AZ-900 Fundamentals Revision Notes

AZURE ROLES

Shared Responsibility Model

- Cloud security is a shared responsibility of both cloud providers and customers.
- Azure has many **security certifications** from outside auditors.

Physical security:

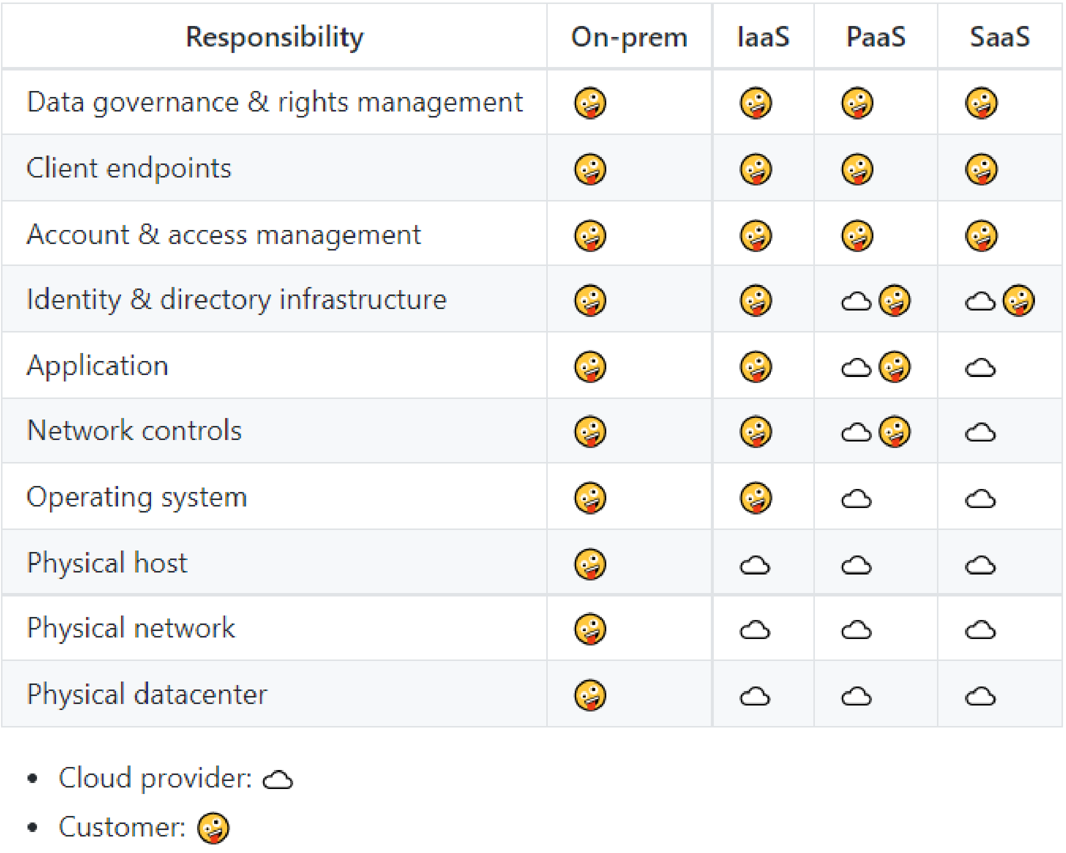
- Handled by Microsoft.
- Walls, cameras, gates, security personnel.
- Strict procedures for employees.

Digital security:

- Handled by customer + Microsoft.
- Azure has tools to mitigate security threats, consumer is responsible to use the tools.
- For example, role-based access control, multi factor authentication, encryption, monitoring tools such as login failures, suspicious locations, DDoS protection, real-time telemetry & firewalls.

-**Always** retain responsibility for: Data, Endpoints, Accounts, Access management (identities)

Cloud computing levels:



Responsibility	On-prem	IaaS	PaaS	SaaS
Data governance & rights management	🤪	🤪	🤪	🤪
Client endpoints	🤪	🤪	🤪	🤪
Account & access management	🤪	🤪	🤪	🤪
Identity & directory infrastructure	🤪	🤪	☁🤪	☁🤪
Application	🤪	🤪	☁🤪	☁
Network controls	🤪	🤪	☁🤪	☁
Operating system	🤪	🤪	☁	☁
Physical host	🤪	☁	☁	☁
Physical network	🤪	☁	☁	☁
Physical datacenter	🤪	☁	☁	☁

