PERIMETER VS. ZEROTRUST COMPARISON

General Idea

Traditional perimeter security is like having a big fence around your house with one locked door to keep bad people out. It works best if you trust everyone inside and just watch the gate. But as more people started working from home or different places, and using clouds and phones, this fence system isn't enough. If someone sneaks past the gate, they can walk around inside freely and hide, making it hard to spot them. This means perimeter-only security can easily be tricked or bypassed today, as it assumes everything inside is safe, which isn't always true.

VIII. Comparative Analysis: Perimeter vs. Zero Trust

A. Security Effectiveness Comparison

1. **Threat Detection Capabilities**
   - Perimeter relies on blocking attacks at the border; if an attacker bypasses it or is internal, perimeter has limited inside visibility.
   - Zero Trust provides continuous authentication and monitoring for better system-wide visibility.
   - Zero Trust has better and more flexible threat detection since it verifies every access, not just from outside.

2. **Incident Response Efficiency**
   - It is more challenging to spot and stop incidents fast in traditional perimeter since the attacker is inside.
   - Zero Trust restricts an attacker's movement by using least-privilege access and automated response like blocking.
   - Zero Trust reduces detection and response times, allowing faster incident handling.

3. **Attack Surface Reduction Metrics**

   - In perimeter, the whole internal network is trusted, so a breach exposes more systems and data.
   - Zero Trust minimizes exposure by granting least-privilege access only for what is needed.
   - Zero Trust decreases the available attack surface by minimizing excessive access rights.

B. Operational Impact Assessment

1. User Experience Considerations

• Traditional perimeter might limit or slow access for remote users or outside the network.

• Zero Trust requires more authentication, which can seem disruptive, but adaptive methods make it smoother.

• Zero Trust provides a better balance between security and user experience for remote work.

2. Administrative Overhead Evaluation

• Managing perimeter defenses like firewall rules, VPNs, etc., can be time-consuming and complex.

• Zero Trust reduces overhead through centralized policy management and automation.

• While Zero Trust may have initial setup time, long-term maintenance is easier and more scalable.

3. Cost-Benefit Analysis

• Perimeter defenses may have lower upfront costs, but hidden maintenance and breach costs can be high.
• Zero Trust can have higher initial costs due to identity and access management solutions.
• Zero Trust, in the long run, becomes more cost-effective with fewer breaches and outdated solutions.

C. Futureproofing and Adaptability

1. Emerging Threat Landscape Readiness

• Perimeter defenses were not built for modern dynamic environments like clouds, IoT, etc.
• Zero Trust is designed to adapt to these environments by protecting assets, no matter where they are.
• Zero Trust is thus more future-proof against the evolving threat landscape.

2. Technology Evolution Compatibility

• Traditional perimeter defenses can use outdated hardware and software that don’t easily integrate.

• Zero Trust principles are compatible with new cloud, APIs, and automation technologies.
• Zero Trust helps future-proof organizations as they adopt new tech and digital strategies.

3. **Regulatory Compliance Sustainability**

• Perimeter models use many external controls and may not meet the latest regulatory monitoring standards.
• Zero Trust helps meet these compliance requirements with consistent access control and logging.
• Zero Trust is thus better suited for maintaining regulatory compliance. (NIST, GDPR, HIPPA, etc.).

MAIN PROBLEM STATEMENT OF OUR BASELINE PAPER

While Zero Trust Architecture (ZTA) has gained recognition as a prevalent approach for implementing Zero Trust principles in network security, there is currently no standardized or universally accepted method or framework for effectively deploying and managing Zero Trust across different environments such as cloud, edge, IoT, and 5G/6G networks.

This paper addresses the problem by reviewing and comparing current Zero Trust models to identify their strengths, weaknesses, and unresolved challenges, ultimately guiding future research toward more cohesive and adaptable ZTA solutions.