O'REILLY®

Application Security in Azure

February/2020

Overview

What Applications are We Aiming to Protect?

- Hosted in Microsoft Azure

What Applications are We Aiming to Protect?

- Hosted in Microsoft Azure
  - PaaS (Hosted in Azure App Services)
    - Web applications
    - Serverless (e.g. Functions Apps)

What Applications are We Aiming to Protect?

- Hosted in Microsoft Azure
  - PaaS (Hosted in Azure App Services)
    - Web applications
    - Serverless (e.g. Functions Apps)
  - IaaS (Hosted in virtual machines)
    - Any applications

Topics to Cover in This Course

- Protecting applications hosted in the Microsoft Azure cloud

Topics to Cover in This Course

- Protecting applications hosted in the Microsoft Azure cloud
    - Protecting secrets in the application code (Azure KV, MSI)

Topics to Cover in This Course

- Protecting applications hosted in the Microsoft Azure cloud
  - Protecting secrets in the application code (Azure KV, MSI)
  - Protecting virtual machines (NSGs)

Topics to Cover in This Course

- Protecting applications hosted in the Microsoft Azure cloud
  - Protecting secrets in the application code (Azure KV, MSI)
  - Protecting virtual machines (NSGs)
  - Protecting web applications against common attacks (WAF)

Protecting Secrets in the Application Code

Protecting Secrets in the Application Code

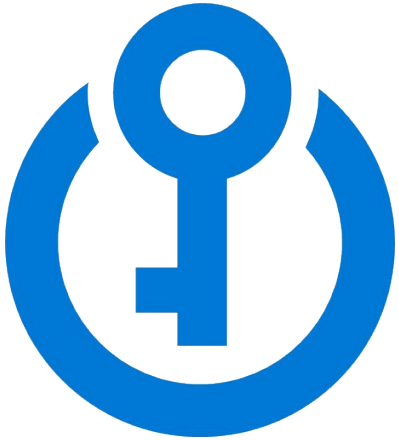
```
public class ValuesController : ApiController
{
    // GET api/values
    public Dictionary<string, string> Get()
    {
        var connectingString = "Server=tcp:azuresqlmsidemosrv.database.windows.net,1433;" +
            "Initial Catalog=MSIDEMO;Persist Security Info=False" +
            ";MultipleActiveResultSets=False;" +
            "Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;";

        var capitals = new Dictionary<string, string>();

        using (var sqlConnection = new SqlConnection(connectingString))
        {
            var sqlCommand = new SqlCommand("SELECT Country, Capital FROM CountryInfo", sqlConnection);

            var accessToken = (new AzureServiceTokenProvider()).GetAccessTokenAsync("https://database.windows.net/").Result;
            sqlConnection.AccessToken = accessToken;

            sqlConnection.Open();

            var reader = sqlCommand.ExecuteReader();
```

Protecting Secrets in the Application Code

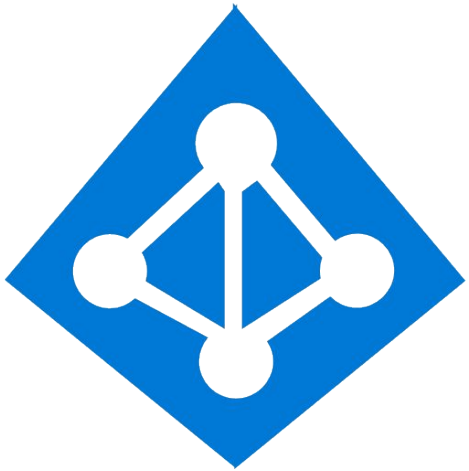
Protecting Secrets in the Application Code

Azure Key Vault

Protecting Secrets in the Application Code



Azure Key Vault



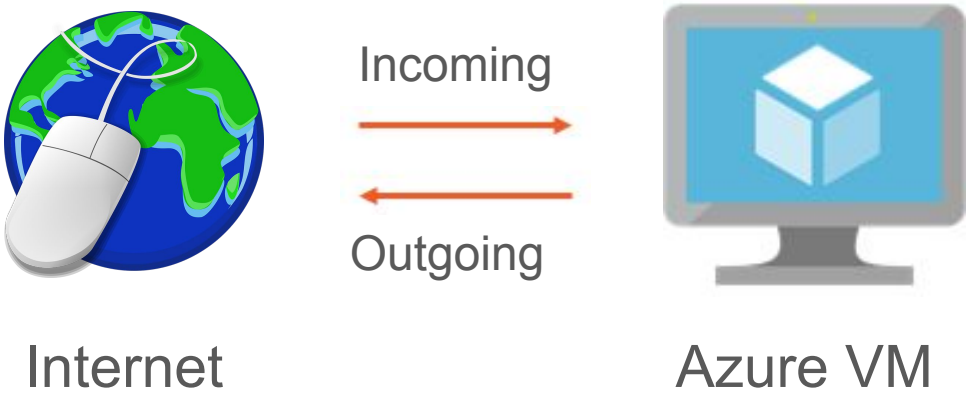
Managed Identity (MSI)

Protecting virtual machines (NSGs)

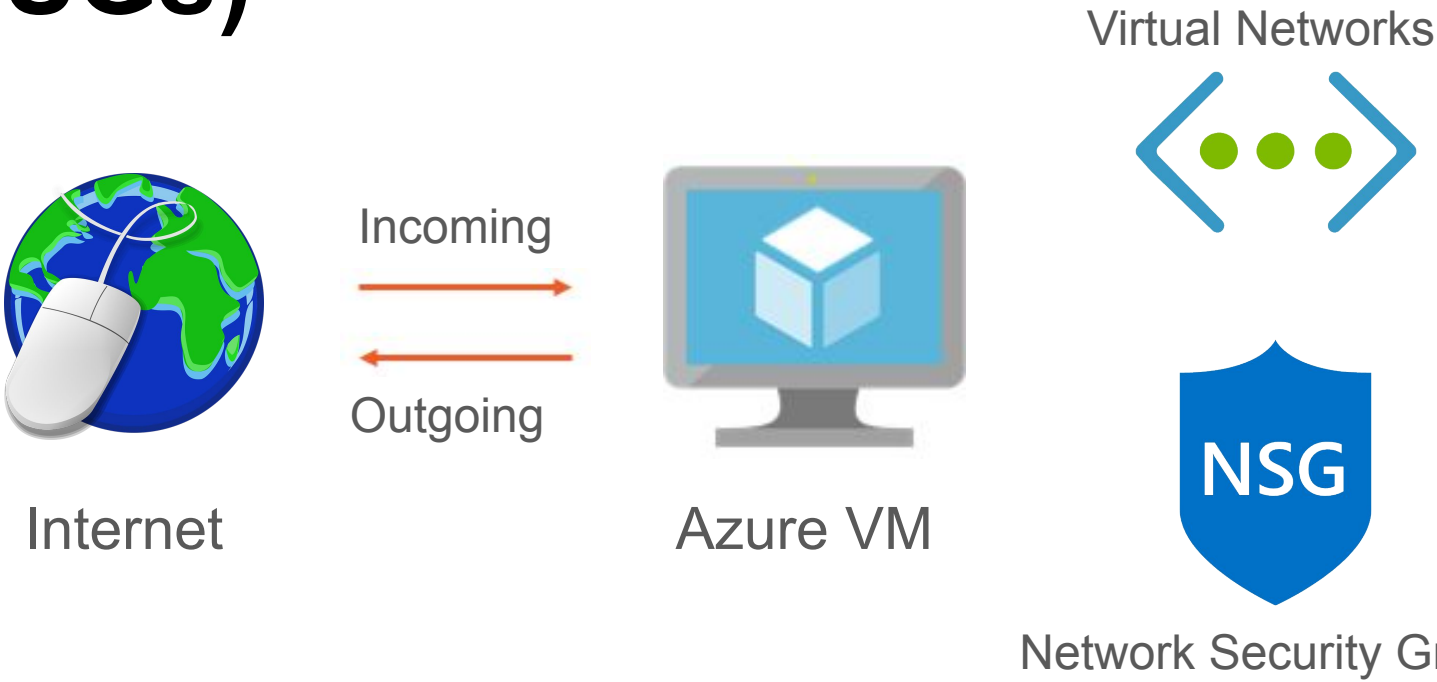
Protecting virtual machines (NSGs)

Azure VM

Protecting virtual machines (NSGs)



Protecting virtual machines (NSGs)



Protecting web applications against common attacks (WAF)

Protecting web applications against common attacks (WAF)

App Services

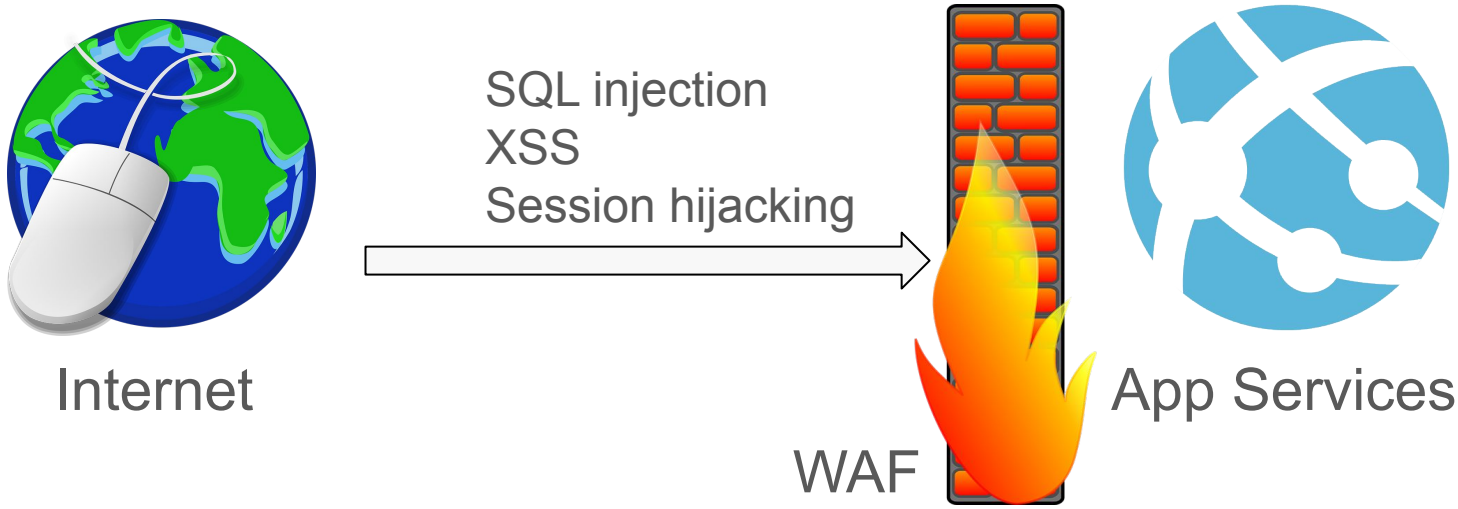
Protecting web applications against common attacks (WAF)

Internet

SQL injection
XSS
Session hijacking

App Services

Protecting web applications against common attacks (WAF)

