Links to the videos regarding the SC-900:

John Savill's Technical Training : https://www.youtube.com/watch?v=Bz-8jM3jg-8&t=2s

freeCodeCamp.org : https://www.youtube.com/watch?v=LLKza5oULAA

Below you will find my notes for the SC-900. This is by no means a full and complete summary for the SC-900. Its purpose was to list the topics I found most important. I encourage you to use this summary as an addition to your learning.

SC-900

AAD AZURE M365

Defense in Depth

- Physical Security
- Identity — MFA
- Perimeter — DDoS
- Network
- Compute
- Application
- Data — Encryption

C onfidentiality

I ntegrity

A vailability

Threats:

- Data Breach - Data
- Dictionary Attack
- Phishing
- Spear Phishing

  ] - Identity

- Ransomware
- Disruptive attack (DDoS)

  ] - Availability

Zero Trust:

Assume Compromise

Verify Everything

- Authentication + Authorization
- Least Privilage + Just in Time JiT
  + Just Enough JEA
- Assume Breach
  - Segment, Encrypt, Detect Threats

Focus:

- Identity
- Device Monitoring
- Applications
- Data Classification
  - Encryption
  - Data Loss Prevention
- Infrastructure

Encryption

Symmetric

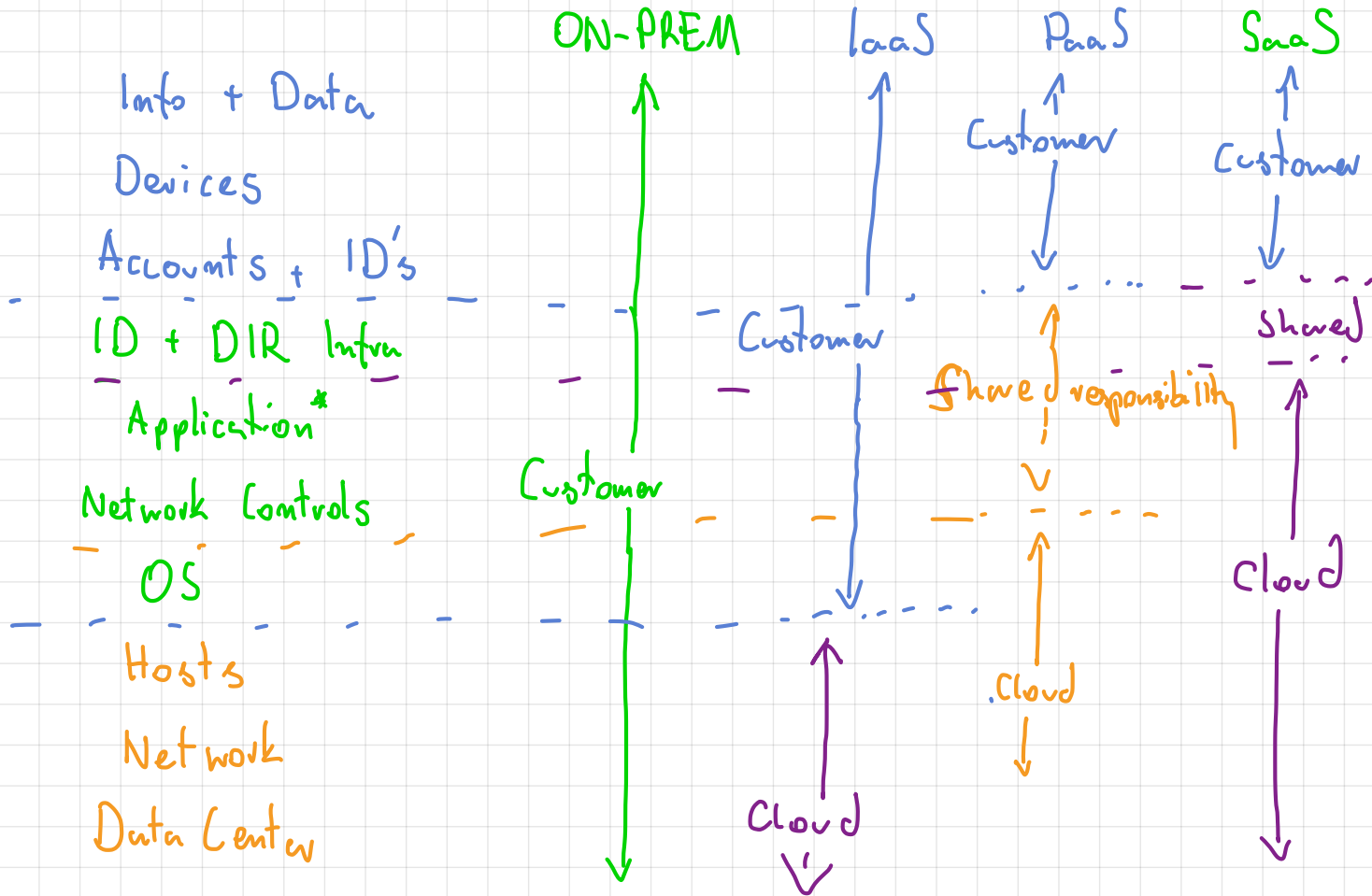
Data —KEY→ Q4.5h (encrypted data) —KEY→

Asymmetric

Public ∧ Private key

Data —Pub→ %SQh —Priv→ Data

Data → # Public [#] Private key ≈ # ← Data → [#] Private



6 Privacy Principles

- Control
- Transparent
- Security
- Strong Legal Protection
- No Content-Based Target
- Benefits to You

TRUST

Service Trust Portal

AZURE AD

AZURE M365

Administration AuthN AuthZ Audit

Azure AD

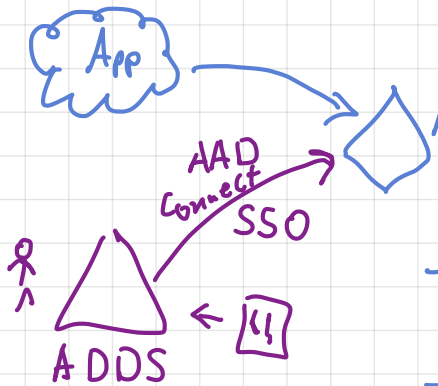
MGMT

Who
|
Am

What
|
Can Do

What
|
Have Done

Modern Authentication
- Token
- Consent
- Policy
- Audit
- Detect Risk



AAD
IdP, OIDC
Identity Provider SAML
- Users
  Guests (B2B)
- SP ← Req. App.
- M. Id
- Groups < Assigned / Dynamic

Authentication

First

Who
|
Am

Password

MFA
↑
Conditional Access
P1 / P2

MFA
- SMS
- CALL
- Auth App
  - 5 OTP
  - 4 OTP
- No Password
  - H4B
  - Auth App
  - FIDO 2

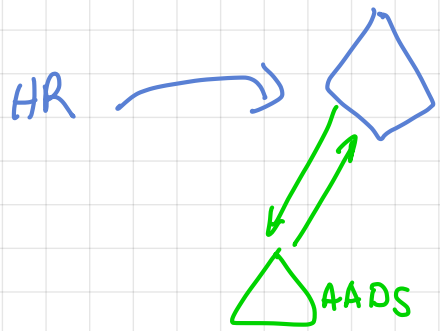
- I know — Pin / Password
- I have — Token / Phone / Laptop
- I am — Biometric

