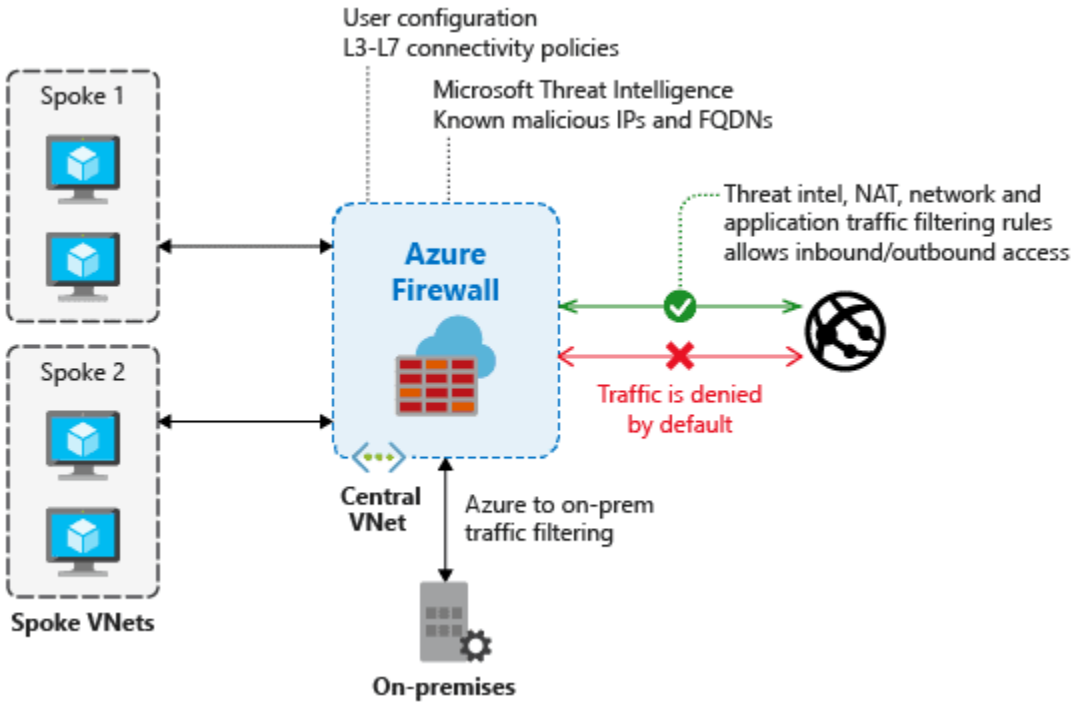
Azure Firewall : Overview and Concepts

Before coming to the Azure Firewall, One question! What do you understand by the word **Firewall**? Let's talk outside the computer world for a minute. In a human world, in simple words, a firewall means that it is a wall that will prevent the fire from getting in or out, which will save us from getting fried or toast.

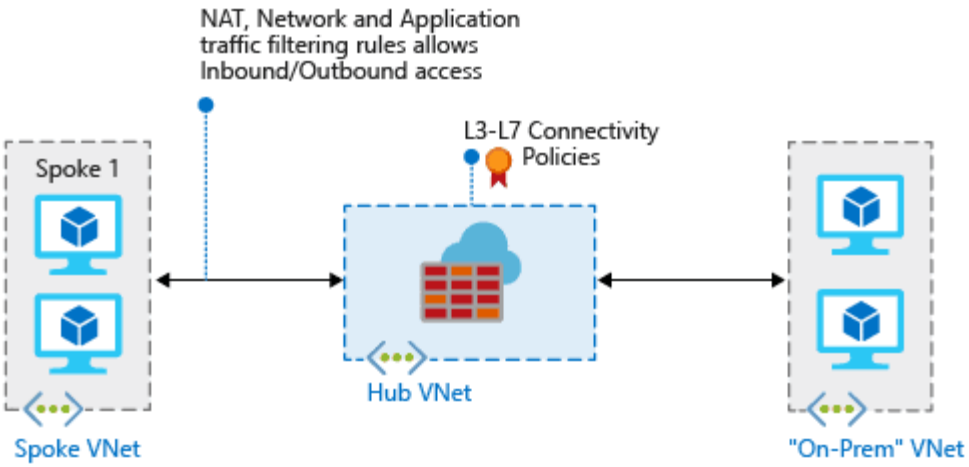
On a similar note, in the computer world, a firewall protects unwanted software from getting into your system while surfing the internet. It creates a wall around your system so that only legitimate sources or files you have permitted to enter your system can penetrate that wall, not others.