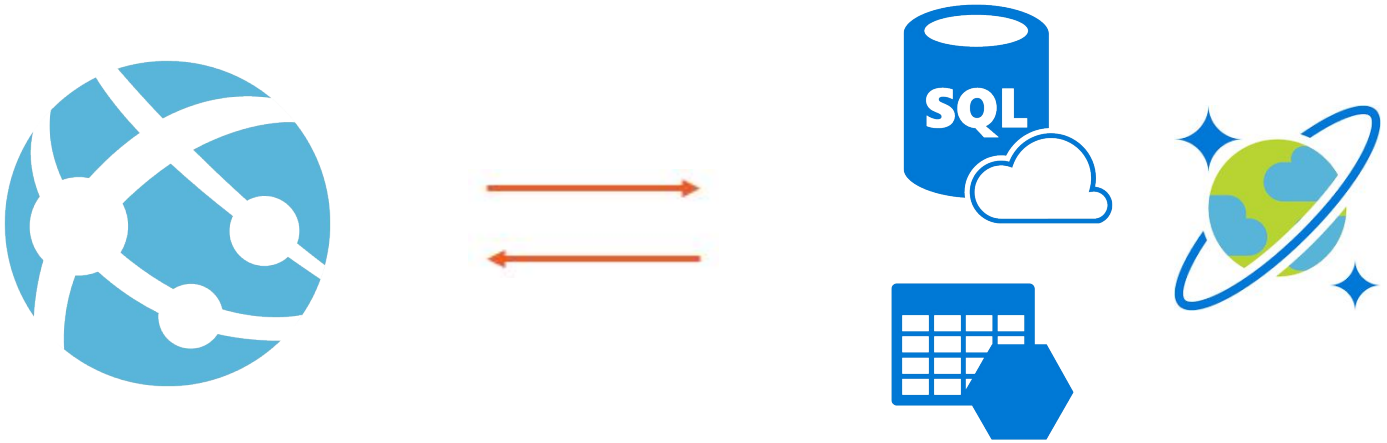


Application Security Comes Hand in Hand with Data Security

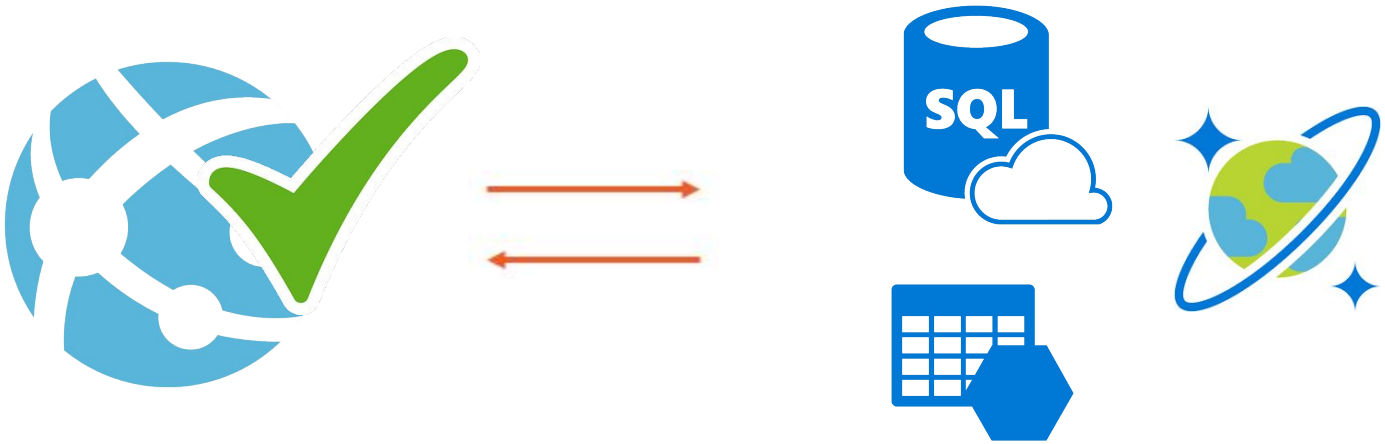
Application Security Comes Hand in Hand with Data Security

Application

Application Security Comes Hand in Hand with Data Security



Application Security Comes Hand in Hand with Data Security



Application Security Comes Hand in Hand with Data Security

Application Security Comes Hand in Hand with Data Security

- Securing Data in Microsoft Azure

Application Security Comes Hand in Hand with Data Security

- Securing Data in Microsoft Azure
  - Securing data in transit
    - SSL/TLS

Application Security Comes Hand in Hand with Data Security

- Securing Data in Microsoft Azure
  - Securing data in transit
    - SSL/TLS
  - Securing data at rest
    - Azure SQL Database
    - Azure Cosmos DB
    - Azure Storage Account

Application Security Comes Hand in Hand with Data Security

- Securing Data in Microsoft Azure
  - Securing data in transit
    - SSL/TLS
  - Securing data at rest
    - Azure SQL Database
    - Azure Cosmos DB
    - Azure Storage Account
  - Securing data in use
    - Azure Confidential Compute

Protecting Secrets in the Code

Azure Key Vault and Managed Identities

Protecting Secrets in the Application Code

Protecting Secrets in the Application Code

```
public class ValuesController : ApiController
{
    // GET api/values
    public Dictionary<string, string> Get()
    {
        var connectingString = "Server=tcp:azuresqlmsidemosrv.database.windows.net,1433;" +
            "Initial Catalog=MSIDEMO;Persist Security Info=False" +
            ";MultipleActiveResultSets=False;" +
            "Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;";

        var capitals = new Dictionary<string, string>();

        using (var sqlConnection = new SqlConnection(connectingString))
        {
            var sqlCommand = new SqlCommand("SELECT Country, Capital FROM CountryInfo", sqlConnection);

            var accessToken = (new AzureServiceTokenProvider()).GetAccessTokenAsync("https://database.windows.net/").Result;
            sqlConnection.AccessToken = accessToken;

            sqlConnection.Open();

            var reader = sqlCommand.ExecuteReader();
```

Protecting Secrets in the Application Code

Protecting Secrets in the Application Code

- Secrets:

Protecting Secrets in the Application Code

- Secrets:
  - Database connection strings

Protecting Secrets in the Application Code

- Secrets:
  - Database connection strings
  - Passwords

Protecting Secrets in the Application Code

- Secrets:
  - Database connection strings
  - Passwords
  - Encryption keys

Protecting Secrets in the Application Code

- Secrets:
  - Database connection strings
  - Passwords
  - Encryption keys
  - Cache connection strings

Protecting Secrets in the Application Code

- Secrets:
  - Database connection strings
  - Passwords
  - Encryption keys
  - Cache connection strings
  - Any sensitive data

Protecting Secrets in the Application Code

- Secrets:
  - Database connection strings
  - Passwords
  - Encryption keys
  - Cache connection strings
  - Any sensitive data
- These secrets should NOT live in the application source code

Protecting Secrets in the Application Code

- Why?

Protecting Secrets in the Application Code

- Why?
  - Code will be checked into the source control.

Protecting Secrets in the Application Code

- Why?
  - Code will be checked into the source control.
  - No easy way to rotate or expire these secrets.

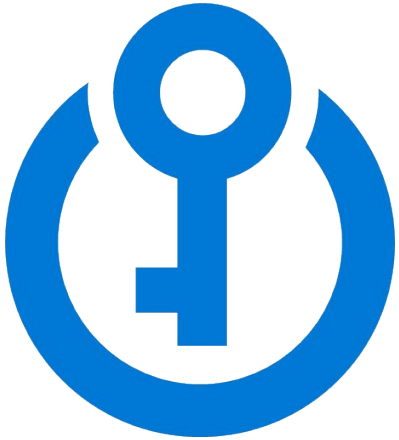
Protecting Secrets in the Application Code

- Why?
  - Code will be checked into the source control.
  - No easy way to rotate or expire these secrets.
  - No easy way to control access to the secrets.

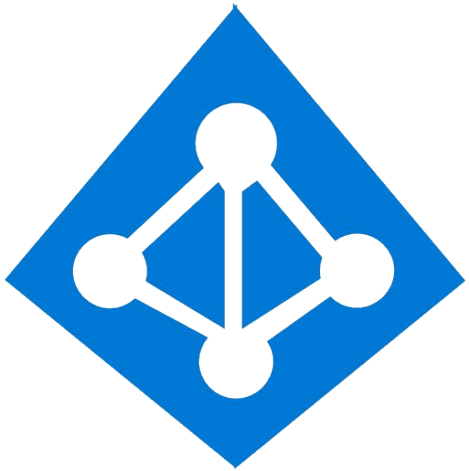
Protecting Secrets in the Application Code

- Why?
  - Code will be checked into the source control.
  - No easy way to rotate or expire these secrets.
  - No easy way to control access to the secrets.
  - Maintenance nightmare

Protecting Secrets in the Application Code

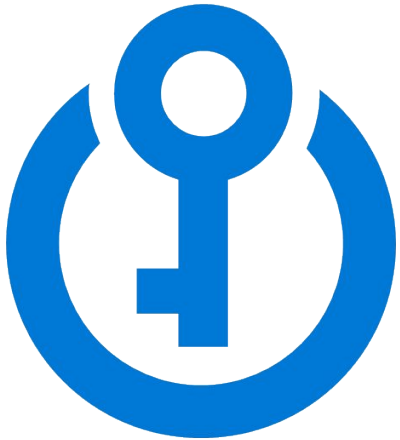


Azure Key Vault



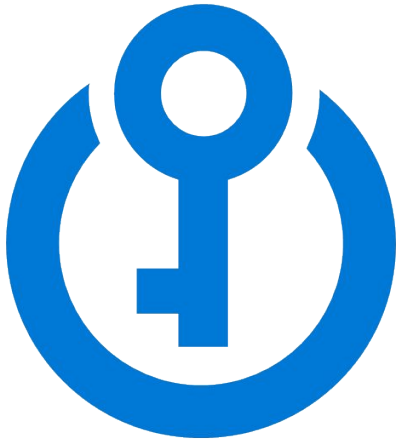
Managed Identity (MSI)

Azure Key Vault



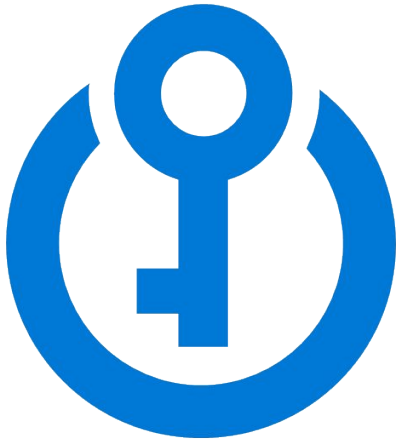
Azure Key Vault

- Can be used to Securely store and tightly control access to:



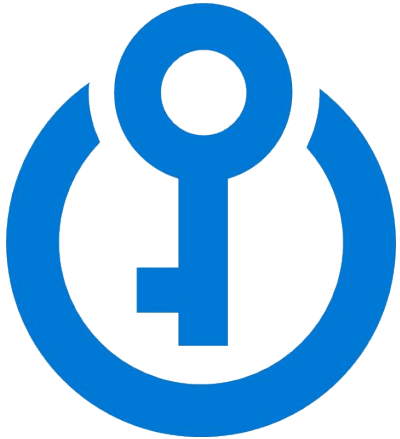
Azure Key Vault

- Can be used to Securely store and tightly control access to:
  - Tokens



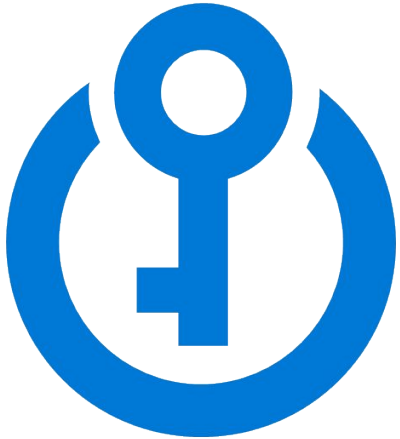
Azure Key Vault

- Can be used to Securely store and tightly control access to:
  - Tokens
  - Passwords



