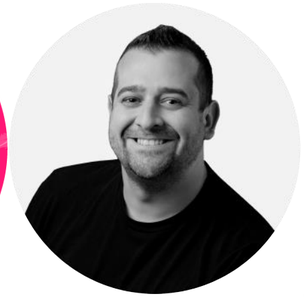
Microsoft Security, Compliance, and Identity Fundamentals: Security Solutions

Infrastructure Security Services in Microsoft Azure



Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

- Azure network security groups
- Azure Firewall
- Azure DDoS Protection
- Azure Web Application Firewall
- Azure Bastion
- Azure Key Vault
- Encryption on Azure

Azure Network Security Groups

Azure Network Security Groups (NSG)

Filter network traffic to/from Azure resources in an Azure Virtual Network

NSG work with security rules

- Decide traffic to allow or block based on rules

Network Security Groups Configurations

Name

Priority

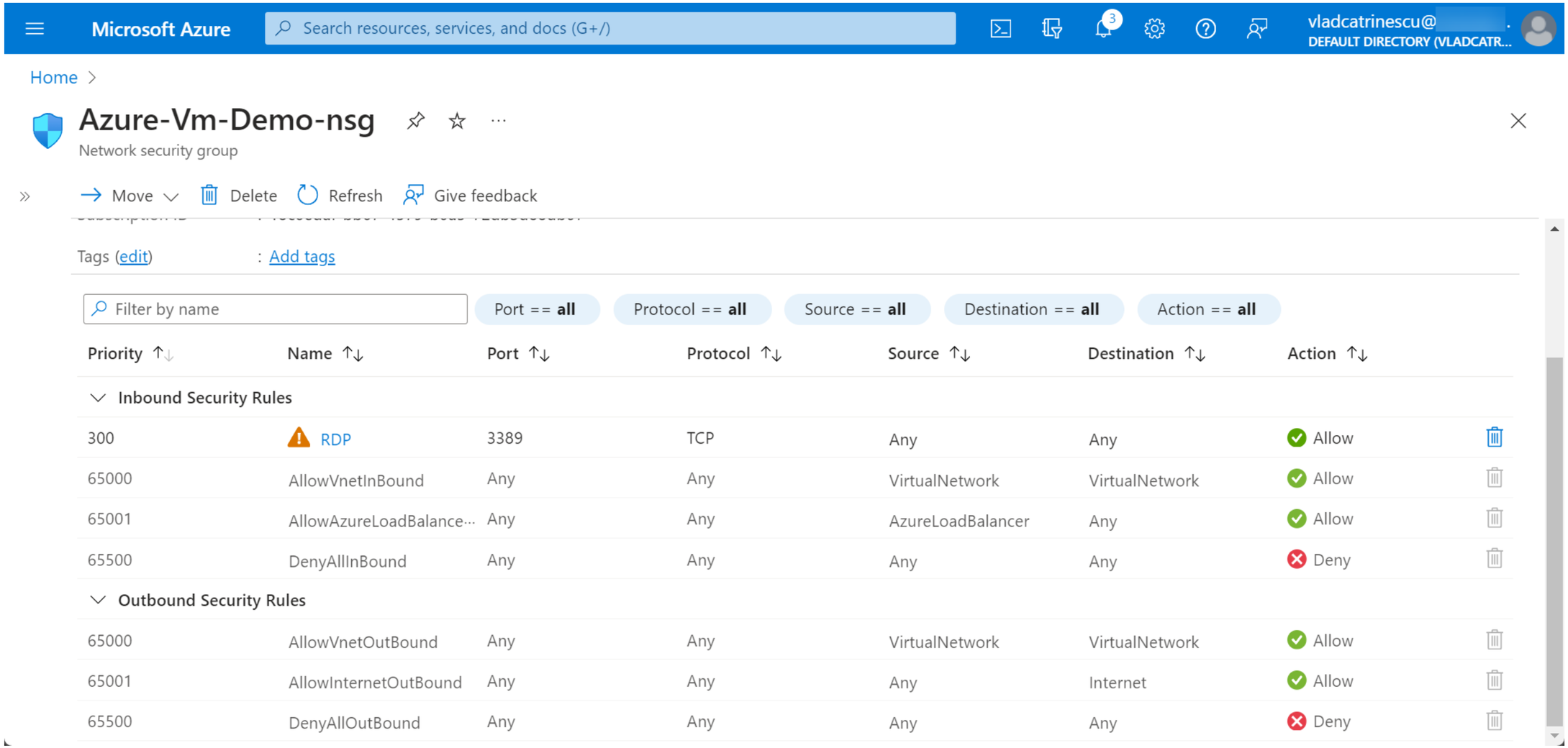
Source and Destination

Protocol and Port Range

Direction

