



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:azuresqlmsidemossrv.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();

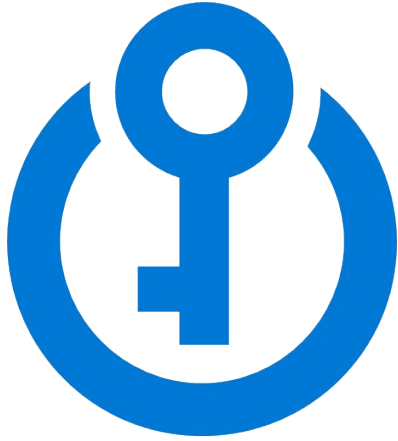
            var reader = sqlCommand.ExecuteReader();
        }
    }
}
```



Protecting Secrets in the Application Code



Protecting Secrets in the Application Code



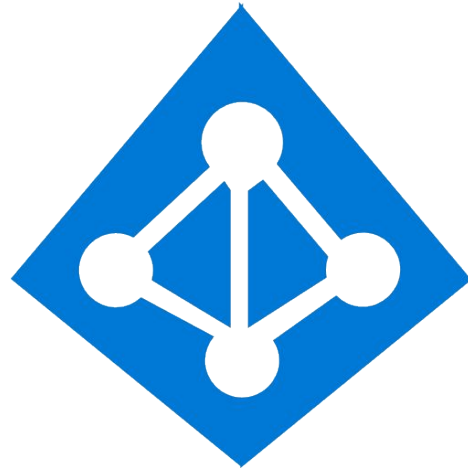
Azure Key Vault



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)



Internet

Incoming



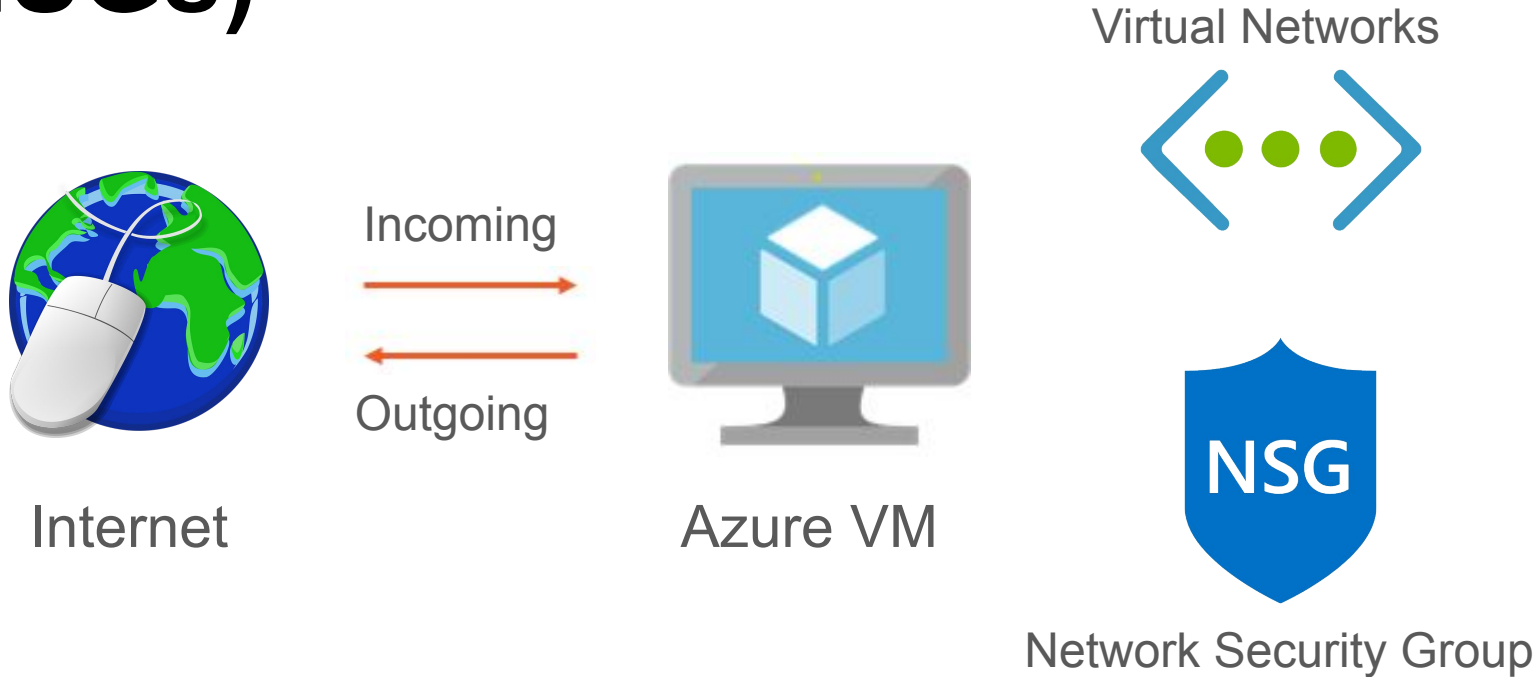
Outgoing



Azure VM



Protecting virtual machines (NSGs)



Protecting web applications against common attacks (WAF)



Protecting web applications against common attacks (WAF)



App Services

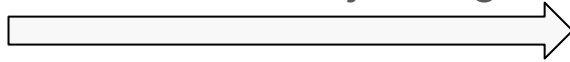


Protecting web applications against common attacks (WAF)



Internet

SQL injection
XSS
Session hijacking



App Services

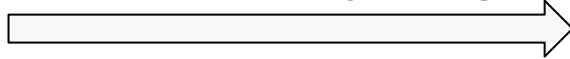


Protecting web applications against common attacks (WAF)

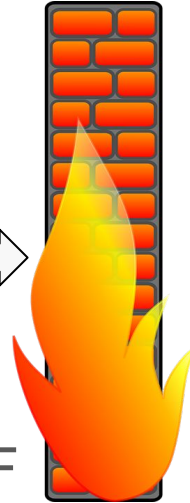


Internet

SQL injection
XSS
Session hijacking



WAF



App Services



Application Security Comes Hand in Hand with Data Security



Application Security Comes Hand in Hand with Data Security



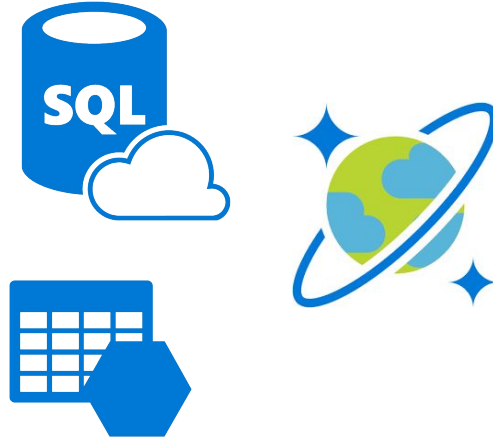
Application



Application Security Comes Hand in Hand with Data Security



Application



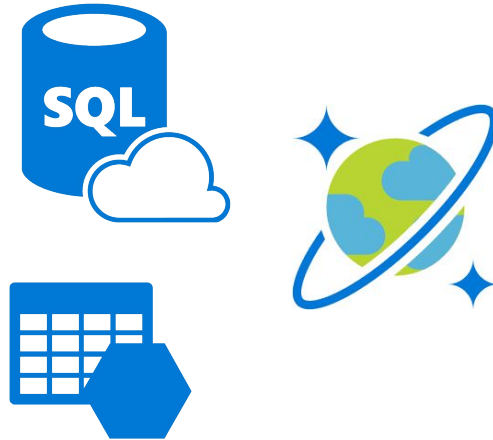
Data



Application Security Comes Hand in Hand with Data Security



Application



Data



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:azuresqlmsidemossrv.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.

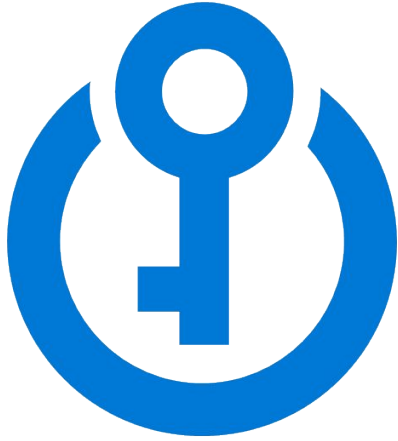


Protecting Secrets in the Application Code

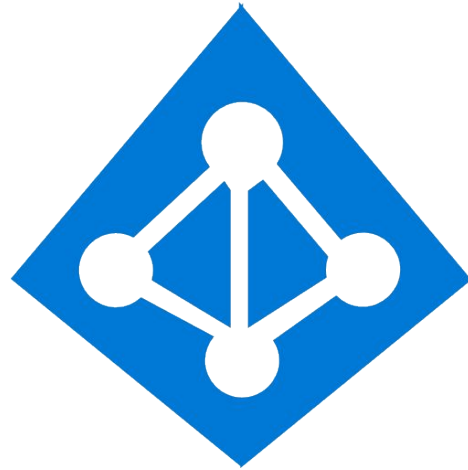
- Why?
 - Code will be checked into the source control.
 - No easy way to rotate or expire these secrets.
 - No easy way to control access to the secrets.
 - Maintenance nightmare



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

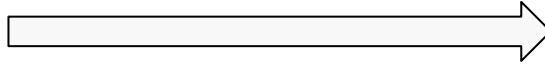


Azure Key Vault

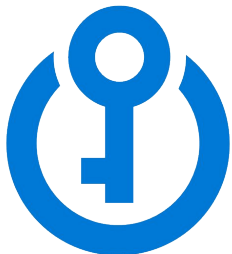


Stores the connection string
in the code

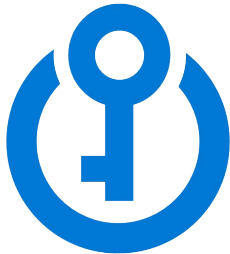
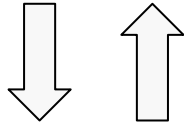
Use the connection string



Azure Key Vault



Azure Key Vault



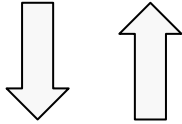
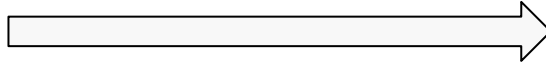
Gets the connection string
from Azure Key Vault
(at runtime)



Azure Key Vault



Use the connection string



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



Protecting Secrets in the Application Code