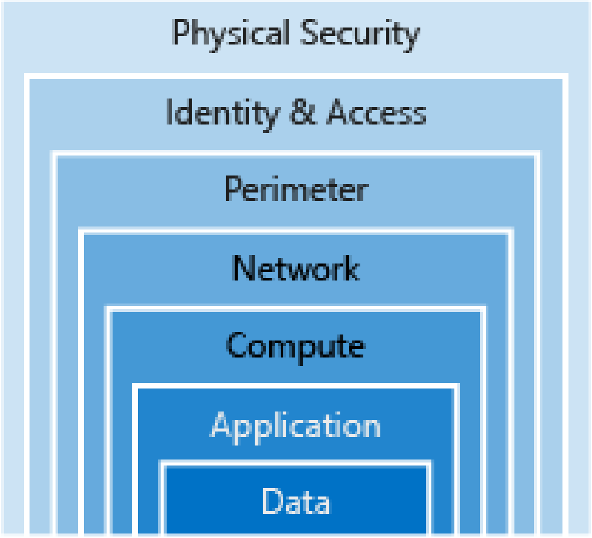
- Cloud provider: ☁
- Customer: 🤪

Defence in Depth:

- Strategy to slow the advance of an attack to get unauthorized access to information.
- Layered approach: Each layer provides protection, so if one layer is breached, a subsequent prevents further exposure.

- Applied by Microsoft, both in physical data centers and across Azure services.

Layers:



Data:

- In almost all cases attackers are after data.
- Data can be in database, stored on disk inside VMs, on a SaaS application such as Office 365 or in cloud storage.
- Those storing and controlling access to data to ensures that it's properly secured.
- Often regulatory requirements dictates controls & processes
- to ensure confidentiality, integrity, and availability.

Application:

- Ensure applications are secure and free of vulnerabilities.
- Store sensitive application secrets in a secure storage medium.
- Make security a design requirement for all application development.
- Integrate security into the application development life cycle.

Compute:

- Secure access to virtual machines.
- Implement endpoint protection and keep systems patched and current.
- Malware, unpatched systems, and improperly secured systems open your environment to attacks.

Networking:

- Limit communication between resources.
- Deny by default.
- Allow only what is required.
- Restrict inbound internet access and limit outbound, where appropriate.
- Implement secure connectivity to on-premises networks.

Perimeter:

- Use distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.

- Use perimeter firewalls to identify and alert on malicious attacks against your network.

Identity and access:

- Control access to infrastructure and change control.
- Access granted is only what is needed
- Use single sign-on and multi-factor authentication.
- Audit events and changes.

Physical security:

- Building security & controlling access to computing hardware.
- First line of defence.

Azure Security Center:

- Monitoring service that provides threat protection across all services
- Both in Azure, and on-premises.
- Gives security recommendations based on your configurations, resources, and networks.
- Part of cis security, https://www.cisecurity.org/cis-benchmarks/
- Automatic security assessments through continuous monitoring to identify potential vulnerabilities before they can be exploited.
- Just-in-time access control for ports through **Azure Defender**.
- Analyses & identifies identify potential inbound attacks.
- Helps to investigate threats and any post-breach activity that might have occurred.
- **Control apps**:
  - Only the apps you validate are allowed to execute.
  - Uses machine learning to detect and block malware from being installed on services
- Helps with compliance through continuous assessments & recommendations.

Tiers:

Free:

- Available as part of any Azure subscription
- Limited to assessments and recommendations of Azure resources only.

Azure Defender:

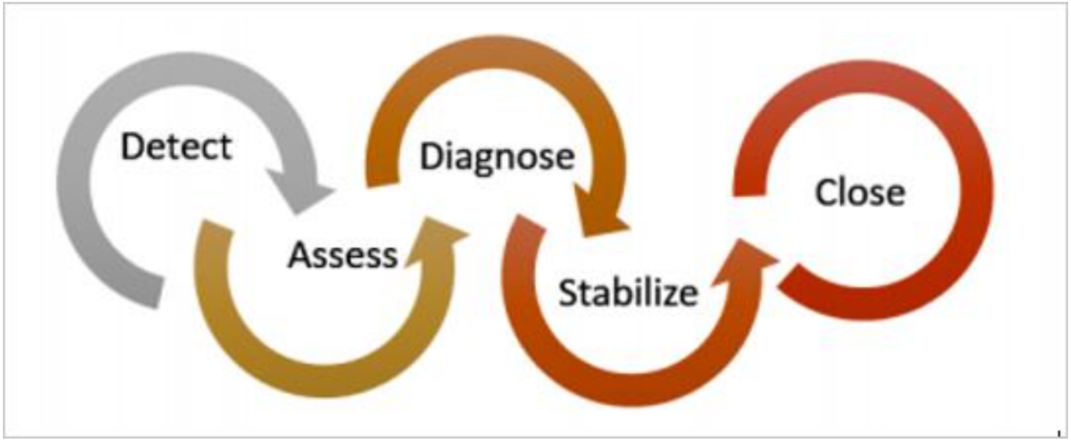
- Formerly known as **Azure security center standard edition**.
- Provides a full suite of security-related services including:
  i. Continuous monitoring
  ii. Threat detection
  iii. Just-in-time access control for ports
- $15 per node per month, 30-day free trial available.
- To upgrade to the Standard tier, you must be assigned the role of **Subscription Owner**, **Subscription Contributor**, or **Security Admin**.

