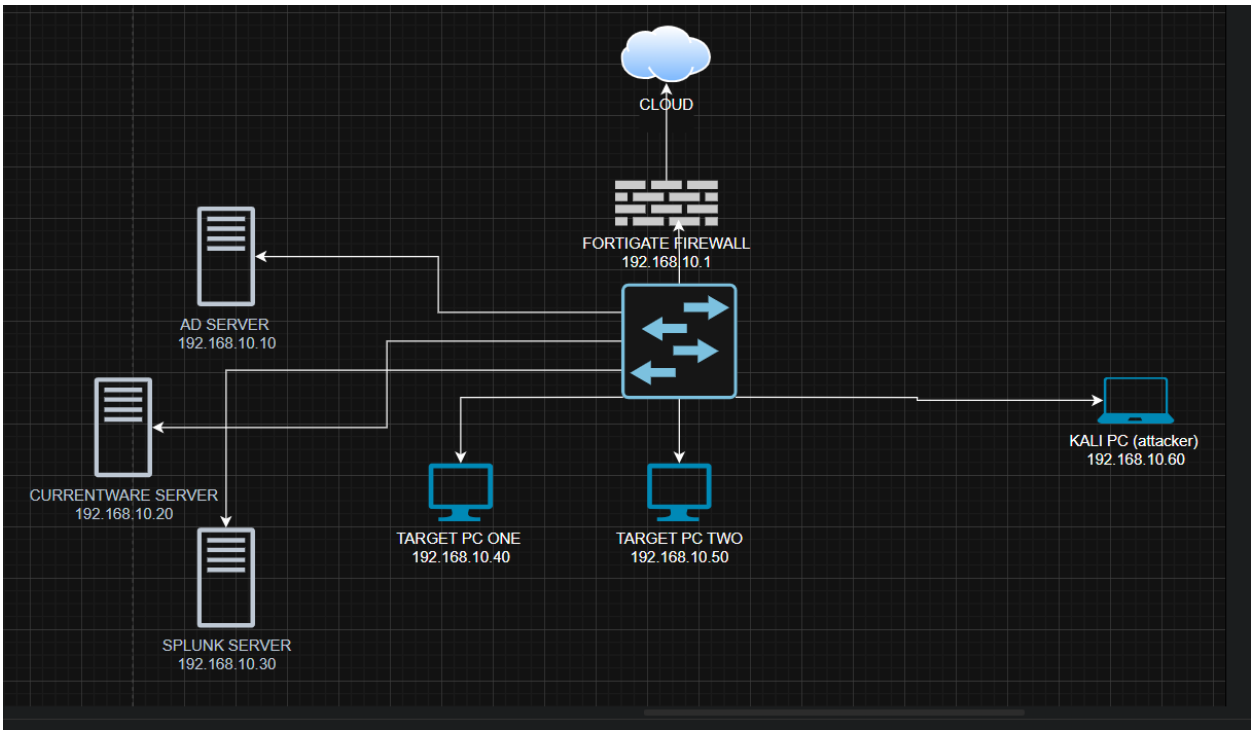
Network Architecture and Security Assessment

Project overview



Software: Draw.io

This document provides an in-depth explanation of the network architecture diagram submitted for analysis. The diagram represents a simplified network setup, including servers, client devices, a firewall, and an external cloud connection. The purpose of this document is to outline the components, their interconnections, IP addressing scheme, and potential security considerations, with a focus on the role of the Kali PC (attacker) as indicated.

1. Network Architecture Description

The network diagram illustrates a local area network (LAN) protected by a FortiGate Firewall, with connectivity to an external cloud service. The key components and their relationships are as follows:

- **FortiGate Firewall (192.168.10.1)**
    - Acts as the central gateway and security device, managing traffic between the internal LAN and the external cloud.

