Azure Security Services.
# Firewall and DDoS Protection

Azure Firewall Overview

❑ Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources

❑ You can use an Azure Firewall to grant access to resources in a VNET, based on the originating/source IP address

❑ Only clients from these granted IP addresses will be allowed to the internal resource

Azure Firewall

❑ Access is permitted/denied through firewall rules, that you create and specify ranges of IP addresses

Azure Firewall Example

☐ Azure Firewall supports inbound and outbound filtering

10.0.1.0/24 SUBNET 1

Non-HTTP/S Protocols (RDP, SSH, FTP)

INTERNET

Azure Firewall

10.0.0.0/16

Virtual Network
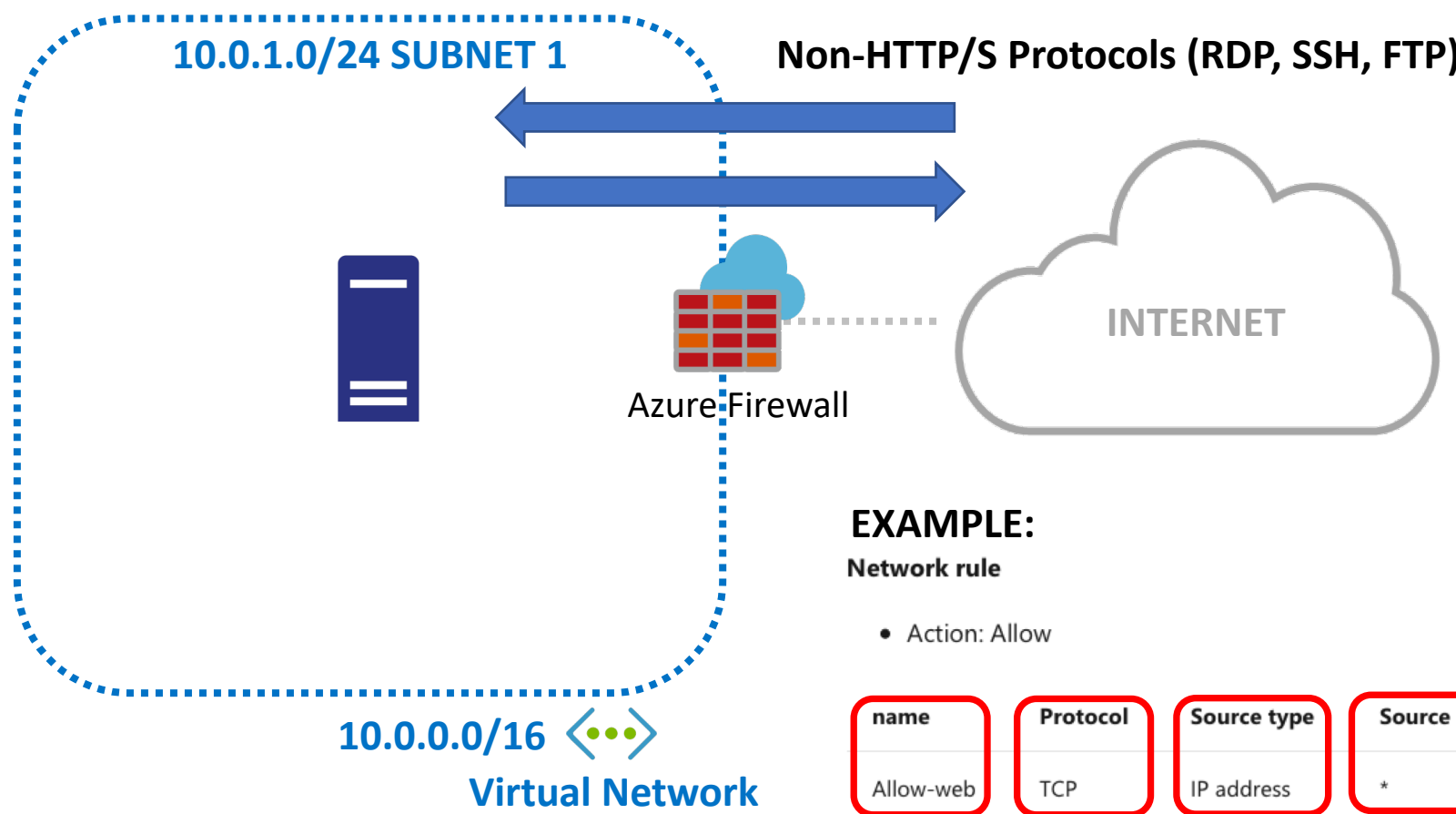
EXAMPLE:

Network rule

- Action: Allow

name	Protocol	Source type	Source	Destination type	Destination address	Destination ports
Allow-web	TCP	IP address	*	IP address	*	80,443

What is DoS and DDoS ?

❑ Denial of Service (DoS) is a type of attack that aims to overwhelm a network resource by sending huge number of requests, so that the resource becomes slow/unresponsive

❑ A Distributed Denial of Service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or
more web servers

❑ Azure DDoS protection provides
defense against DDoS attacks

Azure DDoS Service Tiers

- ❑ Basic
  - ❑ Enabled by default
  - ❑ Always-on traffic monitoring and real-time mitigation of common network-level attacks
  - ❑ Free, implies no cost

- ❑ Standard
  - ❑ Advanced mitigation capabilities over Basic tier
  - ❑ Can mitigate volumetric attacks, protocol attacks and application layer attacks
  - ❑ Price is based on usage, on a monthly basis

DDoS Attack Types

- Volumetric attacks
  - The victim is flooded (at the network layer – IP) with a huge amount of traffic, that seems to be legit

- Protocol attacks
  - Attacks target layer 3 and layer 4 protocol stack
  - Common example: SYN flood attacks (TCP, layer 4)

- Application layer attacks
  - Target web applications
  - Common examples: SQL injection, cross-site scripting

Microsoft Azure Fundamentals

Microsoft Azure Fundamentals
Training Bootcamp

Thank you