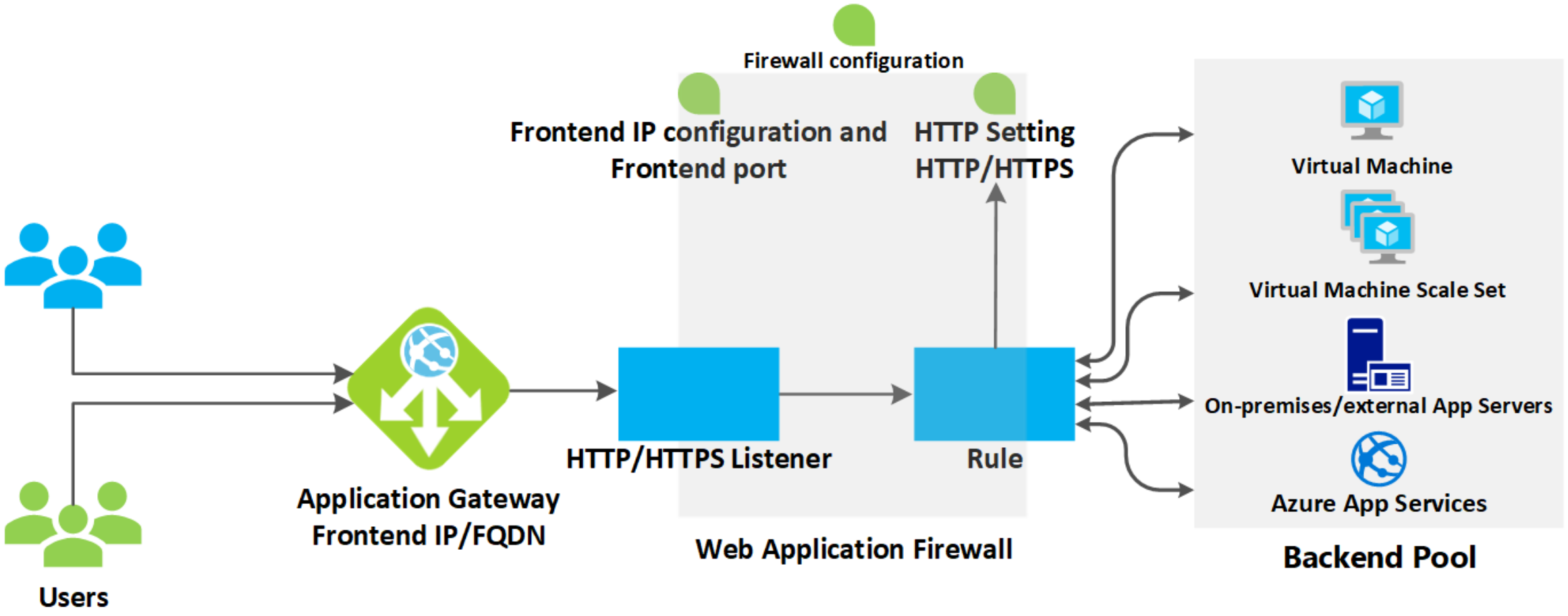
Securing Web Applications Hosted in Azure