```
public class ValuesController : ApiController
{
    // GET api/values
    public Dictionary<string, string> Get()
    {
        var connectingString = "Server=tcp:azuresqlmsidemossrv.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));

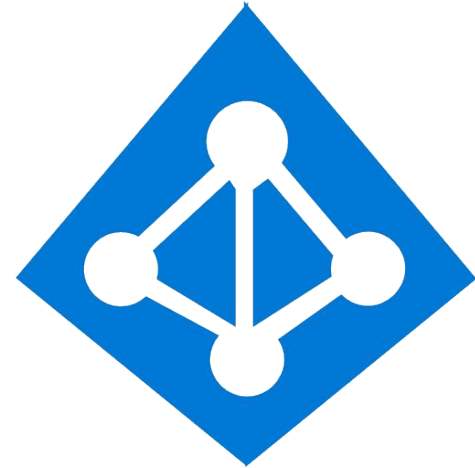
    var secretUrl = "https://kv-msi-01.vault.azure.net/secrets/myname/56c2905096f14c689d928da072139c72";
    var secret = kv.GetSecretAsync(secretUrl).Result;
    var myName = secret.Value;

    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)
{
    // ...
}
```

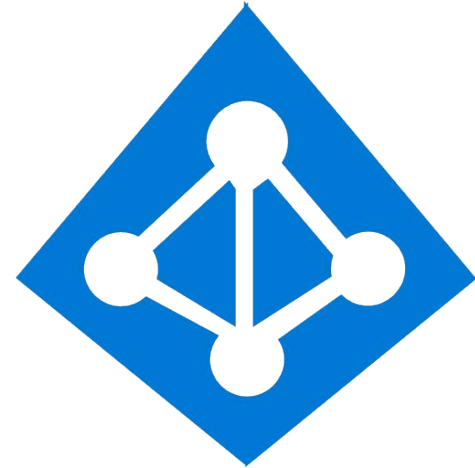


Managed Identity (MSI)



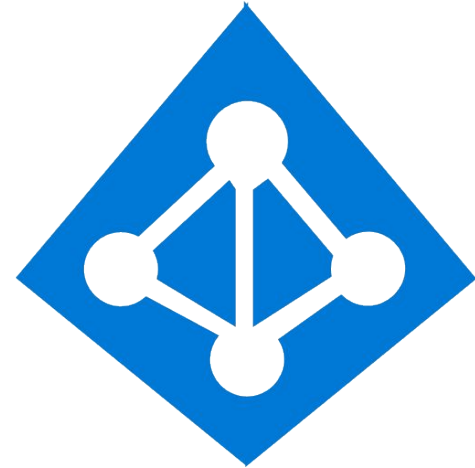
Managed Identity (MSI)

- Provides Azure services with an automatically managed identity.



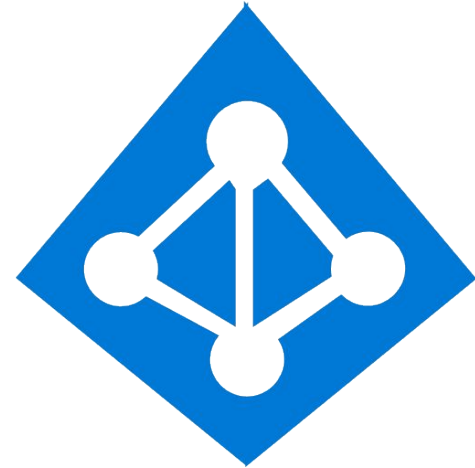
Managed Identity (MSI)

- 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();

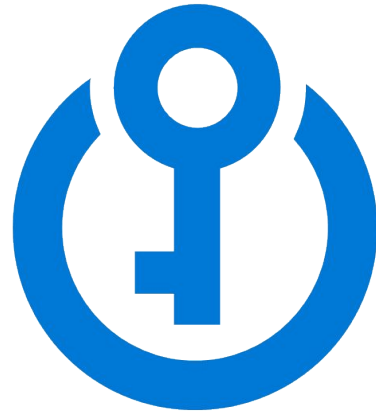
        var reader = sqlCommand.ExecuteReader();

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

        sqlConnection.Close();
    }
}
```