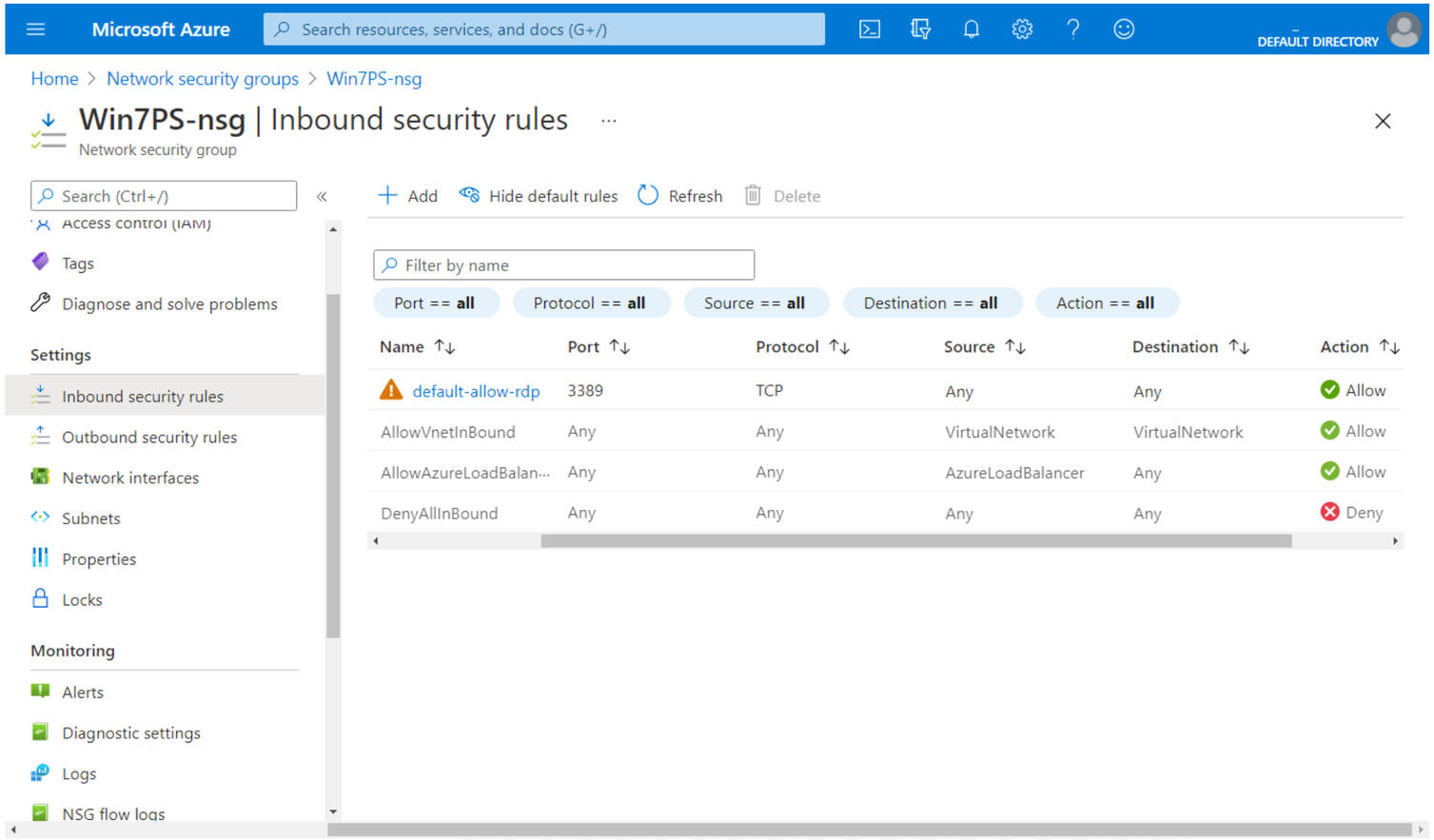
Action

Network Security Groups Example



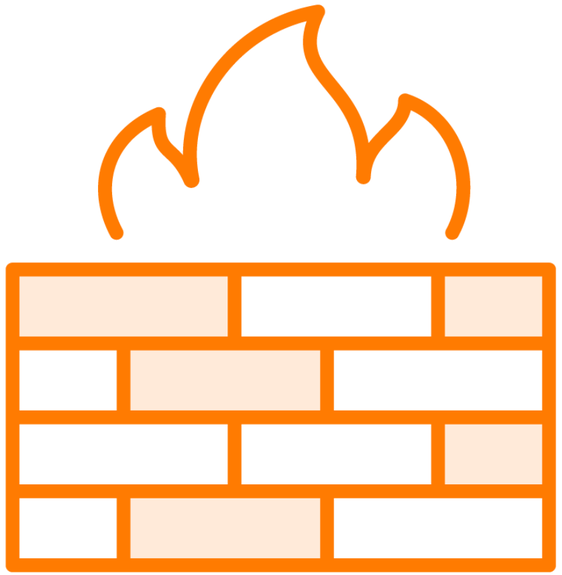
NSG are created in a Virtual Network

Can be assigned to multiple subnets or network interfaces



Azure Firewall

Azure Firewall



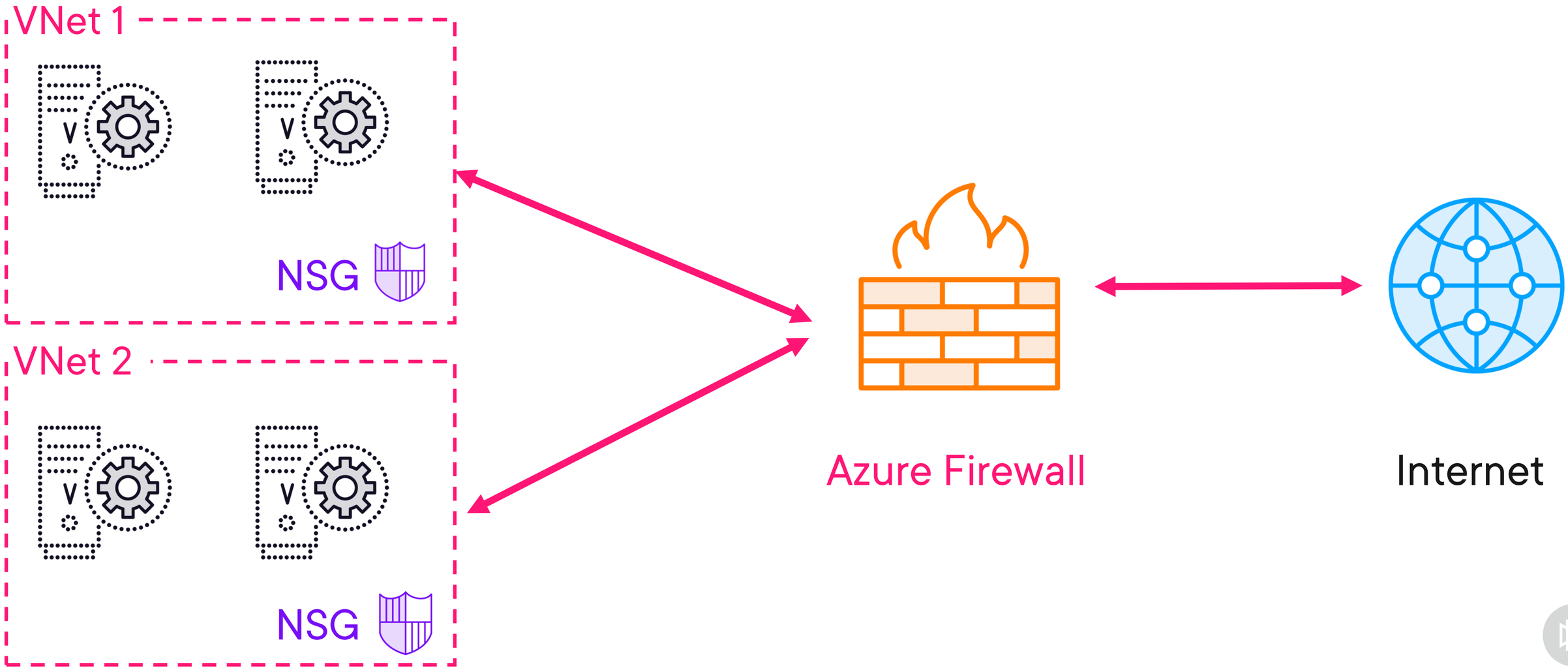
Cloud-based network security service that protects your Azure Virtual Network resources

