AZURE 900 CLOUD FUNDAMENTALS

Microsoft Certification AZ-900: Network Security Services



- DDOS attacks targeted at resources through public interne endpoint
- Exhausts resources & application becomes slow/unresponsive
- Azure DDOS protection mitigates using MS global network's scale & elasticity in Azure regions to block access
- Mitigates volume (flood network with traffic), protocol (target becomes inaccessible) and resource/application layer (disrupt data transmission of web apps) attacks

- Distributed network layers traffic filtering to/from Azure resources in a VN (for each subscription)
- Multiple in/outbound security rules
- Filter by source & destination IP, port and protocol

AZURE
DISTRIBUTED DENIAL
OF SERVICE (DDOS)
PROTECTION

NETWORK

SFCURITY

GROUP

NGS

NETWORK SECURITY SERVICES

> AZURE ASG

- Application Security Group: group resources with similar filtering requirements/functions
- Config network security of application
 - Reuse security policy

 Centralized dashboard to view, manage and monitor services

• ML identifies threats & recommend mitigative actions

Resource
Access
Control

- Access granted based on IP address for a request
- Firewall rules specify whitelisted IF addresses, network protocols and port information
- Manage connectivity policies centrally
- Network & application protection across subscriptions/VNs

AZURE FIREWALL

A7IIRF

SECURITY

CENTER

Managed, cloud-based network security service for Azure Virtual Network resources Features

- High availability
- Unrestricted scalability
- In/outbound filter rules
- Azure Monitor logging 8 analytics

Azure
Application
Gateway

 Web Application Firewall (WAF): centralized, inbound protection for your web applications against common exploits and vulnerabilities.