Key Vault References for App Services and Azure Functions



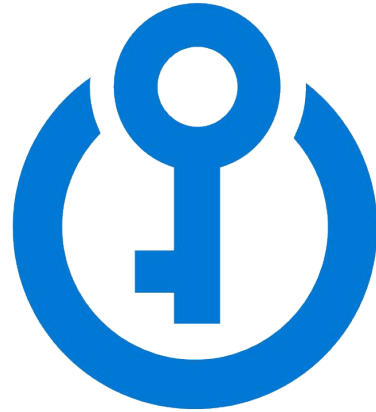
Key Vault References

```
roller.cs  appsettings.json  X
http://json.schemastore.org/appsettings

1  {
2    "Logging": {
3      "LogLevel": {
4        "Default": "Information",
5        "Microsoft": "Warning",
6        "Microsoft.Hosting.Lifetime": "Information"
7      }
8    },
9    "AllowedHosts": "*",
10   "mySecret" : "Key value from app settings"
11 }
12
```

Key Vault References

- Only works for Azure App Services and Azure Functions



Key Vault References

- Only works for Azure App Services and Azure Functions
- Move your app settings to an Azure Key Vault secret



Key Vault References

- Only works for Azure App Services and Azure Functions
- Move your app settings to an Azure Key Vault secret
- Reference the KV secret using the special syntax



Key Vault References

- Only works for Azure App Services and Azure Functions
- Move your app settings to an Azure Key Vault secret
- Reference the KV secret using the special syntax
- No code changes is required



Use Key Vault references - Azure

docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references

Filter by title

Create static HTML site

Run Windows container

Tutorials

Samples

Concepts

How-To guides

Configure app

Deploy to Azure

Map custom domain

Secure app

Add SSL cert

Authenticate users

Advanced auth

Restrict access

Use a managed identity

Reference secrets from Key Vault

Use SSL cert in code

Download PDF

Reference syntax

A Key Vault reference is of the form `@Microsoft.KeyVault({referenceString})`, where `{referenceString}` is replaced by one of the following options:

Reference string	Description
<code>SecretUri=secretUri</code>	The SecretUri should be the full data-plane URI of a secret in Key Vault, including a version, e.g., https://myvault.vault.azure.net/secrets/mysecret/ec96f02080254f109c51a1f14cdb1931
<code>VaultName=vaultName;SecretName=secretName;SecretVersion=secretVersion</code>	The VaultName should be the name of your Key Vault resource. The SecretName should be the name of the target secret. The SecretVersion should be the version of the secret to use.

For example, a complete reference with Version would look like the following:

Copy

```
@Microsoft.KeyVault(SecretUri=https://myvault.vault.azure.net/secrets/mysecret/ec96f02080254f109c51a1f14cdb1931)
```

Alternatively:

Copy

```
@Microsoft.KeyVault(VaultName=myvault;SecretName=mysecret;SecretVersion=ec96f02080254f109c51a1f14cdb1931)
```

Is this page helpful?

Yes

No

In this article

Granting your app access to Key Vault

Reference syntax

Source Application Settings from Key Vault

Troubleshooting Key Vault References

Protecting Secrets in Code

1. Azure Key Vault
2. Managed Service Identity
3. Azure Key Vault References



Demo

- Protecting secrets with Azure Key Vault
- Credential-free code with Key Vault References



