Introduction to DDoS protection and Azure Firewall

DDoS protection

A Distributed denial of service (DDoS) attack attempts to exhaust an application's resource making the application unavailable to legitimate users. Azure DDoS protection provides the following tiers.

Basic

- Automatically enabled as part of the Azure platform.
- Always-on traffic monitoring, and real-time mitigation of common network-level attacks, provide the same defenses utilized by Microsoft's online services.
- Protection is provided for IPv4 and IPv6 Azure public IP addresses.

Standard

- Provides additional mitigation capabilities over the Basic service tier that are tuned specifically to Azure Virtual Network resources
- Provide protection against volumetric attacks, Protocol attacks, Resource layer attacks.
- Provides different metrics, alerts and mitigation reports

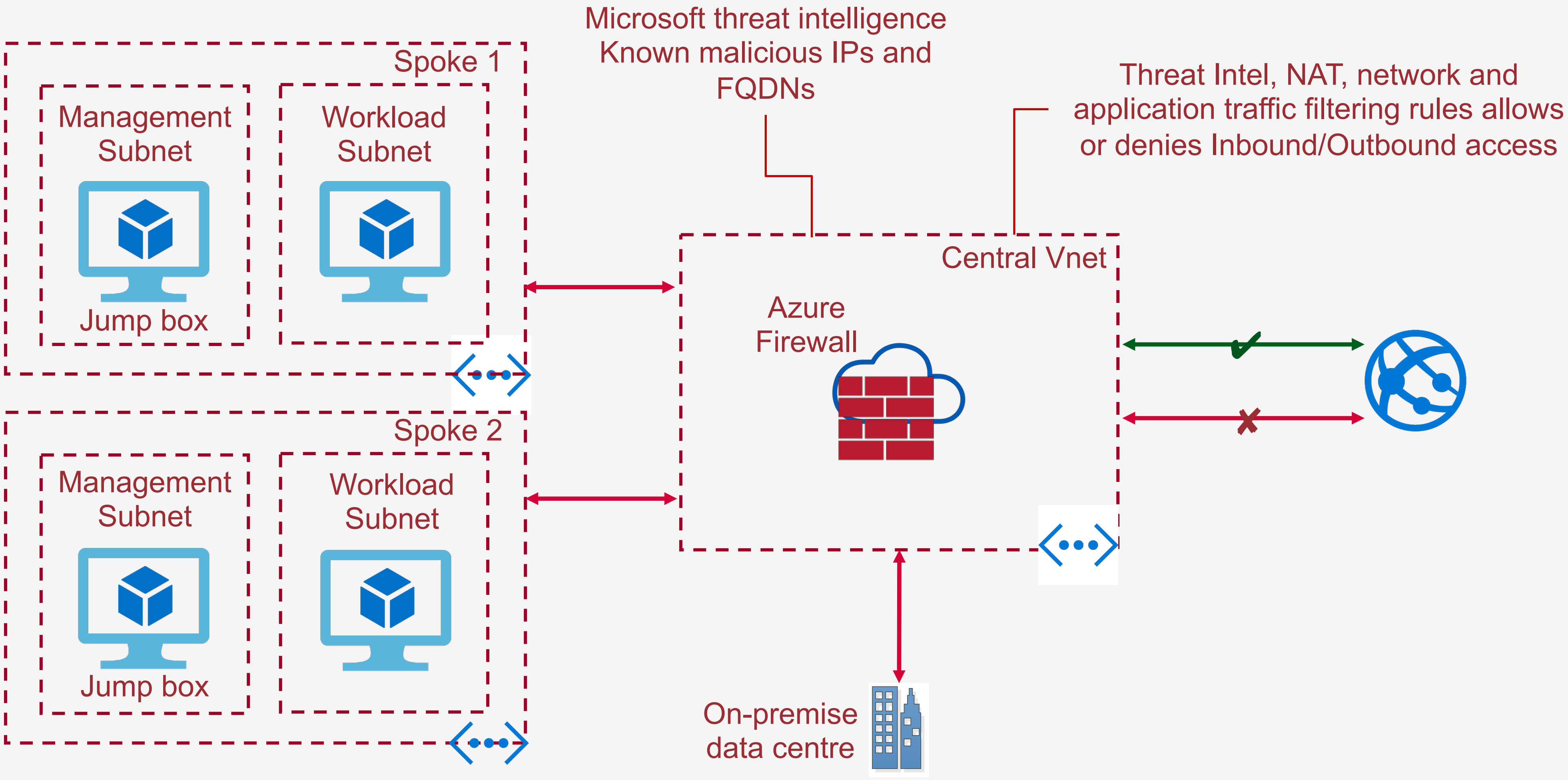
Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