    - IP Address: 192.168.10.1 (likely the default gateway for the internal network).
    - The firewall is depicted with bidirectional arrows, indicating it facilitates both incoming and outgoing traffic.
- **Cloud**
    - Represents an external cloud service or the internet, connected to the FortiGate Firewall.
    - This connection suggests the network supports cloud-based applications or services.
- **Internal Servers**
    - **AD Server (192.168.10.10)**
        - Likely an Active Directory server, managing user authentication and network policies.
        - Connected directly to the firewall, indicating its critical role in the network.
    - **Currentware Server (192.168.10.20)**
        - Possibly a server for monitoring or managing endpoint security and employee activity (e.g., internet usage or application control).
        - Connected to the firewall, suggesting it interacts with other network devices.
    - **Splunk Server (192.168.10.30)**
        - A data analytics and monitoring server, likely used for log management and security information/event management (SIEM).
        - Connected to the firewall, indicating its role in network oversight.
- **Client Devices**
    - **Target PC One (192.168.10.40)**
        - A client workstation within the LAN, potentially a target for security testing or attacks.
    - **Target PC Two (192.168.10.50)**
        - Another client workstation, similarly, positioned as a potential target.
    - Both PCs are connected to the firewall, suggesting they operate within the same subnet and are subject to firewall rules.
- **Kali PC (Attacker) (192.168.10.60)**
    - A device running Kali Linux, a distribution commonly used for penetration testing and ethical hacking.
    - Labeled as "attacker," indicating it is likely simulating an attack or conducting a security assessment on the network.
    - Connected to the firewall, suggesting it is part of the internal network, possibly for controlled testing purposes.

2. IP Addressing Scheme

The network utilizes a private IP address range of 192.168.10.0/24, a common choice for small to medium-sized LANs. The specific IP assignments are:

- Firewall: 192.168.10.1
- AD Server: 192.168.10.10
- Currentware Server: 192.168.10.20
- Splunk Server: 192.168.10.30
- Target PC One: 192.168.10.40
- Target PC Two: 192.168.10.50
- Kali PC (Attacker): 192.168.10.60

This sequential allocation suggests a manually configured or statically assigned IP scheme, which is typical in controlled environments like test labs or small networks.

3. Network Topology and Connectivity

- The topology is a star configuration with the FortiGate Firewall at the center, connecting all internal devices to the cloud.
- All internal devices (servers and PCs) communicate through the firewall, which likely enforces security policies such as access control lists (ACLs), intrusion prevention, and traffic filtering.
- The Kali PC's position within the internal network implies it has legitimate access, possibly for authorized penetration testing or as part of a simulated attack scenario.

4. Security Considerations

Given the presence of a Kali PC labeled as "attacker," this network setup may be part of a security testing or training environment. Key considerations include:

- **Firewall Configuration**: The FortiGate Firewall is critical for protecting the network. It should be configured with strong rules to prevent unauthorized access, especially from the Kali PC if it is simulating an external threat.
- **Segmentation**: The lack of additional subnets or VLANs suggests all devices are on the same broadcast domain, increasing the risk of lateral movement if the Kali PC compromises a target.

- **Monitoring**: The Splunk Server can be leveraged to detect and respond to suspicious activity initiated by the Kali PC.
- **Target Vulnerability**: Target PC One and Target PC Two may be configured with known vulnerabilities for testing purposes, making them prime targets for the Kali PC.
- **AD Server Security**: As a central authentication server, the AD Server is a high-value target. Robust access controls and monitoring are essential to prevent compromise.

5. Potential Use Case

This network diagram likely represents a controlled environment for:

- **Penetration Testing**: The Kali PC is used to simulate attacks on Target PC One and Target PC Two to identify weaknesses.
- **Security Training**: Staff or students may use this setup to learn about network security, attack vectors, and defense mechanisms.
- **Proof of Concept**: Testing firewall rules, intrusion detection, or security software (e.g., Currentware) in a safe, isolated network.

6. Recommendations

- **Isolate the Kali PC**: If not already implemented, consider placing the Kali PC on a separate VLAN or network segment to limit its access to critical systems like the AD Server.
- **Enhance Monitoring**: Ensure the Splunk Server is configured to log and alert on unusual activity, especially from the Kali PC's IP (192.168.10.60).
- **Regular Updates**: Keep all systems, including the firewall, servers, and client PCs, updated to mitigate known vulnerabilities.
- **Access Controls**: Implement strict user access policies on the AD Server to prevent unauthorized escalation.

7. Conclusion

The network architecture depicted is a well-organized LAN with a focus on security and monitoring, as evidenced by the FortiGate Firewall, Splunk Server, and Currentware Server. The inclusion of a Kali PC as an attacker suggests an active security testing or educational scenario. Proper configuration and monitoring are essential to ensure the network remains

secure, especially given the potential vulnerabilities of the target PCs and the critical role of the AD Server.

For further details or to explore specific configurations (e.g., firewall rules or Splunk logs), please provide additional context or request an analysis of uploaded files or links.