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



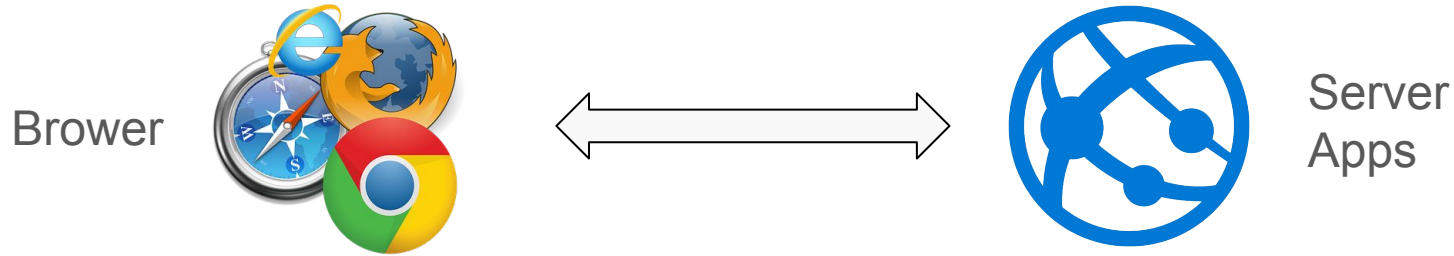
Securing Communications

SSL & TLS

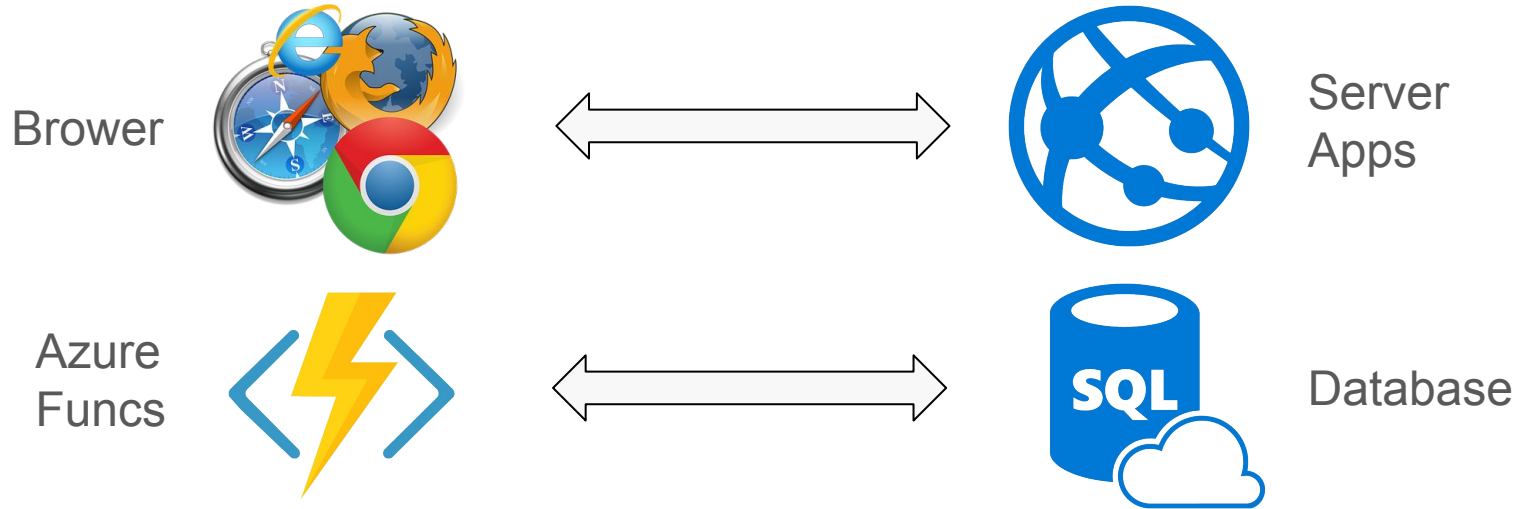
Securing Communications



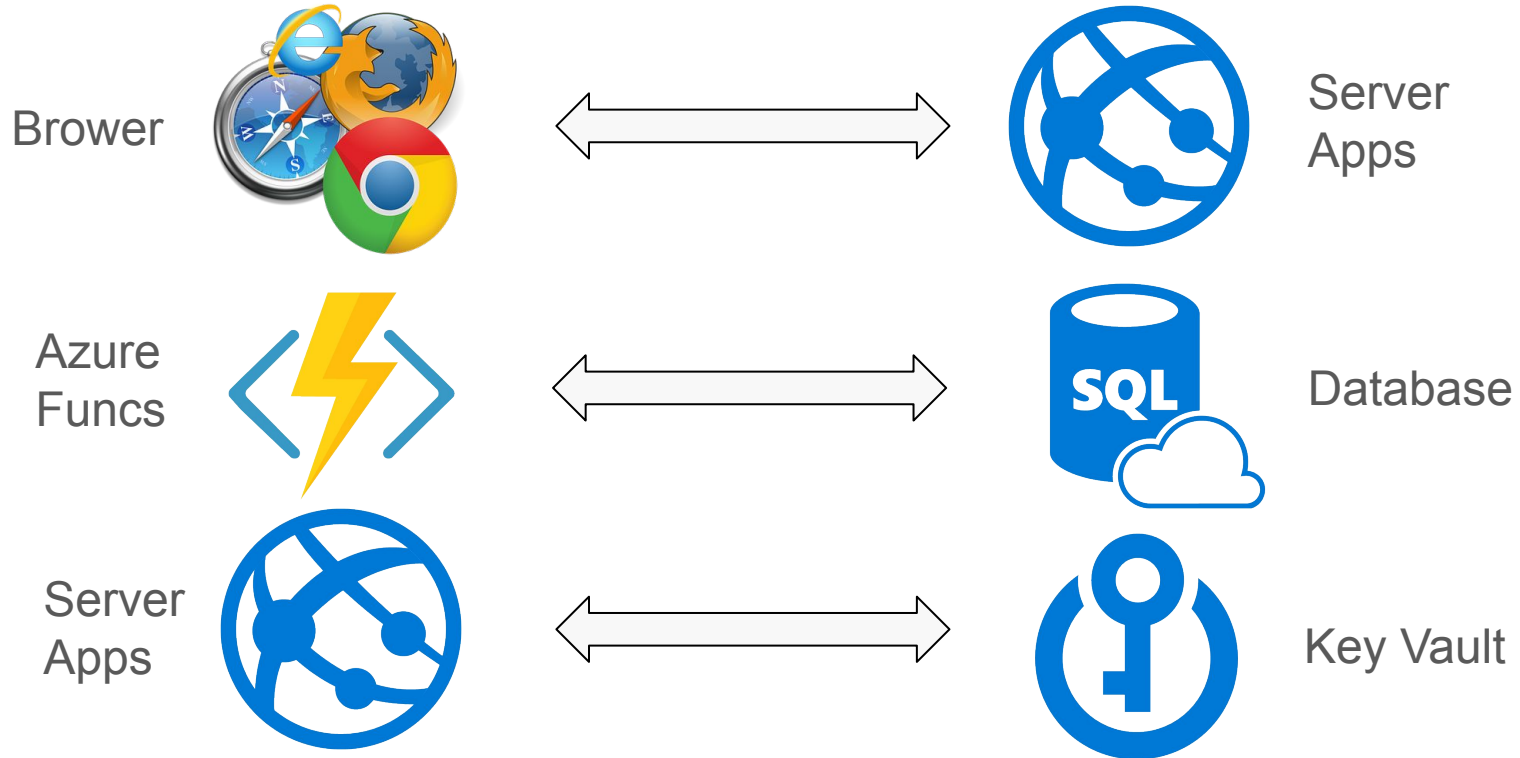
Securing Communications



Securing Communications



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

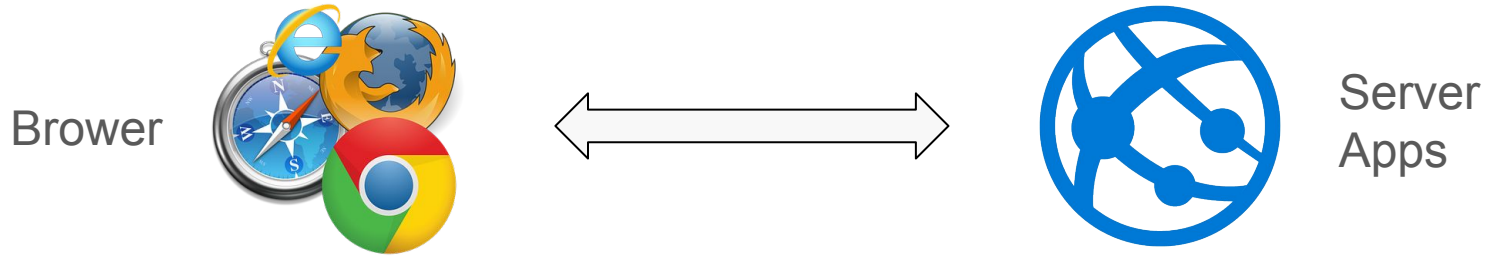


Securing Communications

- 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



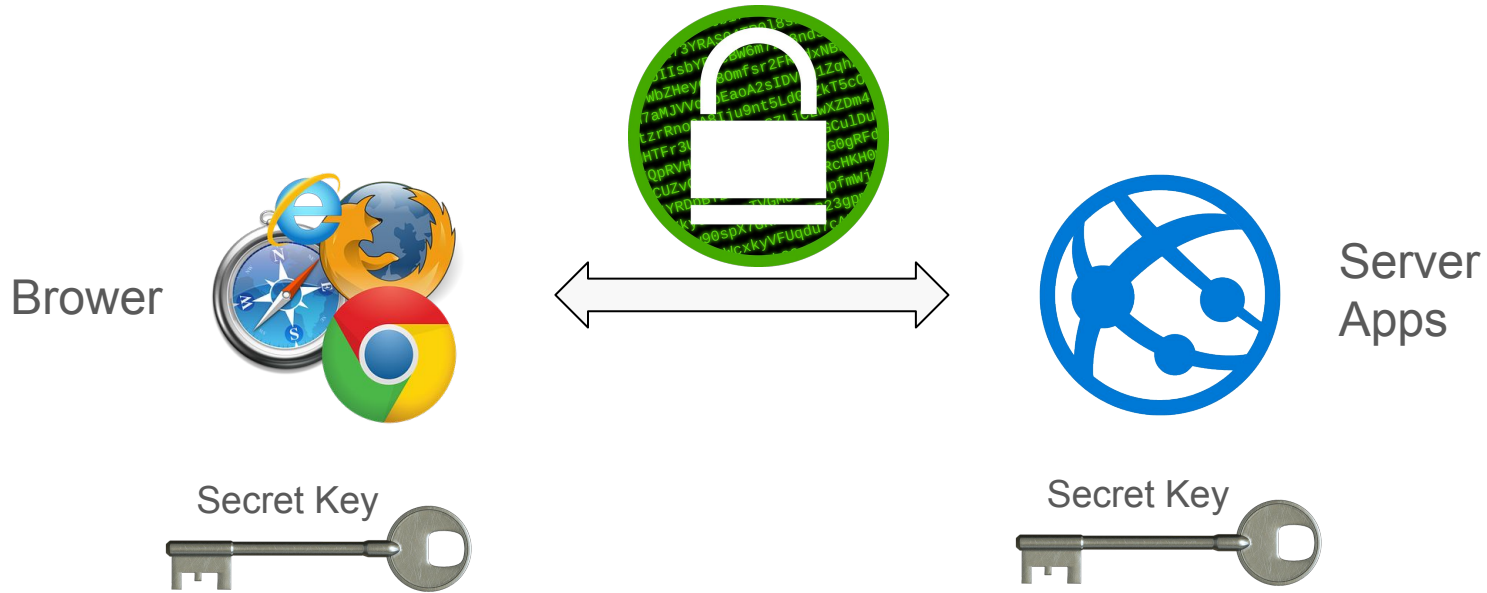
Securing Communications (SSL)