Use-cases:

Incident response:

- Have an incident response plan in place before an attack occurs.

Incident response stages:



- You can use Security Center during the detect, assess and diagnose stages.

Detect:

- Review the first indication of an event investigation.
- For example, you can use the Security Center dashboard to review the initial verification that a high-priority security alert was raised.

Assess:

- Perform the initial assessment to obtain more information about the suspicious activity.
- For example, obtain more information about the security alert.

Diagnose

- Conduct a technical investigation and identify containment, mitigation, and workaround strategies.
- Follow the remediation steps described by Security Center in that particular security alert.

Recommendations to enhance security:

Security policy:

- Set of controls that are recommended for resources within that specified subscription or resource group.
- You can reduce the chances of a significant security event by configuring a security policy.

Recommendations:

- Based on security policies for potential vulnerabilities.
- Guide you through the process of configuring the needed security controls.
- For example, if you have workloads that do not require the Azure SQL Database Transparent Data Encryption (TDE) policy, turn off the policy at the subscription level and enable it only in the resources groups where SQL TDE is required.

Identity and Access (Azure AD)

- Old-school corporate security.
- Network perimeters, firewalls, and physical access controls.
- Does not work good with bring your own device (BYOD), mobile apps, and cloud applications.

- Identity meaning new primary security boundary.
- Proper authentication and assignment of privileges is critical to maintaining control of your data.
- Allows to maintain a security perimeter outside physical control.
- Possible to always be sure who has the ability to see & manipulate data and infrastructure with **single sign-on** and appropriate **role-based access** configuration.

Authentication and authorization:

- Azure provides services to manage both through **Azure Active Directory**.

Authentication:

- Verification of a person or service looking to access a resource.
- Establishes if they are who they say they are.
- Challenges a party for legitimate credentials, and provides the basis for creating a security principal for identity and access control use.
- Sometimes called **az AuthN.**

Authorization:

- Establishes what level of access an authenticated person or service has.
- Specifies what data they're allowed to access and what they can do with it.
- Sometimes shortened to ****AuthZ**.**

Azure Active Directory:

- Called also as **Azure AD**.
- Cloud-based identity service.
- Can synchronize with existing on-premises Active Directory or can be used stand-alone.
- Allows to share identities in cloud (for example Office 365), mobile on-premises applications.
- No SLA for free tier, 99.9% for standard & premium.

Some services:

- **Authentication.**
  - Self-service password reset.
  - [Multi-factor authentication MFA.
  - Custom banned password list, and smart lockout services.
- **Single-Sign-On (SSO).**
- **Application management.**

Manage cloud and on-premises apps using Azure AD Application Proxy, SSO, the My apps portal (also referred to as Access panel), and SaaS apps.

- **Business to business (B2B) identity services:** Manage guest users and external partners.
- **Business-to-Customer (B2C) identity services:** Customize and control how users sign up, sign in, and manage their profiles when using apps & services.
- **Device Management**
  - Manage how your cloud or on-premises devices access your corporate data.

Single sign-on:

- More identities for single user.
- More passwords & harder for users to remember them.

- More risk of credential-related security incident.
- Harder management: more account lockouts and password reset requests.
- if a user leaves an organization meaning all identities must be tracked down.
- Single sign-on (SSO) means single identity.
- Mean one password to access across all applications
- Less effort to manage for example if someone leaves an organization
- Allows you to use third-party for example on-prem identities in Azure.

SSO with Azure Active Directory:

- Ability to combine data sources into an intelligent **security graph**.
- Graph enables the ability to.
- Provide threat analysis.
- Real-time identity protection.
- Applied to all accounts in Azure AD (can be synchronized from on-prem).
- Centralized identity provider is good.
- Centralized security controls, reporting, alerting, and administration of the identity infrastructure.
- For example, allows signing into email and Office 365 documents without having to reauthenticate.