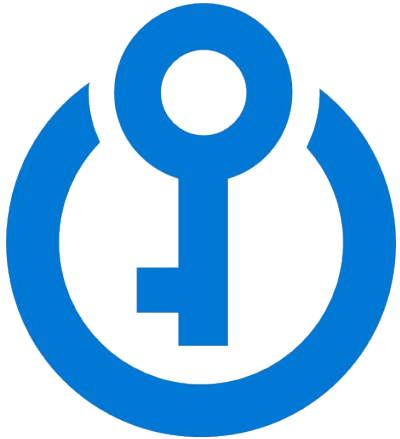
Azure Key Vault

- Can be used to Securely store and tightly control access to:
  - Tokens
  - Passwords
  - Certificates



Azure Key Vault

- Can be used to Securely store and tightly control access to:
  - Tokens
  - Passwords
  - Certificates
  - API keys, and other secrets

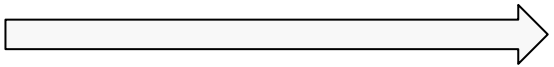


Azure Key Vault

Stores the connection string in the code

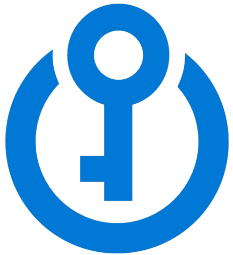
Azure Key Vault

Use the connection string

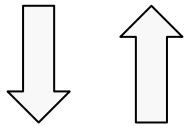


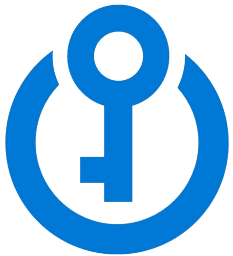
Stores the connection string
in the code

Azure Key Vault



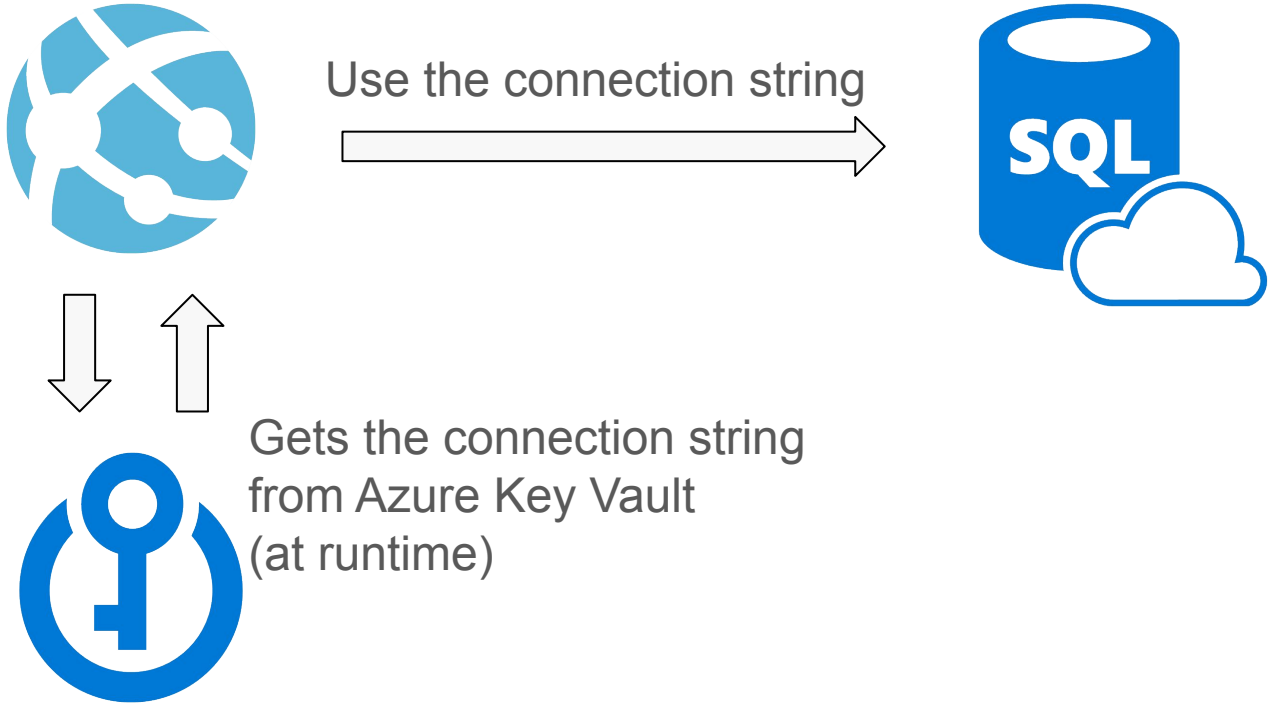
Azure Key Vault





Gets the connection string
from Azure Key Vault
(at runtime)

Azure Key Vault



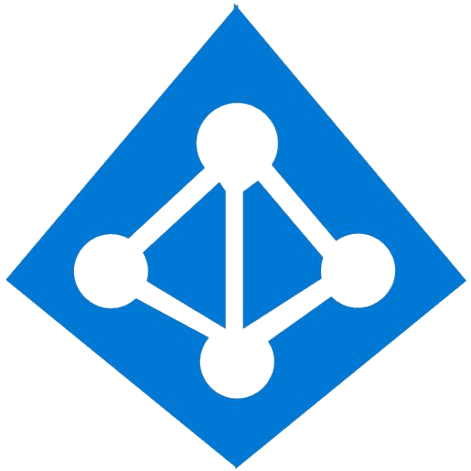
Protecting Secrets in the Application Code

```
public class ValuesController : ApiController
{
    // GET api/values
    public Dictionary<string, string> Get()
    {
        var connectingString = "Server=tcp:azuresqlmsidemosrv.database.windows.net,1433;" +
            "Initial Catalog=MSIDEMO;Persist Security Info=False" +
            ";MultipleActiveResultSets=False;" +
            "Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;";

        var capitals = new Dictionary<string, string>();

        using (var sqlConnection = new SqlConnection(connectingString))
        {
            var sqlCommand = new SqlCommand("SELECT Country, Capital FROM CountryInfo", sqlConnection);

            var accessToken = (new AzureServiceTokenProvider()).GetAccessTokenAsync("https://database.windows.net/").Result;
            sqlConnection.AccessToken = accessToken;

            sqlConnection.Open();

            var reader = sqlCommand.ExecuteReader();
```

Protecting Secrets in the Application Code

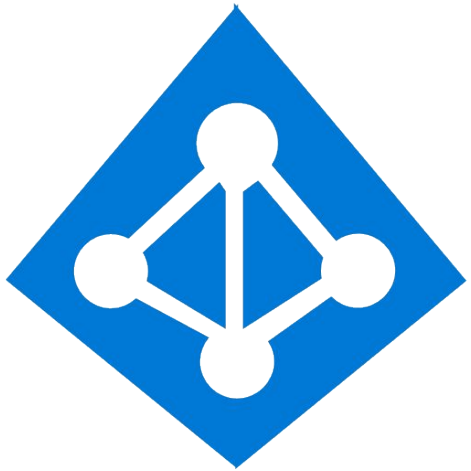
```
[FunctionName("GetSecretFromKV")]
public static  IActionResult Run(
    [HttpTrigger(AuthorizationLevel.Function, "get", "post", Route = null)] HttpRequest req,
    ILogger log)
{
    var kv = new KeyVaultClient(new KeyVaultClient.AuthenticationCallback(GetAccessToken));

    var secretUrl = "https://kv-msi-01.vault.azure.net/secrets/myname/56c2905096f14c689d928da072139c72";
    var secret = kv.GetSecretAsync(secretUrl).Result;
    var myName = secret.Value;

    return myName != null
        ? (ActionResult)new OkObjectResult($"Hello, {myName}")
        : new BadRequestObjectResult("Please pass a name on the query string or in the request body");
}

private static async Task<string> GetAccessToken(string authority, string resource, string scope)
{
```

Managed Identity (MSI)



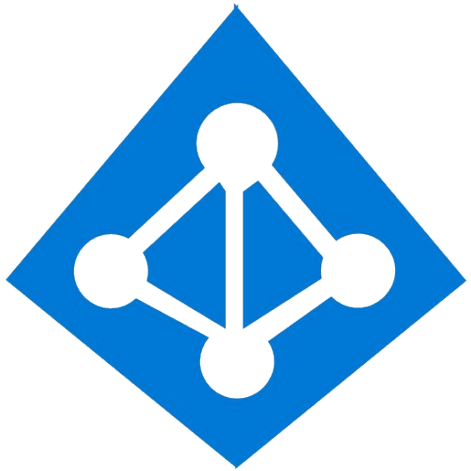
Managed Identity (MSI)

- Provides Azure services with an automatically managed identity.



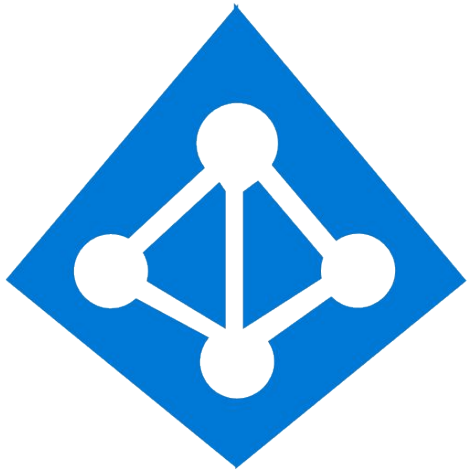
Managed Identity (MSI)

- Provides Azure services with an automatically managed identity.
- Authenticate to any supporting service without any credentials in your code.



Managed Identity (MSI)

- Provides Azure services with an automatically managed identity.
- Authenticate to any supporting service without any credentials in your code.
- You can achieve **credential-free code**.



