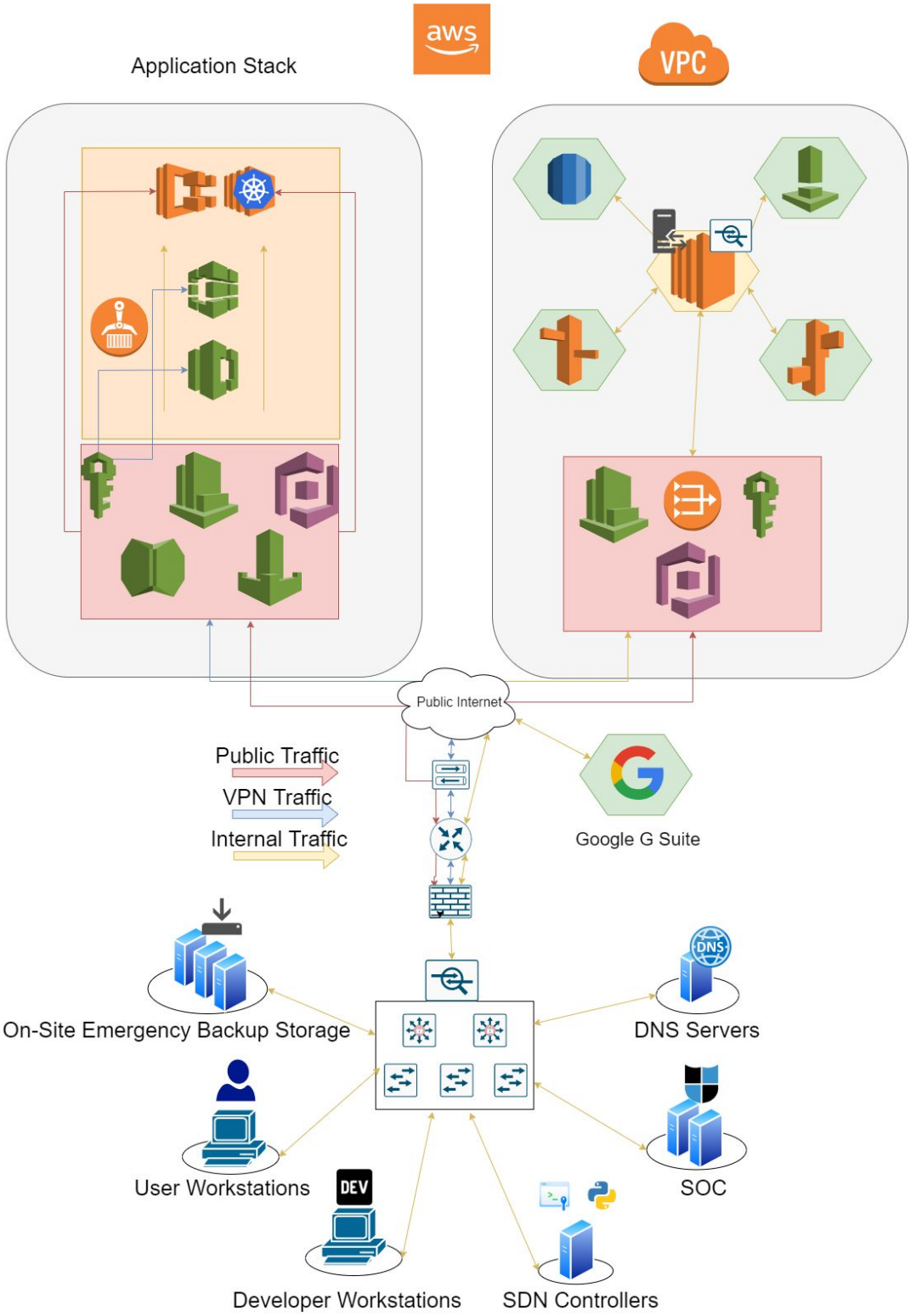
Cloud Network Design:

This design incorporates public cloud IaaS, PaaS and SaaS along with on-premise equipment.



- AWS Inspector and CloudWatch will alert engineers to unauthorized access to cloud resources. The increased isolation of systems in a cloud environment and the combination of IaaS and PaaS services means that a threat actor who has root access to a reverse proxy instance will not be able to pivot around the environment without exploiting many other vulnerabilities, drastically increasing attack complexity. Redundancy and quick response time allow engineers the ability to replace a compromised instance and make any necessary patches or changes without disrupting the flow of traffic. An attacker would need to access the server and upload their payload without raising any alarms in order to disrupt or compromise any other resources on the network. The extreme exploit complexity required to compromise the confidentiality, integrity, and availability of data in this cloud network while remaining unnoticed is an acceptable risk.

- If this company decided to use Kubernetes on Amazon EC2 instances, the company is responsible for keeping the instance patched and maintained. If a vulnerability is exploited and a threat actor gains access to the EC2 instance, a new instance could be easily spun up and the containers serving the application could be created without any downtime after the vulnerability is patched. The cloud databases and other resources will be managed by AWS, and the AWS shared responsibility model dictates that Amazon is responsible for keeping its hardware, software, and infrastructure secure. This design allows engineers more agility when responding to incidents in the cloud.

- The presence of a SOC allows internal network activity to still be monitored properly. If a backdoor goes undiscovered, the rest of the network will remain safe until the attacker attempts to pivot, escalate privileges, or inject some kind of payload. If any of these events are detected, the workstation will be quarantined and investigated. When the entry point for the backdoor is detected, the rest of the systems on the network will be scanned for this intrusion. Much of the critical infrastructure will be off-premise, so the attacker will have no way to

access them without compromising the workstation of a cloud engineer or security personnel. 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.

- Utilizing AWS Route53 allows the company to rely on Amazon to secure the hardware and software behind the service in accordance with the AWS shared responsibility model. If the internal DNS servers are compromised, a threat actor would be able to misdirect internal 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.

- Amazon RDS allows this company to defer the security of less sensitive data to Amazon while focusing on storing more sensitive data on-site. If a threat actor gains admin access to an internal 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.