Multi-factor authentication:

- Called also MFA.
- Requires two or more elements for full authentication.

Element categories are:

- **Something you know:** A password or the answer to a security question.
- **Something you possess:** For example, a mobile app that receives a notification or a token-generating device.
- **Something you are:** For example, a fingerprint or face scan used often on mobile devices.

- Enable it wherever possible for more security.

Azure AD MFA:

- Integrates also with other third-party MFA providers.
- Always use at least for Global Administrator role in Azure AD.
- You can activate conditionally using **Azure AD Identity Protection**.
- Any time a user is signing in from an unknown computer.

Providing identities to services:

- Valuable for services to have identities.
- Often, and against best practices, credential information is embedded in configuration files.
- With no security around these configuration files, anyone with access to the systems or repositories can access these credentials and risk exposure.

AZ-900 Fundamentals Revision Notes

Service identities in Azure AD:

Service principals:

- **Identity**: A thing that can be authenticated.
  - For example, users with user name & password.
  - For example, applications or other servers with secret keys or certificates.
- **Principal:** an identity acting with certain roles or claims
  - You can have same identity but different role which you are executing.
  - Running `sudo` on a Bash prompt or on Windows using **"run as Administrator."**
  - Groups are often also considered principals because they can have rights assigned.
- **Service principal** meaning an identity that is used by a service or application that can be assigned roles.

Managed identities:

- Azure infrastructure automatically takes care of authenticating the service and managing the account.
- Can be instantly created for any Azure service that supports it.
- Allows the authenticated service secure access of other Azure resources just like any AD account.

Roles in Azure:

- All co-exists.
- Three categories: **classic roles, azure roles, azure ad roles.**

Classic roles:

- Before Role-based access control was introduced there were 3 roles:
  - **Account Administrator:** One per Azure account.
  - **Service Administrator:** One per Azure subscription.
  - **Co-Administrator:** 200 per subscription.

Role-based access control:

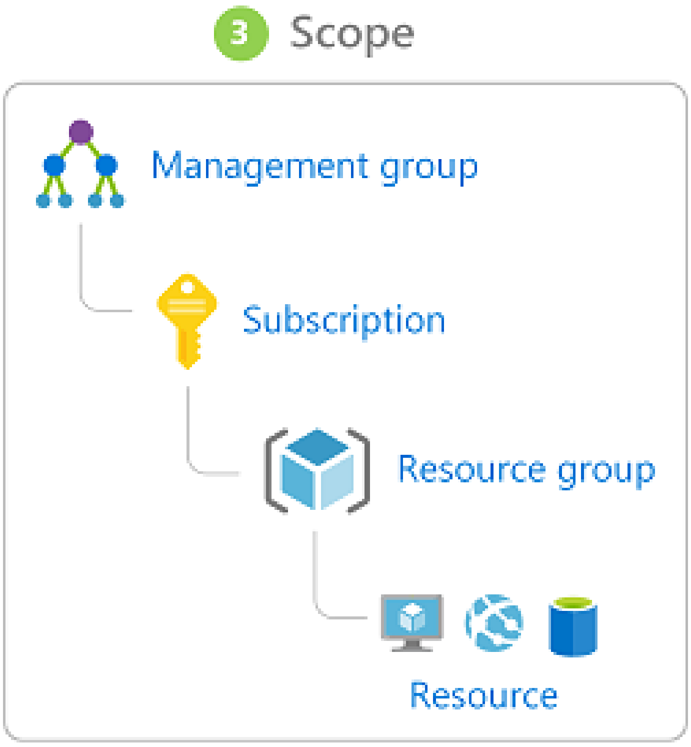
- Called also **Azure roles.**
- Provides fine-grained access management for Azure resources.

- **Role:**
  - Sets of permissions.
  - For example, **"Read-only" or "Contributor"**.
  - Identities are mapped to roles directly or through group membership.

- **Role assignments:**
  - When you are assigned to a role, RBAC allows you to perform specific actions, such as read, write, or delete.

    Examples are:
    - Allow one user to manage VMs in a subscription.
    - Allow an application to access all resources in a resource group.
- Can be granted at the service instance level, but they also flow down the Azure Resource Manager hierarchy.
  - Roles assigned at a higher scope, like an entire subscription, are inherited by child scopes, like service instances.

