William Fan

NWIT 245

June 6th 2025

Prof. Lemma

Project 1: Enterprise-Level Firewall Design and Selection Research Report

**Overview**

As digital transformation accelerates, legacy electronic appliances and perimeter-based firewalls are becoming increasingly obsolete. In light of the rising threat of ransomware and the growing complexity of cloud breaches, MC Cyber Inc. requires a firewall infrastructure that is not only reliable and secure, but also scalable and composable — capable of expanding in tandem with our evolving architecture. To stay competitive and secure, our enterprise must transition from outdated perimeter firewalls to a modern Next-Generation Firewall (NGFW) architecture.

This proposal outlines a structured approach to selecting and implementing a robust firewall infrastructure using Juniper Networks’ five-step methodology, enhanced with Gartner’s strategic framework and AWS architectural best practices. The plan emphasizes the need for 24/7 availability with built-in redundancy, secure access for remote users, deep threat detection, regulatory compliance (GDPR, HIPAA, PCI-DSS), and seamless cloud integration based on Zero Trust principles. Ultimately, MC Cyber Inc. must evaluate and select the most suitable firewall vendor to support our long-term growth and security objectives.

**What is a Firewall Design?**

A firewall design is a comprehensive and strategic plan that defines the deployment, configuration, total cost of ownership (TCO), timeline, and management of firewall devices within an enterprise environment. It should incorporate a zoning strategy—similar to a conceptual network architecture diagram—detailing internal zones, the demilitarized zone (DMZ), external zones, and intermediary segments. The design must also specify the deployment model (e.g., routed or transparent mode), traffic flow policies, access control lists (ACLs), logging and documentation standards, and compatibility with the organization’s broader cybersecurity infrastructure. The primary objective is to establish clear security boundaries and effectively mitigate both internal and external threats by addressing all critical technical and operational components.  
  
**Using Juniper’s Five-step Firewall Design Methodology**

We are going to be using Juniper’s Five-Step Firewall Design Methodology to convince you of our thought process on how to pick out our best strategic plan for our NGF.

The first part is **Define Security Requirement:** our MC CYBR Inc. has 500+ internal users at any given time across multiple headquarters and time zones, which requires multi-site connectivity and mobile access to our resources. These resources include web services, file servers, databases, and cloud applications. Since our largest branch is in Paris with 750+ employees, we define peak usage hours as 9 AM – 5 PM CEST. As the headquarters is located in Paris, we must comply with local data protection regulations, particularly concerning personal data usage. The Security Requirements include:

• GDPR (EU data protection regulation)

• HIPAA (U.S. healthcare data regulation)

• PCI-DSS (payment security standard)

• NIST 800-53 controls

• Ensuring multi-site VPN connectivity

• Securing cloud access points and hybrid-cloud traffic

• Protection against modern threats like DDoS, zero-days, and more

The second part is **Defining an overall Security Policy**, which includes the following principles:

• Only authorized internal employees and verified external partners can access corporate systems

• All inbound traffic is denied by default (implicit deny); only specific services such as HTTPS, DNS, SMTP, and RDP are whitelisted per zone

• DMZ web servers allow HTTP but strictly disallow FTP, SSH, and Telnet

• Logging is mandatory for critical rule actions and modifications

• Multi-factor authentication (MFA) is required for all remote VPN access

• Endpoints must run anti-malware and be fully patched before connecting

The third part is **Firewall Philosophy**. This is the core mindset every security professional must understand. Our firewall must support high availability, redundancy, and centralized management. To align with this philosophy, we must implement:

• Layered security architecture

• Security automation

• Zero Trust Networking

Additionally, the firewall **must implement layered security**,

• Enforce the principle of least privilege

• Support identity-based access

• Provide application-layer filtering

• Enable URL filtering

• Include IDS/IPS (Intrusion Detection/Prevention Systems)

• Perform Deep Packet Inspection (DPI)

Next, we address **Identify Permitted Communications**. Employees must be trained to understand which communications are allowed and which are restricted. The following chart is a rough mock-up of what basic network segmentation might look like:

| Source Zone | Destination Zone | Allowed Services |
| --- | --- | --- |
| Internal | DMZ | HTTPs Only(Web App.) |
| Internal | External | DNS, HTTPs |
| Remote Users | Internal | VPN, AD, Email Services |
| External | DMZ | HTTPs Only |

Access Control list examples include 1) Allow internal DNS queries to external DNS, Implicitly Deny all external inbound except TCP (Port 80) to DMZ, and 3) block traffic from unauthorized IP ranges and countries automatically

Last but not least, to protect various network zones and functions, we should identify the **Firewall Enforcement Points**

1. Edge Firewall that controls the ingress/egress operation on network perimeter
2. DMZ Firewall which segregates client-facing services from internal services
3. Cloud Firewall that secures AWS VPC access and hybrid cloud traffic
4. Internal Segregation Firewall(ISFW): prevents lateral movement between internal departments, prevents insider threats

**Budget**:

1. $300,000 - $330,000 including:

2) Firewall hardware/software

3) Centralized management console

4) Personnel training program

5) 10% vendor discount for enterprise licensing commitment

**Current Product Comparison & Analysis:**

**Cisco Mesh Hybrid Firewall:**

This product is capable of AI-powered policy enforcement and visibility, hybrid-cloud and container support, centralized control with multi-vendor compatibility and high scalability. But this product might be too far-fetched for our current plan.

**Palo Alto PA-7500 NGFW:**

The PA-7500 is a high-performance Next-Generation Firewall built for enterprise-grade environments. It delivers application-aware traffic control, real-time threat prevention powered by machine learning, Zero Trust segmentation, and deep cloud integration with AWS and Azure.

### **Why Network Baselines Matter**

Creating a network traffic baseline in a firewall strategic plan is critical for identifying abnormal patterns. It enhances the detection of anomalies, including zero-day exploits, brute-force attacks, and unexpected FTP traffic. Tools like Palo Alto’s traffic analyzer or Splunk dashboards help automate and visualize this detection process, enabling faster threat identification and response.

### **Personal Training and Awareness**

To ensure maximum ROI on our firewall investments, I propose implementing a structured training program consisting of three phases, each lasting one week, to ensure all new personnel are qualified to operate the NGFW:

* Phase 1: Vendor-provided training, such as the Palo Alto Certified Network Security Engineer (PCNSE) course, to establish foundational technical knowledge.
* Phase 2: Internal training focused on Standard Operating Procedures (SOPs) and tabletop exercises, ensuring that trainees understand all operational protocols.
* Phase 3: Simulated red-team attacks and blue-team defensive exercises, to reinforce the ability to respond effectively in real-world scenarios and operate on both offensive and defensive sides of the system.

Additionally, I recommend that all technicians obtain at least one firewall-related certification, sponsored by the company, to promote continual professional development and skill advancement.

### **Conclusion & Recommendation**

The proposed deployment of the Palo Alto PA-7500 NGFW offers the scalability, redundancy, and compliance capabilities required by our enterprise. This solution fits within our $350,000 budget and stands out due to its machine learning-based threat prevention, cloud-native architecture compatibility, and role-based access control (RBAC) features. The enterprise can expect up to a 40% improvement in threat response speed and a 25% reduction in total cost of ownership (TCO) over the next five years.