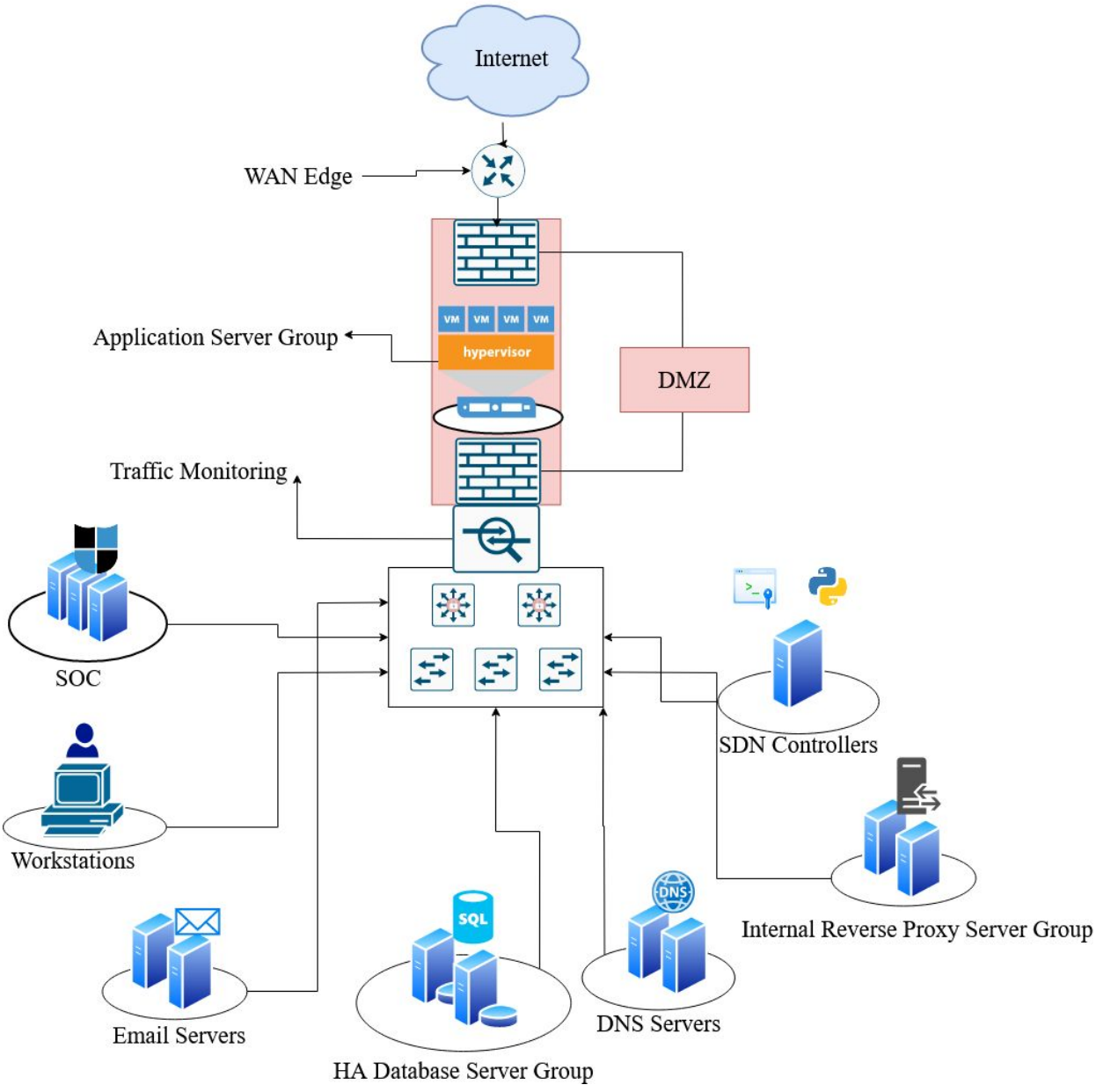
On-Site Network Design:

This design focuses on companies that have the resources to build, maintain, and secure on-site infrastructure. Please look to the cloud design and write up for an architecture that limits overhead by utilizing cloud resources.



- The web (reverse proxy) server group contains servers with different software that can accomplish the same goals, meaning that one compromised server will not allow the rest of the group to be exploited. Servers in this group will also be running processes on virtual machines rather than physical hardware, allowing each instance to be isolated from the other. If an attacker gains access to any virtual server instance in this group the confidentiality, integrity, and availability of data will not be at risk. Proper monitoring will notify engineers of any unauthorized commands, failed authentication, or suspicious data exfiltration on the servers. All traffic sent between these servers will be encrypted, so an attacker who accesses the servers will not be able to view any sensitive information. An attacker would need to compromise a server and inject their payload without triggering alerts. The isolation of the virtual instances greatly increase the complexity required for a successful attack

- If an attacker exploits a vulnerability in the application cluster and gains root access to the servers, the confidentiality, integrity, and availability of sensitive data moving in and out of the application will remain, and the internal network will still have all necessary protections to keep data safe. The virtual instances hosting the application will have limited access to other resources, and the data stored in the application database will be properly encrypted, with the keys and certificates not being held on these external servers. SSH keys that can access other machines will not be stored on these instances, and only the public keys will be viewable by the attacker, helping to limit pivoting. The application exists within a DMZ, so there are still multiple layers of defense between the attacker and internal company resources. If the attacker is running commands as root that is outside of the normal operations of that server, engineers will be notified. A snapshot of that instance will be saved for investigation, and the instance will be shut down. An attacker would need to bypass the DMZ firewall and all access controls that stop the application instances from accessing internal infrastructure, greatly increasing attack complexity.

- If a backdoor is opened on the average user workstation, an attacker will have very low access to company resources. Once this backdoor is discovered by the SOC, the workstation will be quarantined, user accounts will be reset, and any sensitive information available to this user will be considered compromised. After the workstation is investigated, attachment filters will be updated to limit this specific kind of exploit in future attacks. User training will be updated to reflect this incident. Separation of duties between engineers and security personnel will mean that if an attacker gains access to one of their workstations, they will not be able to compromise critical infrastructure without a very advanced attack or by gaining control of multiple devices.

- A DNS poisoning attack would allow a threat actor to misdirect traffic until discovered, but the data being sent will be encrypted so the confidentiality of data will not be compromised. The SOC will also be monitoring DNS operations and will react if data is being redirected to the wrong IP address. If a threat actor seeks to misdirect traffic and cause DOS, network analytics and health reports will notify engineers of the issue, and suspicious IP or MAC addresses will be blocked.

- All devices attempting to access company resources will notify security and network controls, allowing automated systems to permit or deny devices based on a series of scans. Attackers who successfully deploy a man-in-the-middle attack will have to bypass these controls. Attackers who are able to listen to network traffic will have only encrypted packets to view, and the SOC will be notified of the new presence. Forcing an attacker to try and break AES encryption to view network traffic is an acceptable risk.

- If a threat actor gains admin access to a database server, the exposure of sensitive data will be minimal. The admin user on each database may have access to delete and change data, the data itself will be encrypted with the keys not stored on the same database server. The SOC will be notified of any kind of mass data exfiltration occurs on the database server, and database contents will be

frequently backed up to limit the loss of data if the attacker decides to delete the database. A threat actor would need to gain root/admin access to other devices on the network without raising any alarms to obtain the encryption keys, break AES encryption, or brute force hashed passwords stored on the database.