Credential-free Code

Credential-free Code

Credential-free Code

```
try
{
    using (var sqlConnection = new SqlConnection(connectingString))
    {
        var sqlCommand = new SqlCommand("SELECT Country, Capital FROM CountryInfo", sqlConnection);

        var accessToken = (new AzureServiceTokenProvider()).GetAccessTokenAsync("https://database.windows.net/").Result;
        sqlConnection.AccessToken = accessToken;

        sqlConnection.Open();

        var reader = sqlCommand.ExecuteReader();

        while (reader.Read())
        {
            capitals.Add(reader["Country"].ToString(), reader["Capital"].ToString());
        }

        sqlConnection.Close();
    }
}
```

Demo

- Protecting secrets with Azure Key Vault
- Credential-free code with Managed Identities (MSI)

Exercise

- Working with the Azure Key Vault
  - Change the existing application to read secrets from KV
  - Verify the updated application

Q&A

Break (5 minutes)

Q&A

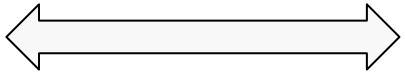
Securing Communications

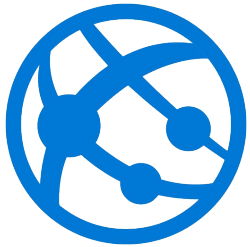
SSL & TLS

Securing Communications

Securing Communications

Brower

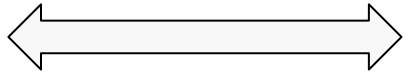




Server
Apps

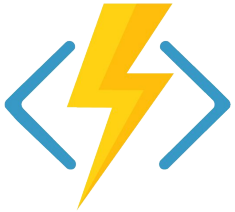
Securing Communications

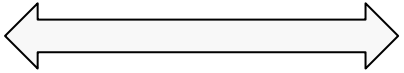
Brower



Server
Apps

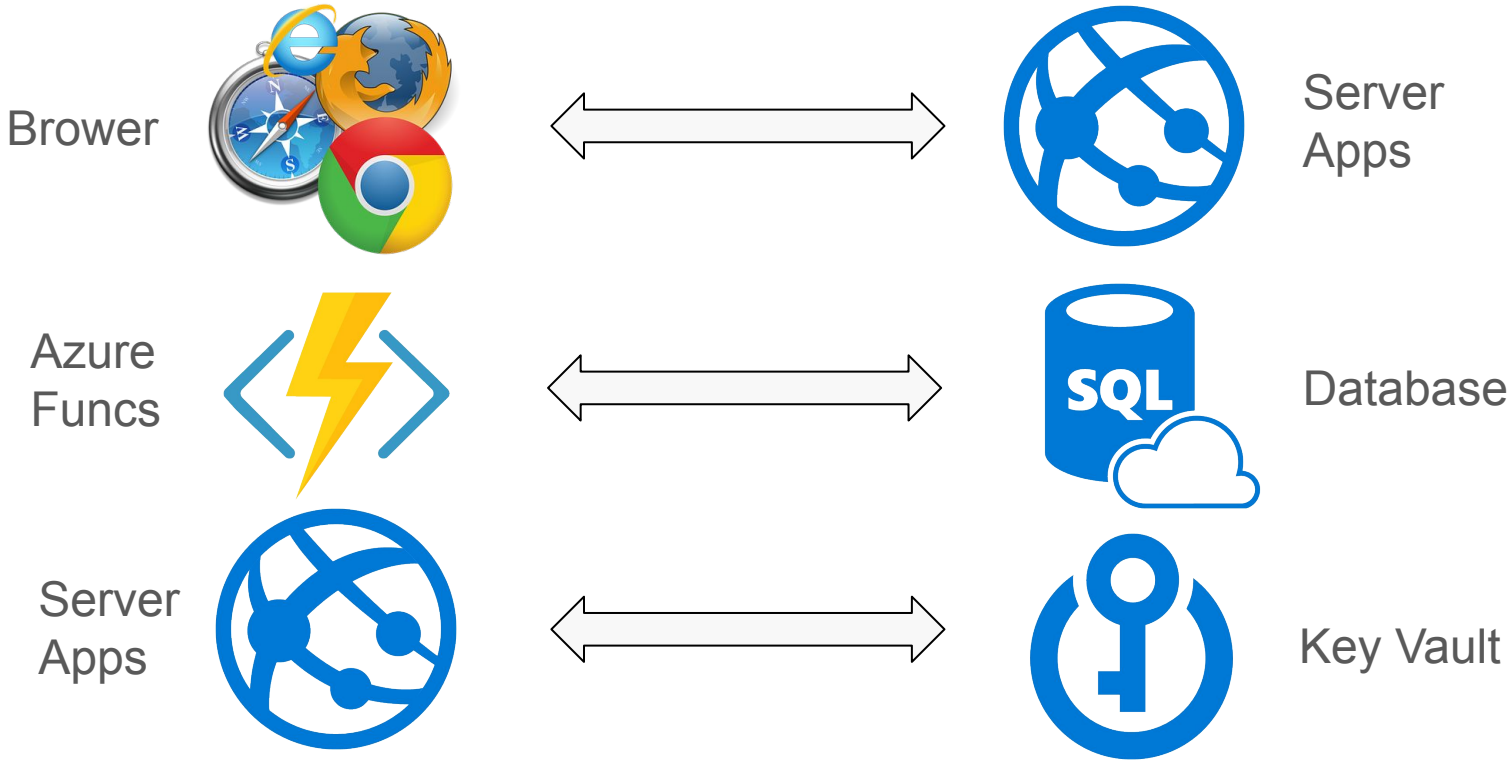
Azure
Funcs





Database

Securing Communications



Securing Communications

Securing Communications

- All communications should be protected

Securing Communications

- All communications should be protected
    - Client to server

Securing Communications

- All communications should be protected
  - Client to server
  - Server to server

Securing Communications

- All communications should be protected
  - Client to server
  - Server to server
  - Process to process

Securing Communications

- All communications should be protected
  - Client to server
  - Server to server
  - Process to process
- SSL/TLS is the main technology used to protect communications

Securing Communications

- All communications should be protected
  - Client to server
  - Server to server
  - Process to process
- SSL/TLS is the main technology used to protect communications
  - Encrypts the packets at the source

Securing Communications

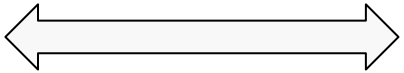
- All communications should be protected
  - Client to server
  - Server to server
  - Process to process
- SSL/TLS is the main technology used to protect communications
  - Encrypts the packets at the source
  - Decrypts the packets at the destination

Securing Communications

- All communications should be protected
  - Client to server
  - Server to server
  - Process to process
- SSL/TLS is the main technology used to protect communications
  - Encrypts the packets at the source
  - Decrypts the packets at the destination
  - Public and private keys are used

Securing Communications (SSL)

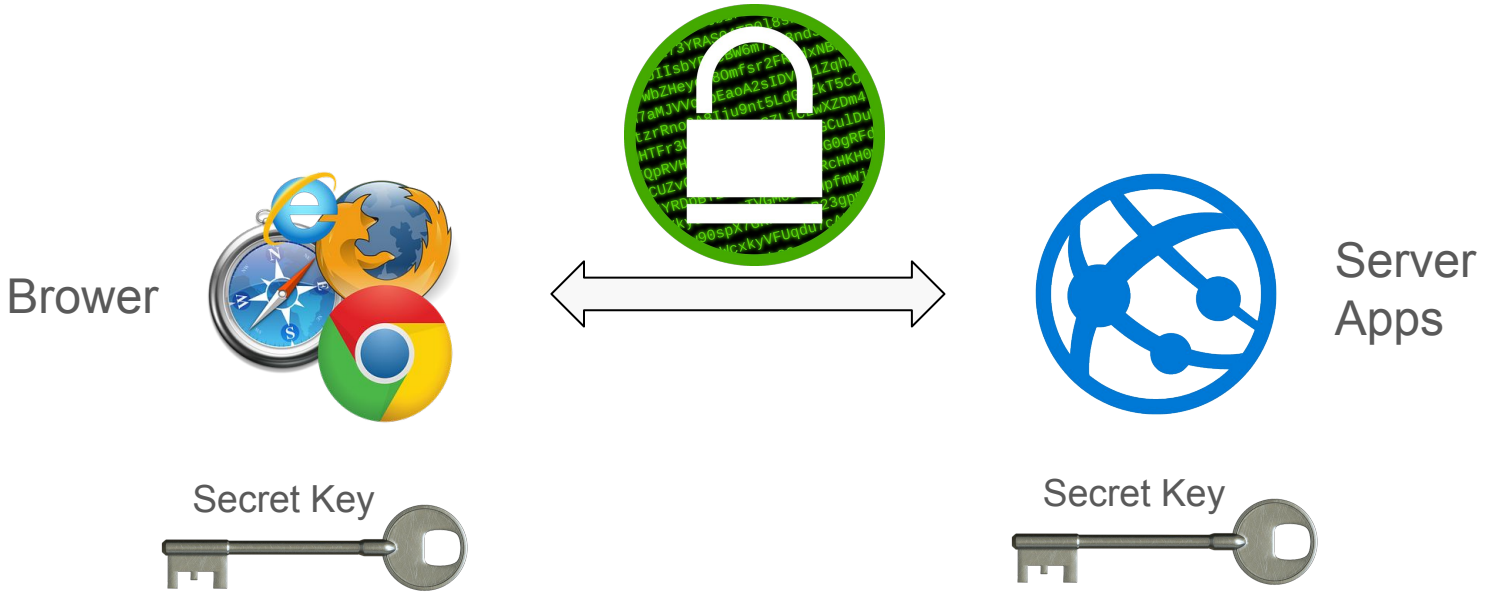
Brower



Server
Apps

Securing Communications (SSL)

Securing Communications (SSL)



Securing Communications (SSL)

Securing Communications (SSL)

- SSL protocol is deprecated

Securing Communications (SSL)

- SSL protocol is deprecated
- Transport Layer Security (TLS) has replaced it

Securing Communications (SSL)

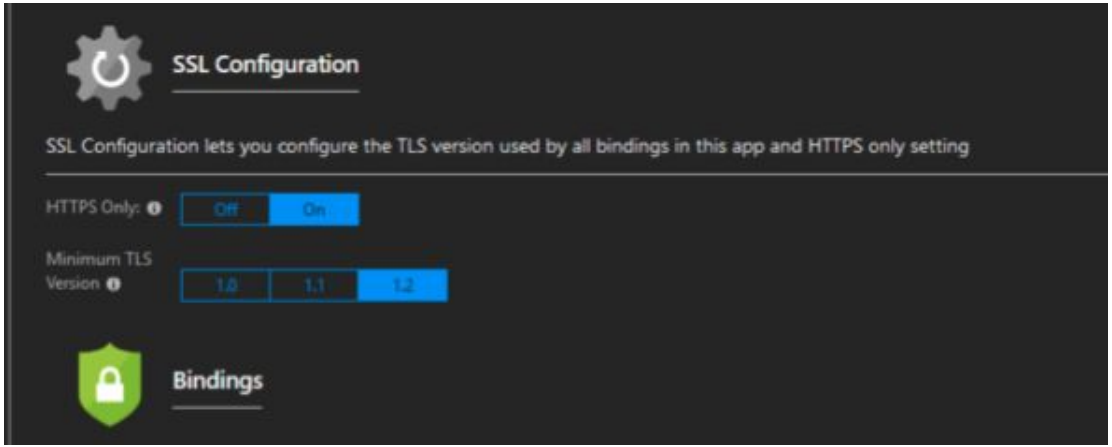
- SSL protocol is deprecated
- Transport Layer Security (TLS) has replaced it
    - TLS 1.0, 1.1, 1.2 & 1.3

Securing Communications (SSL)

- SSL protocol is deprecated
- Transport Layer Security (TLS) has replaced it
  - TLS 1.0, 1.1, 1.2 & 1.3
- Microsoft Azure

Securing Communications (SSL)