AZ-900 Fundamentals Revision Notes



- Segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

- **Four fundamental Azure roles:**
  - Owner.
  - Contributor.
  - Reader.
  - User Access Administrator.

Azure AD Roles

On-tenant level:

- **Global Administrator:** Person who signs up for Azure AD tenant, can do anything.
- **User Administrator, Billing Administrator.**

Privileged Identity Management:

- Also known as **Azure AD Privileged Identity Management (PIM)**
- Includes ongoing auditing of role members.
- Needed as their organization changes and evolves.

Provides:

- Oversight of role assignments
- Self-service
- Just-in-time role activation
- Azure AD and Azure resource access reviews.

Encryption (Azure Key Vault, Certificates):

- Process of making data unreadable and unusable to unauthorized viewers.
- To use or read the encrypted data, it must be decrypted with a secret key.
- Last & strongest line of defence in a layered security strategy.

Types Of Encryptions:

Symmetric encryption:

- Uses the same key to encrypt and decrypt the data.
- For example, A desktop password manager application like password orbit encrypts your passwords with your key (derived from your master password & key file). The same key is used when the data needs to be retrieved.

Asymmetric encryption:

- Uses a public key and private key pair.
- Either key can encrypt but a single key can't decrypt its own encrypted data.
- To decrypt, you need the paired key.
- Used for things like Transport Layer Security (TLS) (used in HTTPS) and data signing.

Encryption Methods /Ways:

Encryption at rest:

- Encryption of data at rest.
- Data at rest mean data that has been stored on a physical medium and examples are server disk, database or storage account.
- Ensures that data is unreadable without decryption keys/secret
- For example, if an attacker obtains a hard drive with encrypted data and did not have access to the encryption keys, the attacker would not compromise the data without great difficulty.
- Good to encrypt meaning critical financial information, intellectual properties, personal data about customers, employee’s data, even keys & secrets used for the encryption of the data itself.

Encryption in transit:

- Data actively moving from one location to another, for example, across the internet or through a private network.
- Protects the data from outside observers.
- Only the receiver has the secret key that can decrypt the data to a usable form.
- Secure transfer can be handled by several different layers.
- For example, in application layer such as HTTPS and in network layer which is a secure channel like virtual private network (VPN).

Encryption on Azure:

- For raw storages: Azure Storage Service Encryption.
- For virtual machine disks: Azure Disk Encryption.
- For databases: Transparent data encryption (TDE).
- For secrets: Azure Key Vault.

Azure Storage Service Encryption:

- Allows you encrypt raw storage.
- Automatically encrypts your data before persisting it to Azure Managed Disks, Azure Blob storage, Azure Files, or Azure Queue storage.
- And decrypts the data before retrieval.
- The handling of process is transparent to applications.
- Encryption, encryption at rest, decryption, and key management.

AZ-900 Fundamentals Revision Notes

Azure Disk Encryption:

- Helps you encrypt your Windows and Linux IaaS virtual machine disks.
- Uses BitLocker in Windows and the dm-crypt in Linux to provide volume encryption for the OS and data disks.
- Integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.
- And you can use managed service identities for accessing Key Vault.

Transparent data encryption (TDE):

- **Protection for:**
  - Azure SQL Database: Enabled by default.
  - Azure Synapse Analytics.
- **Performs real-time encryption and decryption at rest of:**
  - the database.
  - associated backups.
  - transaction log files.
- **Uses a symmetric key called the database encryption key:**
  - Bring your own key (BYOK) is also supported with keys stored in Azure Key Vault.

Azure Key Vault:

- Stores & manages.
- **Secrets:** such as passwords, certificates, Application Programming Interface (API) keys, and other secrets.
- **Keys:** create and control the encryption keys used to encrypt your data.
- **Certificates:** provision, manage, and deploy your public and private SSL / TLS.
- You can create a policy that directs Key Vault to manage the life cycle of a certificate.
- You can provide contact information for notification about life-cycle events of expiration and renewal of certificate.
- You can automatically renew certificates with selected issuers.

Read more on Azure certificates.

- Keys/secrets can be either protected by software or hardware security modules (HSMs).
- Provides secure access, permission control (RBAC) & access logging.
- Simplifies administration for example easier to enrol/renew certs.
- Integrate with other Azure services such as storage accounts, container registries, event hubs.
- Applications with managed service identities enabled can automatically and seamlessly acquire the secrets they need.

