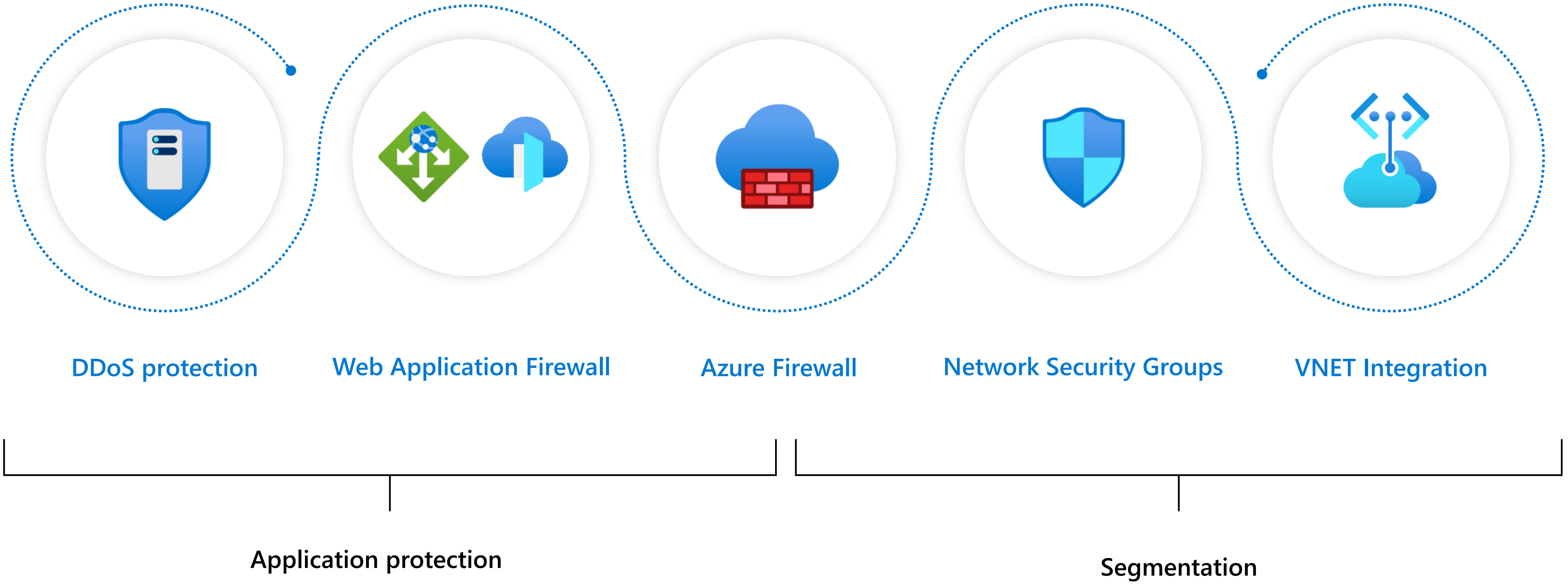
Virtual Network
Virtual WAN
ExpressRoute
VPN
DNS

DDoS Protection
Azure WAF
Azure Firewall
Azure Firewall Manager
Network Security Groups
Service Endpoints/Private Link

Network Watcher
ExpressRoute Monitor
Azure Monitor
Virtual Network TAP

CDN
Front Door
Traffic Manager
Application Gateway
Load Balancer

Protection services enabling zero trust



DDoS protection

Web Application Firewall

Azure Firewall

Network Security Groups

VNET Integration

Application protection

Segmentation

What is Azure Firewall?

Cloud native stateful Firewall as a service

Central governance of all traffic flows

Built-in high availability and auto-scale (30 Gbps)

Network, NAT, application traffic filtering (L3-L7)

Complete Virtual Network protection

Filter Internet, spoke-spoke, and hybrid network traffic

Azure Security Center Integration for Just In Time access `

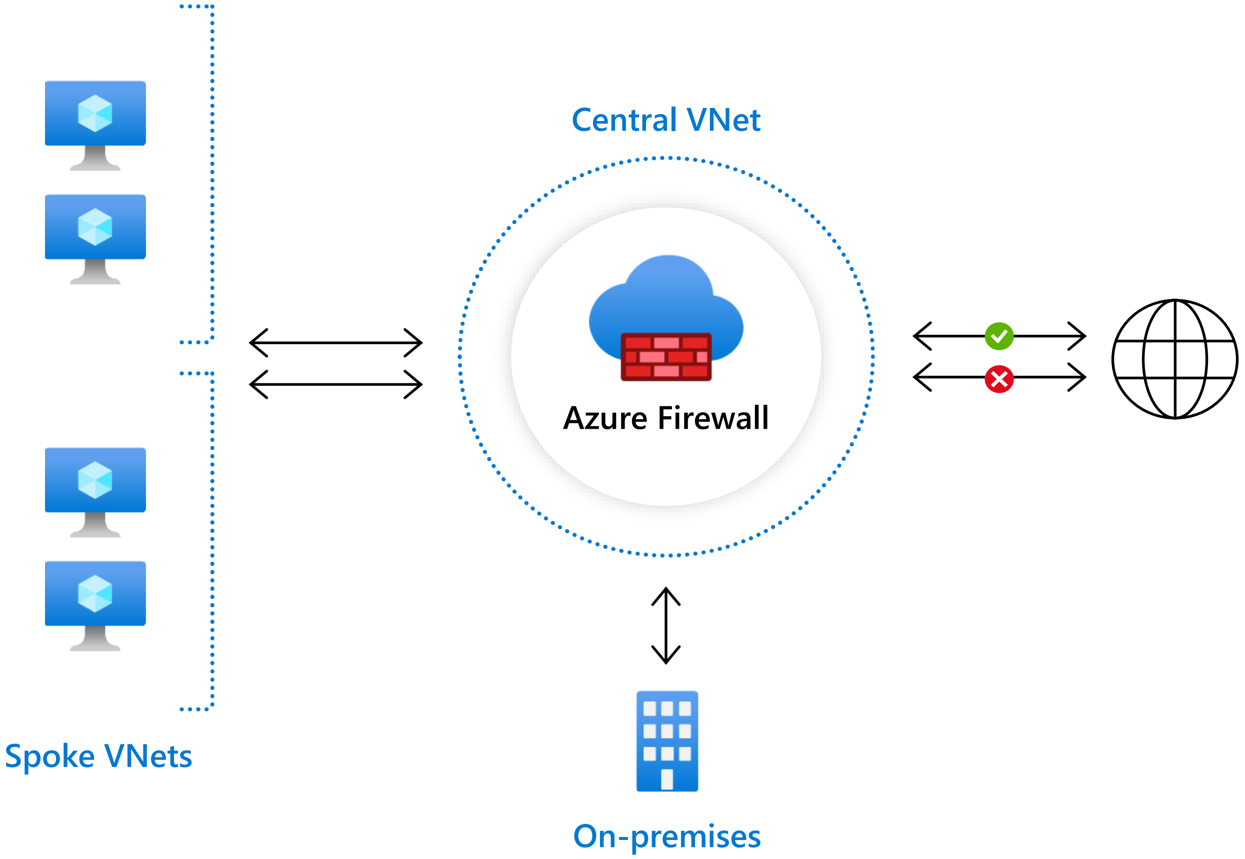
Centralized logging + monitoring

Archive and analyze logs

Azure Sentinel Integration using built-in Connectors

Best for Azure

DevOps integration, Microsoft Threat Intelligence, 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