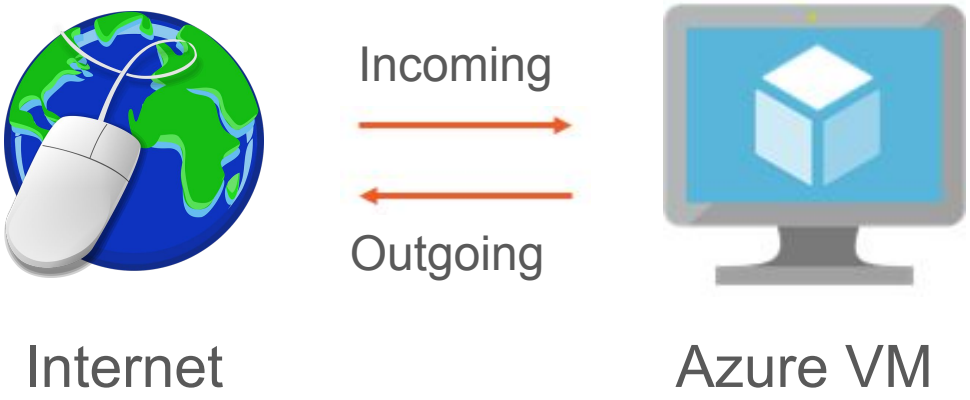
- SSL protocol is deprecated
- Transport Layer Security (TLS) has replaced it
  - TLS 1.0, 1.1, 1.2 & 1.3
- Microsoft Azure
  - 1.0, 1.1, 1.2



Protecting Virtual Machines

Network Security Groups (NSGs) & ASGs

Protecting virtual machines (NSGs)



Protecting virtual machines (NSGs)

Internet

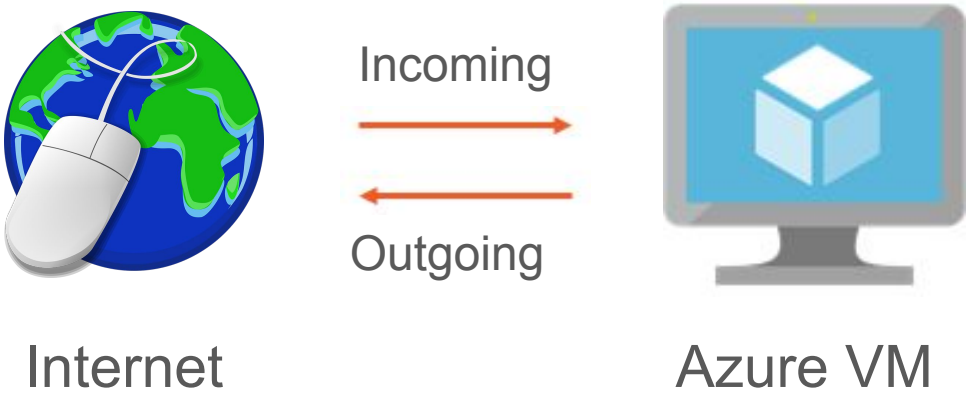
Incoming

Outgoing

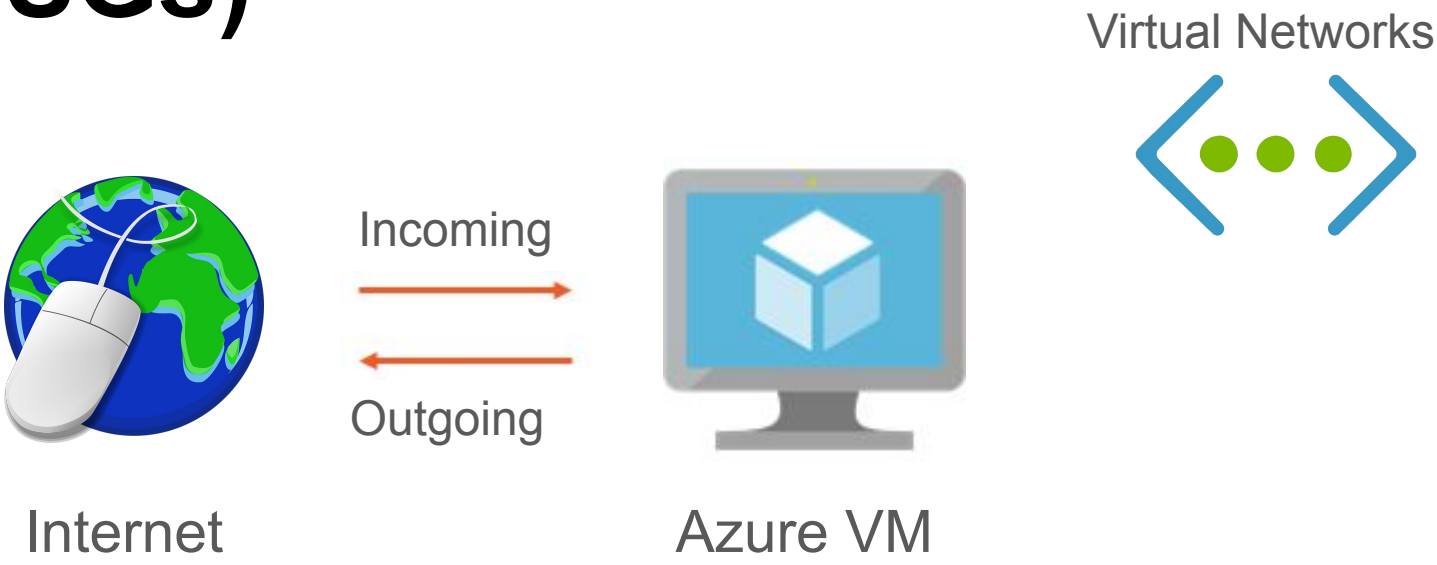
Azure VM

- Unprotected TCP ports:
  - 3389
  - 22
  - 80
  - 443
  - 25, 465
- Any IP is allowed
- Incoming & outgoing

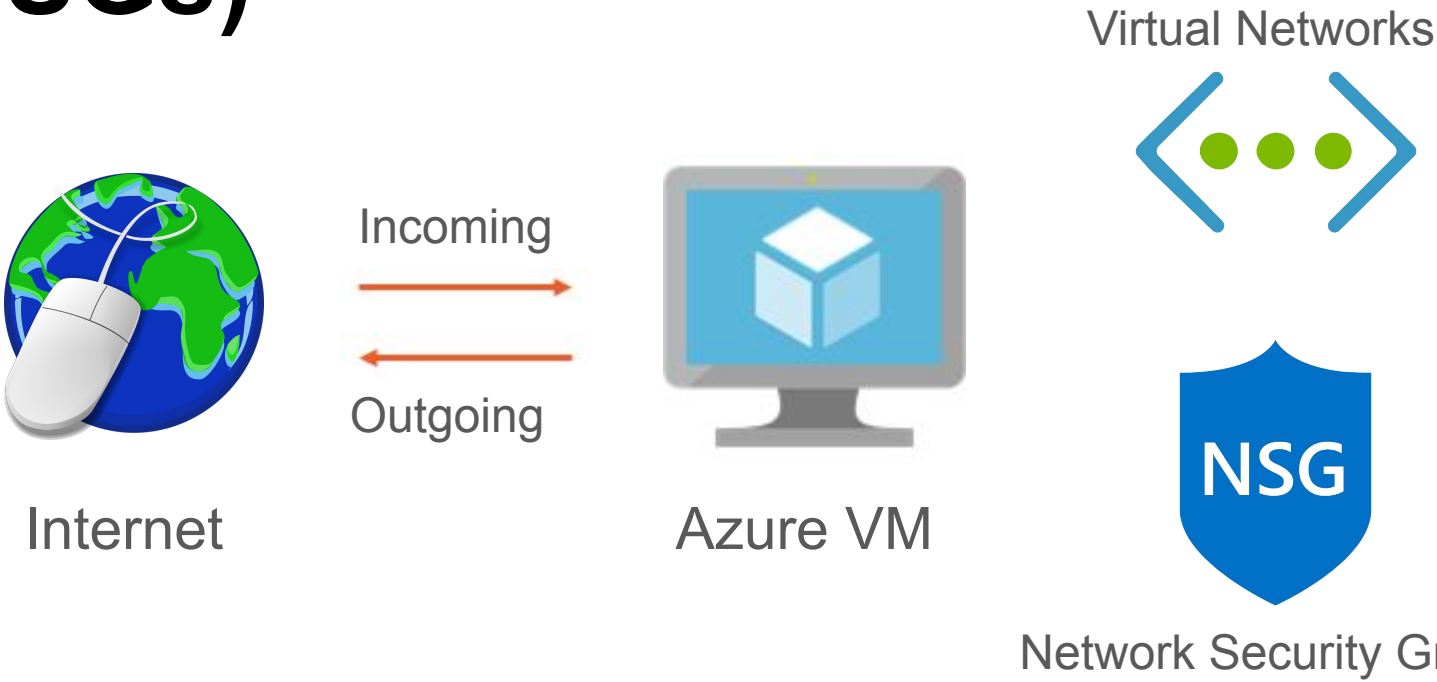
Protecting virtual machines (NSGs)



Protecting virtual machines (NSGs)



Protecting virtual machines (NSGs)

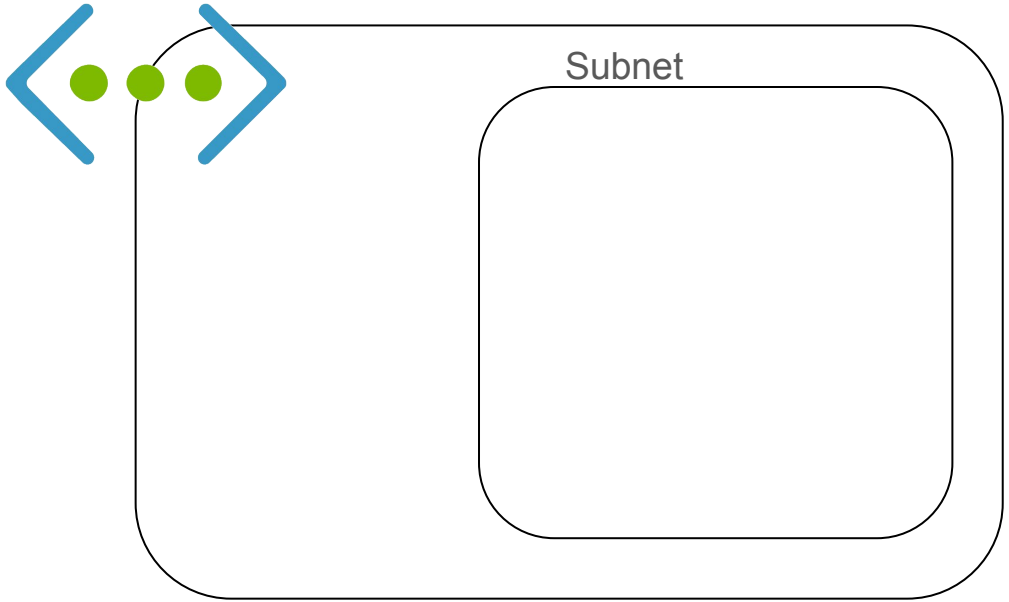


Protecting virtual machines (NSGs)

Protecting virtual machines (NSGs)

