**Sample Group Project Solution**

**Project Title:** **Enhancing Cybersecurity in a Financial Institution Using Palo Alto Firewalls**  
**Industry:** **Banking & Finance**  
**Company:** **Fictional Bank (SecureBank)**  
**Software/System:** **Palo Alto Firewalls for Network Security**  
**Group Members:** 5 Students  
**Duration:** 11 Weeks

**Weekly Deliverables and Sample Solutions**

**Week 1: Team Formation & Topic Allocation**

**Deliverable:**

* Team registration and assigned topic: **Cybersecurity in Banking using Palo Alto Firewalls.**
* Initial research on **SecureBank’s IT environment.**

**Sample Solution:**  
SecureBank is a **mid-sized financial institution** facing cybersecurity challenges due to increased cyber threats. The bank uses **on-premise and cloud-based services** but lacks **robust network security** measures. Palo Alto Firewalls is identified as the best solution for **intrusion prevention and network segmentation**.

**Week 2: Research on Industry Best Practices**

**Deliverable:**

* Industry compliance research (e.g., PCI-DSS, ISO 27001, NIST).
* Best practices for **financial cybersecurity**.

**Sample Solution:**

* **Regulatory Compliance**: PCI-DSS mandates encryption of transactions, multi-factor authentication, and firewall implementation.
* **Cybersecurity Threats**: DDoS attacks, phishing, ransomware, and insider threats.
* **Best Practices**:
  + Using **Zero Trust Network Architecture (ZTNA)**.
  + Implementing **AI-powered threat detection**.
  + Regular **penetration testing** and **employee security training**.

**Week 3: IT Infrastructure & Software Analysis**

**Deliverable:**

* Document SecureBank’s **current IT network**.
* Identify weaknesses in the **existing security architecture**.

**Sample Solution:**

* **Current IT Setup:** SecureBank has **1 data center, 10 branch offices, and 2 cloud-based services (AWS & Azure)**.
* **Security Weaknesses:**
  + Outdated firewall with **static rule-based filtering**.
  + Lack of **real-time network monitoring**.
  + **Poor access control policies**, leading to insider threats.
* **Proposed Improvement:** Deployment of **Palo Alto Next-Generation Firewalls (NGFWs)** with **AI-based threat detection and intrusion prevention.**

**Week 4: Risk Assessment & Security Concerns**

**Deliverable:**

* Conduct a **risk analysis** of the bank’s cybersecurity infrastructure.
* Identify top **security vulnerabilities**.

**Sample Solution:**

| **Threat Type** | **Risk Level** | **Mitigation Strategy** |
| --- | --- | --- |
| Phishing Attacks | High | Email filtering, security training |
| Ransomware | High | Endpoint protection, backup strategies |
| DDoS Attacks | Medium | Implement **Palo Alto DDOS Protection Module** |
| Unauthorized Access | Medium | **Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC)** |

**Week 5: Ethical & Legal Considerations**

**Deliverable:**

* Identify **ethical concerns** in cybersecurity policies.
* Review **privacy laws (GDPR, CCPA, APRA regulations in Australia).**

**Sample Solution:**

* **Ethical Issues**: Over-monitoring employees, potential privacy violations.
* **Legal Compliance**:
  + **Australia’s Privacy Act (APRA Guidelines):** Banks must protect financial data and ensure **secure transactions**.
  + **GDPR**: Ensuring customer **consent** for data collection.
  + **PCI-DSS**: Mandatory **firewall protection** for financial transactions.

**Week 6: IT Project Management & Software Development Lifecycle**

**Deliverable:**

* Compare **Agile vs. Waterfall approaches** for cybersecurity implementation.
* Propose a **project plan** for firewall deployment.

**Sample Solution:**

* **Chosen Model: Agile with DevSecOps Integration**
* **Deployment Timeline:**
  + **Week 1-2**: Risk assessment, stakeholder approval.
  + **Week 3-5**: Deploy Palo Alto NGFW in the main data center.
  + **Week 6-8**: Implement security policies in branch offices.
  + **Week 9-11**: Conduct penetration testing & employee training.

**Week 7: Proposal for IT Improvements**

**Deliverable:**

* Draft **proposal document** outlining the **implementation plan** and **budget analysis**.

**Sample Solution:**

* **Solution: Deploy Palo Alto Firewalls with Threat Intelligence Cloud.**
* **Justification:**
  + AI-driven **real-time threat detection**.
  + Automated **Zero-Day attack response**.
  + Improved **network segmentation & access control**.
* **Estimated Budget:** **$300,000** for hardware, licensing, and training.
* **Expected ROI:**
  + **50% reduction in security incidents.**
  + **75% reduction in downtime.**
  + **80% compliance improvement (PCI-DSS & GDPR).**

**Week 8: Implementation Challenges & Change Management**

**Deliverable:**

* Identify challenges in **deploying a new firewall** in a financial institution.
* Propose **employee training and change management strategies**.

**Sample Solution:**

* **Challenges:**
  + Resistance from **employees unfamiliar with new security policies**.
  + Integration issues with **existing banking software**.
  + **Downtime risks** during firewall migration.
* **Change Management Strategy:**
  + **Executive buy-in and leadership training.**
  + **Step-by-step migration** to prevent downtime.
  + **Mandatory cybersecurity training** for all employees.

**Week 9: Ethical Hacking & Testing the System**

**Deliverable:**

* Conduct a **security audit** using ethical hacking techniques.
* Identify and fix vulnerabilities.

S**ample Solution:**

* **Penetration Testing Results:**
  + **3 Major vulnerabilities found** (unauthorized admin access, weak encryption, DDoS vulnerability).
  + **Fixed by deploying Palo Alto firewall rules and IDS (Intrusion Detection System).**

**Week 10: Report Compilation & Peer Review**

**Deliverable:**

* Compile the full **professional IT report**.
* Conduct **peer review and revisions.**

**Sample Solution:**

* **Professional Report Contents:**
  + **Executive Summary**
  + **Current IT State & Security Risks**
  + **Proposed Firewall Solution**
  + **Risk Mitigation Plan**
  + **Budget & ROI Analysis**
  + **Testing & Evaluation Results**
  + **Conclusion & Future Recommendations**

**Week 11: Final Presentation**

**Deliverable:**

* **Present findings** in a 10-minute professional group presentation.
* **Use PowerPoint & real-time demo of a firewall dashboard.**

**Sample Solution:**

* **Slide 1:** Introduction & Overview
* **Slide 2:** Current Cybersecurity Challenges
* **Slide 3:** Proposed Firewall Solution (Palo Alto)
* **Slide 4:** Implementation Plan & Costs
* **Slide 5:** Ethical Hacking Results
* **Slide 6:** Final Recommendations
* **Live Demo:** Showing firewall attack detection in action.

**🚀 Final Outcome**

✅ **Faster firewall deployment** (**20% improvement in cyber resilience**).  
✅ **Stronger compliance with banking security laws**.  
✅ **Better employee awareness of cybersecurity risks**.  
✅ **ROI: Estimated cost savings of $500,000 over 3 years** due to reduced security incidents.