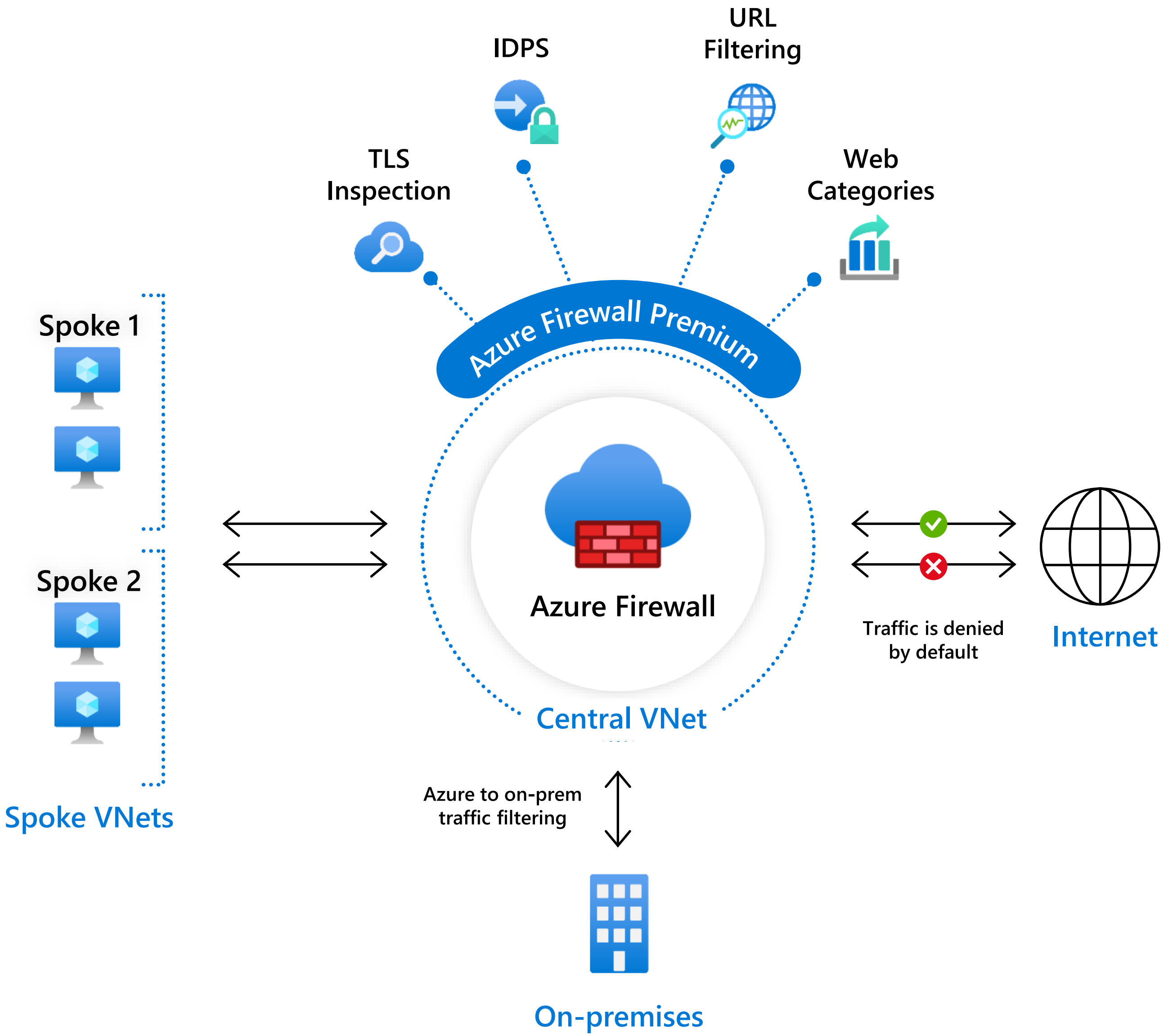
Allow or deny user access to website categories such as gambling, social media and others

Web categories maintained and continuously updated

URL based category matching

Azure Firewall Standard

Including all standard firewall capabilities



Azure Firewall

Key features

ICSA labs CERTIFIED FIREWALL - CORPORATE

Application rules

FQDN Filtering (HTTP/S, MSSQL)

FQDN Tags (e.g., Windows Update, Azure Backup, ASE,HDI)

Fully stateful network rules

Service Tags

NAT support

Default Source Network Address Translation (SNAT)

Destination Network Address Translation (DNAT)