Gabriel McNeilly
CLOUD & QA ENGINEER

@gmcneilly software-tester.io

Azure Application Gateway



WAF on an Application Gateway

Protects against many types of attacks using defined rules

A WAF policy includes all the rules applied by the WAF

WAF policies can be applied to various scopes

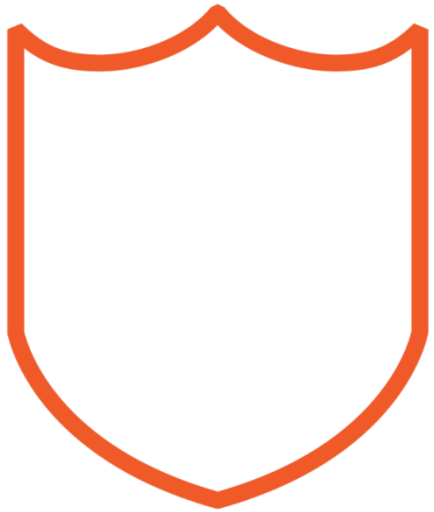
2 modes: detection and prevention

Integrates with Azure Security Center, Azure Monitor and Azure Sentinel

Azure-managed Rules

OWASP

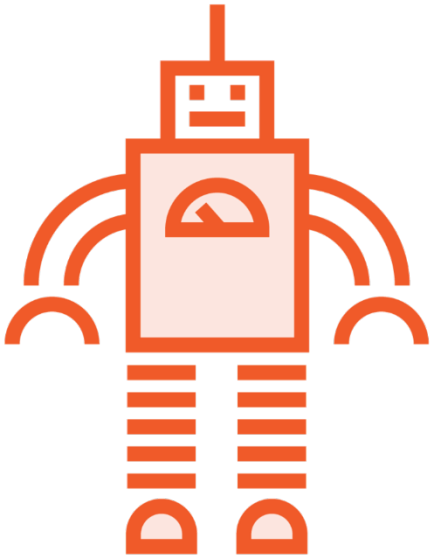
OWASP CRS Rule sets



Protect against a variety of common attacks

Enabled by default

Custom Rules



Block malicious bots

Only allow certain countries

Block specific IP ranges

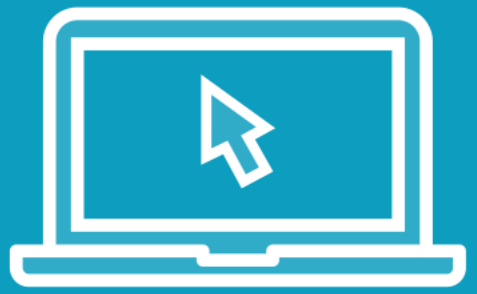
Protect against additional attacks

Rule Definitions

```
{"customRules": [{
        "name": "blockMaliciousBot",
        "ruleType": "MatchRule",
        "priority": 2,
        "action": "Block",
        "matchConditions": []
}]}
```

```
"matchConditions": [
{               "matchVariable":"RequestHeaders",
    "operator": "User-Agent",
    "matchValues": [“badbot“]
 }
]
```

