**Secure Network Connectivity – Objetive Domain**

**Describe the concept and functionality of:**

* Defense in depth
* Network Security Groups(NSG)
* Azure Firewall
* Azure DDoS protection

Nuvem é mais Segura que a estrutura legal, datacenter de nível 3.

**Defense in depth**

**- A layered approach to securing computer systems.**

**- Provides multiple levels of protection.**

**- Attacks against one layer are isolated from subsequent layers.**

Physical Security

Identity & Access

Perimeter

Compute

Network

Data

Application

**Shared Security**

* **Migrating from customer- controlled to cloud-based datacertes shifts the responsibility for security.**
* **Security becomes a shared concern between cloud providers and customers.**

**Tabela

Descrição gerada automaticamente**

**Network Security Groups(NSGs)->** Filter network traffic to and from Azure resources on Azure Virtual Networks.

* Set inbound and outbound rules to filter by source and destination IP address, port, and protocol.
* Add multiple rules, as needed, within subscription limits.
* Azure applies default, baseline security rules to new NSGs.
* Override default rules with new, higher priority rules.
* Firewall interno
* Gratuito
* Ruim para utilizar externamente
* Lê de cima para baixo
* Existe regras default
* É possível priorizar as regras

**Azure Firewall ->** A stateful, managed Firewall as a Service(FaaS) that grants/denies server access based on originating IP address, in order to protect network resources.

* Applies inbound and outbound traffic filtering rules
* Built-in high availability
* Unrestricted cloud scalability
* Uses Azure Monitor logging
* Solução de ambiente externo
* Criar regras e Nats
* Firewall Camada de 4

**Azure Application Gateway** also provides a firewall, Web Application Firewall(WAF). WAF provides centralized, inbound protection for your web applications. Outro produto, tem recurso de WAF, SE VC TEM UMA APP QUE TEM BRECHA DE SEGURANÇA, FIREWALL DO NIVEL DE APLICAÇÃO.

**Azure Distrbuted Denial of Service(DDoS) protection** DDoS attacks overwhelm and exhaust network resources, making apps slow or unresponsive.

* **Sanitizes unwanted network traffic before it impacts service availability.**
* **Basic service tir is automatically enabled in Azure.**
* **Standard service tier adds mitigation capabilities that are tuned to protect Azure Virtual Network resources.**
* **NÃO É UM SERVIÇO OPCIONAL, ESTÁ PRESENTE EM TUDO.**
* **GRATUITO, OU PODE SER PAGO(PARA TER ACESSO AS CONFIGURACOES).**

**Defense in Depth Reviewed**

**Combining network security solutions**

**- NSGs** with **Azure Firewall** to achieve defense in depth.

- **Perimeter layer** protects your network boundaries with Azure DDoS Protection and Azure Firewall.

- **Networking layer** only permits traffic to pass between networked resources with Network Group(NSG) inbound and outbound rules.

**Walkthrough – Secure network traffic**

**Create and configure inbound & outbound security port rules.**

1. Deploy a custom template to create virtual machine
2. Create a network security group
3. Create an inbound security port
4. Configure an outbound security port rule to deny Internet Acess