Threat Intel

Deny and Alert on known malicious IPs and domains

Monitoring

Azure monitor logging

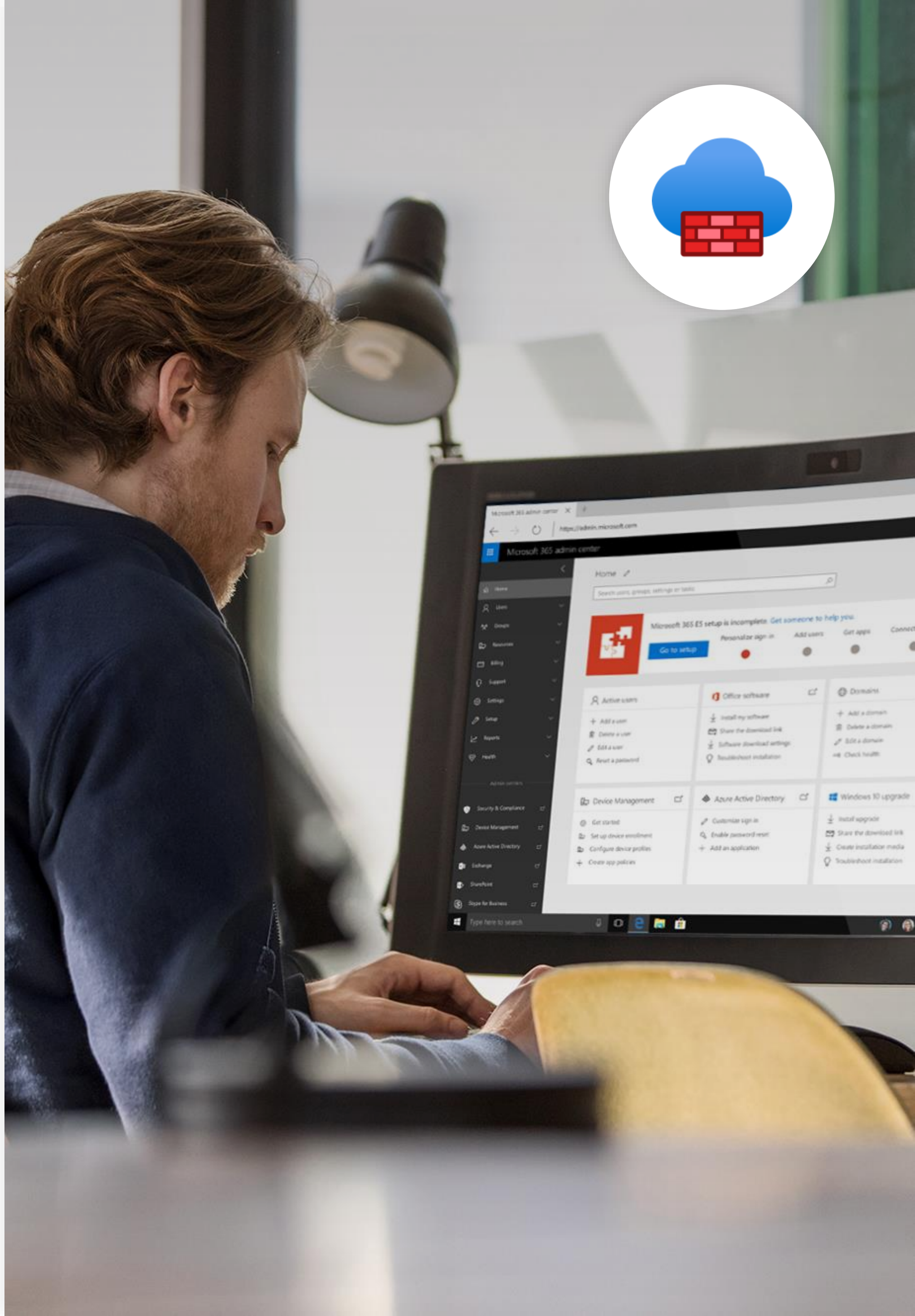
Azure monitor metrics

Scale and availability

Built-in auto scale (30 Gbps) and HA

Multiple public IPs – up to 250

Availability Zones (99.99% SLA)



Azure Firewall

Recently Released Features

New Scenarios

Windows Virtual Desktop Integration

Native forced tunneling support

Custom DNS + DNS Proxy (GA)

Traffic Filtering

FQDNs in network rules (GA)

Management

IP Groups

Auto SNAT configuration – customized private ranges

Compliance + Certifications

HIPAA Compliance

ICSA Labs Certified

Azure Firewall vs. NVAs

Feature	Azure Firewall	NVAs
FQDN filtering (no SSL termination)	✓	✓
Inbound/Outbound traffic filtering rules by IP address (source and destination), port, and protocol (5-tuple rules)	✓	✓
Network Address Translation (SNAT+DNAT)	✓	✓
Traffic filtering based on threat intelligence feed to identify high risk sources/ destinations (e.g., C&C, botnet, etc.)	✓	✓
Full logging including SIEM integration	✓	✓
Built-in HA with unrestricted cloud scalability (auto scale as traffic grows)	✓	
Azure Service Tags and FQDN Tags for easy policy management	✓	
Integrated monitoring and management, zero maintenance—cloud service model	✓	
Easy DevOps integration using REST/PS/CLI/Templates	✓	Templates
SSL termination with Deep Packet Inspection (DPI) to identify known threats (e.g., viruses, spyware)	Roadmap	✓
Traffic filtering rules by target URI (full path - incl. SSL termination)	Roadmap	✓
Central management	Firewall Manager	✓
Application and user aware traffic filtering rules	Roadmap	✓
IPSEC and SSL VPN gateway	Azure VPN GW	✓
Advanced Next Generation Firewall features (e.g. Sandboxing)	Roadmap	Vendor Dependent

Pros

Azure Firewall is auto scalable and highly available

Zero maintenance—service model

Azure specialization—Service Tags and FQDN tags

Best for Azure. Ideal fit for DevOps integration

Significant cost saving for most customers

Cons

Limited Next Generation Firewall features—main gap is IDS/IPS

Azure Firewall rule types

Destination Network Address Translation (DNAT)

- Inbound traffic filtering is enabled by mapping of your firewall public IP and port to a private IP and port.
- DNAT rules are applied in priority before network rules.

Network rules

- Network rules are created to control traffic for any protocol using FQDN’s or IP addresses.
- Network rule collections are higher priority than application rule collections, and all rules are terminating.

Application rules

- Application rules is used to allow HTTP/S traffic or Azure SQL traffic using fully qualified domain names (FQDNs) and FQDN tags e.g WVD, AKS, Windows update etc.

Azure Firewall—FQDN tags (Application Rules)

- **An FQDN tag represents a group of fully qualified domain names (FQDNs) associated with well known Microsoft services**
- **FQDN tags can be used in application rules to allow the required outbound network traffic through your firewall**

Supported tags:

Windows Update

Windows Diagnostics

Microsoft Active Protection Service (MAPS)

