1. NIST 800-207

https://csrc.nist.gov/pubs/sp/800/207/final

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture*. https://doi.org/10.6028/nist.sp.800-207

1. **Increasing Complexity of Enterprise Infrastructures**: The paper discusses how modern enterprise infrastructures have become more complex, encompassing internal networks, remote offices, mobile individuals, and cloud services, which makes traditional perimeter-based network security insufficient.
2. **Introduction of Zero Trust (ZT) Model**: In response to the limitations of perimeter-based security, the paper introduces the "zero trust" model. This approach focuses on data and service protection and extends to all enterprise assets and subjects (including end users and non-human entities), assuming no implicit trust within the network.
3. **Principles of Zero Trust Architecture (ZTA)**: ZTA is an enterprise cybersecurity architecture based on zero trust principles, designed to prevent data breaches and limit internal lateral movement. It involves continually authenticating and authorizing each access request and minimizing resource access only to those who need it.
4. **ZT as a Set of Guiding Principles**: Zero trust is not a single architecture but a set of principles for workflow, system design, and operations, applicable to any security posture level. Transitioning to ZTA involves evaluating organizational risk and incrementally implementing zero trust principles and technology solutions.
5. **Integration with Existing Cybersecurity Policies**: For effective implementation, zero trust must be balanced with existing cybersecurity policies and practices like identity and access management, continuous monitoring, and best practices to enhance security posture.
6. **Historical Development of Zero Trust in Cybersecurity**: The concept of zero trust has evolved over time, with earlier initiatives focused on securing individual transactions and moving away from perimeter-based security models. Federal agencies have been shifting towards zero trust principles for over a decade, influenced by various programs and frameworks.
7. **Document Structure for ZT and ZTA Guidance**: The publication is structured to define zero trust and ZTA, document logical ZT components, present use cases, discuss threats specific to ZTA, and outline how ZTA principles align with existing federal agency guidance. It also provides a roadmap for organizations transitioning to a ZTA.