Overview of Azure Firewall

Azure Firewall is a controlled security utility that defends your **Azure Virtual Network resources**. It comes with **high availability** and unlimited **cloud scalability,** Which means that you don't have to deploy additional infrastructure for high availability like two firewalls or three firewalls and also no need for the load balancer. An important point to note here is that by default Azure Firewall blocks all the traffic.



You can deploy a **Firewall** on each virtual network. But usually, users will use it on a **central virtual network** and compare it to **other virtual networks** on the hub and speaker models. You can then set the default route from the **peered virtual networks** to purpose to the present **central firewall virtual network**. **Global VNet peering** is supported, however, it is not suggested attributable to potential performance and latency problems across regions. For most reliable production, deploy one firewall per region.



This model's advantage is that the ability to **centrally exert management** on multiple spoke **VNETs** across totally different subscriptions. There are price savings as you do not have to be compelled to deploy a firewall in every **VNet** separately. savings ought to be measured versus the associate peering cost supported by the **client traffic patterns**.

Concepts of Azure Firewall

Controlling outbound network access is an essential part of the overall network security plan. For example, you may want to limit access to a website, or you may wish to restrict outbound IP addresses or ports. With a firewall, you can configure applications rules that define fully qualified Domain names that can be accessed from a subnet. Also, you can configure network rules so that you can define source address, protocol destination, and destination addresses.

In Azure Firewall **Network rule collections** are a higher preference than **application rule collections.**
There are three types of rule collections:

- **Application rules:** Configure **Fully qualified domain names** (FQDNs) that can be reached from a subnet.
- **Network rules**: Configure rules that include source addresses, protocols, destination ports, and destination addresses.
- **NAT rules:** To allow incoming Internet connections by Configuring **DNAT** rules

Azure Firewall : Overview and Concepts

August 10, 2021 by Utkarsh Agarwal Agarwal Leave a Comment

Before coming to the Azure Firewall, One question! What do you understand by the word **Firewall**?