Firewall as a service with built-in high availability and unrestricted cloud scalability

Azure Firewall allows you to secure multiple subscriptions/virtual networks

- Able to create L3 – L7 policies

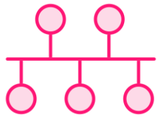
Azure Firewall vs. Azure NSG High-level Overview



Azure Firewall and Azure NSG are complementary. Together they provide better “Defense-in-Depth” network security.

Azure Firewall Features

Built-in high availability



Network and application-level filtering

Outbound SNAT (source network address translation) and inbound DNAT (destination network address translation)

Multiple public IP addresses

Threat intelligence and integration with Azure Monitor

Azure Firewall SKUs

Azure Firewall Basic

Recommended for SMB customers with throughput needs of 250 Mbps.

Azure Firewall Standard

Recommended for customers looking for Layer 3–Layer 7 firewall and needs autoscaling to handle peak traffic periods of up to 30 Gbps.

Azure Firewall Premium

Recommended to secure highly sensitive applications. It supports advanced threat protection capabilities like malware and TLS inspection.

Feature Comparison

Feature Category	Feature	Firewall Basic	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 250Mbps	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)			✓

https://learn.microsoft.com/en-us/azure/firewall/choose-firewall-sku

Azure DDoS Protection

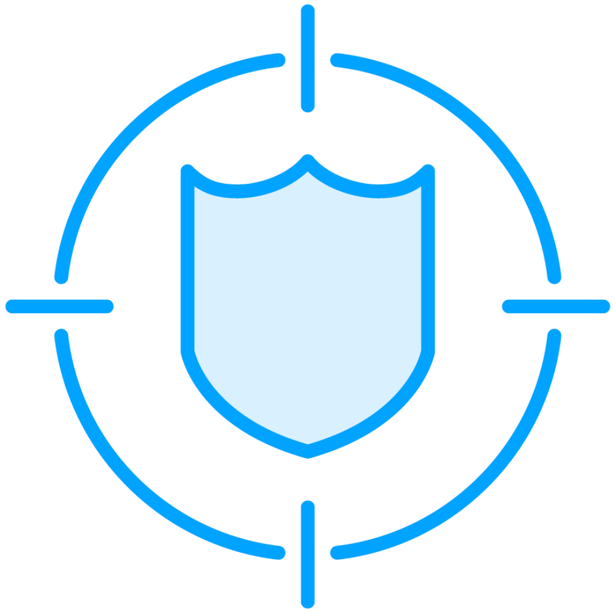
Distributed Denial of Service Attacks

Distributed denial of service (DDoS) attacks are some of the largest availability and security concerns facing customers that are moving their applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

Most Frequent Types of DDoS attacks

Volumetric attacks	These are volume-based attacks that flood the network layer with seemingly legitimate traffic, overwhelming the available bandwidth
Protocol attacks	Protocol attacks render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols
Resource layer attacks	These attacks target web application packets, to disrupt the transmission of data between hosts

Azure DDoS Infrastructure Protection



Every property in Azure is protected with DDOS Infrastructure protection

- At no additional cost!