Demo



Add a WAF to an Application Gateway

Configure a global WAF policy

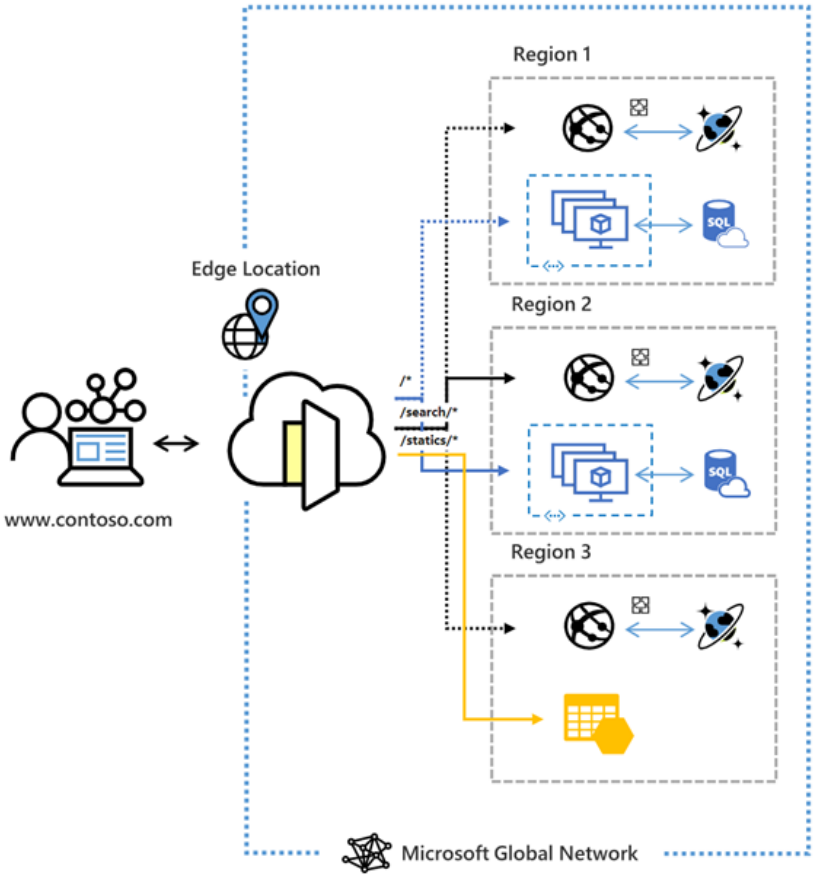
Create and assign a custom rule

Azure Front Door

Azure Front Door vs. Application Gateway

The primary difference is that Front Door is a global service whereas Application Gateway is a regional service

