Secure Network Architecture Design & Risk Assessment

Acme AeroTech

Designing Secure, Segmented Network Architectures with Risk-Based Decision Making

---

Wayne Howlett
Aspiring Security Engineer

Security Engineering Portfolio
April 2026

1. Executive Summary

This project focuses on assessing and improving the network security posture of a fictional aerospace company, Acme AeroTech. The original network design lacked segmentation and proper access controls, creating multiple security risks including unrestricted lateral movement, exposure of critical systems, and weak boundary protections.

Through a structured analysis of the existing architecture, key vulnerabilities were identified and prioritized based on risk. A redesigned network architecture was then developed using segmentation, a DMZ, and controlled inter-zone communication to reduce the attack surface and improve overall resilience.

The final design demonstrates how layered security controls and architectural improvements can significantly strengthen an organization's defensive posture while supporting operational requirements.

---

2. Scenario Overview

Acme AeroTech is a mid-sized aerospace company with approximately 75 employees and a small IT team managing its infrastructure. The organization recently secured a government contract requiring stronger cybersecurity controls, but its existing network is outdated and lacks modern security practices.

The current network operates as a flat architecture, where users, servers, and IoT devices all share the same network space. Public-facing services are not properly isolated, and wireless access is directly connected to internal systems.

The goal of this project was to evaluate the risks associated with this design and develop a more secure, segmented architecture aligned with modern security principles.

---

3. Current Network Analysis

The original network design presented several critical weaknesses. A flat network structure allowed unrestricted communication between devices, meaning that any compromised system could potentially access all other systems within the environment.

From a security standpoint, this creates a high-risk scenario. If an attacker were able to compromise a user workstation, they could move laterally across the network and reach critical assets such as servers or the database without encountering meaningful barriers. Additionally, the absence of a DMZ meant that public-facing services were placed within the internal network, increasing the likelihood that external threats could directly impact sensitive systems.

Other weaknesses included:

- Lack of defined trust boundaries
- Minimal access control enforcement
- Limited visibility into network activity

These issues combined to create an environment that was both vulnerable and difficult to defend.

---

4. Vulnerability & Risk Assessment

A structured risk analysis was performed to prioritize vulnerabilities based on their potential impact.

High-risk issues include the flat network architecture, which enables unrestricted lateral movement, and the exposure of critical assets such as the database within the internal environment. These vulnerabilities could lead to full network compromise if exploited. Medium-risk issues included the presence of IoT devices on the same network as critical systems and weak segmentation between user and server environments. These conditions increase the attack surface and create additional entry points.

Lower-risk issues included the lack of centralized monitoring and logging, which limits visibility but does not directly enable compromise. Understanding these risks helped guide the design of the improved architecture.

4A. Threat Perspective Analysis

From an attacker's perspective, the original network design presented an easy path to compromise. A single successful breach, such as through a phishing attack or weak credentials, could allow an attacker to move laterally across the network with minimal resistance.

This means that low-value systems could be used as entry points to reach high-value targets, including servers and sensitive data.

In the redesigned architecture, segmentation and firewall enforcement disrupt this attack path. Systems are isolated into separate zones, and all communication is controlled through defined policies. This forces an attacker to bypass multiple layers of defense, significantly increasing the difficulty of exploitation and reducing the likelihood of widespread compromise.

---

5. Secure Architecture Design

The redesigned network architecture introduces segmentation and centralized control to address the identified risks.

A Next-Generation Firewall (NGFW) serves as the central control point, managing all traffic between network zones. The network is divided into multiple VLANs based on function and risk level.

The design includes:

- A DMZ for public-facing services
- A user network for employee workstations
- A server network for critical systems
- A dedicated IoT network for less secure devices
- Separate wireless networks for corporate and guest access

This structure ensures that systems are isolated appropriately and that communication between them is controlled and monitored.

---

6. Security Controls Implemented

The redesigned architecture incorporates multiple layers of security controls. Network segmentation using VLANs separates systems into logical groups, reducing the attack surface and limiting lateral movement. A DMZ is implemented to isolate public-facing services from internal systems.

Firewall rules enforce strict communication policies. Only required traffic is allowed between zones, and unnecessary access paths are blocked. For example, internet traffic is limited to the DMZ, and access to the database is restricted to authorized services only.

IoT devices are isolated from internal systems to prevent them from being used as an entry point for attacks. Guest wireless access is also separated to ensure it cannot interact with corporate resources.

Logging and monitoring capabilities are included to provide visibility into network activity and support future integration with SIEM tools.

6A. Design Decisions & Justification

Each design decision was made to address a specific risk.
VLAN segmentation was implemented to prevent unrestricted communication between systems and reduce the blast radius of a potential compromise. The DMZ was introduced to protect internal systems from external threats.

The database was isolated because it represents a critical asset. Restricting access ensures that only necessary systems can interact with it.

IoT devices were separated due to their typically weaker security posture. Isolating them reduces the risk of them being exploited as a pivot point into the network.

These decisions reflect a deliberate approach to security architecture rather than a simple configuration change.

---

7. Security Architecture Principles Applied

This design incorporates key security principles.

Defense in depth is achieved by layering multiple security controls, ensuring that failure of one control does not result in total compromise.

Least privilege is enforced by allowing only necessary communication between systems. Segmentation limits lateral movement, and isolation protects critical assets.

These principles collectively improve resilience and align the design with modern security practices.