App Service Environment

Azure Backup

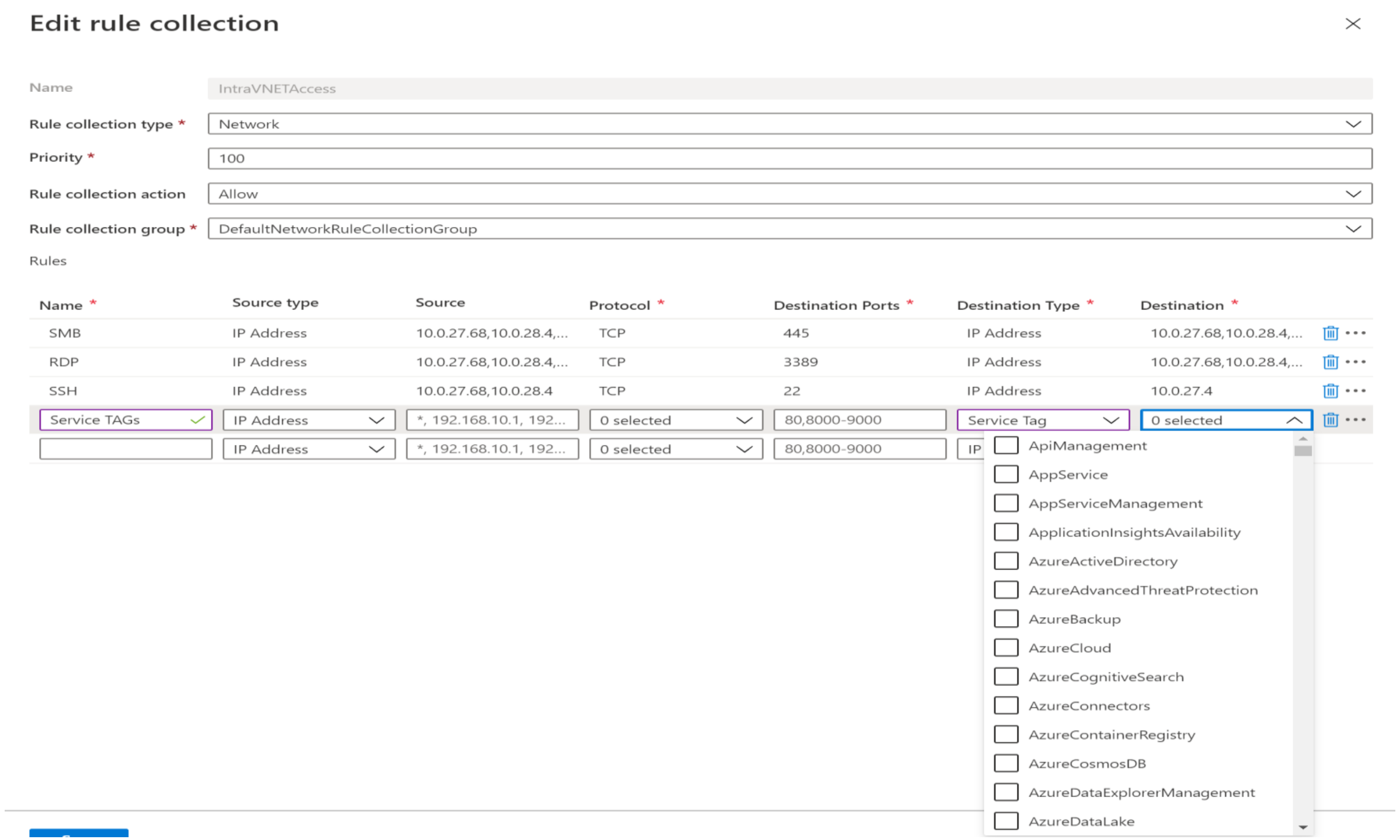
HDInsight

Azure Kubernetes Service

Windows Virtual Desktop

Azure Firewall—Service tags (Network Rules)

- A service tag represents a group of IP address prefixes for a given Azure service.
- Azure Firewall service tags can be used in the network rules destination field.



Edit rule collection

Name	IntraVNETAccess
Rule collection type *	Network
Priority *	100
Rule collection action	Allow
Rule collection group *	DefaultNetworkRuleCollectionGroup

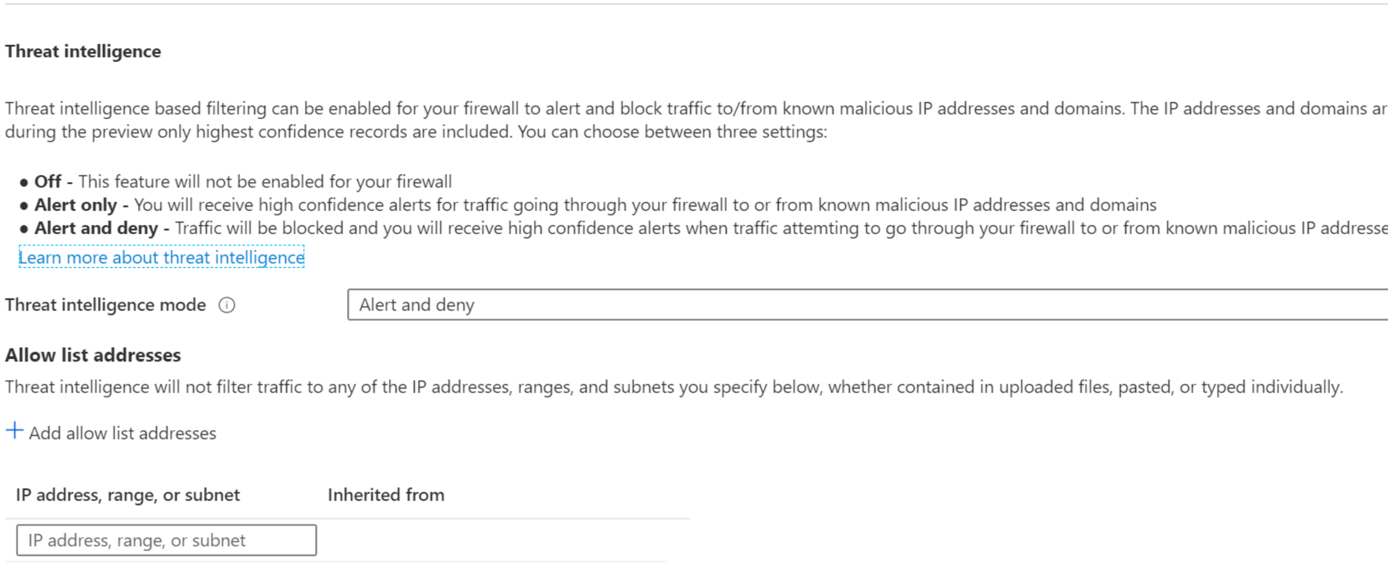
Rules

Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
SMB	IP Address	10.0.27.68,10.0.28.4,...	TCP	445	IP Address	10.0.27.68,10.0.28.4,...
RDP	IP Address	10.0.27.68,10.0.28.4,...	TCP	3389	IP Address	10.0.27.68,10.0.28.4,...
SSH	IP Address	10.0.27.68,10.0.28.4	TCP	22	IP Address	10.0.27.4
Service TAGs	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	Service Tag	0 selected
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	IP	

□ ApiManagement
□ AppService
□ AppServiceManagement
□ ApplicationInsightsAvailability
□ AzureActiveDirectory
□ AzureAdvancedThreatProtection
□ AzureBackup
□ AzureCloud
□ AzureCognitiveSearch
□ AzureConnectors
□ AzureContainerRegistry
□ AzureCosmosDB
□ AzureDataExplorerManagement
□ AzureDataLake

Azure Firewall—Threat Intel

- Microsoft Intelligent Security Graph powers Microsoft Threat Intelligence to create a high confidence list of known malicious IP addresses and domains
- Azure firewall can be configured to alert and deny traffic to and from known malicious IP addresses and domains in near real-time.
- Threat intel works on both inbound and outbound traffic through azure firewall



Threat intelligence

Threat intelligence based filtering can be enabled for your firewall to alert and block traffic to/from known malicious IP addresses and domains. The IP addresses and domains ar during the preview only highest confidence records are included. You can choose between three settings:

- **Off** - This feature will not be enabled for your firewall
- **Alert only** - You will receive high confidence alerts for traffic going through your firewall to or from known malicious IP addresses and domains
- **Alert and deny** - Traffic will be blocked and you will receive high confidence alerts when traffic attemting to go through your firewall to or from known malicious IP addresse

