**Network Segmentation By Temitayo Kayode**

**Network Segmentation and Its Contribution to Network Security**

**Network Segmentation** is the practice of dividing a larger network into smaller, isolated segments. This approach enhances security by limiting the scope of potential breaches and improving traffic management. Here’s how segmentation contributes to network security and the overall security of an organisation:

**Improved Security Posture**

**Limiting Lateral Movement:** By segmenting the network, even if an attacker gains access to one segment, they cannot easily move laterally to other parts of the network. This containment strategy significantly reduces the potential damage of a breach.

**Access Control:** Different segments can have tailored access controls, ensuring that only authorised personnel can access sensitive information. This minimises the risk of insider threats and unauthorised access.

**Enhanced Performance and Management**

**Reduced Congestion:** Segmentation helps in managing network traffic more efficiently, reducing congestion and improving overall network performance. For example, separating guest networks from internal networks ensures that high-traffic activities do not impact critical operations.

**Simplified Troubleshooting**: Isolating network segments makes it easier to identify and resolve issues, as problems can be contained within a specific segment without affecting the entire network.

**Regulatory Compliance**

**Scope Reduction:** By segmenting networks, organisations can limit the scope of systems that need to comply with regulatory requirements. This reduces the complexity and cost of compliance efforts.

**Data Protection:** Segmentation ensures that sensitive data is isolated and protected, which is crucial for meeting data protection regulations.

**Protection of Critical Assets**

**Isolating Vulnerable Devices**: Network segmentation can protect devices that are inherently less secure by isolating them from the rest of the network. For instance, medical devices in a hospital can be segmented from the main network to prevent potential attacks.

**Granular Security Policies:** Segmentation allows for the implementation of granular security policies tailored to the specific needs of each segment, enhancing the overall security posture.

**Microsegmentation**

**Granular Control:** Microsegmentation takes the concept further by applying more granular policies at the application level. This approach provides even finer control over network traffic and enhances security by isolating workloads and applications.

**Importance of an Up-to-Date Information System Security Baseline**

An up-to-date Information System Security Baseline is crucial for maintaining a robust security posture. It ensures that all security measures are current and effective against the latest threats. Here’s why it’s important:

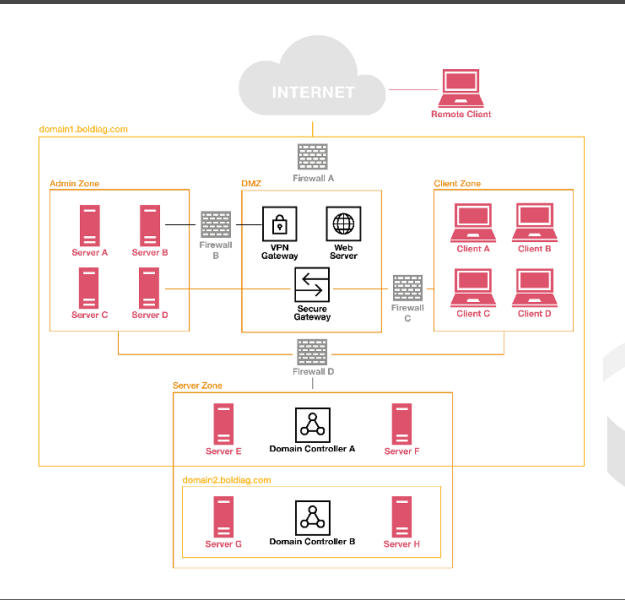
**Consistency:** Provides a consistent framework for implementing security measures across the organisation.

**Effectiveness:** Ensures that security controls are effective against emerging threats.

**Compliance:** Helps in meeting regulatory requirements by maintaining up-to-date security standards.

**Risk Management:** Facilitates better risk management by providing a clear benchmark for evaluating security practices.

**Network Segmentation Provided by Boldi AG**

****

Network Segmentation Diagram

**Domain:** A namespace that logically divides an organisation’s network objects that share the same directory.

**Admin Zone:** A special-purpose server zone, e.g., central logging, Security Information and Event Management (SIEM).

**Server Zone:** A general-purpose server zone, e.g., application servers, database servers.

**Client Zone:** A general-purpose client zone, e.g., user laptops.

**Firewall Configuration Using Whitelisting and Blacklisting**

**Firewall A:** This firewall is on the perimeter of the network, so all malware should be blacklisted. (Remote clients still need to access the network.)

**Blacklist:** Signature-Based Malware

**Firewall B:** Since this firewall is in a special-purpose server zone for administrators, it is important to whitelist administrators so that no one without admin privileges can access it.

**Whitelist:** Authorised Administrators

**Firewall C:** This firewall protects the general-purpose server zone, so it should whitelist known and trusted servers while blacklisting unauthorised access.

**Whitelist:** Trusted Servers

**Blacklist:** Unauthorised Access

**Firewall D:** This firewall is for the general-purpose client zone, so it should whitelist known and trusted clients while blacklisting potential threats.

**Whitelist:** Trusted Clients

**Blacklist:** Potential Threats