Azure Front Door



Works at layer 7

It is cross-region

Uses anycast and split TCP

It is a modern CDN

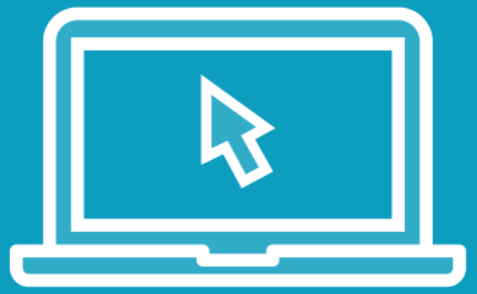
Key Benefits of Azure Front Door

Centrally manage web application security

Greatly improved performance

Availability & DDoS Protection

Demo

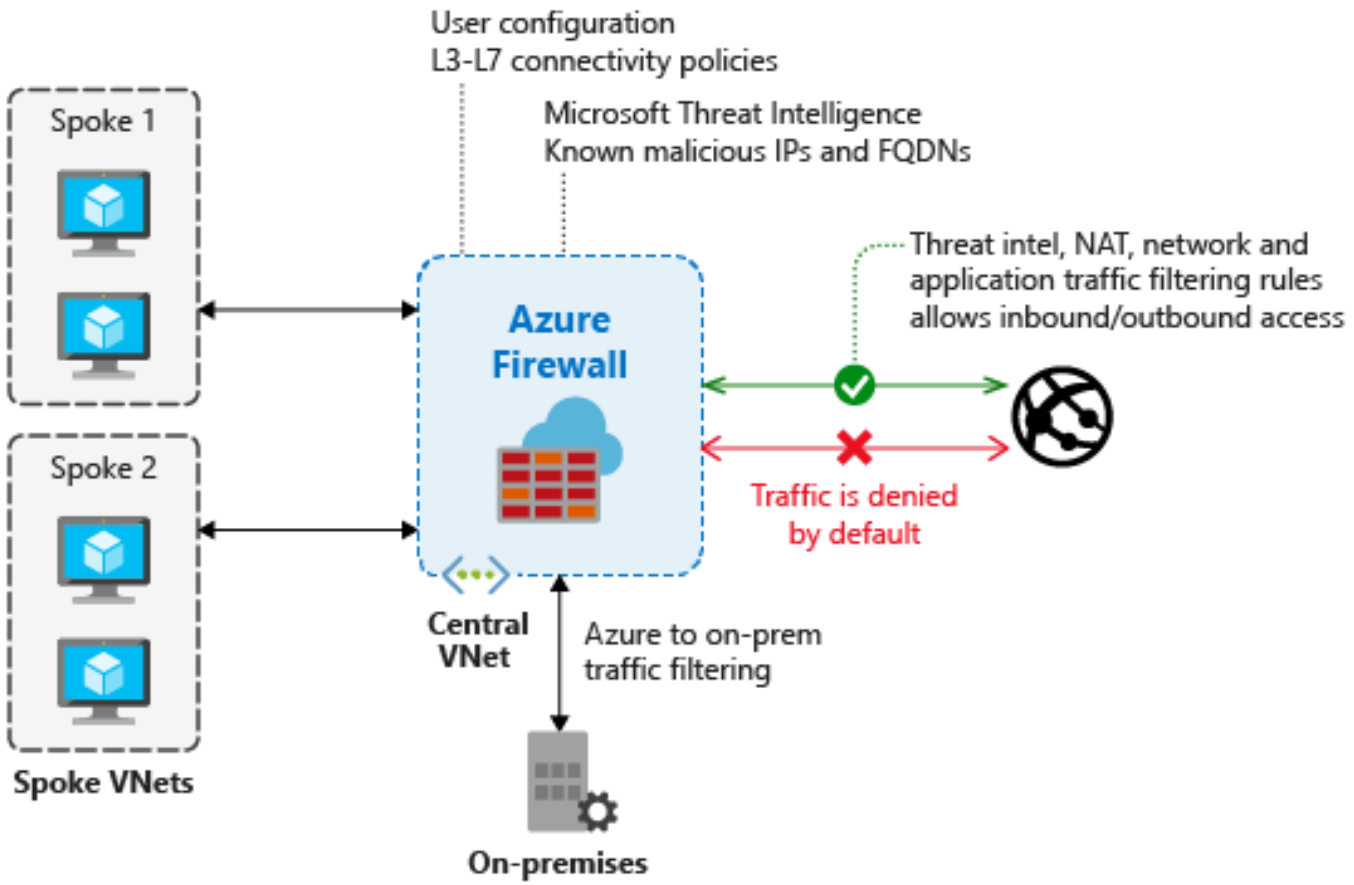


Deploy an Azure Front Door for a global web service

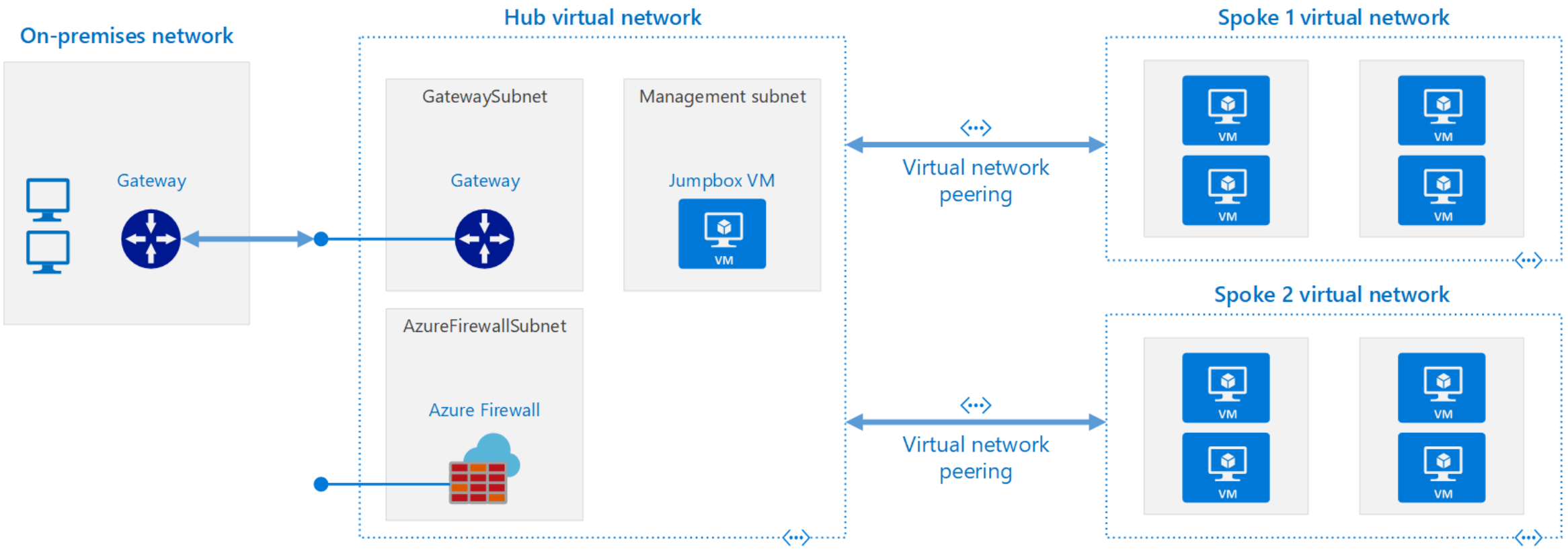
Configure a rules engine to apply security headers