Learn more about threat intelligence

Threat intelligence mode ⓘ: Alert and deny

Allow list addresses

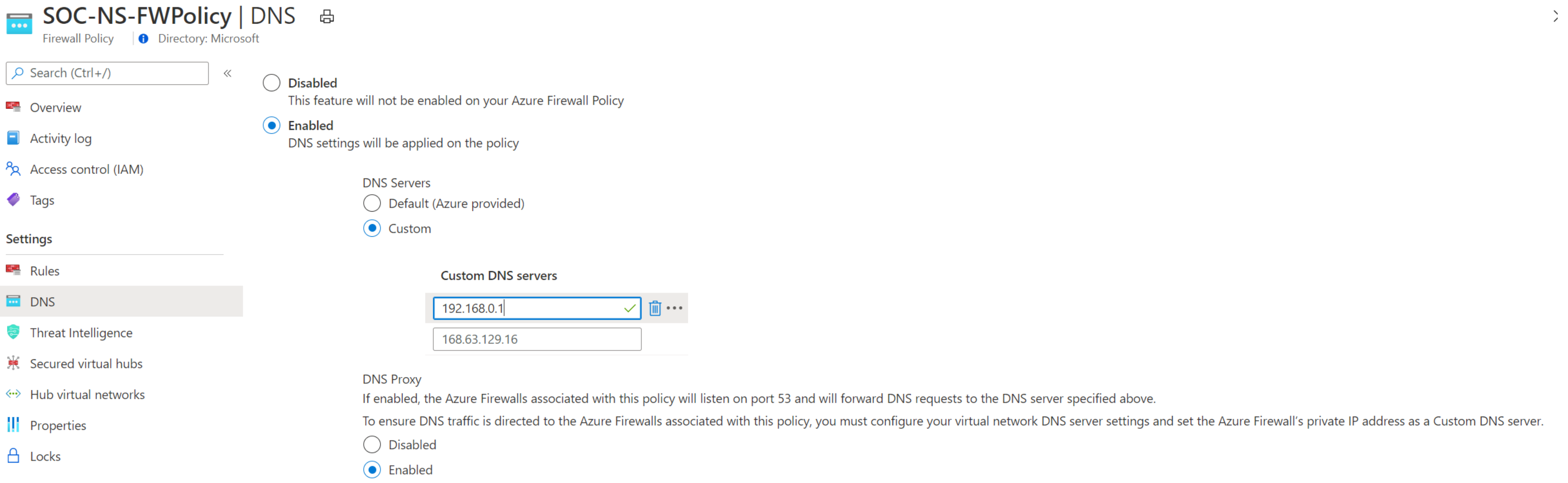
Threat intelligence will not filter traffic to any of the IP addresses, ranges, and subnets you specify below, whether contained in uploaded files, pasted, or typed individually.

+ Add allow list addresses

IP address, range, or subnet	Inherited from
IP address, range, or subnet	

Azure Firewall—Custom DNS and DNS Proxy

- By default Azure Firewall translates the FQDN to an IP address(es) using Azure DNS and does rule processing.
- Azure Firewall now supports Custom DNS which means you can use your corporate DNS to resolve both internal and external names.
- You can configure Azure Firewall to act as a DNS proxy.



SOC-NS-FWPolicy | DNS

Firewall Policy | Directory: Microsoft

○ Disabled
This feature will not be enabled on your Azure Firewall Policy

● Enabled
DNS settings will be applied on the policy

DNS Servers
○ Default (Azure provided)
● Custom

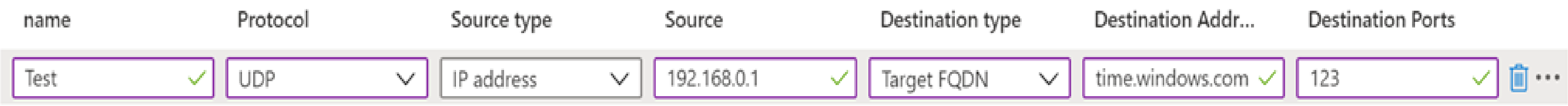
Custom DNS servers
192.168.0.1
168.63.129.16

DNS Proxy
If enabled, the Azure Firewalls associated with this policy will listen on port 53 and will forward DNS requests to the DNS server specified above.
To ensure DNS traffic is directed to the Azure Firewalls associated with this policy, you must configure your virtual network DNS server settings and set the Azure Firewall's private IP address as a Custom DNS server.
○ Disabled
● Enabled

Azure Firewall—FQDN Filtering in Network Rules

- FQDN filtering capability in network rules allows you to filter outbound traffic using FQDNs with any TCP/UDP protocol (including NTP, SSH, RDP, and more)

- DNS proxy on Azure firewall must be enabled to use FQDN’s in network rules

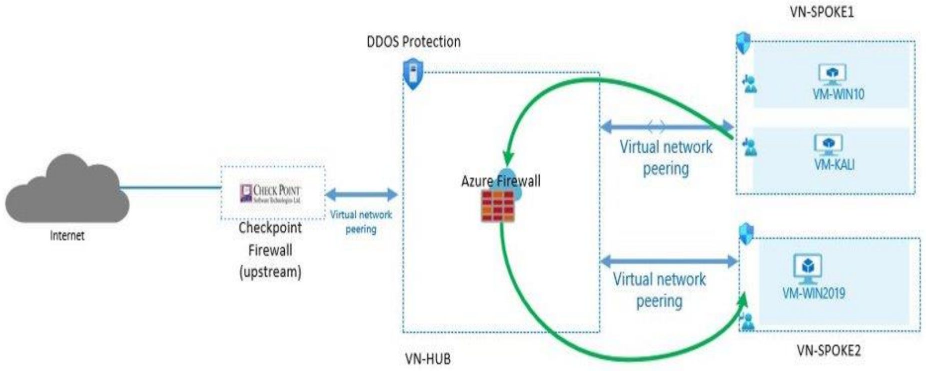


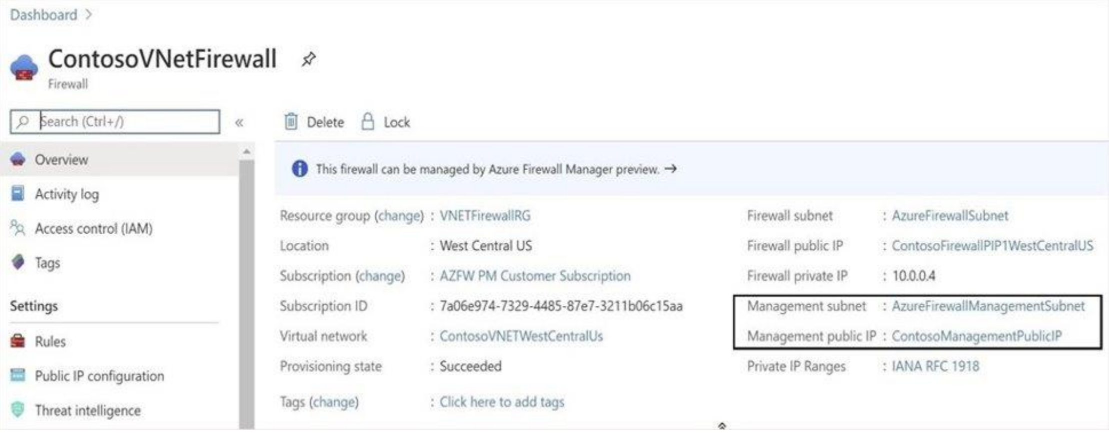
name	Protocol	Source type	Source	Destination type	Destination Addr...	Destination Ports
Test	UDP	IP address	192.168.0.1	Target FQDN	time.windows.com	123