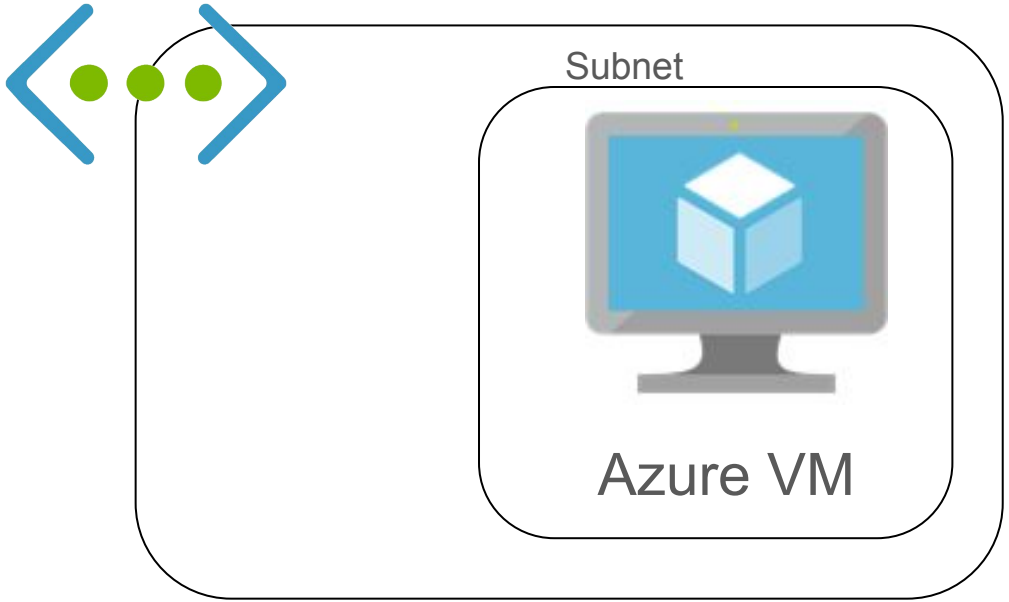
1. Create a VN

Protecting virtual machines (NSGs)



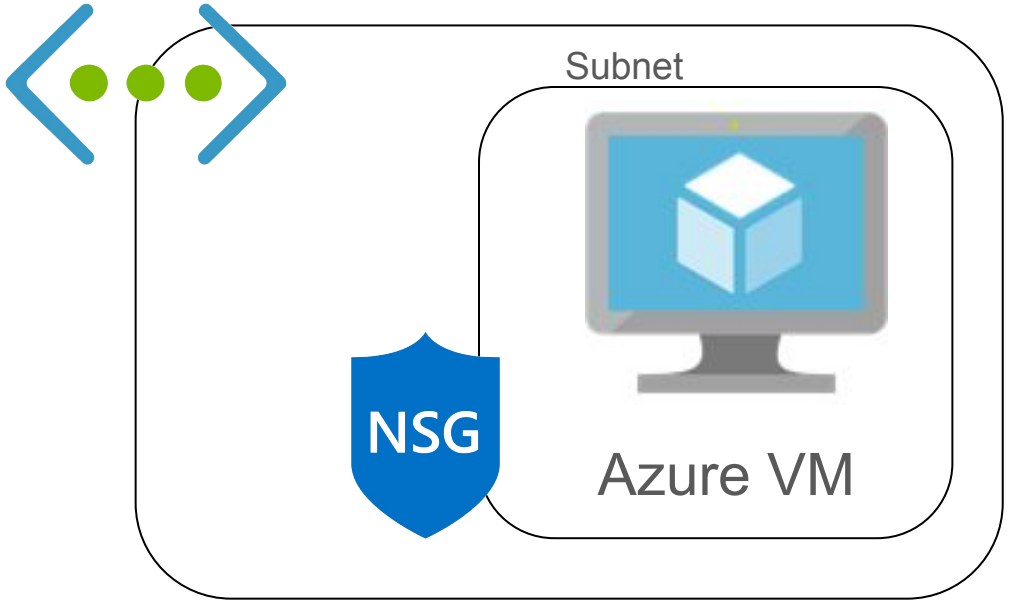
1. Create a VN
2. Add a subnet to VN

Protecting virtual machines (NSGs)



1. Create a VN
2. Add a subnet to VN
3. Add your VM to the subnet

Protecting virtual machines (NSGs)



1. Create a VN
2. Add a subnet to VN
3. Add your VM to the subnet
4. Assign NSG to the subnet

Protecting virtual machines (NSGs)

- Network Security Groups (NSGs)

Protecting virtual machines (NSGs)

- Network Security Groups (NSGs)
  - Filter network traffic to and from Azure resources

Protecting virtual machines (NSGs)

- Network Security Groups (NSGs)
  - Filter network traffic to and from Azure resources
    - Using security rules

Protecting virtual machines (NSGs)

- Network Security Groups (NSGs)
  - Filter network traffic to and from Azure resources
    - Using security rules
      - Inbound

Protecting virtual machines (NSGs)

- Network Security Groups (NSGs)
  - Filter network traffic to and from Azure resources
    - Using security rules
      - Inbound
      - Outbound

Protecting virtual machines (NSGs)

- Network Security Groups (NSGs)
  - Filter network traffic to and from Azure resources
    - Using security rules
      - Inbound
      - Outbound
    - Security rules have priorities

Protecting virtual machines (NSGs)

- Network Security Groups (NSGs)
  - Filter network traffic to and from Azure resources
    - Using security rules
      - Inbound
      - Outbound
    - Security rules have priorities
      - Lower priority number overrides higher numbers

Security Rules - Inbound

Inbound

AllowVNetInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowAzureLoadBalancerInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow

DenyAllInbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Security Rules - Inbound

Inbound

AllowVNetInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowAzureLoadBalancerInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow

DenyAllInbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Security Rules - Inbound

Inbound

AllowVNetInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowAzureLoadBalancerInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow

DenyAllInbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Security Rules - Inbound

Inbound

AllowVNetInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowAzureLoadBalancerInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow

DenyAllInbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Security Rules - Outbound

Outbound

AllowVnetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowInternetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	Any	Allow

DenyAllOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Security Rules - Outbound

Outbound

AllowVnetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowInternetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	Any	Allow

DenyAllOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Security Rules - Outbound

Outbound

AllowVnetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowInternetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	Any	Allow

DenyAllOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Security Rules - Outbound

Outbound

AllowVnetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

AllowInternetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	Any	Allow

DenyAllOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

Security Rule Properties

Security Rule Properties

1. Name

Security Rule Properties

1. Name
2. Priority (100-4096)

Security Rule Properties

1. Name
2. Priority (100-4096)
3. Source / Destination (IP, IP range or service tag)

Security Rule Properties

1. Name
2. Priority (100-4096)
3. Source / Destination (IP, IP range or service tag)
4. Protocol (TCP, UDP, Any)

Security Rule Properties

1. Name
2. Priority (100-4096)
3. Source / Destination (IP, IP range or service tag)
4. Protocol (TCP, UDP, Any)
5. Direction (Inbound, Outbound)

Security Rule Properties

1. Name
2. Priority (100-4096)
3. Source / Destination (IP, IP range or service tag)
4. Protocol (TCP, UDP, Any)
5. Direction (Inbound, Outbound)
6. Port (Single or range)

Security Rule Properties

1. Name
2. Priority (100-4096)
3. Source / Destination (IP, IP range or service tag)
4. Protocol (TCP, UDP, Any)
5. Direction (Inbound, Outbound)
6. Port (Single or range)
7. Access (Allow, Deny)

Demo

- Controlling incoming and outgoing traffic for VMs
  - Network Security Groups (NSGs)

Exercise

- Working with Network Security Groups (NSGs)
  - Allow Remote Desktop for a VM
  - Examine security rule properties and priority

Q&A

Break (5 minutes)

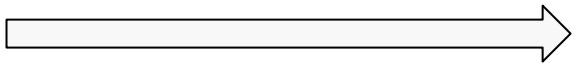
Q&A

Protecting Web Applications

Azure Web Application Firewall (WAF)

Protecting web applications against common attacks (WAF)

Internet



App Services

Protecting web applications against common attacks (WAF)

Internet

SQL injection
XSS
Session hijacking

App Services

Protecting web applications against common attacks (WAF)

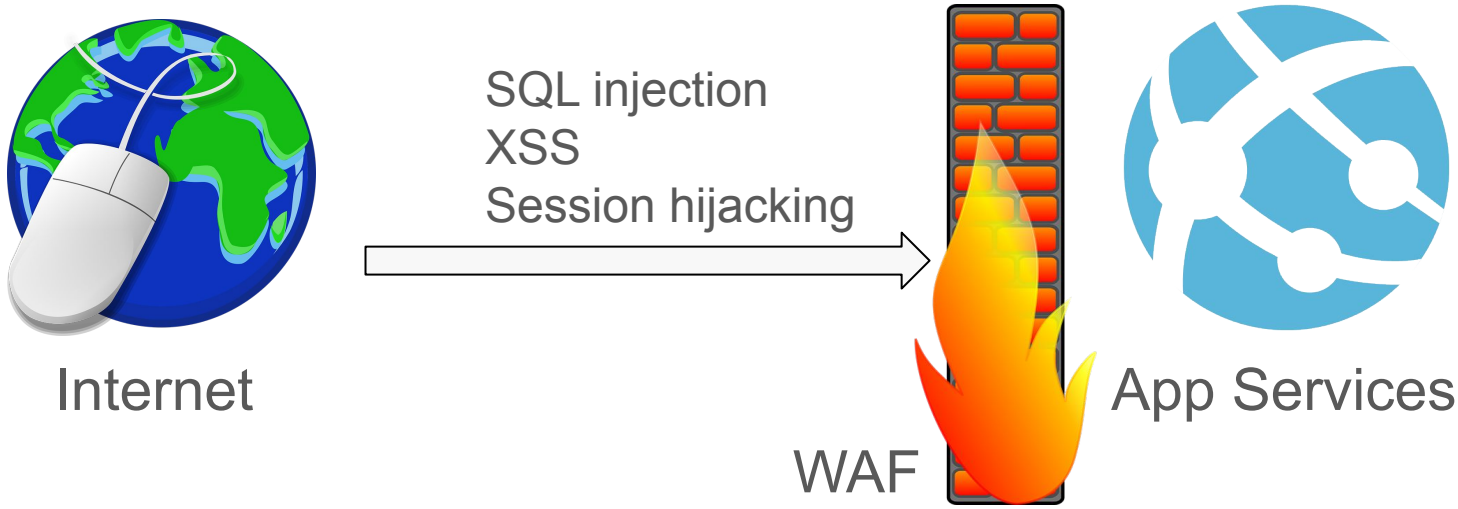
Internet

SQL injection
XSS
Session hijacking

Deal with the attacks at the code level

App Services

Protecting web applications against common attacks (WAF)



Protecting web applications against common attacks (WAF)

Protecting web applications against common attacks (WAF)

- SQL-injection

Protecting web applications against common attacks (WAF)

- SQL-injection
- Cross-site scripting (XSS)

Protecting web applications against common attacks (WAF)

- SQL-injection
- Cross-site scripting (XSS)
- Remote file inclusion

Protecting web applications against common attacks (WAF)

- SQL-injection
- Cross-site scripting (XSS)
- Remote file inclusion
- Missing HTTP headers