Azure Firewall

Azure Firewall



Hub-spoke Topology



Demo

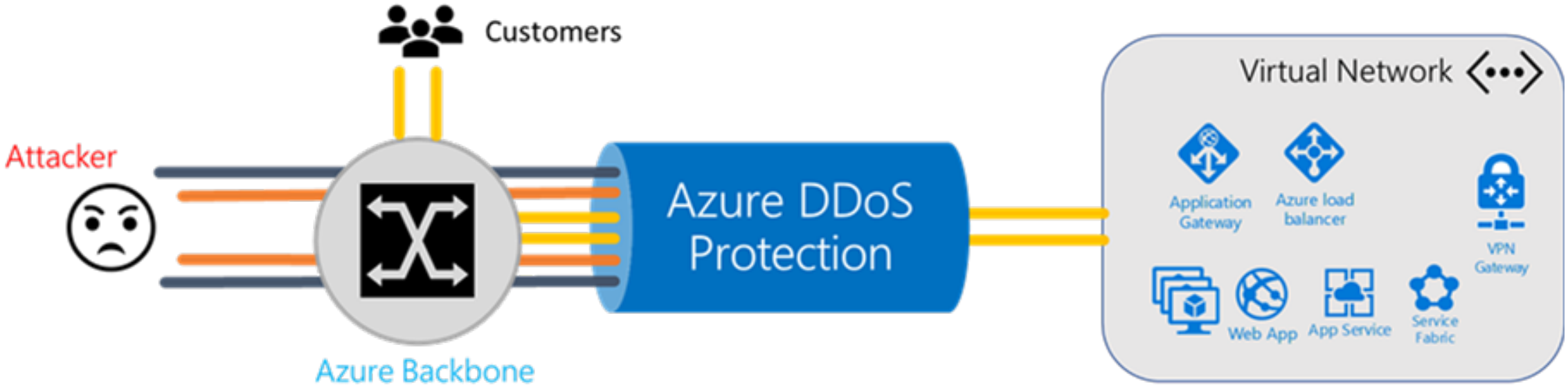
Deploy an Azure firewall

Configure routing

Add a firewall rule

Implement DDoS Protection

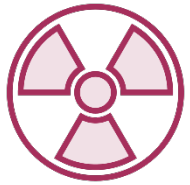
Azure DDoS Protection



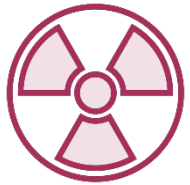
Basic vs. Standard

Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	●	●
Automatic attack mitigations	●	●
Availability guarantee		●
Cost Protection		●
Mitigation policies tuned to customers application		●
Metrics & alerts		●
Mitigation reports		●
Mitigation flow logs		●
DDoS rapid response support		●

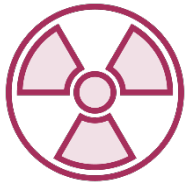
DDoS Attack Types



Volumetric attacks (network layer)



Protocol attacks (network and transport layer)



Resource layer attacks (application layer)

Demo

Create a DDoS protection plan

Assign it to a virtual network