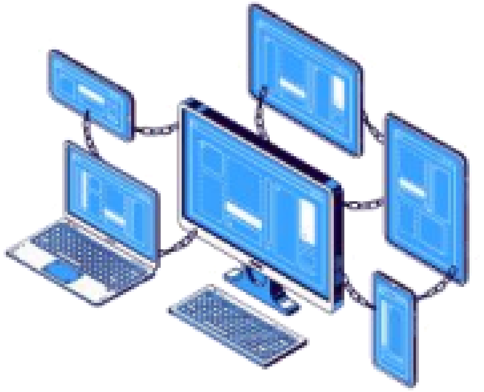
Bansilal Ramnath Agarwal Charitable Trust’s

Vishwakarma Institute of Technology, Pune-37

Department Of Artificial Intelligence and Data Science

COMPUTER NETWORK
Activity 5



Class: - SY BTECH

Branch: - AIDS

Batch 1- Group 4

23. Avishkar Ghodke
26. Jineshwari Bagul
40. Devang Deshpande
55. Anuj Gosavi
57. Hardik Rokde

1. Identification of types of Utilities for server

Tools that help in server management, monitoring, security and performance enhancement are known as server utilities. Based on their functioning they are grouped into multiple types:

1. **Monitoring & Performance Utilities:** Track server health, logs, and network activity.
   a. **System Resource Management:**
      - Its purpose is to track CPU, RAM, Disk & Network which is then used for performance optimization.
      - It prevents overheating, storage flaws, memory leakage & network bottleneck cases.
      - Ex: Grafana, Prometheus, Nagios, etc.

   b. **Network Monitoring:**
      - As the name suggests it deals with network traffic analysis, bandwidth usage & detects any connectivity issues.
      - It helps to identify unauthorized access to sites, unusual or slow network speeds and packet loss to help maintain consistency.
      - Ex: Wireshark, PRTG Network Monitor, etc.

   c. **Log Monitoring & Analysis:**
      - It facilitates troubleshooting and security audits by tracking & analyzing system logs.
      - Therefore it helps to detect errors, security threats & system failures.
      - Ex: Logstash, Graylog, etc.

2. **Security & Backup Utilities:**

   a. **Firewall & Intrusion Detection**
      - It acts as a wall between unauthorised access or cyber threats and the server.
      - It serves its purpose by blocking malicious IPs or any brute force attacks & also detects intrusion.
      - Ex: IPTables, Fail2Ban, etc.

   b. **Antivirus & Malware Protection**
      -

   c. **Backup & Disaster recovery**
      -

3. **Server Administration & Configuration Utilities:**
   a. **Remote Access & Management**

   b. **Configuration Management**

   c. **Database Management**

4. **Cloud Management & Virtualization Utilities:**
   a. **Virtualization & Container Management**