Analyzes network traffic and discards anything that looks like a DDOS attack

- No user configuration or application changes

Protects all Azure services

- Including PaaS services

Two Premium SKUs

DDoS IP Protection

Pay-per-protected IP model SKU providing premium DDOS mitigation features and tuning capabilities

199$/IP/Month

DDoS Network Protection

Full network DDoS protection service with premium features such as DDoS rapid response support and cost protection

$2,944/month for 100 IPs

https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-sku-comparison

DDoS Network Protection Premium Features

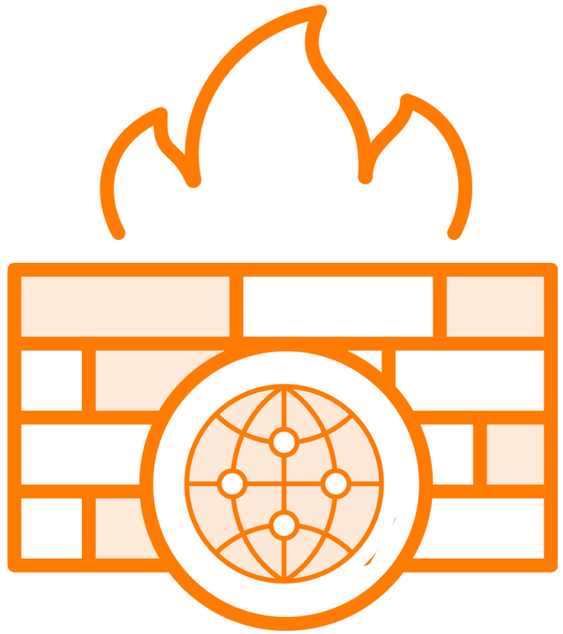
DDoS rapid response support

Cost protection

WAF discount

Azure Web Application Firewall

Azure Web Application Firewall (WAF)



Provides centralized protection of your web applications from common exploits and vulnerabilities

