# Enterprise Firewall Design and Selection

Introduction and Guide:

You are to do Enterprise Firewall Design research. Your research must be between 3 to 5 pages with a minimum of 700 words. When you perform your research, please start within our textbook (Chapters 3 and 4 and the slides we went over along your notes-if any). Then utilize some of the reputable sites, such as Cisco, SolarWinds, Juniper, Microsoft etc. Add your resources at the end.

Your writing and documentation must be at college level. Add a conclusion based on your opinion after answering question #6.

Objective:

Design and select a firewall solution for MC CYBR Inc., a 2,500-employee enterprise reliant on Cisco infrastructure but open to alternatives. The solution must address security, scalability, cloud integration, remote workforce needs and other options, such as IDS/IPS functionality already available or ready.

Scenario:

Company Overview:

MC CYBR Inc. is a technology services and consulting company headquartered in Germantown, MD, with five global branch offices in London, Sydney, Bangalore, Tokyo, and Paris. The company operates in a hybrid IT environment, leveraging both on-premises infrastructure and cloud-based services through AWS and Microsoft Azure. Its network infrastructure is primarily built on Cisco devices, including routers, switches, and ASA firewalls.

However, with the current growth of sophisticated attack types, the company is facing significant security and performance challenges with its current firewall setup. The aging Cisco ASA firewalls lack Next-Generation Firewall (NGFW) capabilities, leading to limitations in scalability, threat detection, and overall network security. As a result, MC CYBR Inc. is exploring alternative firewall solutions to enhance security, improve performance, and ensure seamless integration with its existing Cisco-based infrastructure. If needed, the company willing to move to a different vender.

Security Requirements:

1. **High Availability:** 24/7 operation with redundancy.
2. **Scalability:** Support for future expansion.
3. **Remote Workforce Security:** Secure access for remote employees.
4. **Data Protection:** Compliance with GDPR, PCI-DSS, HIPAA.
5. **Traffic Inspection:** Deep packet inspection (DPI) to detect threats.
6. **Cloud Integration:** Secure connectivity with AWS/Azure.

Assignment Guidelines:

NOTE: In Addition to the 7 guidelines below, you also must include “The Five Sequential Steps to Follow When Designing a Firewall” that we covered in class (also attached as Supporting Materials) and any additional criteria from our textbook. When it comes to the Cisco supporting materials, just review it for yourself as it is an entire chapter of an eBook.

1. *Firewall Selection Criteria:*
   * Key factors: throughput, security features, cost, ease of management, and compatibility with Cisco infrastructure.
2. *Types of Firewalls & Vendor Evaluation:*
   * Compare **Packet Filtering, Stateful Inspection, Proxy, NGFW, and Cloud Firewalls**.
   * Analyze Cisco Firepower vs. competitors (Palo Alto, Fortinet, Check Point) based on MC CYBR Inc.’s needs.
3. *Firewall Architecture Design:*
   * **Placement:** Perimeter, internal, cloud environments.
   * **Redundancy:** High availability setup.
   * **Network Segmentation:** DMZ, internal, external zones.
   * **Remote Access Controls:** Secure VPN and IAM.
   * **Cisco Integration:** How the new firewall fits within the existing infrastructure.
   * **Deliverable:** A conceptual network diagram.
4. *Firewall Features & Capabilities:*
   * Required features: DPI, IDS/IPS, VPN, application filtering, IAM, logging & reporting.
   * Compare how Cisco ASA/Meraki vs. Palo Alto, Fortinet, and Check Point meet these needs.
5. *Firewall Vendor & Product Evaluation:*
   * Assess **Cisco Firepower, Palo Alto NGFW, Fortinet FortiGate, Check Point NGFW**.
   * Compare each vendor’s pros/cons, costs, support, and security certifications.
6. *Cost Analysis:*
   * Estimate **initial, maintenance, licensing, and hardware/virtual appliance costs**.
   * Compare Total Cost of Ownership (TCO) across vendors.
   * **Cisco Transition Plan:** If moving away, steps to phase out Cisco firewalls.
7. *Conclusion & Recommendation:*
   * Final selection based on cost, security, and business alignment.
   * Justification for retaining or replacing Cisco infrastructure.

Deliverables:

1. **Minimum 700-word report** covering all outlined sections.
2. **Firewall architecture diagram** comparing Cisco and alternative solutions.
3. **Cost breakdown table** for firewall options.

Evaluation Criteria:

* Clear, well-structured selection and design process.
* Strong justification for chosen firewall and vendor.
* Feasibility of implementation and cost analysis.
* Compliance and risk management coverage.

Resources:

* Firewall vendor documentation (Cisco, Palo Alto, Fortinet, Check Point).
* **Industry Reports:** Such as Gartner Magic Quadrant, cybersecurity best practices.
* **Case Studies:** Cisco to non-Cisco transitions.

**Note:** The decision to move away from Cisco must be based on a comprehensive comparison of performance, security, and cost benefits.

Extra! Extra!

The following optional steps will earn you up to additional 5% of the project.

1. ***Implementation timeline*** for firewall deployment.
2. ***Compliance & Risk Management****:*
   1. Regulatory compliance (GDPR, HIPAA, PCI-DSS).
   2. Risk mitigation strategies (unauthorized access, data breaches).
3. ***Implementation Plan****:*
   1. **Timeline:** Deployment phases.
   2. **Resources:** Staff, training, contingency plans.

Questions:

1. Describe what a “firewall design” is.

2. List and describe the five steps to follow when designing an enterprise firewall.

3. If you are to perform research for your organization, to select the best Firewall available, list the requirements you would define prior to selecting the device. Review Selecting and using a Firewall – Pp-90. However, your research is not limited on software firewall alone.

4. Describe why developing and setting a network traffic baseline profile that shows network’s normal traffic patterns can be beneficial.

5. List best practices in firewall management and describe their importance. Make sure to include regulatory and/or compliance related requirements, firewall features in your list.

6. Finally, to enhance the overall security posture of your organization’s network security, list other servers, hosts, security zones such as DMZ, Honeypot/net etc., you would consider in the design process of the firewall.

**Note**: Make sure to include the security policy of the organization and how it can be used to select a firewall. Start on the following pages of our text. 77, 90, 101, 110, 113, and 115 The Juniper and Cisco sites we visited in class are vastly different from each other and the Cisco is too detailed for this research. Meaning, the Juniper is short and precise, while the Cisco is literally a large eBook (what I provided is only a chapter of the eBook). So, please do not spend too much time on the Cisco document.

The End!