**ĐỀ THI CUỐI KỲ MÔN TẤN CÔNG MẠNG**

**ĐỀ 1**

Thời gian làm bài: 75 phút (Sinh viên không được sử dụng tài liệu)

|  |  |  |  |
| --- | --- | --- | --- |
| Số câu trả lời đúng | Điểm bài thi | | Họ tên và chữ ký của cán bộ chấm thi |
| Ghi bằng số | Ghi bằng chữ | ……………………………………….. |
|  |  |  |

Mã số thí sinh:…18520551……………

Họ và tên thí sinh……………Đoàn Văn Đắc……..…...

Lớp………NT534.M11.ANTT…...

Câu 1: Hãy trình sự khác biệt giữa Firewall truyền thống và Firewall thế hệ mới?

|  |  |  |
| --- | --- | --- |
|  | Firewall truyền thống | NG Firewall |
| Khả năng hiển thị application và kiểm soát application | Chỉ được một phần | Hiển thị chi tiết và sâu |
| CAPEX và OPEX | Cần mua vào bảo trì riêng | Giảm thiểu chi phí do được tích hợp |
| IPS | Không hỗ trợ | Có hỗ trợ |
| NAT | Có hỗ trợ | Có hỗ trợ |
| Có các dịch vụ identity | Không hỗ trợ | Có hỗ trợ |
| Traffic filtering (bất kể Port, IP và protocol) | Không hỗ trợ | Có thể filtering sâu và chi tiết vào các traffic |
| VPN | Có hỗ trợ | Có hỗ trợ |
| Mức độ nhận biết application | Nhận diện kém | Nhận diện được bất kể các application bất kể port, protocol hay các chiến thuật tránh né hoặc ssl |
| Layer làm việc | Layer 2 và 4 | Từ layer 2 đến layer 7 |
| Thông lượng và hiệu suất | Thấp hơn NGFW và giảm khi bổ sung thêm các service | Cao hơn tradition FW, không thay đổi khi thêm dịch vụ bổ sung |
| Reporting | Report chuẩn | Báo cáo chi tiết cấp độ người dùng theo cận real time, với nhiều report option như định dạng downlaod… |

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

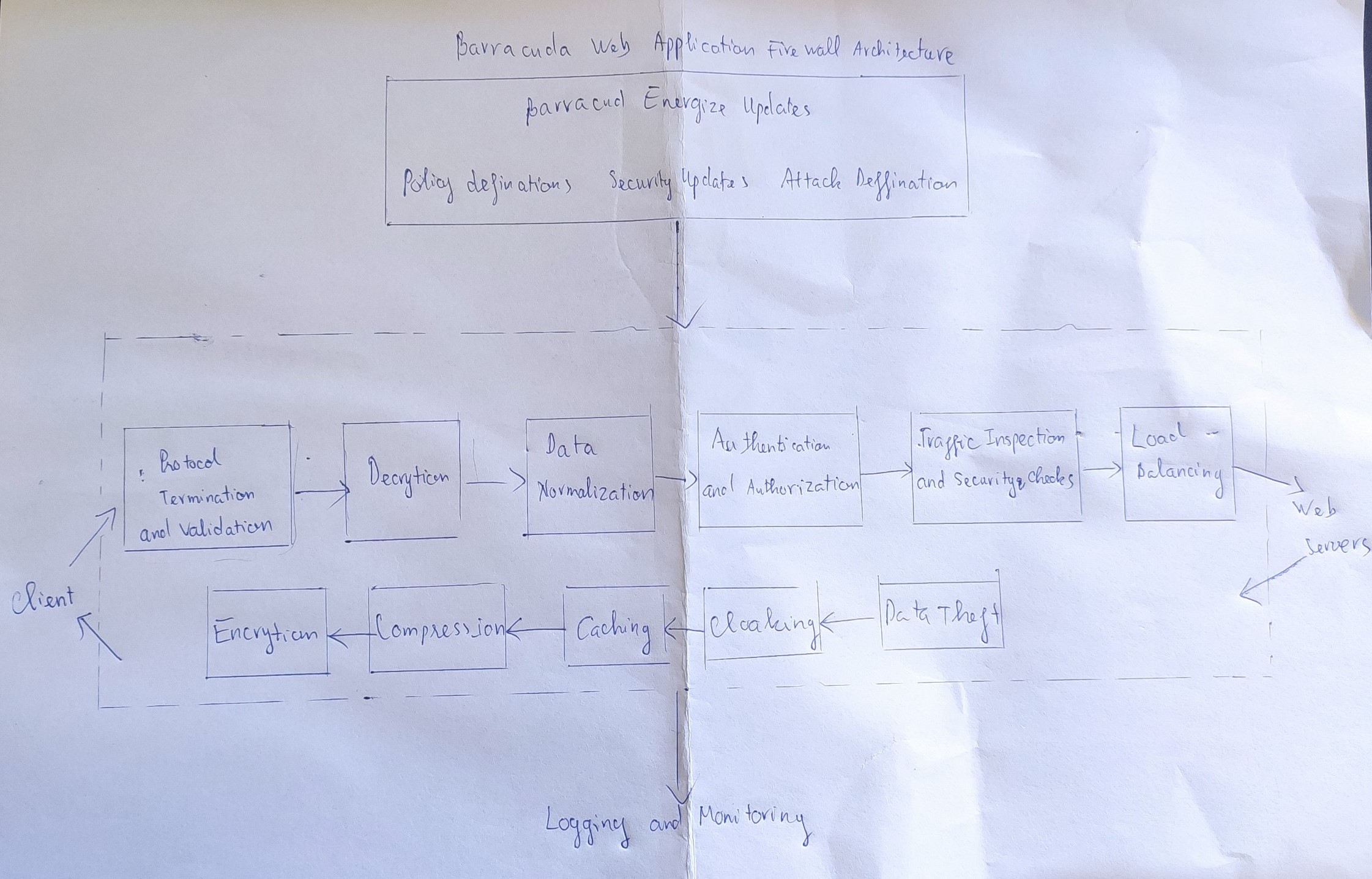
………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