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



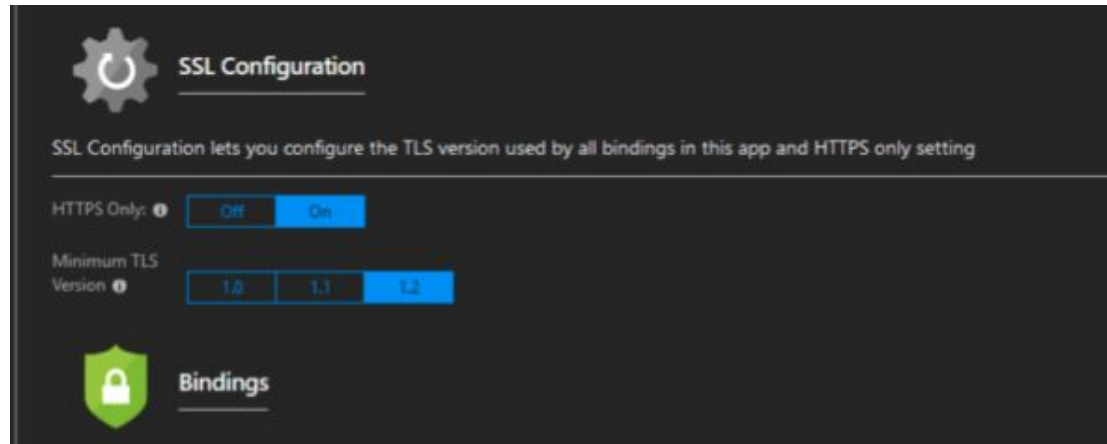
Securing Communications (SSL)

- 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)



Internet

Incoming



Outgoing



Azure VM



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)



Internet

Incoming



Outgoing



Azure VM



Protecting virtual machines (NSGs)



Internet

Incoming

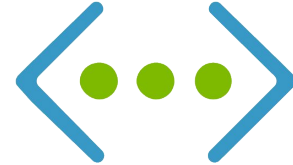


Outgoing

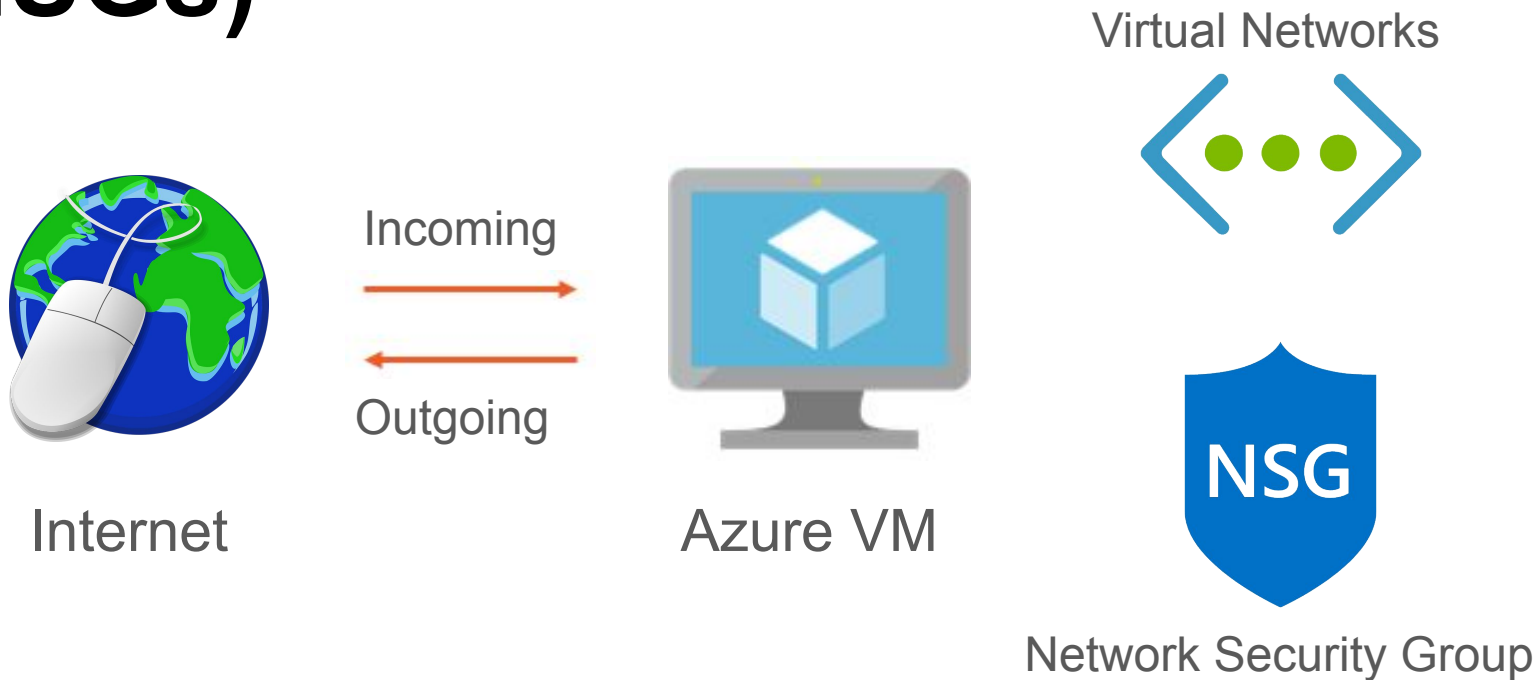


Azure VM

Virtual Networks



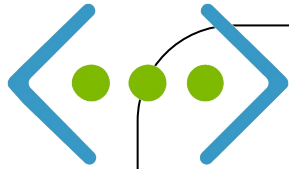
Protecting virtual machines (NSGs)



Protecting virtual machines (NSGs)



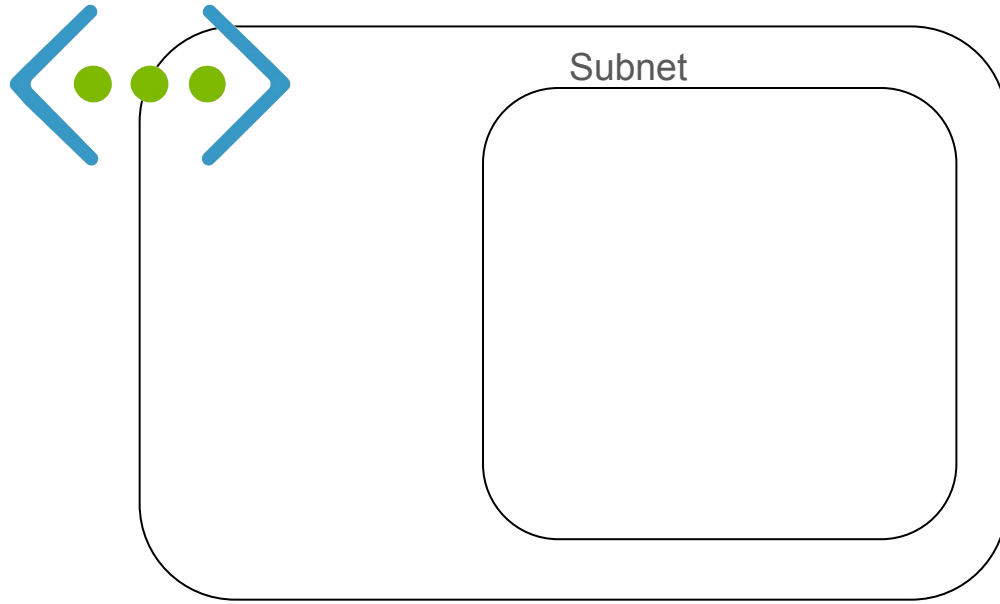
Protecting virtual machines (NSGs)



