# Network Segmentation

- Network segmentation enhances security by dividing a network into isolated subnetworks, limiting the impact of attacks and aiding in IAM implementation through Access Control Lists.
- Firewall configurations can be set to blacklist suspicious IP addresses, whitelist specific IP ranges, and control communication between different network zones.
- Suggested configurations include blacklisting suspicious IPs, whitelisting IPs from DMZ and Server Zone, allowing communication between Admin Zone, Server Zone, and DMZ, and permitting communication between Admin Zone and Client Zone.
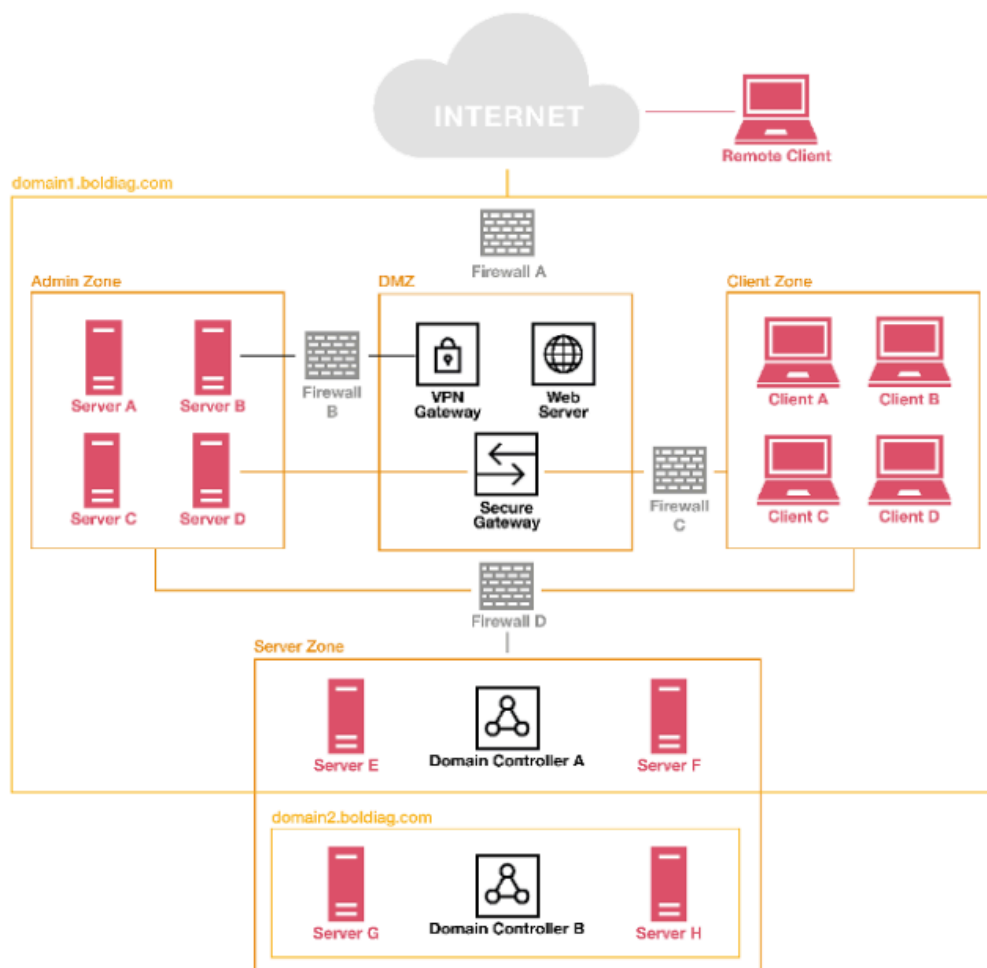
Configurations for Firewalls

Firewall A: Blacklist suspicious IP addresses, those raise flags in the systems or have attempted DDoS the company.

Firewall B: Whitelist only IP addresses of devices from VPN Gateway.

    VPN Gateway:

        Inbound: Allow VPN connections from external users.

        Outbound:

            Allow: VPN traffic to Admin Zone

            Deny: Direct Internet access from the VPN Gateway to ensure all traffic is routed through the firewall for monitoring

    Web Server:

        Outbound (to Admin Zone):

            Deny: Direct access from the web server to the Admin Zone should be denied as we need to avoid un-monitoring traffic.

Firewall C: Only allow communications from Admin Zone and Client Zone through the Secure Gateway:

    Whitelist IP addresses from the Client Zone to DMZ

    Whitelist IP addresses from the DMZ to Client Zone

Firewall D: Only allow communications between the Admin Zone, Server Zone and Server Zone.

    From Admin Zone:

        Inbound: Allow communications from Client Zone and Server Zones. IP addresses from these two zones can be whitelisted

        Outbound: Allow traffics to Server Zone and Client Zones (Depending on the usage, we may specify particular protocols)

    From Client Zone:

        Inbound: whitelist IP addresses from Admin Zone and Server Zone

        Outbound: whitelist IP addresses from Admin Zone and Server Zone

    From Server Zone:

        Inbound: whitelist IP addresses from Admin Zone and Client Zone

        Outbound: whitelist IP addresses from Admin Zone and Client Zone