Authorization

RBAC
- Azure
- AAD ← M365
  + Custom

Conditional Access

Audit / Gov



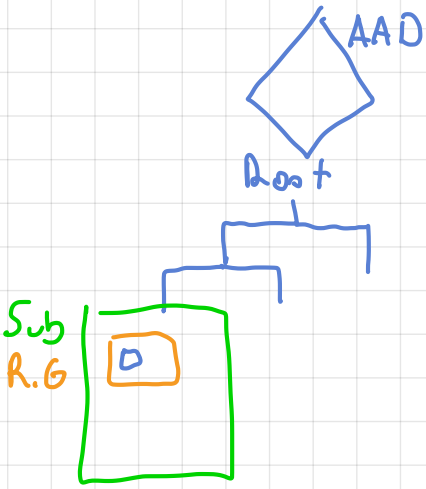
Group - Dynamic

P2
- PIM
- Access Review
  - app
  - role
  - group
- AAD IP

Azure

Governance

- RBAC
- Policy
- Budget



Lock
- cannot delete
- read only

MGMT Plane

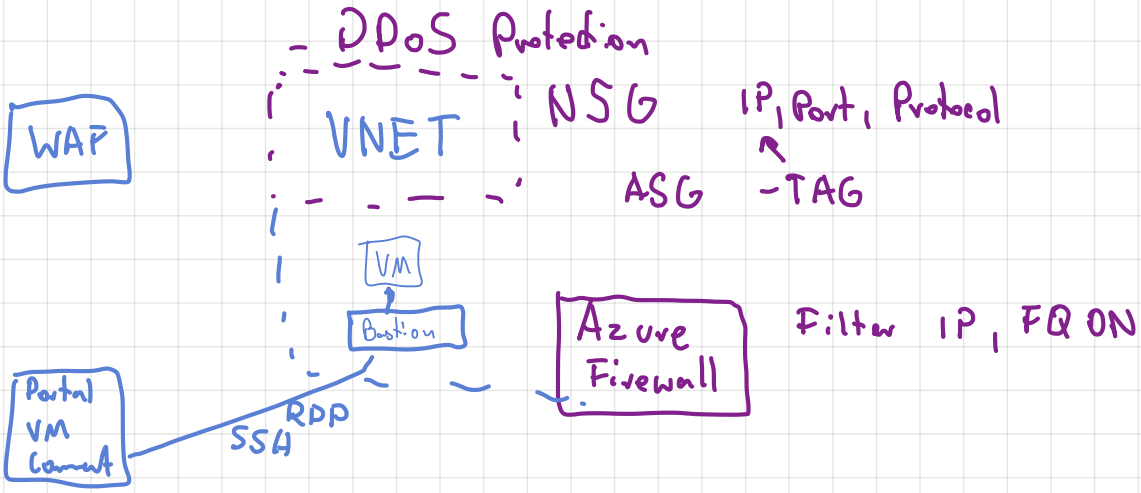
BLUEPRINT

RG
RBAC
Policy
ARM Templates

- Don't lock
- Don't Delete
- read only

ARM
JSON

Network + Data



Azure Security Center

Secure Score

⇐ Compliance

⇐ Protection

Sentinel

M365

Defender

- Identity – AD Domain Controllers
- Endpoint
- CAS (Cloud App Security) - Discovery, Control
- Office 365

