ManageEngine

7 tenets of Zero Trust security approach

As per the NIST Special Publication 800-207, any Zero Trust architecture needs to adhere to the following seven tenets:

1. All data sources and computing services are considered resources.

What this means:
Be it an IoT device, a SaaS product, or a personal device—if it's within the enterprise network or can access enterprise owned data and services, it should be counted as a resource.

2. All communication is secured, regardless of network location.

What this means:
Never automatically trust a user or device based on its network location. Whether an access request comes via the enterprise network or from a non-enterprise network, it must meet the same security requirements.

3. Access to individual enterprise resources is granted on a per-session basis.

What this means:
Evaluate the requester's trustworthiness before granting access every single time. Ensure you give them the least privileges needed to complete their tasks, and that granting access to one resource doesn't automatically grant access to others.

4. Access to resources is determined by dynamic policy.

What this means:
Define your list of resources, your organization's members, and who has what level of access to which resources. Take into account contextual information like location, device state, network context, etc. and vary authentication methods based on the sensitivity of the resource being accessed. That is, the stringency of reauthentication should be proportional to sensitivity.

5. Monitor and measure the integrity and security posture of all owned and associated assets.

What this means:
Monitor and evaluate the security posture of all devices accessing your network—this includes known vulnerabilities, patch status, and other cybersecurity risks—before granting it access. Devices that are unmanaged, new to the network, or are managed but are known to have vulnerabilities should be treated differently from managed devices that are known to be secure.

6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

What this means:
Ensure you're continuously checking for threats and reassessing the trust given to users accessing your resources. Use identity and access management solutions to control access and enforce MFA for access to enterprise resources. Make sure to continuously monitor user activities, reauthenticating and reauthorizing them when needed.

7. Collect as much information as possible about the current state of assets, network infrastructure and communications, and how it is used to improve security posture.

What this means:
Collect and analyze data about device security postures, network traffic, access requests, etc., to improve your organization's security posture. This data can also provide additional context for the requirements under tenet 4.

Reference

National Institute of Standards and Technology Special Publication 800-207, Zero Trust Architecture

Learn more about Zero Trust at
manageengine.com/zerotrust