3/28/2025

Pennsylvania State University
College of Information Sciences and Technology

IST 554 Graduate Network Security

Project Deliverable 3

Group - 3 : *Aniket Nimbalkar , Gokul Gopakumar, Siddharth Mishra, Sohan Ramalingaiah*

Organization Name : OpenGuardian Solutions
(This is all a hypothetical organization and their current status of where they are as a Startup booming in the IT World)

Organization Expansion (Clarification)

Just to clarify the organization expansion plan, OpenGuardian Solution employees from the offices other than the headquarters will be using BYOD devices for interns and will be provided desktops to WORK FROM HOME. This is following the recent trend of employees and according to the feedback provided by the current members of the organization.
As such, in Project Deliverable 2, Only the headquarters internal network was provided, because all the other offices will be connecting to the network using OpenVPN, and using the Virtual Private Gateway (VGW) & IAM to make sure only authorized users are able to access the resources.

Objective

The proposed network infrastructure integrates on-premises (Cisco-based network provided) and cloud (AWS-based provided) environments to connect new(expansion sites) and existing company sites (Headquarters). While this hybrid approach enhances scalability and performance, it is also accompanied by various security risks that must be addressed. This deliverable identifies likely security vulnerabilities and provides solution alternatives to mitigate them.

Potential Vulnerabilities

AWS

- The AWS architecture relies on Site-to-Site VPNs between regions and headquarters, which could be susceptible to man-in-the-middle (MITM) attacks or weak encryption.

  This communication has to be tested with its reliability by bringing in a small PenTest team that can find ways in the organization to make sure that the data being communicated is safe and secure.
  Another thing to consider during the expansion is to establish a dedicated AWS Direct Connect link. This will reduce network costs,can provide private connectivity, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections for employees as the network becomes more used by more organization folks. Also bypasses public internet risks

- Potential for the Application Load Balancers (ALBs) in AWS public subnets exposing services like SentinelMDR and ComplianceGuard to modern DDoS or brute-force attacks.

  With the infosec team, integrating AWS Shield Advanced for DDoS Protection with the network setup is crucial.
  The most direct benefit, publicly documented, is the fact that NACL rules are evaluated at the AWS network border, rather than by the hypervisors. This means that the dropped traffic doesn't impact the bandwidth available to your resources. Without shield, although your instances don't "see" the malicious DDoS traffic if it's being dropped by a NACL (or an SG, for that matter), it still consumes from the available throughput.
  As an organization, we can have an "insurance" against increased data transfer costs that are a consequence of a DDoS. This is also crucial to consider for a security organization as the costs for protecting that data and mitigations should be considered while setting up a network.

- In the architecture, we haven’t mentioned how the setup for Web Application Firewall (WAF) would be and its Rules that will be setup.

  This is needed to Block SQL injection, XSS, and malicious bot traffic by filtering, monitoring, and blocking malicious web traffic and application-layer attacks.
  WAF positioned in front of the apps can detect abnormal traffic spikes by leveraging machine learning algorithms and comparing current traffic patterns against established baselines.

- Since we are currently using Splunk SIEM to our headquarters network, I think we need to ingest AWS CloudTrail, VPC Flow Logs, and CloudWatch logs efficiently, blocking potential blind spots. Even if logs are collected, there may be no automated workflows to Detect anomalies (e.g., unusual API calls, unauthorized access). Trigger alerts or remediation actions (e.g., blocking an IP, revoking IAM permissions). This could lead to our Security teams relying on manual investigations, delaying the threat response.

We could use GuardDuty for anomaly detection and forward alerts to Splunk with the Amazon EventBridge which can Stream GuardDuty alerts to Splunk HTTP Event Collector (HEC), and the use of a Lambda function to transform and push findings to Splunk.
Now you might be thinking that Splunk already has an add-on for AWS to pull for example Cloudtrail logs, but these require much more overhead, maintenance and cost increases in data volume.

Internal Network (Cisco architecture, Headquarters)

- First thing, we should consider other ways to improve the entry for staff members other than VPN.

  This can be achieved by utilizing Zero Trust Network Access (ZTNA) based on the principle of "Never Trust, Always Verify!". ZTNA assumes that all users, devices, and network traffic—both inside and outside the Headquarters network—are potentially untrusted. In ZTNA, access to network resources is granted only after continuous verification of the user, device, and their behavior.
  The reason ZTNA is not being considered for the AWS network at this time is that AWS Verified Access is still in its early stages, and other alternatives are currently too costly. Given that we may not yet require the added complexity or expense of ZTNA, we will continue to rely on IAM, VGW, and Firewalls to ensure that only authorized users have access until a suitable cost-friendly option is discovered and tested in our dev and test environments.