   b. **Container Orchestration**

   c. **Cloud Management**

5. **Application & Web Server Utilities:**
   a. **Web Server Management**

   b. **Load Balancing & Reverse Proxy**

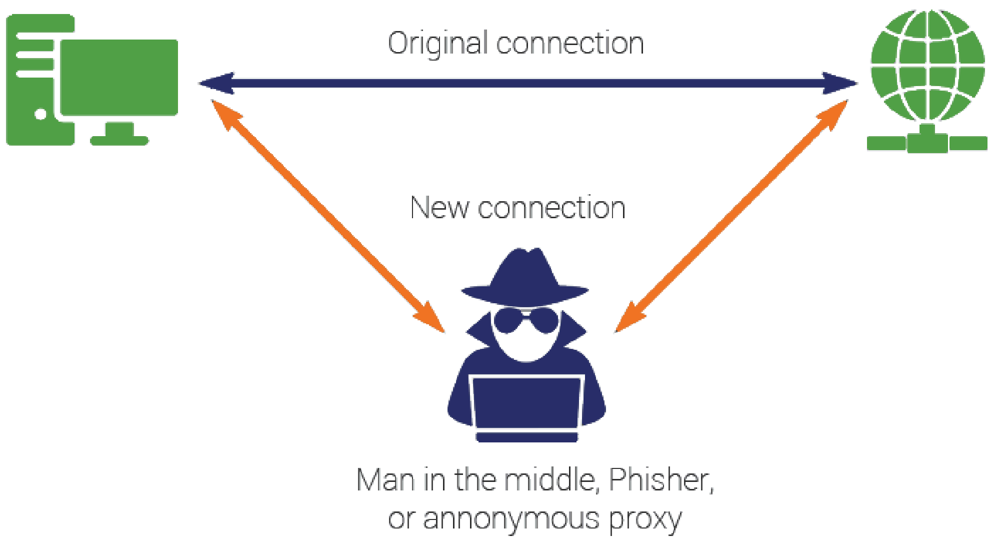
   c. **Caching & Acceleration**

2. Need of Having a Proxy Server

A proxy server is important for network security, performance improvement, and access control. It can act as an intermediary between servers and clients, offering protection from cyber attacks.

1. Protection from Man-in-the-Middle (MITM) Attacks

A MITM attack occurs when an attacker intercepts and alters communications between two parties surreptitiously, resulting in data theft and unauthorized access.



How a Proxy Avoids MITM Attacks:

Encryption & SSL Termination – Ensures data is encrypted prior to transmission, and hackers cannot intercept.

Traffic Filtering – Prevents malicious requests and unauthorized access.

Secure Gateway – Guards clients by hiding their actual IP addresses.

Authentication Control – Allows only valid users to enter the network.

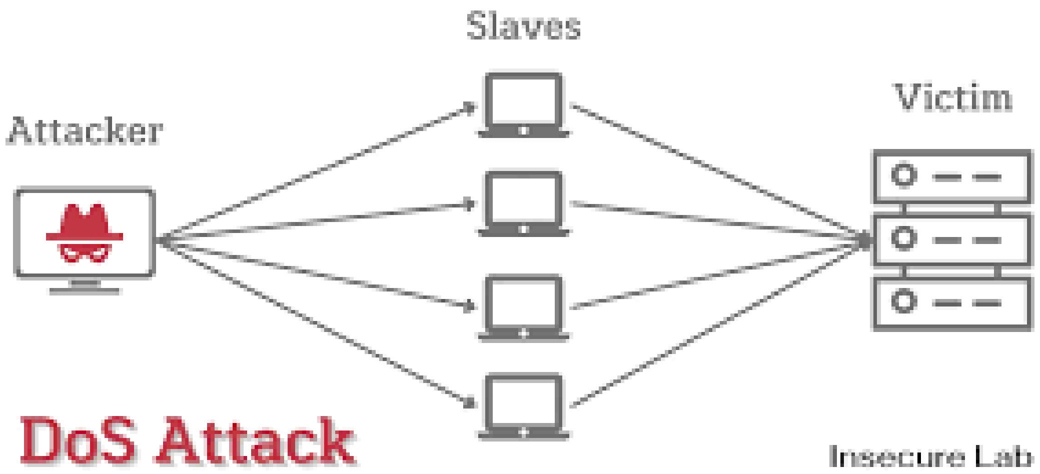
Example:

Without proxy: A hacker intercepts a bank login request on public Wi-Fi and steals credentials.

With a proxy: The request is encrypted, interception is avoided, and user information is secured.

2. Defense Against Denial of Service (DoS) Attacks

A DoS attack overwhelms a server with excessive requests, rendering it slow or totally unresponsive to legitimate users.



How a Proxy Mitigates DoS Attacks:

Traffic Filtering & Rate Limiting – Detects abnormal traffic patterns and blocks spurious requests.

Load Balancing – Spreads traffic across multiple servers to avoid overloading.

IP Blocking & Access Control – Blocks malicious IP addresses and detects them.

Caching Mechanism – Returns cached content to minimize unnecessary server requests.

Example:

Without a proxy: A DDoS attack makes millions of spam requests, taking down a website.

With a proxy: A reverse proxy (e.g., Cloudflare, Nginx) blocks bot traffic and directs valid traffic, making the website available.