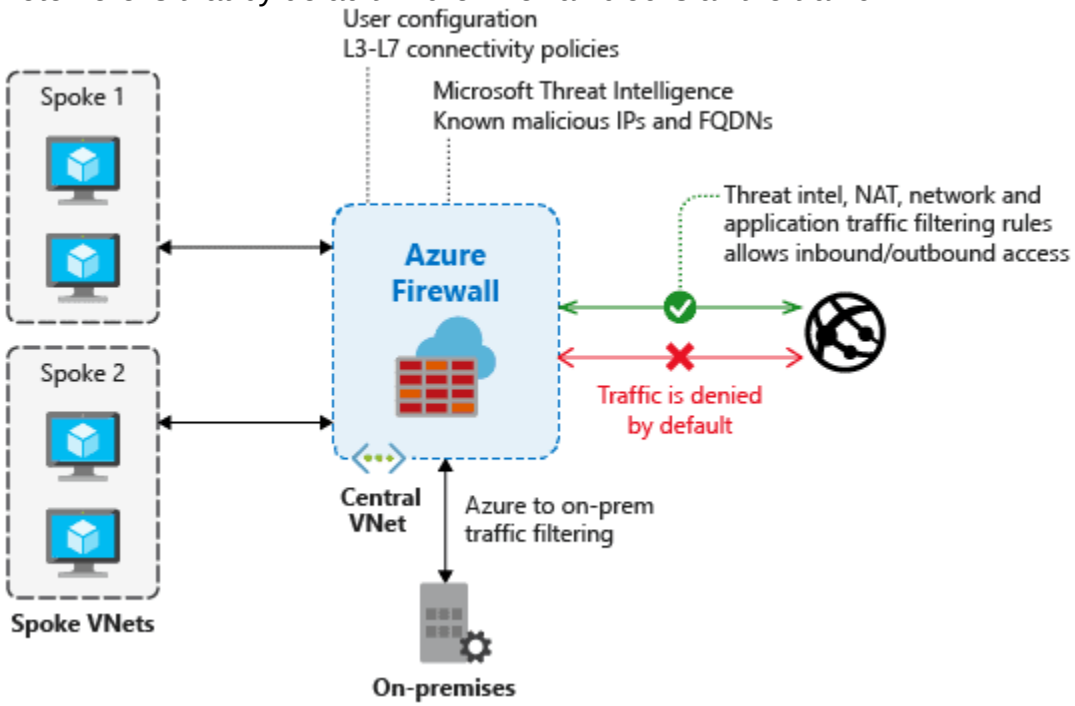
Let’s talk outside the computer world for a minute. In a human world, in simple words, a firewall means that it is a wall that will prevent the fire from getting in or out, which will save us from getting fried or toast.
On a similar note, in the computer world, a firewall protects unwanted software from getting into your system while surfing the internet. It creates a wall around your system so that only legitimate sources or files you have permitted to enter your system can penetrate that wall, not others.

In this blog, you will see a brief introduction about Azure Firewall, so let’s get started.

The Topics covered in this blog are:

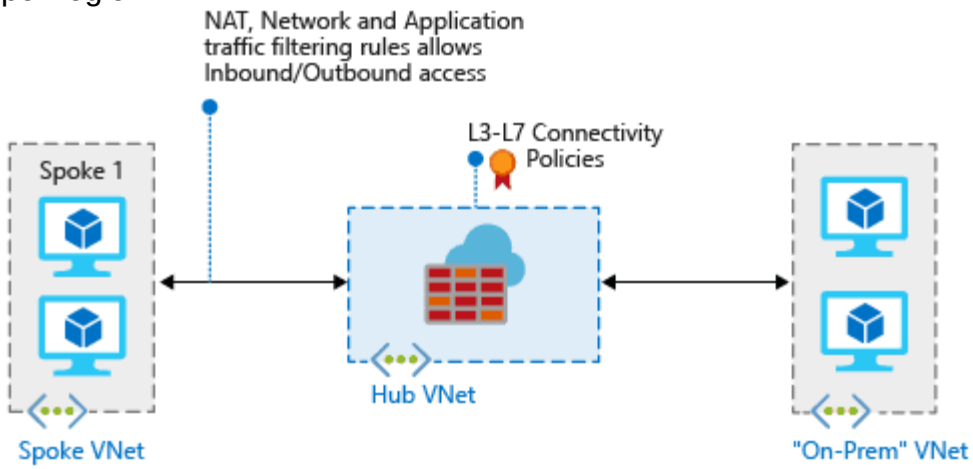
Overview of Azure Firewall

Azure Firewall is a controlled security utility that defends your **Azure Virtual Network resources**. It comes with **high availability** and unlimited **cloud scalability,** Which means that you don’t have to deploy additional infrastructure for high availability like two firewalls or three firewalls and also no need for the load balancer. An important point to note here is that by default Azure Firewall blocks all the traffic.



You can deploy a **Firewall** on each virtual network. But usually, users will use it on a **central virtual network** and compare it to **other virtual networks** on the hub and

speaker models. You can then set the default route from the **peered virtual networks** to purpose to the present **central firewall virtual network**. **Global VNet peering** is supported, however, it is not suggested attributable to potential performance and latency problems across regions. For most reliable production, deploy one firewall per region.