- Now, considering the PC's provided to the headquarters employees, Sales Dept (Win 10) is unsupported by Microsoft (EOL) after October 10, 2025, meaning no security patches.

  As such, we have to consider upgrade all these devices to Windows 11, especially since the sales team may not be as strong with IT best practices as compared to some of the other teams in the organization. A solid plan incorporating all currently utilized tools and technologies used by the Sales team needs to be created and tested by Q2 (Quarter 2) and by Q3 (Quarter 3), all the PC's used must be the latest versions.

- Single Point of failure, Cisco firewall is a choke point—if it fails, the entire network is exposed! Adding with No HA (High Availability) pair in the internal network means downtime during updates/attacks. During the previous audit and checks for NIST and PCI-DSS, The auditor may have accepted compensating controls (e.g., quick manual recovery and DRP setup). But the current setup is just hitting the borderline. We still got certified for NIST and PCI-DSS as some QSAs (Qualified Security Assessors) are lenient on HA if other controls are strong.

  Now a solution to the HA problem is to deploy a Failover ASA Pair (Active/Standby), where two identical Cisco ASA appliances run in Active/Standby mode. The primary ASA would handle all the traffic and the secondary would monitor the primary via a failover link and would take over within very few seconds if primary fails. This would be the cost effective, immediate remedy to the issue, but ideally, with costs and overhead considerations, we can combine ASA's firewall with IPS, malware detection & SSL inspection.

- Unsecured Access to Essential Infrastructure. Server rooms containing switches, servers, and cables are only secured with basic keys and low-cost monitoring cameras (e.g. Wyze Cam), still allowing unauthorized contractor, visitor, or nefarious insider access. It provides a serious risk of rogue device insertion (e.g., stealthy Raspberry Pis or network taps) which could enable backdoor access, data intercept, or DoS attacks—too often overlooked during cybersecurity planning. The current setup again is just within the limit for PCI-DSS and NIST compliance standards.

  An easy but effective solution is to install smart keycard or PIN-code locks (e.g. Schlage Sense, August Smart Lock or Samsung EZON). This ensures that only authorized IT staff can enter (logs show who opened the closet and when).

Summarized

✅ Must-Do (Low Cost)

- AWS VPN Encryption & Reliability Testing: Engage a small PenTest team to validate Site-to-Site VPN security against MITM/weak encryption.
  Windows 10 EOL Mitigation: Upgrade Sales Dept PCs to Windows 11 by Q3 2025 (unsupported OS = high risk).
- Server Room Physical Security: Replace basic locks with smart keycard/PIN-code locks (e.g., Schlage Sense) to log access.
- Splunk Log Integration: Ingest AWS CloudTrail, VPC Flow Logs, and CloudWatch logs to reduce blind spots.
- Cisco Firewall High Availability (HA): Deploy Failover ASA Pair (Active/Standby) to eliminate single-point-of-failure risk.

💰 Worth It If Budget Allows

- AWS Direct Connect: Establish dedicated private connectivity to reduce costs, improve bandwidth, and bypass public internet risks.
- Zero Trust Network Access (ZTNA) for HQ: Replace VPNs with ZTNA for staff access ("Never Trust, Always Verify").
- Enhanced Firewall Features: Combine Cisco ASA with IPS, malware detection, and SSL inspection for deeper security.

🔒 High-Security (Compliance/Advanced Threats)

- AWS Shield Advanced + WAF : Deploy Shield for DDoS protection and WAF to block SQLi/XSS/bot traffic (machine-learning-based filtering).
- GuardDuty + Splunk Automation : Use GuardDuty for anomaly detection and forward alerts to Splunk via EventBridge/Lambda for automated remediation.
- NACL Optimization : Leverage NACL rules at AWS network border to mitigate DDoS bandwidth consumption.

🛡️ Compliance: Current setups barely meet GDPR, CCPA,PCI-DSS, NIST (auditors lenient but risky).

🤖 Automation: Reduce manual investigations via Splunk/GuardDuty integration.

⚖️💰 Cost vs. Security: Balance immediate fixes (e.g., HA pair) with long-term investments (e.g., ZTNA).