3. <u>Properties of proxy server</u>

1.**Intermediary Function :-**

- Acts as a gateway between users and the internet
- Receives requests from clients and forwards them to target servers
- Returns responses from servers back to clients
- Can modify requests and responses as needed

2. **IP Address Masking :-**

- Hides the client's original IP address from destination servers
- Presents its own IP address instead of the client's
- Provides anonymity and privacy for users
- Can make it appear that traffic is coming from a different geographic location

3. **Caching Capabilities :-**

- Stores copies of frequently requested resources locally
- Serves cached content to subsequent requests when possible
- Reduces bandwidth usage and server load
- Improves response times for cached content

4. **Access Control :-**

- Can restrict access to certain websites or services
- Implements content filtering policies
- Enforces authentication requirements
- Manages user permissions and access rights

5. **Load Balancing :-**

- Distributes incoming requests across multiple servers
- Prevents server overload
- Improves overall system performance
- Provides failover capabilities

6. **Security Features :-**

- Filters malicious traffic and content
- Provides protection against DDoS attacks
- Scans for malware and viruses
- Encrypts communication when configured as HTTPS proxy

7. **Protocol Support :-**

- HTTP/HTTPS proxy for web traffic
- SOCKS proxy for general TCP/UDP traffic
- FTP proxy for file transfers
- Application-specific proxies for various protocols

8. **Monitoring and Logging :-**

- Records traffic patterns and user activity
- Generates access logs and usage statistics
- Enables network administration and troubleshooting
- Supports compliance requirements

9. Performance Optimization :-

- Compression of content
- Connection pooling
- Header manipulation
- Request/response optimization

10. Network Architecture Integration :-

- Can be deployed as forward or reverse proxy
- Supports various network topologies
- Integrates with firewalls and other security systems
- Can be chained with other proxies

11. Configuration Options :-

- Customizable routing rules
- Flexible authentication methods
- Bandwidth throttling capabilities
- Quality of Service (QoS) settings

Configuration of a proxy server

Configuring a proxy server involves setting it up to manage requests between clients and the internet. Here's an overview of the key steps in the configuration process:

1. **Install Proxy Software**: Choose appropriate proxy software based on the use case. Popular options include:
    - **Squid** (for caching and forwarding HTTP/HTTPS requests)
    - **Nginx** (for reverse proxying and load balancing)
2. **Basic Configuration**:
    - **Set Ports**: Define the port the proxy will listen on (e.g., port 3128 for Squid).
    - **Access Control**: Configure which devices or IP addresses are allowed to connect. For Squid, this is done using ACLs (Access Control Lists).

    - **Caching**: Set the cache directory and size for improved performance (in Squid, this is done via `cache_dir` settings).
3. **Authentication**: Many proxies require authentication to control access. This can be implemented using basic authentication or integrating with enterprise systems like LDAP.
4. **Security and Filtering**:
    - **Encryption**: Secure connections (especially for reverse proxies) using SSL/TLS encryption.
    - **Content Filtering**: Block or allow specific types of content based on the network's policies (e.g., blocking websites).
5. **Testing**: After configuration, test the proxy by configuring a client device (e.g., a browser) to use the proxy server. Monitor logs to ensure everything is working as expected.

In summary, configuring a proxy server involves installing software, defining access and cache rules, implementing security measures, and testing functionality to ensure smooth operation.

Challenges and Benefits of a Proxy Server

BENEFITS

- Proxy servers ensure that internet access is in control.
- They also ensure privacy because proxy servers mask your real time IP address and other personal details to secure the information that is personal and private to us
- Proxy server ensures that speed of bandwidth is fast. Proxies use to cache the websites or save the newest version of frequently visited websites, instead of resending the site each time anybody accesses it.
- Strong security is provided by the proxy servers servers

DISADVANTAGES OF PROXY SERVERS

- Tracking: The data in proxies can save internal details. If no one from external sources scoops up them this wont be an issue however the issue can originate with the proxy itself. Proxy must only be purchased by someone who has a lot of knowledge about it.
- Security issues: Proxy servers help in keeping info secretive. However their capability of encryption is slightly weak. Several proxies have data encryption ability with the support of secure socket layers. It is not enough to stop the attacks nowadays specifically from the SSL extraction attempts. Data therefore will be very less secure when SSL encryption is applied.

- Proxy servers can be expensive

- Proxy servers may not be compatible all times.

- Proxy servers may be difficult to configure