Protecting web applications against common attacks (WAF)

- SQL-injection
- Cross-site scripting (XSS)
- Remote file inclusion
- Missing HTTP headers
- Bots, crawlers, scanners

Protecting web applications against common attacks (WAF)

- SQL-injection
- Cross-site scripting (XSS)
- Remote file inclusion
- Missing HTTP headers
- Bots, crawlers, scanners
- Oversized request

Protecting web applications against common attacks (WAF)

- WAF is NOT a stand-alone Azure service

Protecting web applications against common attacks (WAF)

- WAF is NOT a stand-alone Azure service
- You can use WAF with the following:

Protecting web applications against common attacks (WAF)

- WAF is NOT a stand-alone Azure service
- You can use WAF with the following:
    - Azure Application Gateway

Protecting web applications against common attacks (WAF)

- WAF is NOT a stand-alone Azure service
- You can use WAF with the following:
    - Azure Application Gateway
    - Azure Front Door

Azure Application Gateway

Azure Application Gateway

- A web traffic load balancer

Azure Application Gateway

- A web traffic load balancer
- Enables you to manage traffic to your web applications

Azure Application Gateway

- A web traffic load balancer
- Enables you to manage traffic to your web applications
- WAF is one of its many features

Azure Application Gateway

- A web traffic load balancer
- Enables you to manage traffic to your web applications
- WAF is one of its many features
    - Traffic load balancer

Azure Application Gateway

- A web traffic load balancer
- Enables you to manage traffic to your web applications
- WAF is one of its many features
    - Traffic load balancer
    - SSL termination

Azure Application Gateway

- A web traffic load balancer
- Enables you to manage traffic to your web applications
- WAF is one of its many features
    - Traffic load balancer
    - SSL termination
    - URL-based routing

Azure Application Gateway

- A web traffic load balancer
- Enables you to manage traffic to your web applications
- WAF is one of its many features
    - Traffic load balancer
    - SSL termination
    - URL-based routing
    - Redirection

Azure Application Gateway

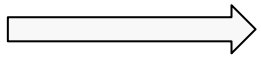
- A web traffic load balancer
- Enables you to manage traffic to your web applications
- WAF is one of its many features
    - Traffic load balancer
    - SSL termination
    - URL-based routing
    - Redirection
    - Session affinity

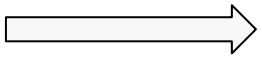
Azure Application Gateway

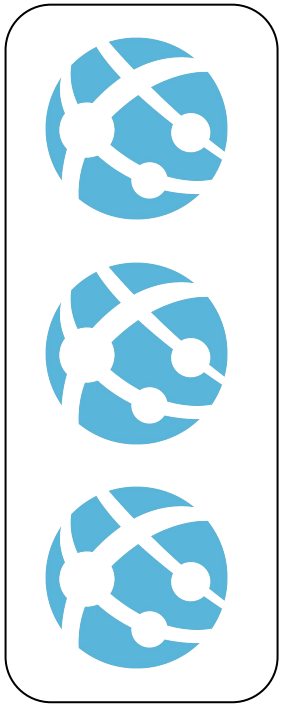
- A web traffic load balancer
- Enables you to manage traffic to your web applications
- WAF is one of its many features
    - Traffic load balancer
    - SSL termination
    - URL-based routing
    - Redirection
    - Session affinity
    - **Web application firewall (WAF)**

Azure Application Gateway

Internet

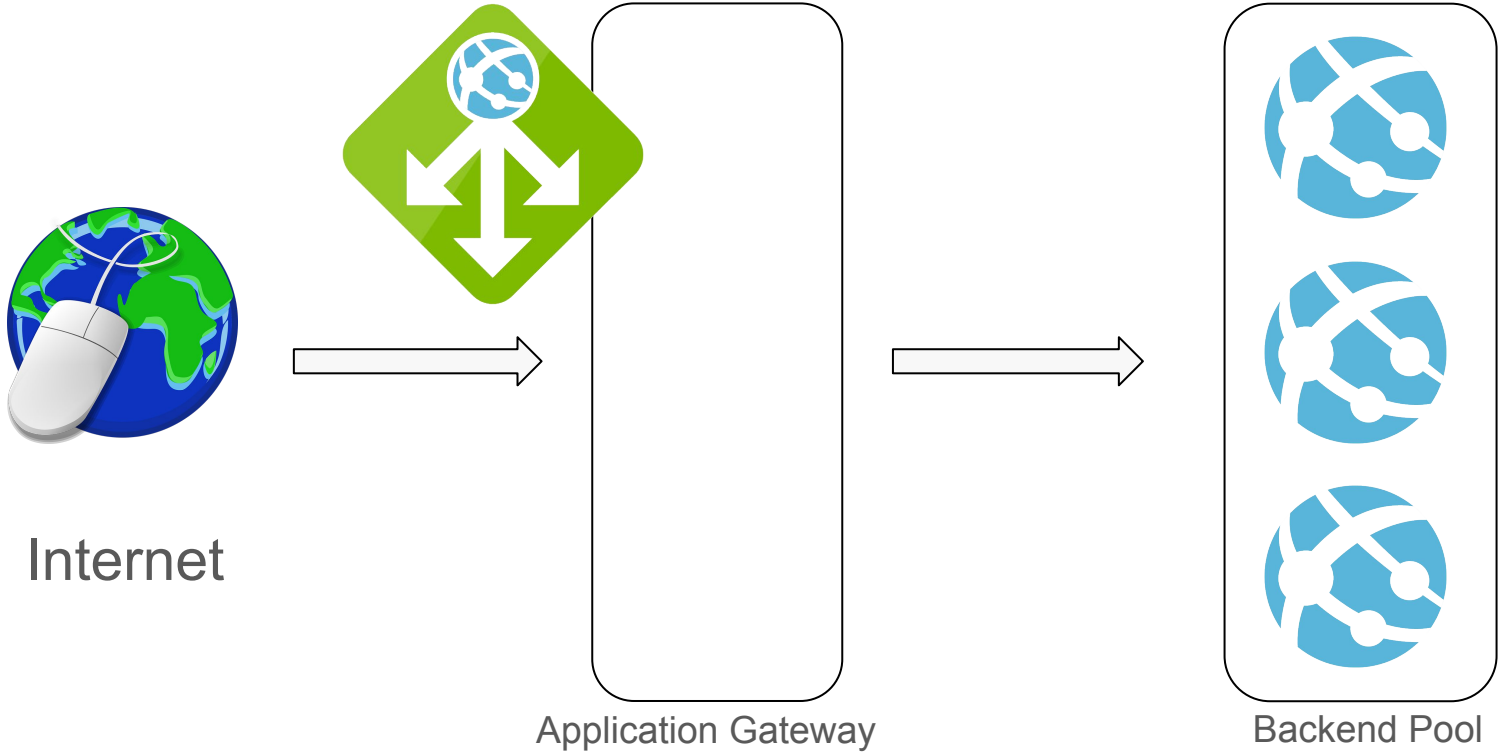




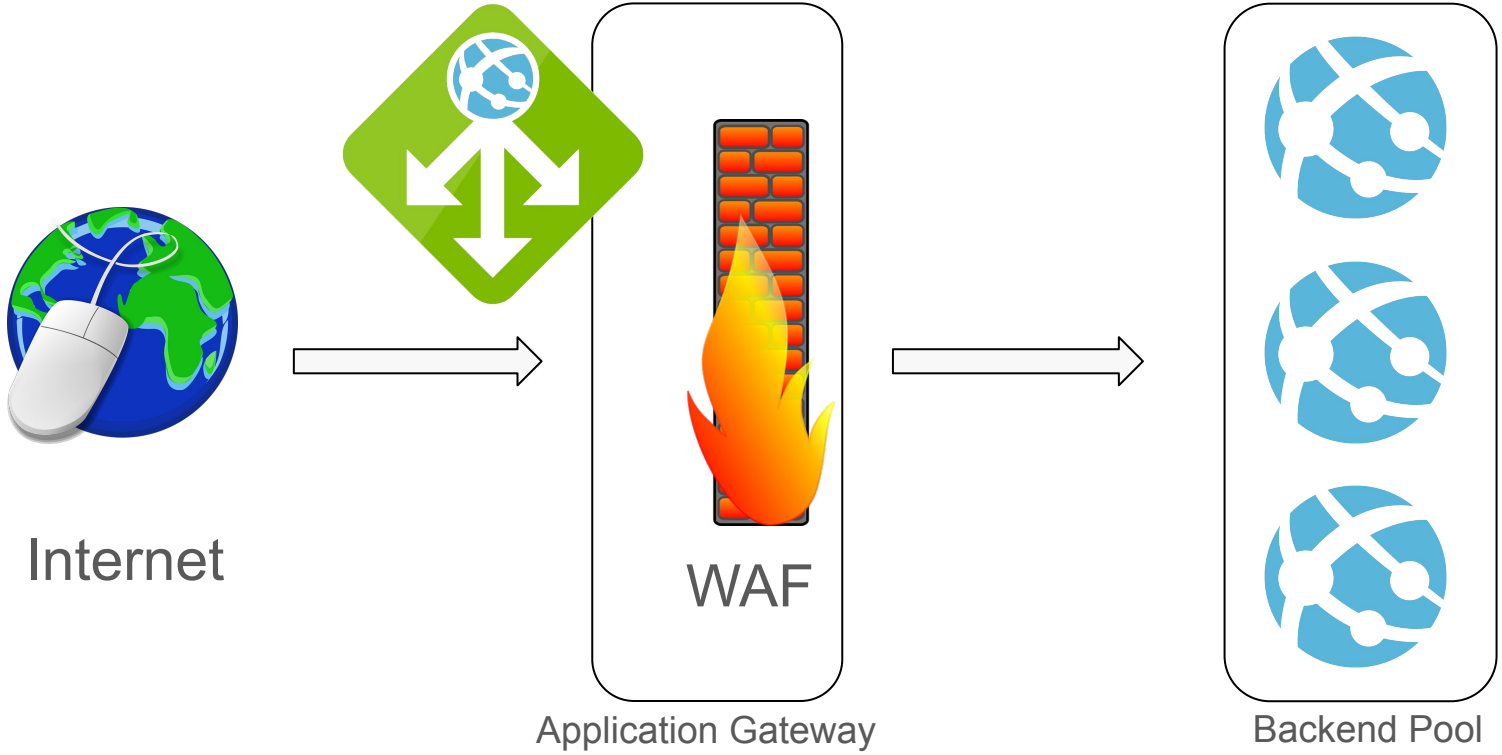


Backend Pool

Azure Application Gateway



Azure Application Gateway



Azure Front Door

Azure Front Door

- A CDN for web applications

Azure Front Door

- A CDN for web applications
- Enables you to optimize your web application traffic

Azure Front Door

- A CDN for web applications
- Enables you to optimize your web application traffic
- WAF is one of its many features

Azure Front Door

- A CDN for web applications
- Enables you to optimize your web application traffic
- WAF is one of its many features
    - Accelerates application performance

Azure Front Door

- A CDN for web applications
- Enables you to optimize your web application traffic
- WAF is one of its many features
    - Accelerates application performance
    - SSL termination

Azure Front Door

- A CDN for web applications
- Enables you to optimize your web application traffic
- WAF is one of its many features
    - Accelerates application performance
    - SSL termination
    - URL-based routing

