LIKE A BOSS

AZ 900 TEST PREP

AZURE SECURITY

Use these notes to help review testable material for the AZ-900 certification exam.

Know the definition and use cases for these Azure Security mechanisms.

Network Security Groups - NSGs filter traffic at the network layer using rules that allow or deny traffic based on what Microsoft calls '5-tuple' information:

1. Protocol – such as TCP, UDP, ICMP
2. Source IP address
3. Source port
4. Destination IP address
5. Destination port

Application Security Groups (ASGs) can apply security riles at scale, because an ASG is a logical grouping of virtual machines.

Azure Firewall is a managed service that filters on more levels than the Network Security Group does. It can filter traffic on OSI layer 3, 4, and 7.

DDoS Protection is automatically enabled as part of the Azure platform. It provides always-on traffic monitoring and real-time mitigation of common network-level attacks, providing the same defenses utilized by Microsoft's own online services. It's possible to upgrade DDoS Protection from Basic to Standard for additional mitigation capabilities

A **User Defined Route** is used to override Azure's default routing behavior between VNets and resources. For example, you can use a UDRs to send traffic between two subnets through a firewall appliance rather than directly between the two subnets.

Two fundamental regarding identity and access control are **authentication** and **authorization:**

- **Authentication** is the process of establishing the identity of a person or service looking to access a resource.
- **Authorization** is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service.

The **Azure Security Center** is a monitoring service that provides threat protection across all of your services both in Azure, and on-premises. It can:

- Provide recommendations based on your configurations, resources, and networks.
- Monitor settings across *on-premises and cloud workloads*, and automatically apply required security to new services as they come online.
- Continuously monitor all your services, and perform automatic security assessments to identify potential vulnerabilities
- Use machine learning to detect and block malware from being installed on your virtual machines and services.
- Analyze and identify potential inbound attacks.

Azure includes the **Azure Information Protection Service (AIP)**, which works *in conjunction with Office 365*, Microsoft's online productivity suite. Use AIP to classify documents (including email) according to how sensitive it is. This allows protection of files even when they are sent outside of your corporate network.

Azure Key Vault allows for secure storage of passwords and other secrets. You can then share those secrets with others without revealing the actual secret.

Azure Advanced Threat protection (ATP) helps monitor users in both cloud and on-prem environments. ATP analyzes user activity, and alerts admins when users engage in unusual behavior.