Classify – retention
Protect
encrypt -> DLP
Data

M365 Security Center

- Secure Score

Device
Identity – APP

INTUNE
- Policy
- Health

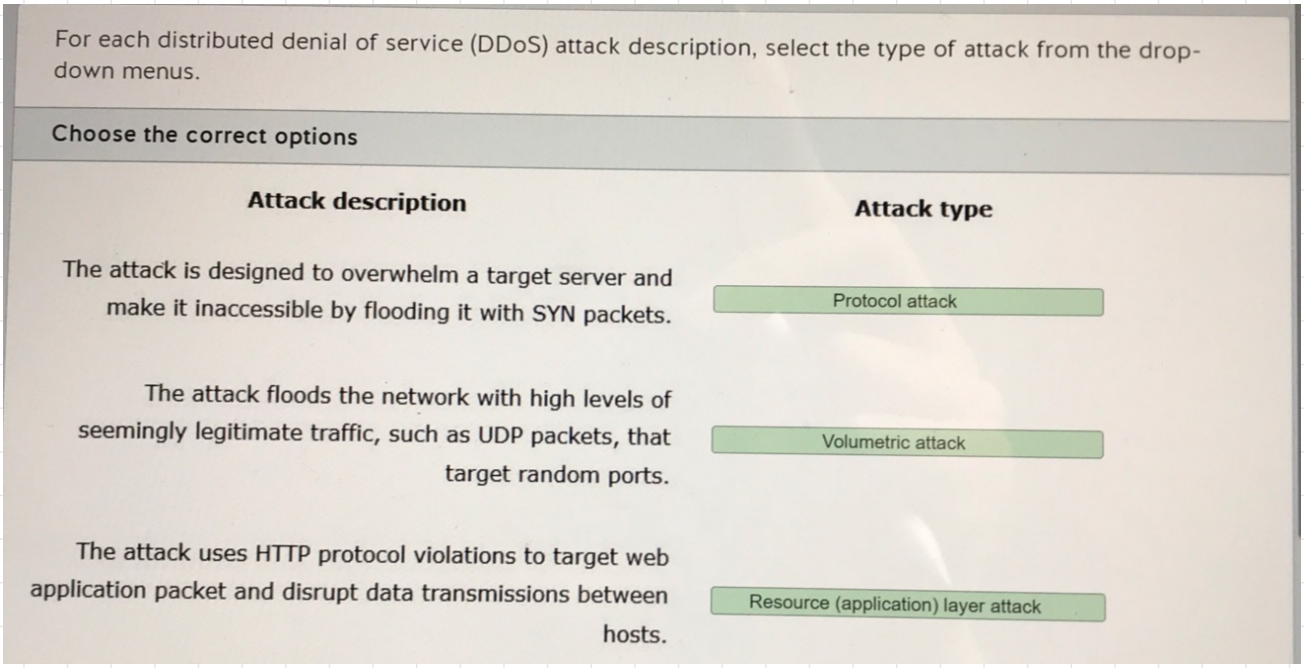
Win, Mac, Android, iOS

device
- MDM - enroll device — Corp. assets
- MAM — app policy — my
  ↑ Application

Exam Questions

Zero Trust Security Model enforces least privileged access. Data and Solutions are protected by limiting user access with Just in Time and Just Enough Access policies.

Defense in Depth is based on a layered security model that discourages attacks and slows advance of an attack.



For each distributed denial of service (DDoS) attack description, select the type of attack from the drop-down menus.

Choose the correct options

Attack description	Attack type
The attack is designed to overwhelm a target server and make it inaccessible by flooding it with SYN packets.	Protocol attack
The attack floods the network with high levels of seemingly legitimate traffic, such as UDP packets, that target random ports.	Volumetric attack
The attack uses HTTP protocol violations to target web application packet and disrupt data transmissions between hosts.	Resource (application) layer attack

Azure Disk Encryption:

- requires Key Vault for key storage
- uses Bitlocker feature for volume encryption on Windows VMs

Identity attacks:

- Phishing
- Brute force - trying passwords

Federated Services:

1) Website uses authentication A
2) User authenticates with B
3) A has trust relationship with B
4) User can access website using auth. B

Hybrid Identity provides a common user identity for authentication and authorization to all resources irrespective of their location

Azure AD registered devices are private devices

Azure AD joined devices exist only in the CLOUD

Hybrid Azure AD joined devices are devices owned by the company

Azure AD MFA, PIM, conditional access -> Premium P2

PIM - Privileged Identity Management is an Azure AD service that enables management, control and monitoring of access to important organizational resources in the cloud

PAM - Privileged Access Management - helps to restrict privileged access. It does not cover cloud resources.

Azure Identity Protection:

sign-in risk
- from anonymous IP address
- atypical travel

user-risk
- leaked credentials
- password spray
- sign in from malware-linked IP

Azure Bastion: intermediate harden instance to use to connect to your target server via SSH or RDP. To give one layer of

1 n.security group to multiple virtual subnets.

1 -> many

Azure Security Benchmark: provides prescriptive best practices and recommendations to help improve the security of workloads, data, services on Azure.

Azure Security Center helps you improve your company's security posture by identifying and performing hardening tasks. It can detect and prevent threats for both cloud-based and on-premises servers and resources.

Azure Sentinel is a security information event management (SIEM) and security orchestration automated response (SOAR) solution.

the SOAR triggers action-driven automated workflows and processes to run security tasks that mitigate the issue

Sentinel is integrated with Azure Monitor Workbooks
You can use Monitor to monitor Sentinel data using templates

Azure Defender:

- advanced protection for Azure and on-prem workloads. It can be found in Az. Security Center

M365 Defender:

- unified pre and post breach enterprise defense suite that natively coordinates
  - responses: detection, prevention, investigation
  - across - endpoints, identities, email, applications

to provide integrated protection against sophis. attacks.