This model's advantage is that the ability to **centrally exert management** on multiple spoke **VNETs** across totally different subscriptions. There are price savings as you do not have to be compelled to deploy a firewall in every **VNet** separately. savings ought to be measured versus the associate peering cost supported by the **client traffic patterns**.

Concepts of Azure Firewall

Controlling outbound network access is an essential part of the overall network security plan. For example, you may want to limit access to a website, or you may wish to restrict outbound IP addresses or ports. With a firewall, you can configure applications rules that define fully qualified Domain names that can be accessed from a subnet. Also, you can configure network rules so that you can define source address, protocol destination, and destination addresses.

In Azure Firewall **Network rule collections** are a higher preference than **application rule collections.**
There are three types of rule collections:

- **Application rules:** Configure **Fully qualified domain names** (FQDNs) that can be reached from a subnet.
- **Network rules**: Configure rules that include source addresses, protocols, destination ports, and destination addresses.
- **NAT rules:** To allow incoming Internet connections by Configuring **DNAT** rules.

Note: FDQN Tags: Represents a group of fully qualified domain names associated with well-known Microsoft services.

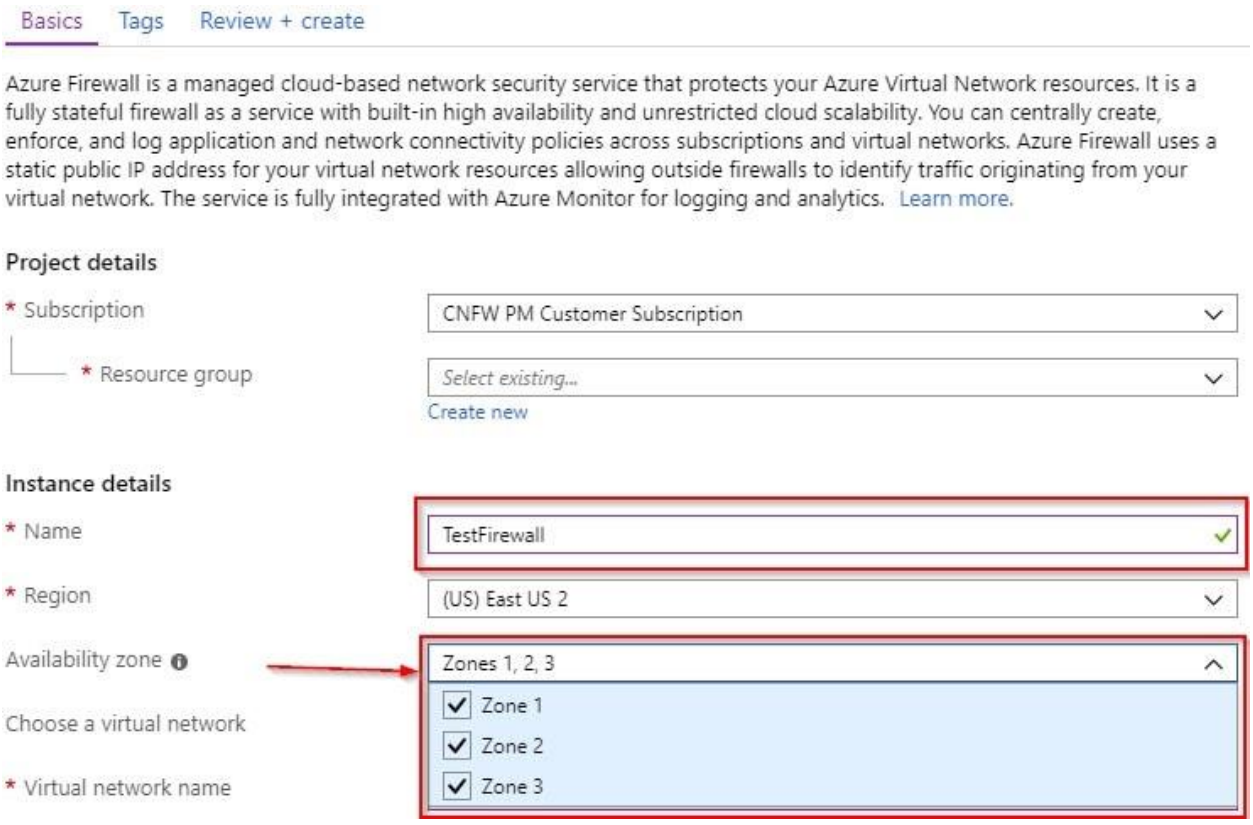
Features of Azure Firewall

Azure Firewall includes the following features:

- Built-in high availability
- Availability Zones
- Unrestricted cloud scalability
- Application FQDN filtering rules
- Network traffic filtering rules