Azure certificates:

Transport Layer Security (TLS):

- Basis for encryption of website data in transit.
- Uses certificates to encrypt and decrypt data.
- Have a life cycle that requires administrator management
- Expired TLS certificates open security vulnerabilities.
- Certificates used in Azure are x.509 v3 that can be y
- Signed by a trusted certificate authority.

- **Self-Signed:**
  - i. Not trusted by default as signed by its own creator.
  - ii. Good for development and testing.
- Can contain a private or a public key.
- Keys have an identifiable thumbprint.
- Used in the Azure configuration file to identify which certificate a cloud service should use.

Types of certificates:

Service certificates:

- Attached to a specific cloud service.
- Enables secure communication to and from the service. For example, if you deploy a web site, you would want to supply a certificate that can authenticate an exposed HTTPS endpoint.
- Defined in your service definition.
- Automatically deployed to the VM that is running an instance of your role.
- You can manage service certificates separately from your services.
- You can also upload service certificates to Azure.

For example, a developer could upload a service package that refers to a certificate that an IT manager has previously uploaded to Azure.

An IT manager can manage and renew that certificate (changing the configuration of the service) without needing to upload a new service package.

- To update a certificate, you don't need to re-deploy a service package, just:
  - Upload a new certificate
  - Change the thumbprint value in the service configuration file.

Management certificates:

- Allow you to authenticate with the classic deployment model.
- Allows automation of configuration and deployment of some Microsoft / Azure services.
- Examples include Visual Studio or the Azure SDK
- Are not related to cloud services.

Network Protection:

- Important to secure your network from attacks and unauthorized access
- Use a layered approach
- Not enough to just focus on securing the network perimeter or the network security between services inside a network.
- Helps reduce your risk of exposure through network-based attacks
- Secure your internet-facing resource, internal resources, and communication between on-premises networks
- Combine multiple Azure networking and security services
- For example, use Azure Firewall to protect inbound and outbound traffic to the Internet, and Network Security Groups to limit traffic to resources inside your virtual networks.

Internet protection:

- Perimeter of the network.
- Focused on limiting and eliminating attacks from the internet.
- Only allow inbound and outbound communication where necessary.
- Ensure they are restricted to only the ports and protocols required.
- You can use Azure Security Center for this.

Firewall:

- Service that grants server access based on the originating IP address of each request.
- Helps you to provide inbound protection at the perimeter
- You create firewall rule
- Firewall rule meaning Ranges of IP addresses to allow access the server.

- Often includes specific network protocol and port information.

Azure Firewall:

- Managed, highly available & scalable, network-level, firewall as a service.
- Inbound protection for mainly non-HTTP/S protocols.
- Remote Desktop Protocol (RDP), Secure Shell (SSH), and File Transfer Protocol (FTP).
- Outbound protection for all ports and protocols.
- Application-level protection for outbound HTTP/S.

Azure Application Gateway:

- Load balancer that includes a **Web Application Firewall (WAF)**.
- Provides protection from common, known vulnerabilities in websites.
- Designed to protect HTTP traffic.

Network virtual appliances (NVAs):

- Ideal options for non-HTTP services or advanced configurations
- Similar to hardware firewall appliances.

Distributed Denial of Service (DDoS) Protection:

- Any resource exposed on the internet is at risk of being attacked by a denial-of-service attack.
- Attacks attempt to overwhelm a network resource.
  - sends so many requests that the resource becomes slow or unresponsive.
- Combine Azure DDoS Protection with application design best practices.

Azure DDoS Protection:

- Brings DDoS mitigation capacity to every Azure region.
- Protects your Azure applications by monitoring traffic at the Azure network edge before it can impact your service's availability.
- You are notified using Azure Monitor metrics within a few minutes of attack detection.

Service tiers

Basic:

- Automatically enabled as part of the Azure platform.
- Always-on traffic monitoring and real-time mitigation of common network-level
- Used by Microsoft's online services use.

Standard:

- Tuned specifically to Microsoft Azure Virtual Network resources
- Requires no application changes.
- Dedicated traffic monitoring and machine learning algorithms.
- Policies are applied to public IP addresses associated with resources deployed in virtual networks
- Example includes Azure load Balancer and Application Gateway.
- **Mitigates against:**

  i. **Volumetric attacks:** The attacker's goal is to flood the network layer with a substantial amount of seemingly legitimate traffic.

  ii. **Protocol attacks:** Render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.

  iii. **Resource (application) layer attacks:** Target web application packets to disrupt the transmission of data between hosts.

Traffic inside your virtual network:

- Allows you to limit communication between resources to only what is required.