Azure Firewall — Force Tunneling

- Forced tunneling redirect all internet bound traffic from Azure Firewall to your on-premises Firewall or to chain it to a nearby (NVA) for additional inspection.

- You cannot migrate an existing firewall deployment to a forced tunneling mode.





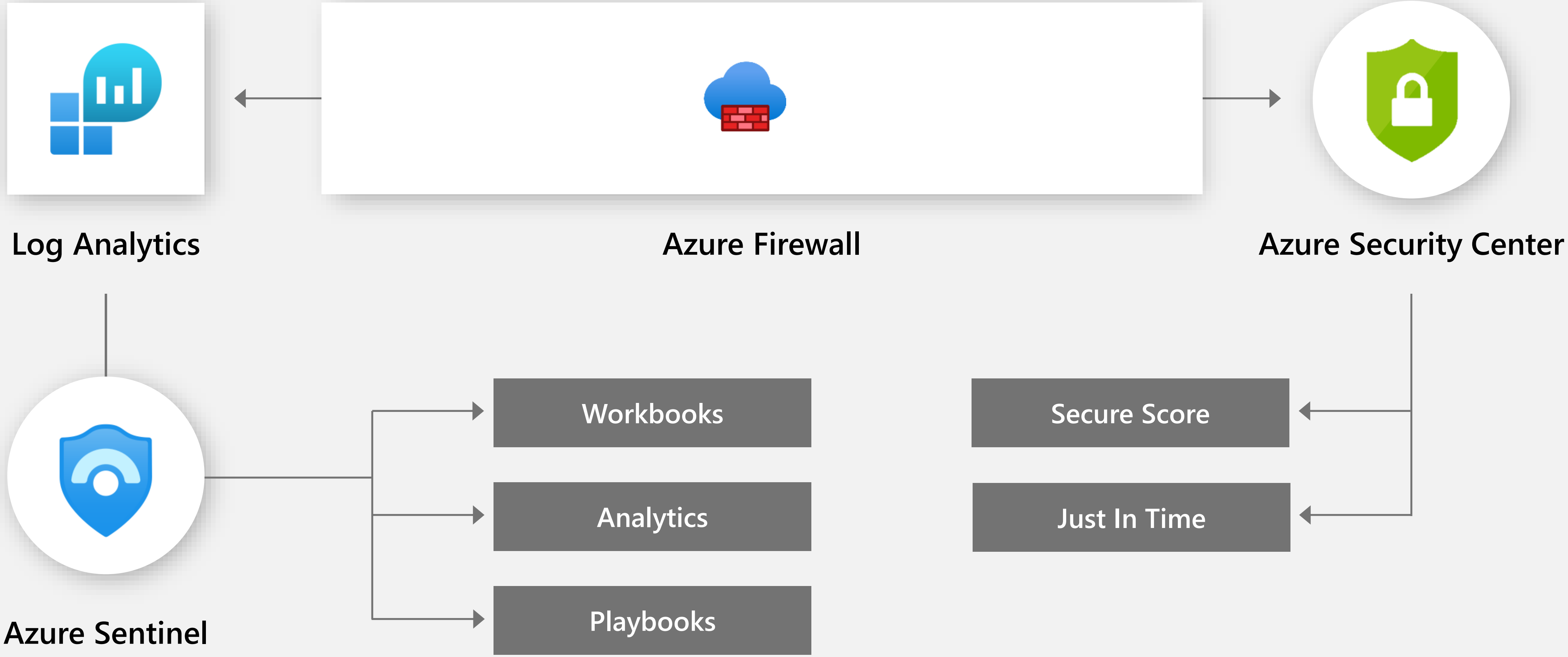
ContosoVNetFirewall

Firewall

This firewall can be managed by Azure Firewall Manager preview. →

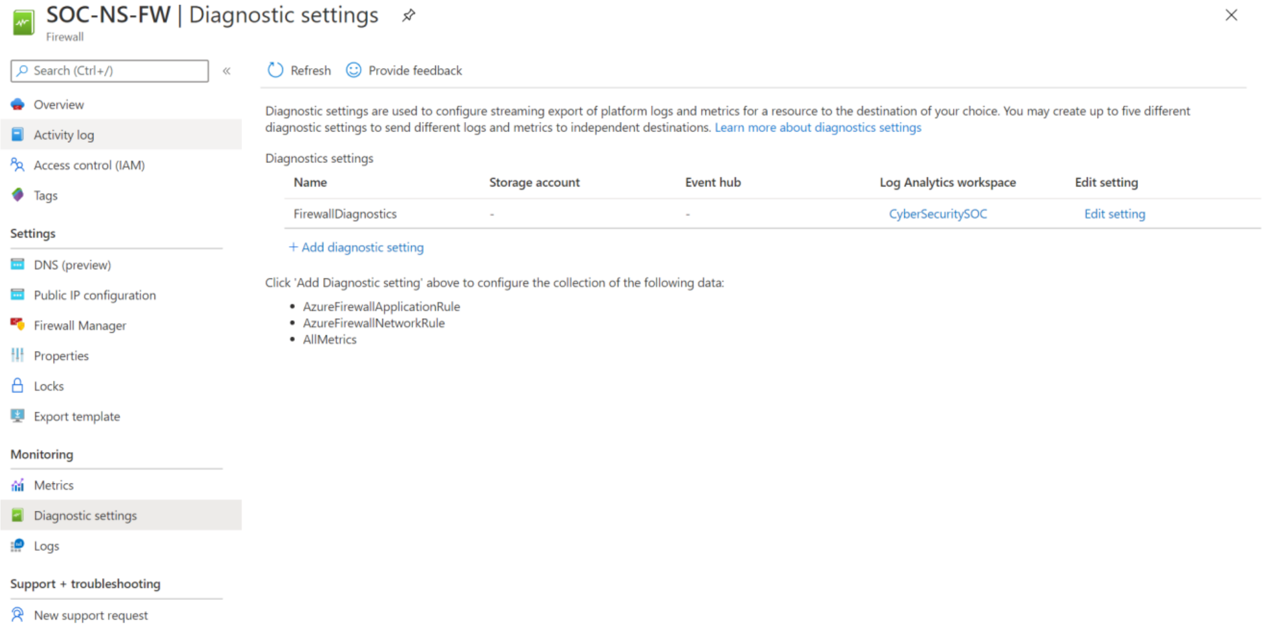
Resource group (change)	: VNETFirewallRG	Firewall subnet	: AzureFirewallSubnet
Location	: West Central US	Firewall public IP	: ContosoFirewallPIP1WestCentralUS
Subscription (change)	: AZFW PM Customer Subscription	Firewall private IP	: 10.0.0.4
Subscription ID	: 7a06e974-7329-4485-87e7-3211b06c15aa	Management subnet	: AzureFirewallManagementSubnet
Virtual network	: ContosoVNETWestCentralUs	Management public IP	: ContosoManagementPublicIP
Provisioning state	: Succeeded	Private IP Ranges	: IANA RFC 1918
Tags (change)	: Click here to add tags		