- FQDN tags
- Service tags
- Threat intelligence
- Outbound SNAT support
- Inbound DNAT support
- Multiple public IP addresses
- Azure Monitor logging
- Forced tunneling
- Web categories
- Certifications

Built-in high availability & Availability Zones

We have built-in **High Availability.** It can be configured at the time of deployment for multiple **Availability Zones,** to increases availability uptime to **99.99%**. When two or more **Availability Zones** are selected uptime **SLA** is offered is **99.99%**. You can deploy **a Firewall** in an **Availability Zone** has no additional cost, but there is the cost for **outbound** and **inbound traffic** data transfer associated with **Availability Zones**.



2. Unrestricted cloud scalability with Threat intelligence

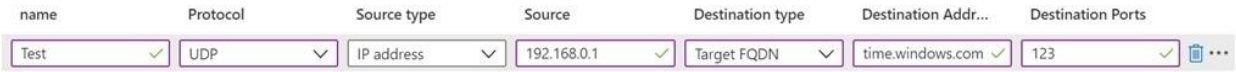
You can scale up **Azure Firewall** as many as you need to accommodate **increasing network traffic flows**, so you don't need to schedule for your **peak traffic**.
You can alert and deny traffic from/to known **malicious IP addresses and domains**, it can be enabled for your firewall using **Threat intelligence-based** filtering. **Microsoft Threat Intelligence feed** is sourced for **malicious IP addresses** and **domains**.

3. Service tags

It helps reduce complexity for security rule creation by designates a group of **IP address prefixes**. **Microsoft** manages the address prefixes embraced by the service tag and automatically updates the service tag as addresses change, because you can't create your own service tag, nor specify which **IP addresses** are inserted within a tag.

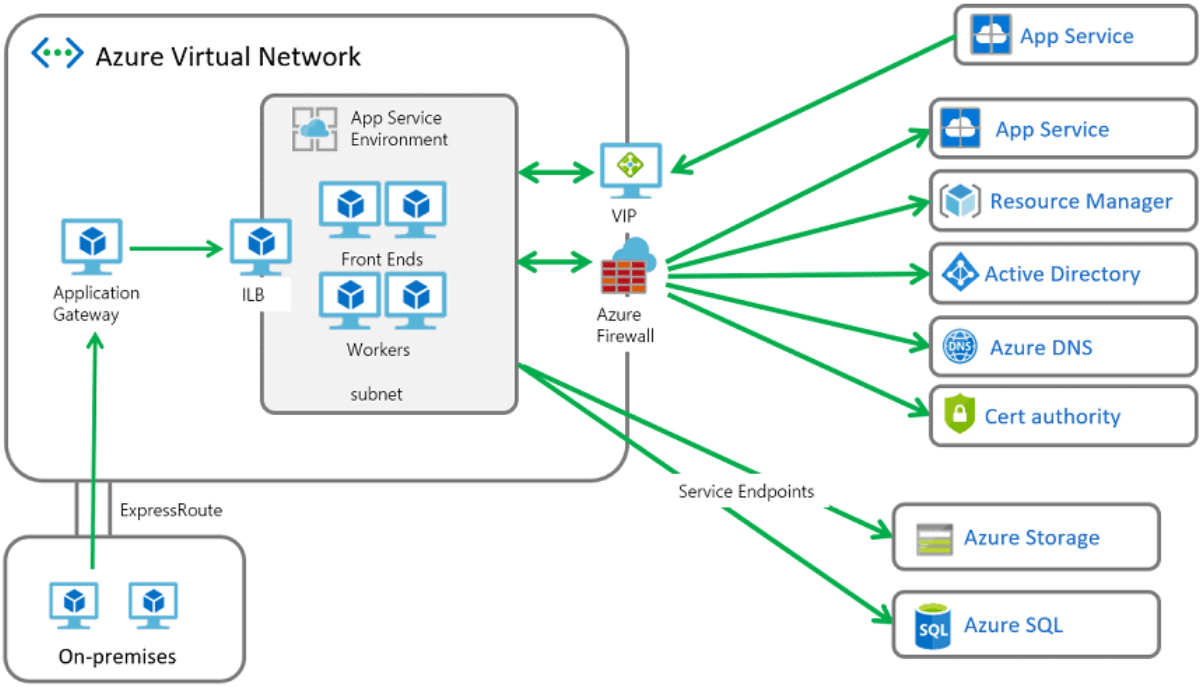
4. Application FQDN filtering rules & FQDN Tags

