Network Topology & Security Risk Assessment Without Agent Installation

A Zero-Overhead Approach Using AWS Native Services

Solution by NTD Cybersecurity Team

Bài toán cần giải quyết

Tình hình thực tế

Đơn vị tiếp nhận một hệ thống **Legacy lớn**, doanh thu khủng, đang chạy trên AWS. Documentation đã cũ nát, đội ngũ cũ đã nghỉ việc.

Không rõ luồng dữ liệu

Không ai biết chính xác Service nào đang gọi Public Internet, Service nào gọi Private, luồng dữ liệu đi ra sao

Rủi ro bảo mật cao

Rủi ro lộ lọt dữ liệu là cực cao do không có visibility vào hệ thống

Yêu cầu giải pháp

Làm thế nào bạn có thể vẽ lại bản đồ kết nối (**Network Topology/Dependency Graph**) của toàn bộ hệ thống này và xác định các rủi ro bảo mật (**Public Exposure**) mà **KHÔNG ĐƯỢC PHÉP** cài thêm agent vào server (để tránh ảnh hưởng hiệu năng) và **KHÔNG** làm gián đoạn dịch vụ?

Tổng quan giải pháp

Painpoint

- Lập network topology **không cài agent**
- Xác định rủi ro bảo mật & lộ dữ liệu ra Internet
- Tránh **ảnh hưởng hiệu năng** trên server
- Không gián đoạn dịch vụ