Azure Firewall – Integration with ASC and Azure Sentinel



Azure Firewall—Diagnostics and Monitoring

- Azure Firewall diagnostic logs can be saved to Storage Account, streamed to Event hubs and/or sent to Log Analytics Workspace.
- AzureFirewallApplicationRule category log each new connection that matches one of configured application rules results in a log for the accepted/denied connection.
- AzureFirewallNetworkRule category log each new connection that matches one of configured network rules results in a log for the accepted/denied connection including threat intel logs.



Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostics settings

Diagnostics settings

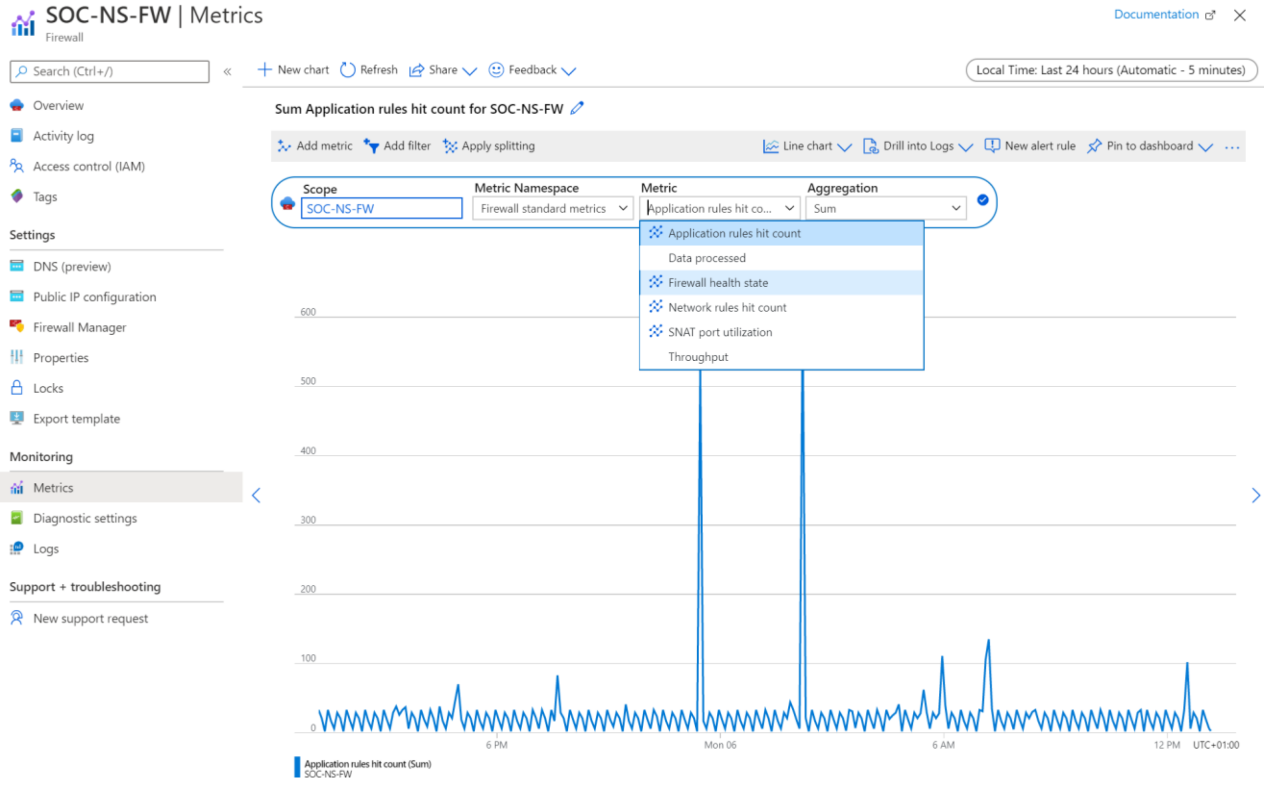
Name	Storage account	Event hub	Log Analytics workspace	Edit setting
FirewallDiagnostics	-	-	CyberSecuritySOC	Edit setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AzureFirewallApplicationRule
- AzureFirewallNetworkRule
- AllMetrics

Azure Firewall—Metrics

- **Metrics are collected every minute and following metrics are available for Azure Firewall**
  - Application rules hit count
  - Network rules hit count
  - Data processed
  - Firewall health state
  - SNAT port utilization
  - Throughput



SOC-NS-FW | Metrics

Firewall

Sum Application rules hit count for SOC-NS-FW

Scope: SOC-NS-FW

Metric Namespace: Firewall standard metrics

Metric: Application rules hit co...