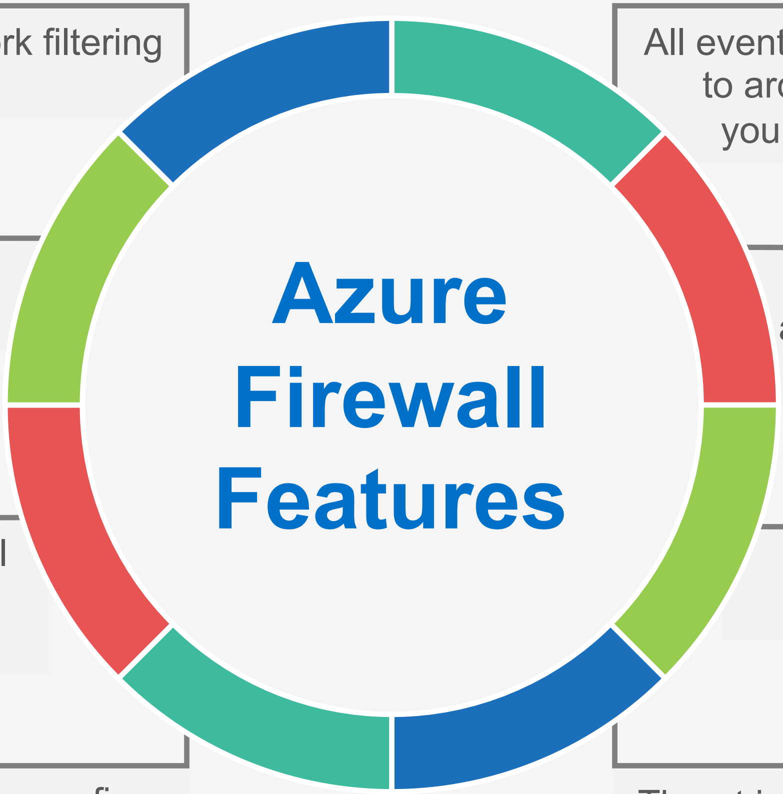
You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network

Network architecture with Azure Firewall


Spoke 1
Management Subnet
Jump box
Workload Subnet
Spoke 2
Management Subnet
Jump box
Workload Subnet
Microsoft threat intelligence Known malicious IPs and FQDNs
Threat Intel, NAT, network and application traffic filtering rules allows or denies Inbound/Outbound access
Central Vnet
Azure Firewall
On-premise data centre

Features of Azure Firewall



Azure Firewall Features

Network traffic filtering rules

You can centrally create allow or deny network filtering rules

Application FQDN filtering rules

You can limit outbound HTTP/S traffic to a specified list of FQDN's including wild cards

FQDN tags

FQDN tags make it easy for you to allow well known Azure service network traffic through your firewall

Service tags

A service tag represents a group of IP address prefixes to help minimize complexity for security rule creation.

Azure Monitor logging

All events are integrated with Azure Monitor, allowing you to archive logs to a storage account, stream events to your Event Hub, or send them to Azure Monitor logs.

Inbound DNAT support

Inbound network traffic to your firewall public IP address is translated and filtered to the private IP addresses on your virtual networks.

Outbound SNAT support

All outbound virtual network traffic IP addresses are translated to the Azure Firewall public IP

Threat intelligence

Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains