Zero Trust Architecture

Listen to the video below and complete the exercises:

https://www.youtube.com/watch?v=txPZa3wLIOE

Exercise 1

Mark the following statements as True (T) or False (F).

1. A traditional network setup assumes that devices and users inside the firewall are safe.
2. The goal of Zero Trust Architecture (ZTA) is to encourage organizations to move away from tracking user activity.
3. ZTA is an official standard or specification that organizations must follow precisely,
4. In a Zero Trust model, every single digital interaction is continuously validated and verified.

Exercise 2

Choose the best answer (A, B, or C) for each question according to the video.

1. What is the main danger of placing the majority of security measures only at the edge of the network?
   a) It makes ZTA too difficult to implement.
   b) It makes it extremely difficult to identify or control an intruder if they successfully breach the initial line of defense.
   c) It replaces the Firewall with a Router.

2. What is the core principle or motto of the Zero Trust model?
   a) Trust implicitly, verify later.
   b) Trust is earned, not given.
   c) Never trust, always verify.

3. According to the video, what are Firewalls designed to do?
   a) Define what a network is by interconnecting devices.
   b) Regulate the flow of network traffic between networks or hosts that have different security levels.
   c) Immediately grant access to internal devices without verification.

Exercise 3

Complete the following sentences with the exact words used in the video.

1. A network is the __________ of computing devices from computers to phones to smart devices.
2. In ZTA, the verification relies on signals to provide the __________ needed to grant __________ to a resource.
3. A Zero Trust architecture does away with any __________ trust and continuously validates it.
4. A zero trust model works on the principle of never trust, always __________.

Exercise 4

Complete the following sentences using the most appropriate cause-and-effect connector:

because - therefore - if - since

1. Zero Trust makes disruption difficult for a malicious actor ____________ every action is subject to some type of evaluation.
2. An organization places the majority of security measures at the edge of the network; _____________, an intruder is difficult to control after breaching the defense.
3. ________________ an organization successfully breaches the initial line of defense, the intruder will be difficult to identify.
4. It can be difficult to implement ZTA ______________ it is an approach to designing an architecture and not a standard specification.