1. Create a VN



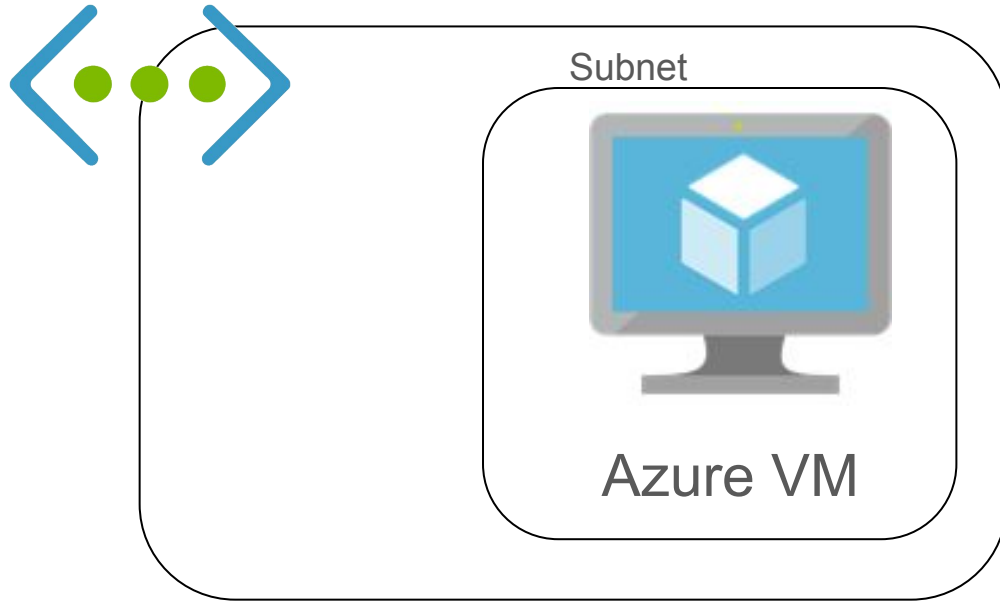
Protecting virtual machines (NSGs)



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



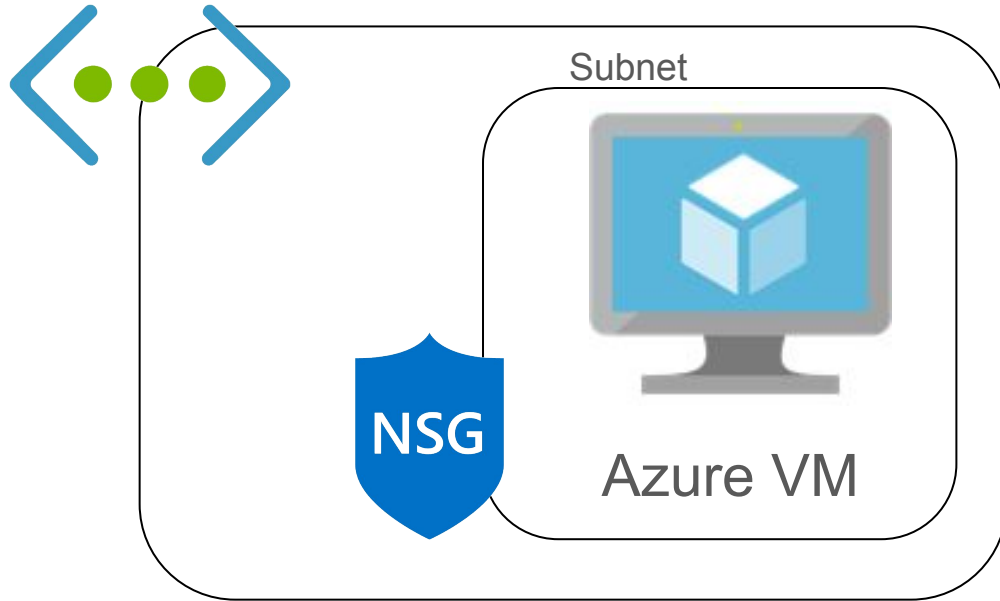
Protecting virtual machines (NSGs)



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



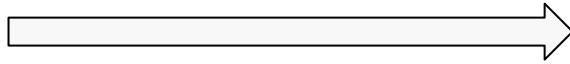
Protecting Web Applications

Azure Web Application Firewall (WAF)

Protecting web applications against common attacks (WAF)



Internet



App Services

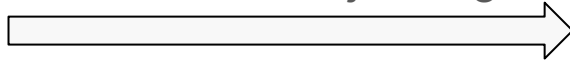


Protecting web applications against common attacks (WAF)



Internet

SQL injection
XSS
Session hijacking



App Services

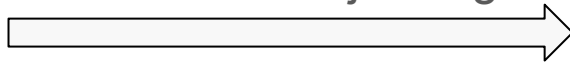


Protecting web applications against common attacks (WAF)



Internet

SQL injection
XSS
Session hijacking



Deal
with
the
attacks
at the
code
level



App Services

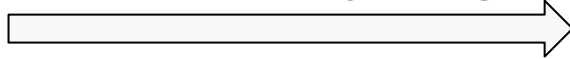


Protecting web applications against common attacks (WAF)

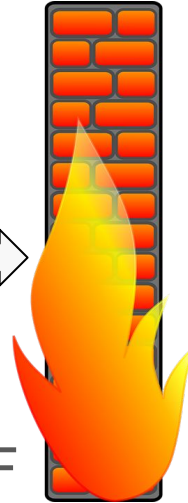


Internet

SQL injection
XSS
Session hijacking



WAF



App Services



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

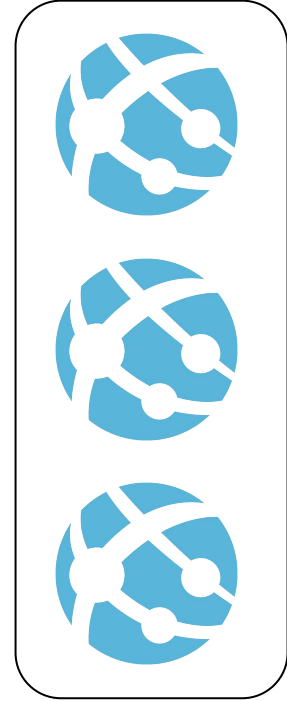
- A web traffic load balancer
- Enables you to manage traffic to your web applications
- WAF is one of its many features
 - Traffic load balancer
 - SSL termination
 - URL-based routing
 - Redirection
 - Session affinity
 - **Web application firewall (WAF)**



