B.Tech, 6^{th} Sem., Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

May 16, 2025

Explain the importance of resilience and recovery in security architecture

Introduction/Motivation

Explain the importance of resilience and recovery in security architecture

Dr. Laxmidhar Biswal

Objectives of this chapter

This chapter explores resilience and recovery in security architecture, covering platform diversity, multi-cloud environments, and operational continuity. It delves into capacity planning across people, technology, and infrastructure, and emphasizes testing strategies like tabletop exercises, failovers, and simulations. We also examine data protection through backup strategies, encryption, replication, and journaling. Lastly, the chapter highlights power resilience through the use of generators and uninterruptible power supplies (UPS).

Explain the importance of resilience and recovery in security architecture

Dr. Laxmidhar Biswal

High Availability Infrastructure

- Designed to resist cyberattacks and operate continuously.
- Capable of real-time detection, mitigation, and self-healing of vulnerabilities.
- Ensures secure data and uninterrupted critical operations amid evolving threats.

Network Load Balancer

- Purpose: Distributes incoming network traffic evenly across multiple servers.
- When Used: During high traffic volumes to prevent overload.
- Function: Routes each request to the least utilized or most available server.

Explain the importance of resilience and recovery in security architecture

Network Load Balancer

- Benefits:
  - Ensures server availability and efficient performance.
  - Prevents any single server from being overwhelmed.
  - Use Cases: Commonly used for web servers, video conferencing, and email systems.
- Diagram Insight
  - Traffic enters via a Virtual IP (VIP) on the frontend.
  - Load balancer directs it to one of the backend web servers in the server farm.

Explain the importance of resilience and recovery in security architecture

Network Load Balancer

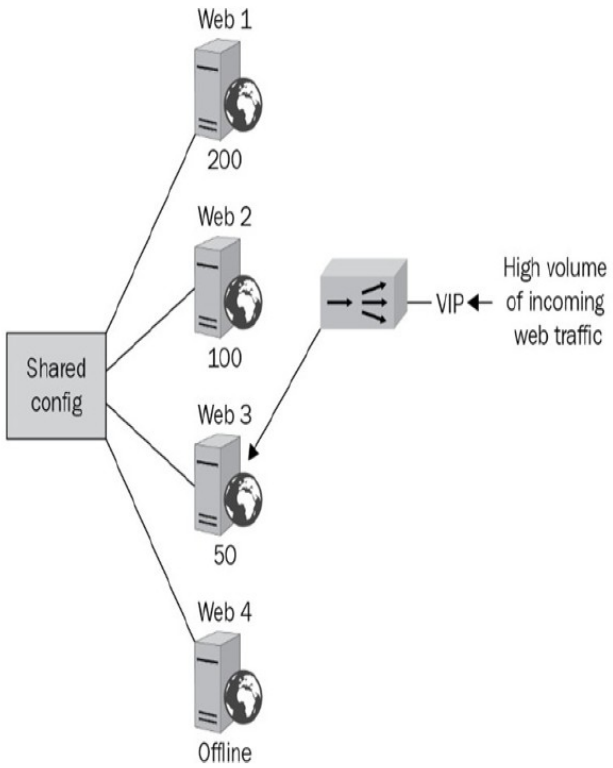

Figure: Load balancer layout

The load balancer uses various scheduling methods to

Explain the importance of resilience and recovery in security architecture

Network Load Balancer

- Least Utilized Host:
  - Monitors server health and workload.
  - Sends traffic to the least busy (online) server.
  - Optimizes resource usage when server load varies.
  - Example: Web 3 selected (50 requests); Web 4 ignored (offline).
  - Requests from the same user may go to different servers for efficiency.
- Affinity (Sticky Session)
  - Routes all requests from the same client to the same server during a session.
  - Based on IP address or session ID.
  - Ensures session persistence for consistent user experience.

Explain the importance of resilience and recovery in security architecture

Network Load Balancer

- DNS Round Robin:
  - Distributes traffic by rotating requests among servers.
  - Starts with the server having the lowest load.
  - Example: Web 1 $\rightarrow$ Web 2 $\rightarrow$ Web 3 $\rightarrow$ back to Web 1, and so on.

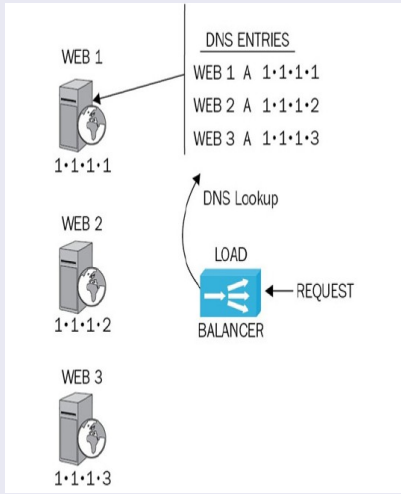

Figure: DNS round robin

Explain the importance of resilience and recovery in security architecture

Load Balancer Configuration

- Active/Active Configuration:
  - All load balancers are active and share traffic.
  - At least two load balancers required.
  - Can cache requests for better performance.
  - Users may be routed to the same load balancer on return visits.
  - Operates near full capacity — failure of one can cause performance drop.
- Active/Passive Configuration:
  - One active, others are passive (standby).
  - Passive nodes monitor the active node.
  - If active fails, a passive takes over automatically.
  - Offers higher reliability and minimal downtime.
- Active/Active: Better performance, less fault tolerance. Active/Passive: Higher reliability, better for redundancy.

Explain the importance of resilience and recovery in security architecture

Clustering

Groups multiple servers (nodes) to act as a single system for high availability.

- Active-Passive Nodes:
  - One active node handles traffic.
  - One passive node stays synchronized and takes over if active fails.
  - Both share a Virtual IP (VIP) and a quorum disk.
- Quorum Disk:
  - Shared storage holding critical config and state info.
  - Acts as neutral arbiter for cluster decisions.
- Witness Server:
  - Independent server that helps avoid split-brain scenarios.
  - Adds reliability by monitoring cluster state.

Explain the importance of resilience and recovery in security architecture

Clustering

Groups multiple servers (nodes) to act as a single system for high availability.

- Heartbeat Communication:
  - Regular status signals sent between active and passive nodes.
  - Passive node detects failure by missing heartbeats and takes over.
- Virtual IP (VIP):
  - Public interface for the cluster.
  - Enables seamless failover without service disruption.

References

 https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question ??

The End