Virtual network security

Network Security Groups (NSGs):

- Provide a list of allowed and denied communication to and from network interfaces and subnets.
- Used for communication between virtual machines.
- Filter network traffic to and from Azure resources in an Azure virtual network.
- By source and destination IP address, port, and protocol.
- Can contain multiple inbound and outbound security rules.

Service endpoints:

- You can restrict access of services to service endpoints.
- Allows you to remove public internet access to your services.
- Service access become limited to your virtual network.

Network integration:

- Integrate on-premises networks vice-versa services in Azure
- Different ways: VPN, ExpressRoute

Virtual private network (VPN):

- Establish secure communication channels between networks.
- Connects Azure Virtual Network to an on-premises VPN device.
- Provide secure communication in-between.

Azure ExpressRoute:

- Use to provide a dedicated, private connection between your network and Azure.
- Lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider.
- Very secure as it sends traffic over the private circuit instead of over the public internet.
- You can send this traffic through appliances for further traffic inspection.

Microsoft Azure Information Protection (AIP):

- Helps to classify and optionally protect (encrypt) documents and emails by applying labels.
- Labels can be applied
  - automatically based on rules and conditions
  - or manually
- Examples are when a user saves a Microsoft Word document containing a credit card number, a custom tooltip is displayed. The tooltip recommends labelling the file as `**Confidential \ All Employees**` configured by the administrator.
- After your content is classified, you can track and control how the content is used. For example, you can:
  - Analyse data flows to gain insight into your business
  - Detect risky behaviours and take corrective measures
  - Track access to documents
  - Prevent data leakage or misuse of confidential information
- You can purchase AIP either as a standalone solution, or through one of the following Microsoft licensing suites:

  - Enterprise Mobility + Security
  - or Microsoft 365 Enterprise

Microsoft Defender for Identity:

- Formerly **Azure Advanced Threat Protection (ATP)**
- Cloud-based security solution that identifies, detects, helps you investigate threats.
- Capable of detecting known malicious attacks and techniques, security issues such as compromised identities, and risks/threats against your network.
- Can be integrated with on-premises Microsoft Defender ATP.

Microsoft Defender for Identity components

Microsoft Defender for Identity portal:

- Own portal at azure portal.
- User accounts must be assigned to an Azure AD security group that has access to the Azure ATP portal to be able to sign in.
- Through it you can monitor and respond to suspicious activity.
- Allows you to create your Azure ATP instance, and view the data received from Azure ATP sensors.
- Monitor, manage, and investigate threats in your network environment.

Microsoft Defender for Identity sensor:

- Sensors are installed directly on your domain controllers.
- Monitors domain controller traffic without requiring a dedicated server or configuring port mirroring.

Microsoft Defender for Identity cloud service:

- Runs on Azure infrastructure.
- Deployed in the United States, Europe, and Asia.
- Connected to **Microsoft Intelligent Security Graph**.
  - Threats signals are seamlessly shared across all the services in Microsoft 365 Defender, 6.5 trillion signals daily.
    - **Microsoft 365 Defender**
      - Formerly known as **Microsoft Threat Protection**.
      - Consists of different Azure security services
      - Examples are: Office ATP, Microsoft Defender ATP, SmartScreen, Exchange Online Protection (EOP).
  - Provides comprehensive security across multiple attack vectors.
  - Allows you to use [Microsoft Graph Security API.
    - Connects Microsoft security products, services, and partners
    - Can be used to:
      i. Streamline security operations.
      ii. Improve threat protection, detection, and response capabilities.

Microsoft Security Development Lifecycle (SDL):

- Set of guidance, best practices, tools, and processes
- Used internally at Microsoft to build more secure products and services.
- Introduces security and privacy considerations throughout all phases of the development process.
- Helps developers:
  i. build highly secure software
  ii. address security compliance requirements
  iii.reduce development costs.

AZ-900 Fundamentals Revision Notes

Provide training:

- Security is everyone's job
- Example are: developers, service engineers, and program and project managers.
- Everyone must understand:
  i. Security basics.
  ii. How to build security into software & services.
  iii. Attacker's perspective, their goals, and the art of the possible.

Define security requirements

- Security requirements must be updated continuously in order to address changes in required functionality and changes to the threat landscape.
- Optimal time to define the security requirements is during the initial design and planning stages.
  - Early planning allows development teams to integrate security in ways that minimize disruption.
- Factors that influence security requirements include, but are not limited to:
  - Legal and industry requirements
  - Internal standards and coding practices
  - Review of previous incidents
  - Known threats
- Track requirements through:
  - work-tracking system
  - telemetry from the engineering pipeline.