We can filter our outbound traffic such as **HTTP/S** or **Azure SQL** traffic to a defined list of **fully qualified domain names (FQDN)** including wild cards, and this feature doesn't need any **TLS** termination.
FQDN Tags permits well-known **Azure service network traffic** within your firewall. If you want to allow **Windows Update network traffic** into your **Azure firewall**. You can do it by building an application rule and enter the **Windows Update tag**, which allows network traffic from **Windows Update** can flow within your firewall.



5. Outbound SNAT & Inbound DNAT support

Azure Firewall public IP (Source Network Address Translation) has all translate outbound virtual network traffic **IP addresses**. **Firewall SNAT** doesn't support when the destination **IP is a private IP range**. we can distinguish and allow traffic beginning from your virtual network to remote Internet destinations. **Destination Network Address Translation (DNAT)** translated and filtered inbound internet network traffic from your firewall public IP address to the **private IP addresses** on your **virtual networks**.



6. Multiple public IP addresses

You can link various **public IP addresses** (up to **250**) with your **firewall**.
This enables the following scenarios:

- **DNAT –** You can translate multiplied **standard port instances** over your backend servers. For example, if you have a couple of public IP addresses, you can translate **TCP port 3389 (RDP)** for both IP addresses.
- **SNAT –**More ports are active for **outbound SNAT** connections, reducing the potential for **SNAT port exhaustion**. At this point, the **Azure Firewall** randomly chooses the origin **public IP address** to utilize for connection. If you hold any downstream filtering on your network, you need to allow all **public IP addresses** linked with your **Azure firewall**. Consider using the **public IP address prefix** to clarifies this configuration.

Pricing and SLA of Azure Firewall

Azure Firewall is a controlled cloud-established network security service that shields your **Azure Virtual Network resources**. It can be seamlessly expanded, requires zero maintenance, and is highly available with unlimited cloud scalability. Setting up a **Firewall** is easy with billing involved of a fixed and variable fee.

Azure Firewall

	Standard	Premium*
Deployment	₹90.057 per deployment hour	₹63.040 per deployment hour
Data Processing	₹1.153 per GB processed	₹0.577 per GB processed

*At Public Preview, price is discounted at 50% on the premium SKU

Azure Firewall provides fully stateful necessary firewall capabilities for **Virtual Network resources**, with built-in high availability and the ability to scale automatically. Microsoft assures you that it will be available at least **99.95%** of that time when deployed inside a single **Availability Zone** and the **Firewall** will be available at least **99.99%** of the time when spread within two or more **Availability Zones** in the corresponding **Azure region**.