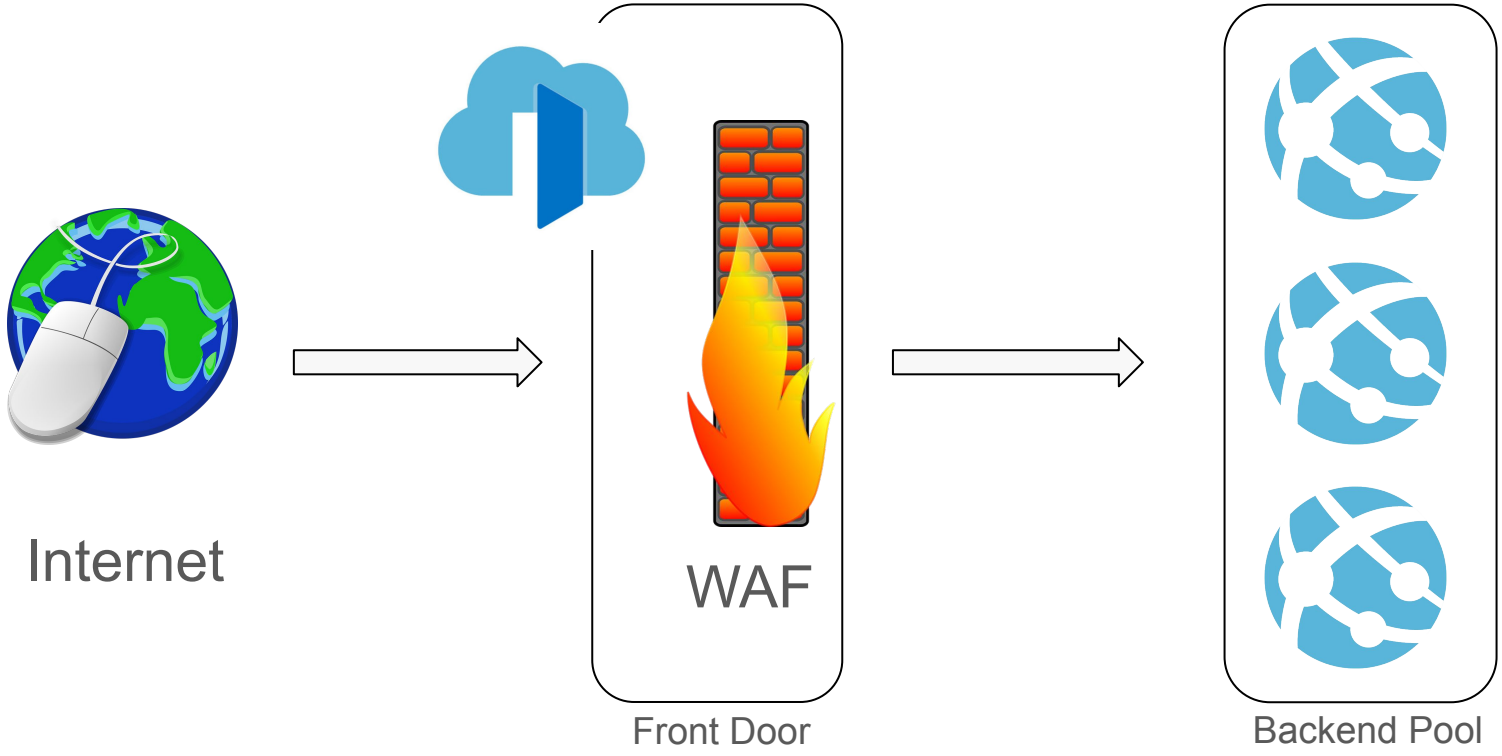
Azure Front Door

- A CDN for web applications
- Enables you to optimize your web application traffic
- WAF is one of its many features
    - Accelerates application performance
    - SSL termination
    - URL-based routing
    - Session affinity

Azure Front Door

- A CDN for web applications
- Enables you to optimize your web application traffic
- WAF is one of its many features
    - Accelerates application performance
    - SSL termination
    - URL-based routing
    - Session affinity
    - **Web application firewall (WAF)**

Azure Front Door



Demo

- Protecting an Azure web application using WAF
  - With the Application Gateway
  - With the Azure Front Door

Exercise

- Working with Web Application Firewall (WAF)
  - Application Gateway

Exam AZ-500

Microsoft Azure Security Technologies

Exam AZ-500

- Skills measured (as of December 4, 2019)
  - Manage identity and access (20-25%)
  - Implement platform protection (35-40%)
  - Manage security operations (15-20%)
  - Secure data and applications (30-35%)

https://docs.microsoft.com/en-us/learn/certifications/exams/az-500

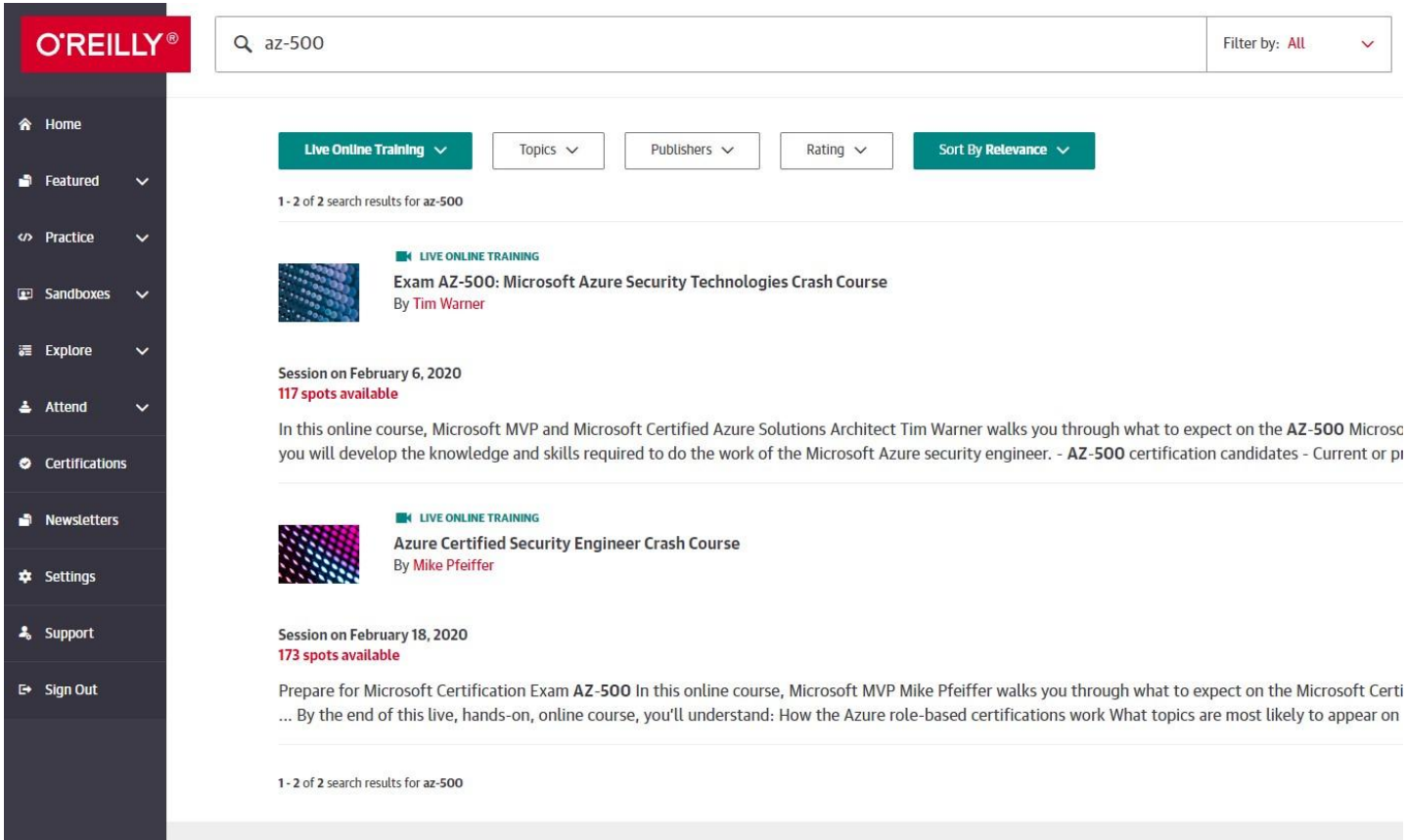
Exam AZ-500


Microsoft
EXAM
Exam AZ-500: Microsoft Azure Security Technologies
The content of this exam was updated on December 4, 2019. Please download the Skills measured document below to see what changed.
Candidates for this exam are Microsoft Azure security engineers who implement security controls, maintain the security posture, manage identity and access, and protect data, applications, and networks. Candidates identify and remediate vulnerabilities by using a variety of security tools, implement threat protection, and respond to security incident escalations. As a Microsoft Azure security engineer, candidates often serve as part of a larger team dedicated to cloud-based management and security and may also secure hybrid environments as part of an end-to-end infrastructure.
Candidates for this exam should have strong skills in scripting and automation; a deep understanding of networking, virtualization, and cloud N-tier architecture; and a strong familiarity with cloud capabilities, Microsoft Azure products and services, and other Microsoft products and services.
Part of the requirements for: Microsoft Certified: Azure Security Engineer Associate
Related exams: none
Important: See details
Go to Certification Dashboard

Exam AZ-500


Microsoft Certified: Azure Security Engineer Associate
Azure Security Engineers implement security controls and threat protection; manage identity and access; and protect data, applications, and networks in cloud and hybrid environments as part of end-to-end infrastructure.
Job role: Security Engineer
Required exams: AZ-500
Important: See details
Go to Certification Dashboard
Certification details
Take one exam
CERTIFICATION EXAM
Microsoft Azure Security Technologies
Earn the certification
ASSOCIATE CERTIFICATION
Microsoft Certified: Azure Security Engineer Associate

Exam AZ-500


O'REILLY®
az-500
Filter by: All
Home
Featured
Practice
Sandboxes
Explore
Attend
Certifications
Newsletters
Settings
Support
Sign Out
Live Online Training
Topics
Publishers
Rating
Sort By Relevance
1 - 2 of 2 search results for az-500
LIVE ONLINE TRAINING
Exam AZ-500: Microsoft Azure Security Technologies Crash Course
By Tim Warner
Session on February 6, 2020
117 spots available
In this online course, Microsoft MVP and Microsoft Certified Azure Solutions Architect Tim Warner walks you through what to expect on the AZ-500 Microsc
you will develop the knowledge and skills required to do the work of the Microsoft Azure security engineer. - AZ-500 certification candidates - Current or pr
LIVE ONLINE TRAINING
Azure Certified Security Engineer Crash Course
By Mike Pfeiffer
Session on February 18, 2020
173 spots available
Prepare for Microsoft Certification Exam AZ-500 In this online course, Microsoft MVP Mike Pfeiffer walks you through what to expect on the Microsoft Certi
... By the end of this live, hands-on, online course, you'll understand: How the Azure role-based certifications work What topics are most likely to appear on
1 - 2 of 2 search results for az-500

Course Repository

https://github.com/zaalion/oreilly-azure-app-security

Q&A

O'REILLY®

Thank you