---

8. Improvements & Future Enhancements

While the redesigned architecture significantly improves security, additional enhancements could further strengthen resilience.

One key improvement would be the implementation of a cloud-based backup and disaster recovery solution. This would protect against data loss scenarios such as ransomware, hardware failure, or system compromise, while providing geographic redundancy.

Additional improvements could include high availability configurations, integration with cloud or hybrid environments, and automated monitoring and incident response workflows.

---

9. Challenges & Lessons Learned

One challenge was balancing technical detail with clarity in the network diagram. As more components were added, multiple iterations were required to maintain readability while preserving accuracy.

Another challenge was translating technical analysis into a structured presentation format, ensuring that both the issues and their impact were clearly communicated.

Due to environmental constraints and limited time for recording, a text-to-speech solution was used for the presentation narration. This approach ensured that the content was delivered clearly and consistently without compromising the quality of the explanation. It also demonstrates adaptability in maintaining professional communication under constraints.

---

10. Conclusion

This project demonstrates how proper network design and segmentation can significantly improve an organization’s security posture. By identifying vulnerabilities and implementing layered controls, the redesigned architecture reduces risk, limits attack paths, and enhances resilience.

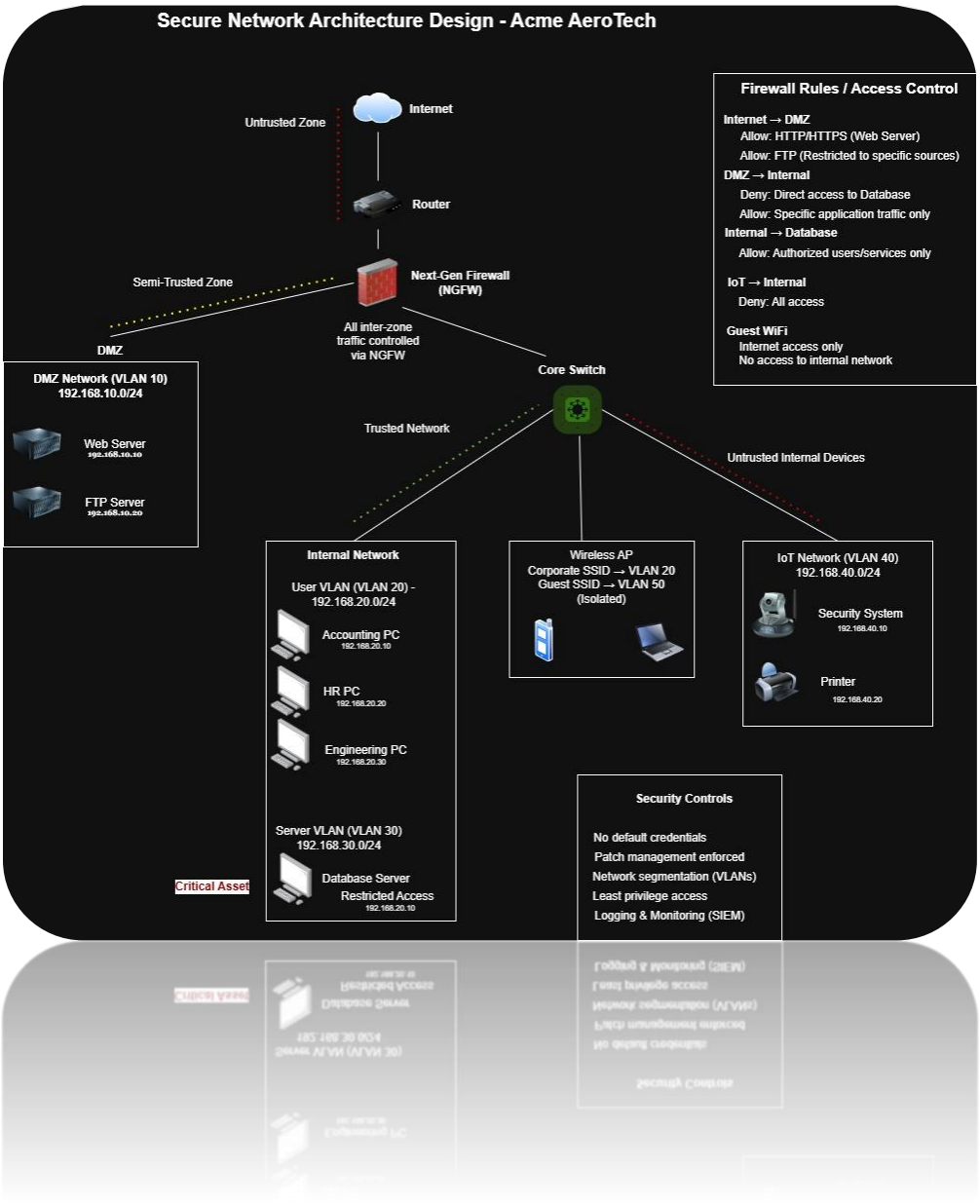
The project also highlights the importance of thoughtful design decisions, clear communication, and adaptability in real-world scenarios.

---

11. Appendix

Figure A1

Secure Network Architecture Diagram – Acme AeroTech



12. Author / Contact

Wayne Howlett
Cybersecurity Portfolio
For questions or discussion regarding this project, feel free to connect:
LinkedIn: *www.linkedin.com/in/wayne-howlett*
Email: *wayne@ihowlett.com*