Define metrics and compliance reporting

- Essential to define the minimum acceptable levels of security quality
- And to hold engineering teams accountable to meeting that criterion.
- Good to define as early as possible to apply standards throughout the entire project.
- Example are: all known vulnerabilities discovered with a **"critical" or "important"** severity rating must be fixed with a specified time frame.
- Track & report security work:
  - Allows to have key performance indicators (KPIs)
  - Ensures security tasks are completed
  - Bug/work tracking mechanism should allow for security defects and security work items
    - to be clearly labelled as security
    - marked with their appropriate security severity.

Perform threat modelling:

- USE in environments where there is a meaningful security risk.
- Allows development teams to consider, document, and discuss the security implications of designs.
- Applying a structured approach to threat scenarios helps a team.
  1. Effectively and less expensively identify security vulnerabilities
  2. Determine risks from those threats
  3. make security feature selections and establish appropriate mitigations.
- You can apply threat modelling at the component, application, or system level.
- **Read more: Threat Modelling.**

Establish design requirements:

- Assurance activities that help engineers implement more secure features; examples are well- engineered for security.
- Methods are cryptography, authentication, and logging.

- Complicated design & security features are likely to result in vulnerabilities.
- Crucial to apply consistently and with an understanding of the protection they provide.

Define and use cryptography standards:

- Encrypt in transit to protect data from being alteration & unintended disclosure when moving.
- Making an incorrect choice when using any aspect of cryptography can be catastrophic.
  - Best to develop clear encryption standards with specifics on every element of the encryption implementation.
- Only use industry-vetted encryption libraries: Encryption should be left to experts.
- See the Microsoft SDL Cryptographic Recommendations whitepaper for more.

Manage security risks from using third-party components:

- Understand the impact of security vulnerability in third-party components to rest of the system.
- Plan to respond when new vulnerabilities are discovered & consider additional validation
- **Read more:**
  - Managing Security Risks Inherent in the Use of Third-Party Components
  - Managing Security Risks Inherent in the Use of Open-Source Software

Use approved tools:

- Define and publish a list of approved tools and their associated security checks.
- Examples are: compiler/linker options and warnings.
- Strive to:
  - use the latest version of approved tools (such as compiler versions)
  - utilize new security analysis functionality and protections.
- **Read more about:**
  - Recommended Tools, Compilers and Options for x86, x64, and ARM processors.
  - SDL Resources.

Perform Static Analysis Security Testing (SAST):

- Analysing source code prior to compilation
  - provides a highly scalable method of security code review
  - helps ensure that secure coding policies are being followed
- Typically integrated into the commit pipeline to identify vulnerabilities each time the software is built or packaged.
- Some offerings replace flawed (for example unsafe/banned) functions while developer is coding.
- **Read more:**
  - Microsoft DevSkim
  - Roslyn Security Guard Rules.
  - Visual Studio Marketplace
  - Analysing C/C++ Code Quality by Using Code Analysis)
  - Microsoft BinSkim on GitHub

Perform Dynamic Analysis Security Testing:

- Performs run-time verification when all components are integrated and running.
- Achieved using a tool.
- For example, a suite of pre-built attacks

- Examples are: to specifically monitor application behaviour for memory corruption, user privilege issues, and other critical security problems.
- Some tools can be more readily integrated into the CI/CD pipeline
- such as web app scanning tools
- Other such as fuzzing requires a different approach.
- **Read more:**
  - Visual Studio Marketplace
  - Automated Penetration Testing with White-Box Fuzzing)

Perform penetration testing:

- Security analysis of a software system by simulating the actions of a hacker.
- Uncovers potential vulnerabilities resulting from examples such as: coding errors, system configuration faults, or other operational deployment weaknesses.
- Finds the broadest variety of vulnerabilities
- Often performed in conjunction with automated and manual code reviews.

Read more:

- Attack Surface Analyzer.
- SDL Security Bug Bar Sample

Establish a standard incident response process:

- Crucial for addressing new threats that can emerge over time
- The plan should be created in coordination with your organization's dedicated Product Security Incident Response Team (PSIRT).
- Your incident response plan should:
  - Include who to contact if a security emergency occurs.
  - Establish the protocol for security servicing (including plans for code inherited from other groups within the organization and for third-party code).
  - Be tested before it is needed.

Read more:

- Using Azure Security Center for an incident response.
- Microsoft Incident Response and shared responsibility for cloud computing.
- Microsoft Security Response Center.