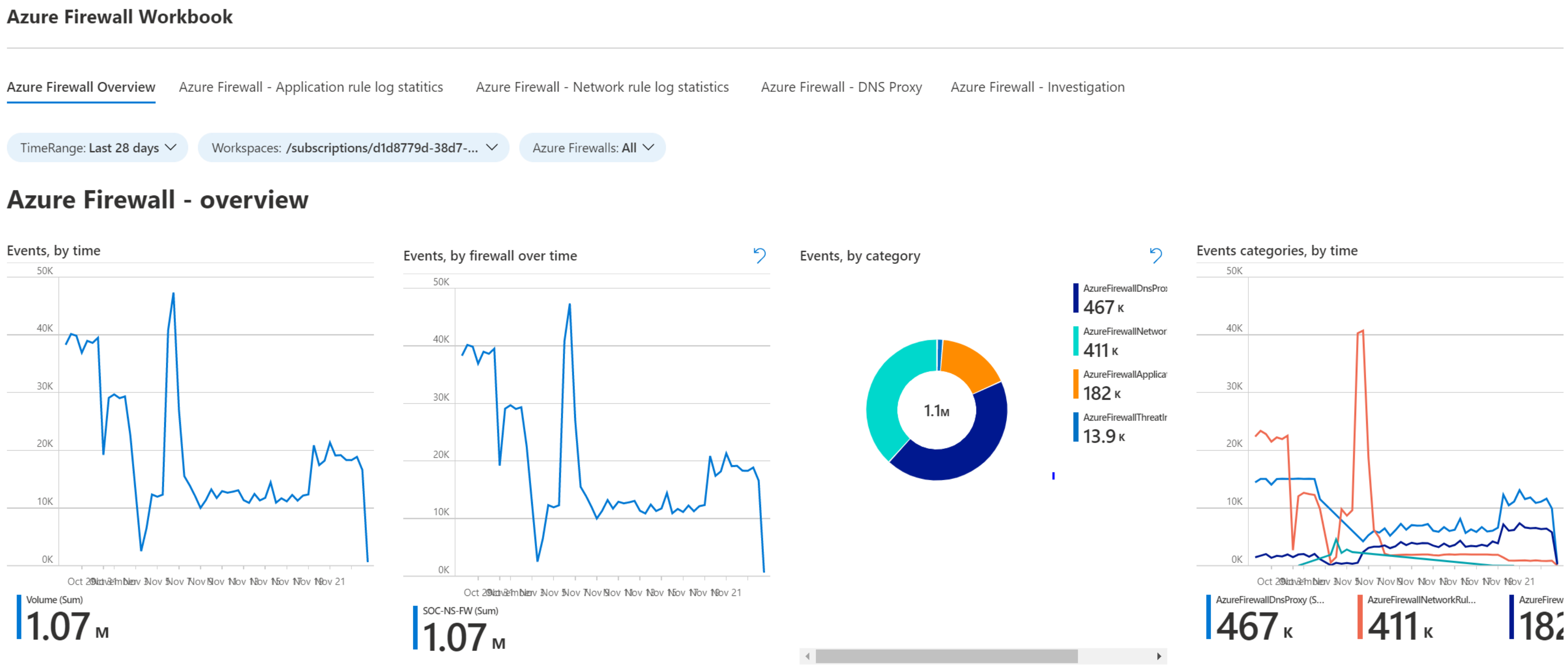
Aggregation: Sum

Local Time: Last 24 hours (Automatic - 5 minutes)

Azure Firewall—Workbook

- Workbooks in Azure Sentinel/Azure monitor allows for graphical visualization of Azure Firewall activity.

- You can download sample workbook to query data from log analytics workspace from github. https://aka.ms/aznetsec



Azure Firewall Workbook

Azure Firewall Overview | Azure Firewall - Application rule log statitics | Azure Firewall - Network rule log statistics | Azure Firewall - DNS Proxy | Azure Firewall - Investigation

TimeRange: Last 28 days | Workspaces: /subscriptions/d1d8779d-38d7-... | Azure Firewalls: All

Azure Firewall - overview

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

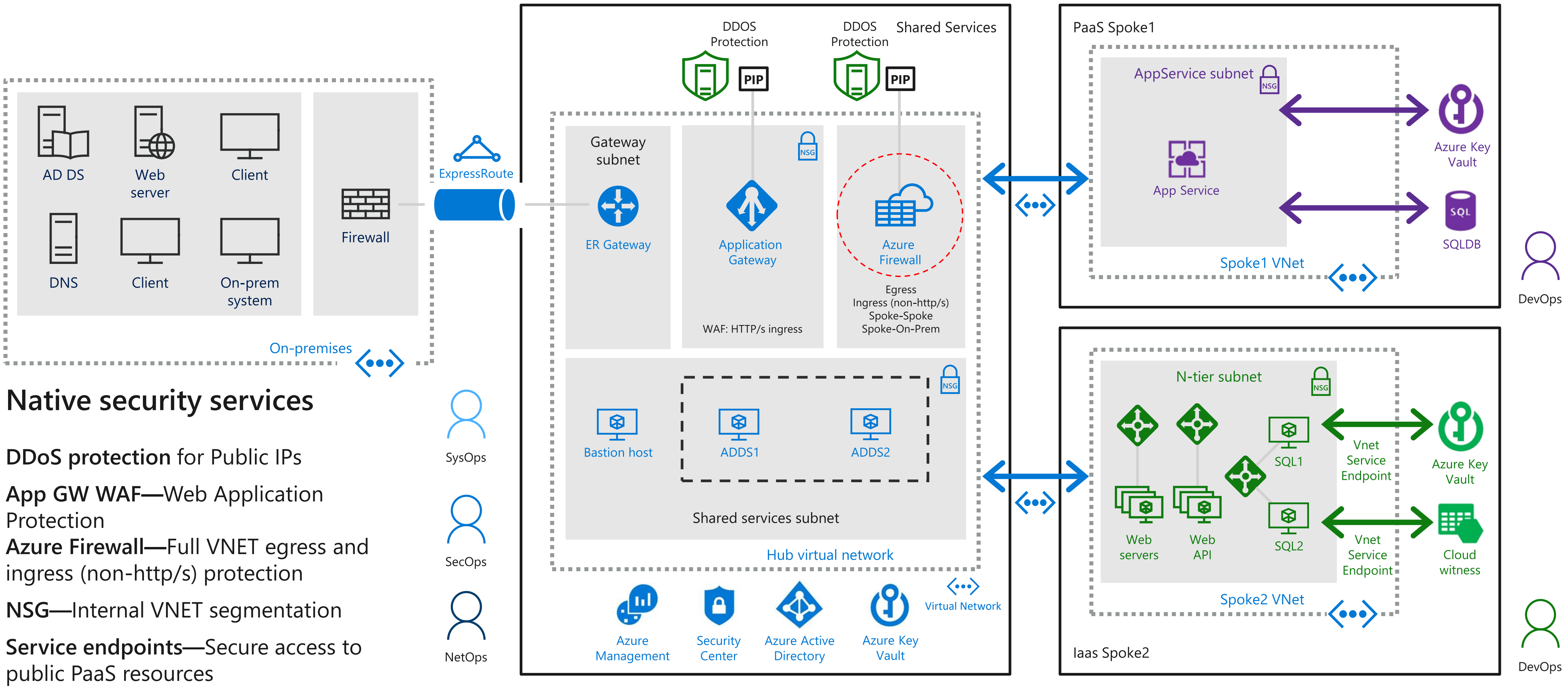
Azure Firewall is a fully stateful centralized network firewall as-a-service, providing network and application-level protection across virtual networks and subscriptions

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

Hybrid Hub & Spoke Architecture



Native security services

DDoS protection for Public IPs

App GW WAF—Web Application Protection

Azure Firewall—Full VNET egress and ingress (non-http/s) protection

NSG—Internal VNET segmentation

Service endpoints—Secure access to public PaaS resources