# Implement Network Security – Azure Firewalls

# About Azure Firewall

# The Azure firewall is a fully managed, cloud-based network security service that protects your azure virtual network resources.

# The Azure firewall has built in high availability and unrestricted cloud scalability, so it does not matter if you are just configuring Azure and you have a few dozen VMS, maybe a few dozen services or applications, or if you have 100 VMS 100 applications, it can scale to that level.

# You can essentially create, enforce and log application and network connectivity policies across multiple subscriptions and across multiple virtual networks.

# As a firewall uses a static public IP address for your virtual network resources, this allows anything outside, it's outside to identify traffic originating from your virtual network

# This as your firewall service is fully integrated with Azure Monitor for logging and Analytics, and that is incredibly detailed level of logging.

1. **Azure Firewall**

**Objective –** To set up an azure firewall to access application**,** the below are High Level steps & azure services involved in setting up azure firewall environment

* Setup a **network** Test environment **– Azure Virtual Network, Subnets & NIC**
* Deploying a firewall – **Azure Firewall**
* Create a default route – **Azure Route**
* Configure an application rule to access to [www.google.com](http://www.google.com)
* Configure a network rule to allow access to external DNS servers
* Configure a NAT rule to allow a remote to test server
* Other services **-- Azure Virtual Machine, Azure Resource Group**
* Finally test the firewall environment.

Single VNet:

Test-FW-VN

**Azure Firewall Diagram**

Firewall Subnet: AzureFireWallSubnet

Test-FW01

Internet

Workload Subnet: Workload\_SN

Srv-World- VM

**Implementation steps**

1. Create a Resource Group
2. Create Virtual Network
3. Creating VMs For Firewall Traffic
4. Azure Firewall Deployment
5. Azure Firewall Deployment VNet and Route configuration
6. Azure Firewall rules collections setup / configuration (to access servers, google, Microsoft)
7. Azure Firewall DNS Configuration
8. Verify Azure Firewall Filters Traffic

# Step 1: Create a Resource Group

# Name: Test-FW-RG

# Region: east US

# Review and Create

# Step 2: Create a Virtual Network

# Name: Test-FW-VNet

# Region: East US, Click Next

# IP address : 10.0.0.0/16

# Subnet 1

# Name: AzureFireWallSubnet : 10.0.1.0/26

# Subnet: to place VM, deploy

# Name: Workload\_SN : 10.0.2.0/24

# Network Infrastructure completed

# Step 3. Creating VMs For Firewall Traffic

# Basic

# Resource Group : Test-FW-RG

# Name : Srv-Work

# Image : Win 2016

# Public inbound Rule ; None , Click Next : NO Changes in Disk

# Networking

# Virtual Network : Test-FW-VN

# Subnet : Workload\_SN

# Public IP: None 🡪 this VM Don’t want to communicate over the internet

# Review + Create

# Step 4. Azure Firewall Deployment

# Search Firewall

# Add New Firewall

# RG : Test-FW-RG

# Name: Test-FW01

# Region : East US

# Virtual Network : Test-FW-VNet

# Public IP Address ; New --> Name : fw-pip

# Review + Create ,

# Note: will take several minutes of time

# Step 5. Azure Firewall Deployment VNet and Route Configuration

# All Service 🡪 Networking 🡪 Route table

# Create a New Route Table

# RG ; Test-FW-RG

# Region : East US

# Name : Firewall-Route

# Review + Create

# Goto Resource 🡪 Under Subnets

# 🡪 Associate 🡪 Open Virtual Network : Test-FW-VNet & Subnet : Workload-SN , Click Ok

# Under Routes

# Add a New Route

# Route name : FW-DG

# Address Prefix : 0.0.0.0/0 – Pass all traffic

# Next Hop Type : Virtual Appliances

# Next Hop Address : get Firewall, Private IP Address : Test-FW01

# Step 6. Azure Firewall Rule collections

# Open azure service, Firewall : Test-FW01 🡪 Under Rules

# Application rule collection

# Click Add Application rule collection

# Name : App-coll1 ; Priority : 200 ; Action : Allow

# Target FQDMs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Source type | Source | Protocol Port | Target FQDNs |
| Allow-Google | IP-Address | 10.0.2.0/24 | http:80,https:443 | www.google.com |

# Click add

# Network rule Collection

# Click Add Network rule collection

# Name : Net-coll1 ; Priority : 200 ; Action : Allow

# Under Rules

# IP Address

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Protocol | Source / Destination type | Source | Destination Address | port |
| Allow-DNS | UDP | IP-Address | 10.0.2.0/24 | 209.244.0.3, 209.244.0.4 | 53 |

# Every thing else white /as -is, click Add

# NAT rule Collection (private to public address translation), similar home net to router

# Click Add NAT rule collection ,add rule for remote desktop

# Name : rdp ; priority : 200

# Under Rules

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Name | Protocol | Source type | Source | Destination Address (Public address of firewall) | Destination / Translated port | Translated Address(IP Address of VM) | Translated por |
| rdp-nat | TCP | IP-Address | \* | Open firewall,click fw-pip get Ip Address | 3389 | Open VM , get Private IP Address | 3389 |

# 

# Click Add

# Done with App ,Net , NAT Rule collection

# Step 7. Azure Firewall DNS Configuration

# Here change Primary and secondary DNS servers of Virtual Machine

# Open Service VM ,

# Under Networking🡪 Network Interface 🡪 DNS servers

# Custom DNS : 209.244.0.3 , 209.244.0.4

# Click save

# Now VM has external name resolution access

# Step 8. Verify Azure Firewall Filters Traffic , get the public address of firewall

# Open service Firewall, Test-FW01

# Click fw-pip, take the public IP Addres

# Log into VM

# Past the Above IP address take , click connect

# Open the browser in the VM

# Google.com will work

# Check Microsoft.com doesn’t work

# Open service Test-FW01 🡪 Rules 🡪 Application collection Collections

# Add

# Target FQDMs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Source type | Source | Protocol Port | Target FQDNs |
| Allow-Microsoft | IP-Address | 10.0.2.0/24 | http:80,https:443 | www.microsoft.com |

# This means adding the rule allows traffics to this site