Câu 2: Hãy trình bày cơ chế hoạt động của Web Application Firewall?

………………………………………………………………………………………………………

-Protocol termination and validation:Clients gửi request nhận thông tin dữ liệu từ port 80 trên protocol

-Decryption:SSL decryption nếu user sử dụng port 443

-Data Normaliztion: tách gói tin ra để xử lí

-Authen và author: kiểm tra session hợp lệ để kết nối hay phising session

-Traffic Inspection and Sec checks: kiểm tra traffic, các phần gói tin tách ra từ Data Normaliztion

-Load balancing: cân bằng tải cho server

-Data Theft: chặn các gói tin không hợp lệ với rule

-Cloaking và Caching: nếu response hợp lệ sẽ đi qua

-Compression: nén lại

-Encryption: mã hóa trước khi gửi về client

…………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

Câu 3: Trong những đồ án môn học mà các nhóm báo cáo:

* + NGINX có những tính năng gì?
  + Để có thể tăng thêm khả năng bảo mật, NGINX đã tích hợp thêm thành phần bảo mật gì? Hãy mô tả cơ thể hoạt động của NGINX khi tích hợp với thành phần bảo mật đó.

**Trả lời:**

**Tính năng NGINX:**

- Hỗ trợ mã hoá SSL và TLS

- Cấu hình linh hoạt; lưu lại nhật ký truy vấn

- Chuyển hướng lỗi 3XX-5XX

- Rewrite URL (URL rewriting) dùng regular expressions

- Hạn chế tỷ lệ đáp ứng truy vấn

- Giới hạn số kết nối đồng thời hoặc truy vấn từ 1 địa chỉ

- Khả năng nhúng mã PERL

- Hỗ trợ và tương thích với IPv6

- Hỗ trợ WebSockets

- Hỗ trợ truyền tải file FLV và MP4

**Để tăng thêm tính bảo mật, NGINX tích hợp thêm Modsecurity:**

Modsecurity hoạt động như một cỗ máy IDPS (Intrustion detection and Prevention system). Quá trình phát hiện xâm nhập nó là tiến trình Modsecurity giám sát luồng dữ liệu HTTP, HTTTPS đi tới ( Request ) hoặc đi ra ( Reponse ) khỏi Web Server và phân tích chúng để có thể tìm ra các dấu hiệu của sự việc bất thường, đó là những vi phạm hay những đe dọa sắp xảy ra vi phạm tới chính sách an ninh của web server , chính sách truy cập , hay hoạt động trái chính sách chuẩn. ………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

……………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

………………………………………………………………………………………………………

----- THE END -----