Security Architecture Report

Organization: MD Multimedia
Prepared by: Cybersecurity Analyst
Date: 2/08/2025

1. Overview

This report outlines a proposed security architecture redesign following a Distributed Denial of Service (DDoS) incident that impacted internal operations for two hours. The attack exploited a misconfigured firewall that failed to limit incoming ICMP (Ping) traffic, overwhelming internal systems and causing complete service disruption.

The redesigned architecture focuses on resilience, segmentation, proactive detection, and rapid recovery in alignment with the NIST Cybersecurity Framework (CSF) domains: Identify, Protect, Detect, Respond, and Recover.

2. Current Network Architecture

2.1 Pre-Incident Overview

Before the incident, the network relied on a flat topology with limited segmentation and an unconfigured perimeter firewall. This allowed external ICMP flood traffic to traverse directly to the internal network. Critical systems such as design servers, marketing platforms, and file storage were located within the same broadcast domain, making the entire infrastructure susceptible to overload.

Key Weaknesses:

- Firewall lacked explicit deny rules for unsolicited traffic.
- No dedicated DDoS protection or upstream filtering.
- Centralized internal network without VLAN segmentation.
- Limited log correlation and alerting capability.

3. Updated Security Architecture (Post-Incident Design)

3.1 Design Principles

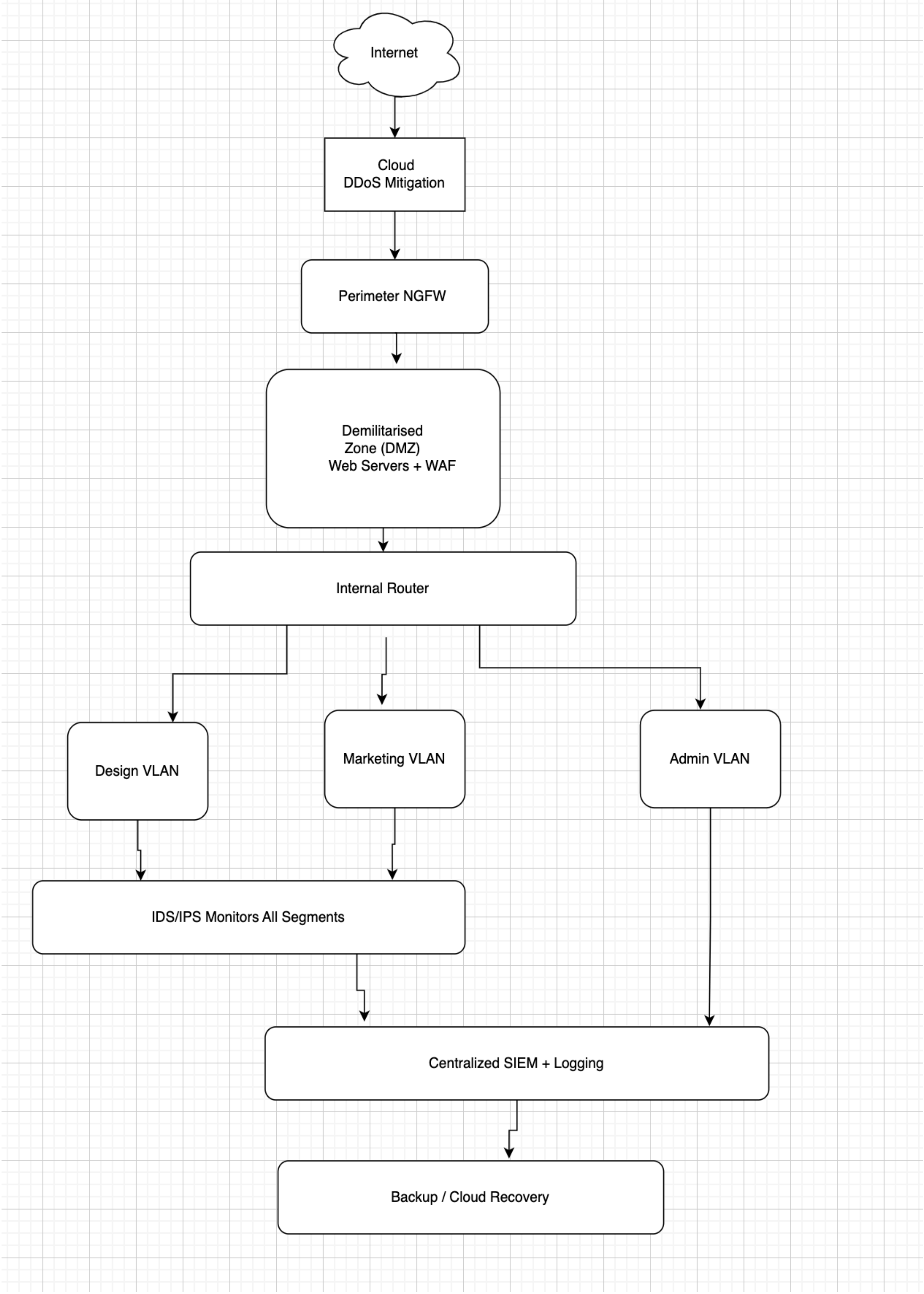
The proposed architecture emphasizes:

- **Defense in Depth:** Multiple layers of protection (firewall, IDS/IPS, WAF, MFA).
- **Zero Trust:** Verification of all users and devices before granting access.
- **Resilience:** Ability to detect, isolate, and recover from disruptions.
- **Visibility:** Centralized monitoring with clear event correlation.

3.2 Architecture Components

Component	Function	Implementation Recommendation
Next-Generation Firewall (NGFW)	Blocks unauthorized and high-volume ICMP traffic; applies rate-limiting rules.	Fully configured with default-deny policy and custom rule sets.
Network Segmentation (VLANs)	Isolates business-critical servers from user and guest networks.	Create VLANs for web servers, design workstations, and management systems.
Intrusion Detection & Prevention System (IDS/IPS)	Monitors for DDoS patterns, anomalous traffic, and signature-based threats.	Integrate with SIEM for continuous tuning and automated responses.
Web Application Firewall (WAF)	Protects web-facing applications against HTTP floods, injection, and cross-site attacks.	Deploy at the DMZ or in front of web servers.
Load Balancer / CDN	Distributes incoming requests to reduce impact from high traffic loads.	Configure with DDoS mitigation services (e.g., rate limits, geo-blocking).
Zero Trust Network Access (ZTNA)	Ensures identity verification for every access request.	Implement MFA and conditional access policies.
SIEM Platform	Aggregates logs from all network and security devices for real-time analysis.	Centralize data and configure correlation rules for ICMP anomalies.
Backup & Disaster Recovery System	Ensures rapid recovery and data integrity after outages.	Maintain encrypted, offsite, and regularly tested backups.

4. Security Architecture Diagram (Conceptual)



5. Implementation Plan

Phase	Action	Responsible Team	Timeframe
Phase 1	Configure NGFW rules to block ICMP floods and implement default-deny policies.	Network Admin	Immediate
Phase 2	Deploy VLAN segmentation and implement Zero Trust policies (MFA, device validation).	Security Team	Short Term (2–4 weeks)
Phase 3	Integrate SIEM with all logging sources and fine-tune IDS/IPS signatures.	SOC Team	Mid Term (4–6 weeks)
Phase 4	Deploy WAF and load balancer for web-facing assets.	Web Ops	Mid Term (6–8 weeks)
Phase 5	Conduct penetration testing and validate backup restoration procedures.	External Security Consultant	Long Term (8–10 weeks)

6. Monitoring and Incident Response

- **SIEM Integration:** Aggregate firewall, IDS/IPS, and server logs for pattern detection.
- **Traffic Baseline:** Establish normal ICMP and HTTP traffic volumes to detect anomalies quickly.
- **Alerting:** Configure threshold alerts for sudden bandwidth spikes or multiple failed authentications.
- **Incident Playbooks:** Maintain predefined DDoS containment playbooks for rapid isolation.
- **Communication Protocols:** Ensure stakeholders and clients receive timely updates during outages.

7. Recovery and Continuous Improvement

- Perform **post-incident reviews** after each event to evaluate containment efficiency.
- Regularly **test backups** and validate data integrity.
- Update firewall and IDS/IPS configurations quarterly.

- Conduct **annual architecture audits** aligned with NIST and ISO 27001 controls.
- Train all staff on **cyber hygiene and incident reporting** procedures.

8. Conclusion

The proposed architecture provides a **layered defense model** that strengthens protection against volumetric DDoS attacks, improves detection through centralized monitoring, and enhances resilience through segmentation and Zero Trust principles.
By implementing these measures, the organization can maintain service continuity, reduce downtime, and protect its digital assets across all departments — ensuring a secure foundation for ongoing multimedia operations.