- SQL injection
- Cross-site scripting
- Remote file inclusion

Single WAF can protect up to 40 web applications

- Centralized management

Pre-built and custom policies

Web Application Firewall Key Benefits

Protection against threats and intrusions

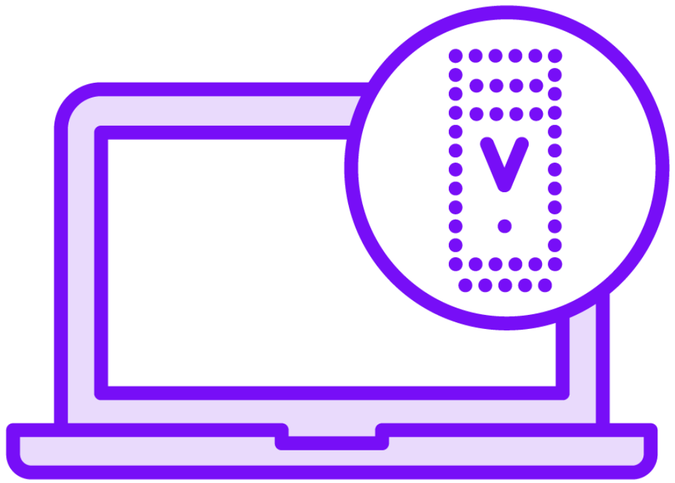
Simpler security management

Improves the response time to a security threat

Built-in monitoring

Azure Bastion

Azure Bastion



Provides secure and seamless RDP/SSH connectivity to your virtual machines

- Directly from the Azure Portal
  - Over TLS

PaaS managed service

No public IP or special tool needed on your virtual machines

Deployed at the virtual network level

Key Azure Bastion Features

RDP and SSH directly in Azure portal

Remote Session over TLS and firewall traversal for RDP/SSH

No Public IP required on the Azure VM

Protection against port scanning

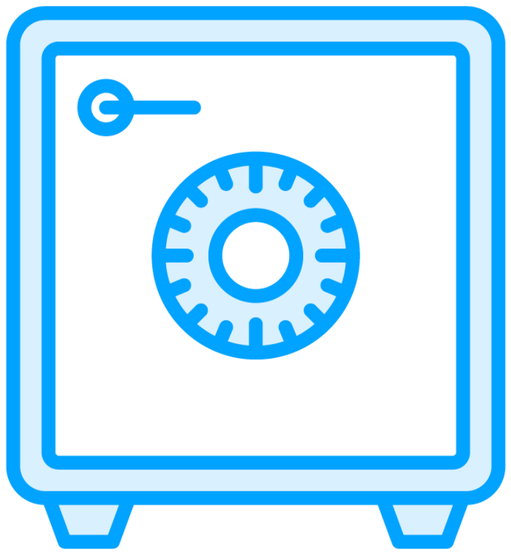
Protect against zero-day exploits

Demo

Azure Bastion

Azure Key Vault

Azure Key Vault



Cloud service for securely storing and accessing secrets

- Passwords
- API keys
- Certificates
- Cryptographic keys

Store secrets based by software or hardware security modules (HSMs)

All secrets are encrypted

Encryption on Azure

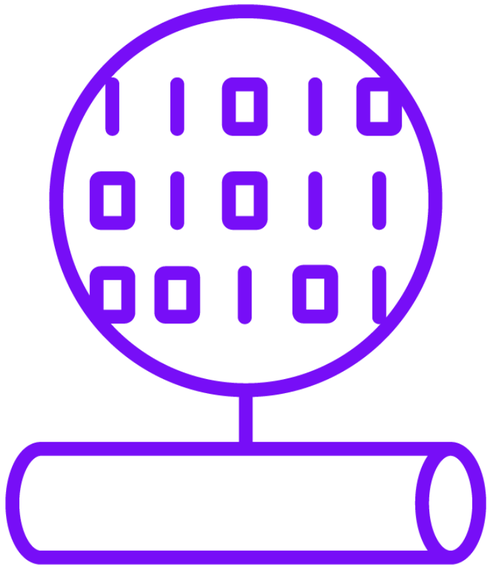
Encryption on Azure

Azure Storage Service Encryption

Azure disk encryption

Transparent data encryption

Azure Storage Service Encryption (SSE)



Azure SSE can automatically encrypt data before it's stored

- Azure Blob, Azure Files, Queue Storage
  - And automatically decrypted when you retrieve it

Process is completely transparent to users

Uses 256-bit Advanced Encryption Standard

- One of the strongest block ciphers available

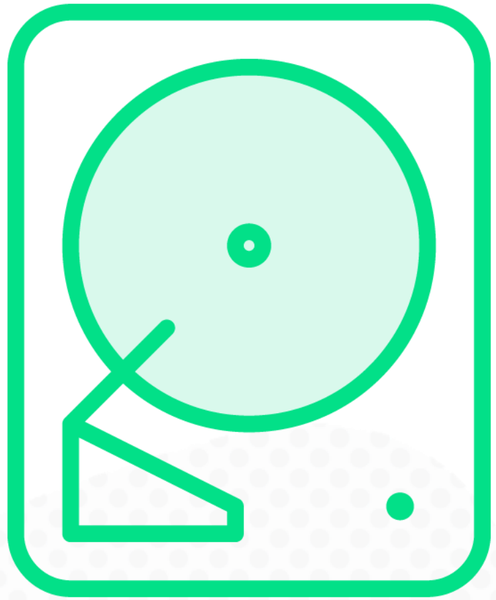
Azure Disk Encryption

Protect Windows and Linux based virtual machines

- Windows BitLocker
- Linux DM-Crypt

Encrypt both OS disks and data disks

Encryption keys and secrets stored in Azure Key Vault



Transparent Data Encryption

Used to encrypt data in real time

- SQL Server
- Azure SQL Database
- Azure Synapse Analytics

Protects data and log files

- Using AES and Triple Data Encryption Standard encryption algorithms

Enabled by default on newly created Azure SQL Databases

Module Conclusion

- Azure network security groups
- Azure Firewall
- Azure DDoS Protection
- Azure Web Application Firewall
- Azure Bastion
- Azure Key Vault
- Encryption on Azure

Up Next:

Security Management Capabilities in Microsoft Azure