Azure Application Gateway



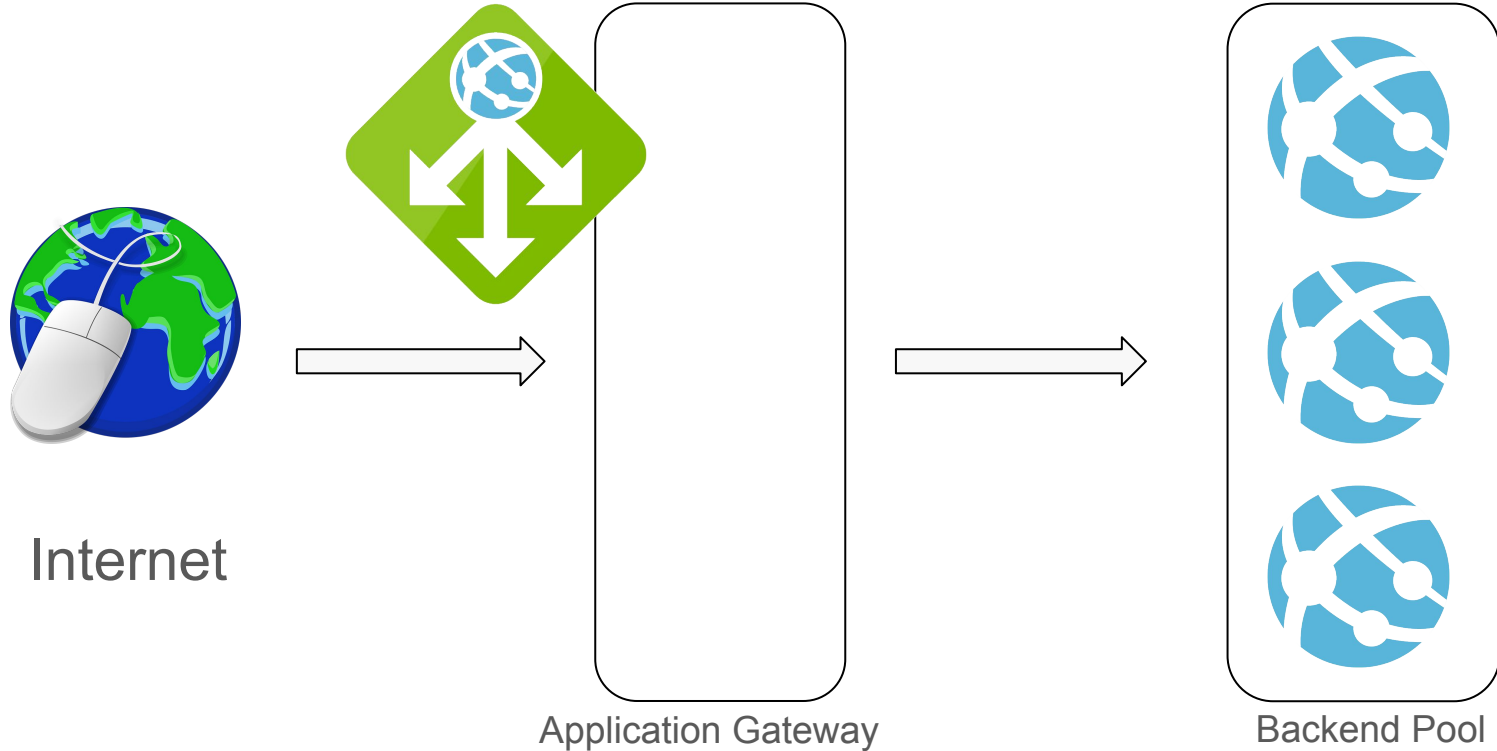
Internet



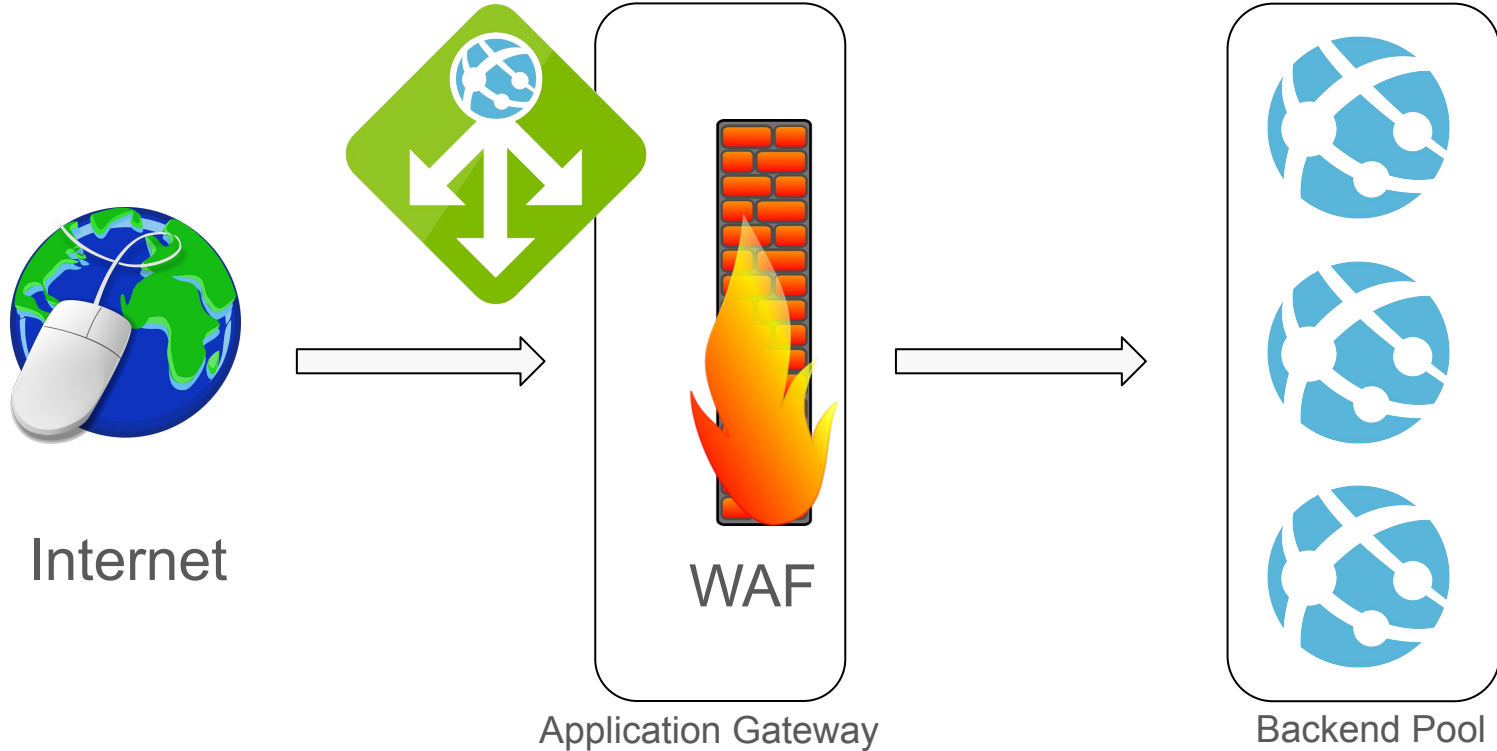
Backend Pool



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

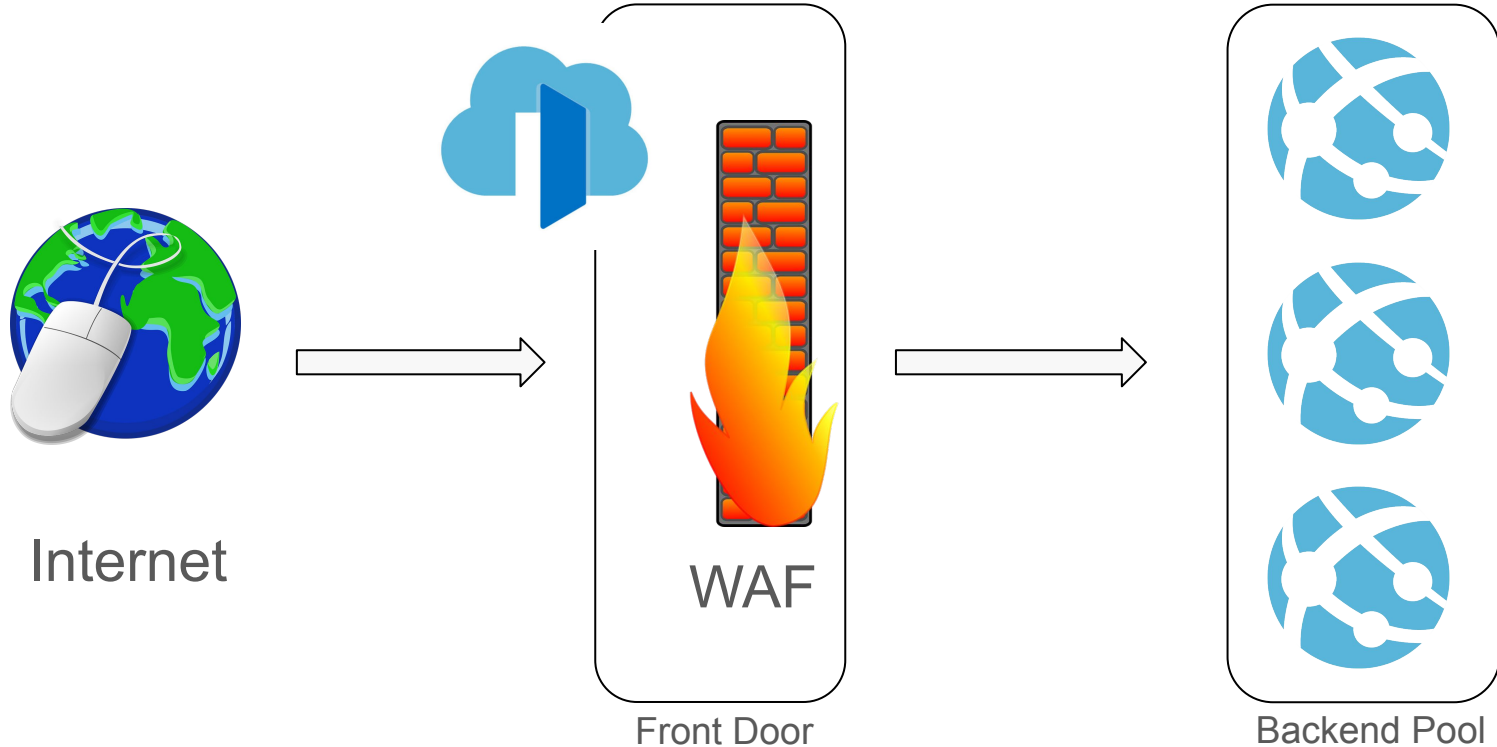


Azure Front Door

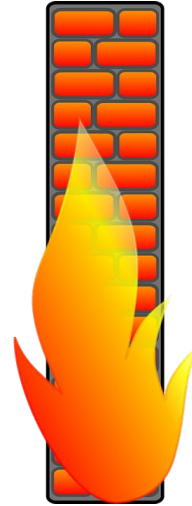
- A CDN for web applications
- Enables you to optimize your web application traffic
- WAF is one of its many features
 - Accelerates application performance
 - SSL termination
 - URL-based routing
 - Session affinity
 - **Web application firewall (WAF)**



Azure Front Door



Custom WAF Rules



Custom WAF Rules

- WAF v2 comes with a pre-configured ruleset
- Protects against common web attacks
 - XSS, SQL injection, etc.
- Write your own rules if needed



Custom WAF Rules

- WAF v2 comes with a pre-configured ruleset
- Protects against common web attacks
 - XSS, SQL injection, etc.
- Write your own rules if needed
 - Allow traffic from USA
 - Block all requests from IP range xxx.xxx.xxx.xxx/xx
 - etc.



- Filter by title
- Azure Web Application Firewall documentation
- > Overview
- > Tutorials
- > Samples
- > Concepts
- > How-to guides
 - Application Gateway
 - Create WAF policy
 - > Configure Web Application Firewall
 - Per-site policies
 - Migrate WAF policy
 - > Customize WAF rules
 - Configure WAF v2 custom rule
 - PowerShell
 - Custom rule examples
 - Bot protection
- Download PDF

Example 2

You want to allow traffic from the US using the GeoMatch operator:

Azure PowerShell Copy

```
$variable = New-AzApplicationGatewayFirewallMatchVariable `
    -VariableName RemoteAddr `

$condition = New-AzApplicationGatewayFirewallCondition `
    -MatchVariable $variable `
    -Operator GeoMatch `
    -MatchValue "US" `
    -Transform Lowercase `
    -NegationCondition $False

$rule = New-AzApplicationGatewayFirewallCustomRule `
    -Name "allowUS" `
    -Priority 2 `
    -RuleType MatchRule `
    -MatchCondition $condition `
    -Action Allow
```

And the corresponding JSON:

JSON Copy

```
{
  "customRules": [
```

Is this page helpful?

Yes No

In this article

- Example 1
- Example 2
- Example 3
- Example 4
- Example 5
- Example 6
- Next steps

Filter by title

Azure Web Application Firewall documentation

> Overview

> Quickstarts

> Application Gateway

> Tutorials

> Samples

> Concepts

> Application Gateway

Managed rules

Custom rules overview

Geomatch custom rules

Request size limits and exclusion lists

WAF Policy overview

Bot protection overview

> Front Door

> How-to guides

> Reference

> Resources

Download PDF

custom rules, see [Create and use custom web application firewall rules](#).

Fields for custom rules

Name [optional]

The name of the rule. It appears in the logs.

Priority [required]

- Determines the rule valuation order. The lower the value, the earlier the evaluation of the rule. The allowable range is from 1-100.
- Must be unique across all custom rules. A rule with priority 40 is evaluated before a rule with priority 80.

Rule type [required]

Currently, must be **MatchRule**.

Match variable [required]

Must be one of the variables:

- RemoteAddr – IP Address/hostname of the remote computer connection
- RequestMethod – HTTP Request method (GET, POST, PUT, DELETE, and so on.)
- QueryString – Variable in the URI
- PostArgs – Arguments sent in the POST body. Custom Rules using this match variable are only applied if the 'Content-Type' header is set to 'application/x-www-form-urlencoded' and 'multipart/form-data'.
- RequestUri – URI of the request
- RequestHeaders – Headers of the request
- RequestBody – This contains the entire request body as a whole. Custom rules using this match variable are only applied if the 'Content-Type' header is set to 'application/x-www-form-urlencoded'.

Is this page helpful?

Yes No

In this article

[Allowing vs. blocking](#)

[Fields for custom rules](#)

[Geomatch custom rules \(preview\)](#)

[Next steps](#)

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



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




[Home](#)
[Featured](#)
[Practice](#)
[Sandboxes](#)
[Explore](#)
[Attend](#)
[Certifications](#)
[Newsletters](#)
[Settings](#)
[Support](#)
[Sign Out](#)

Filter by: [All](#)

[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** Microsoft certification exam. You will develop the knowledge and skills required to do the work of the Microsoft Azure security engineer. - **AZ-500** certification candidates - Current or planned



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 Certified Security Engineer exam. 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 the exam

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