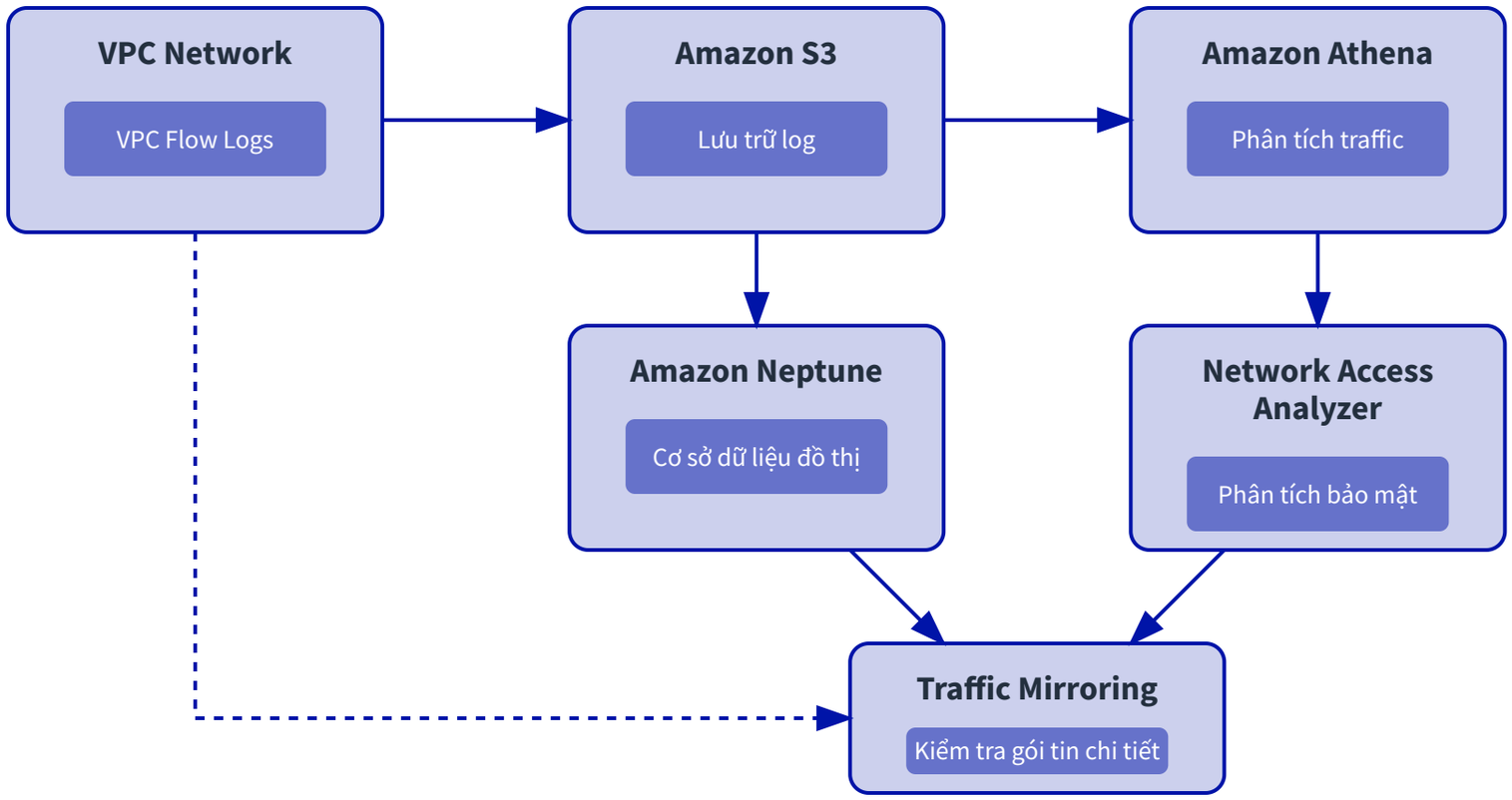
Tổng quan giải pháp

- Dịch vụ **AWS Native** - Zero Overhead
- Quan sát toàn diện mạng
- Phát hiện rủi ro bảo mật tự động

VPC Flow Logs | Neptune | Athena

Network Access Analyzer | Traffic Mirroring

Kiến trúc giải pháp



Giám sát không cần Agent

Quan sát mạng toàn diện

Phát hiện rủi ro tự động

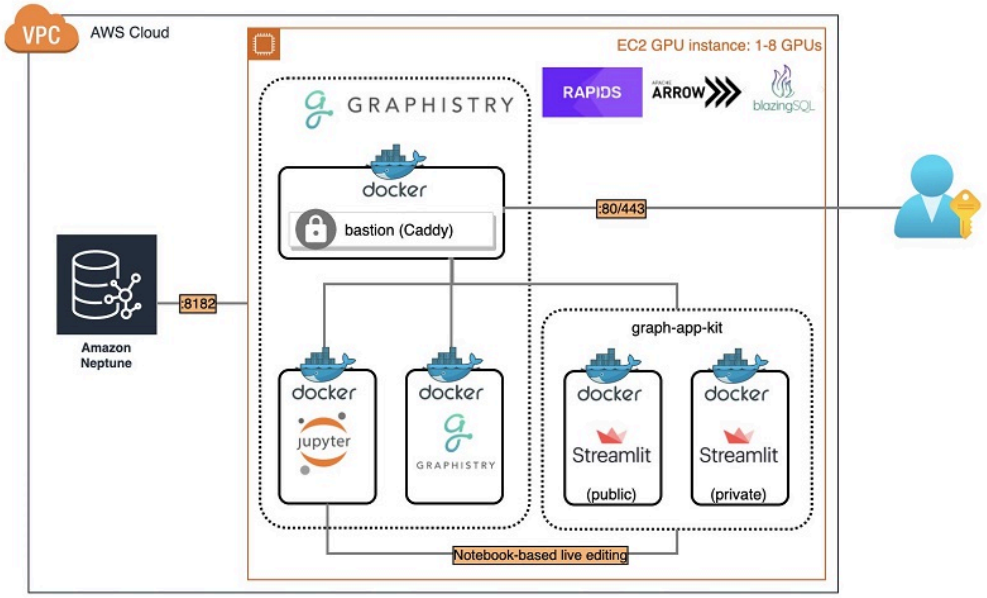
Lập bản đồ mạng: VPC Flow Logs + Amazon Neptune

Bước 1

- Sử dụng **VPC Flow Logs** làm nguồn dữ liệu
- **Lambda** phân tích log và chuyển đổi IP Source/Destination thành nodes và edges
- Lưu dữ liệu vào **Amazon Neptune** (Graph DB)
- Cho phép truy vấn như "IP A kết nối với IP B X lần qua cổng Y"

Lợi ích chính

Tự động hóa đồ thị phụ thuộc mà không cần tác động vào OS



Amazon Neptune Graph Database cho việc trực quan hóa bản đồ mạng

Phân tích traffic & Rủi ro lộ dữ liệu: VPC Flow Logs + Athena

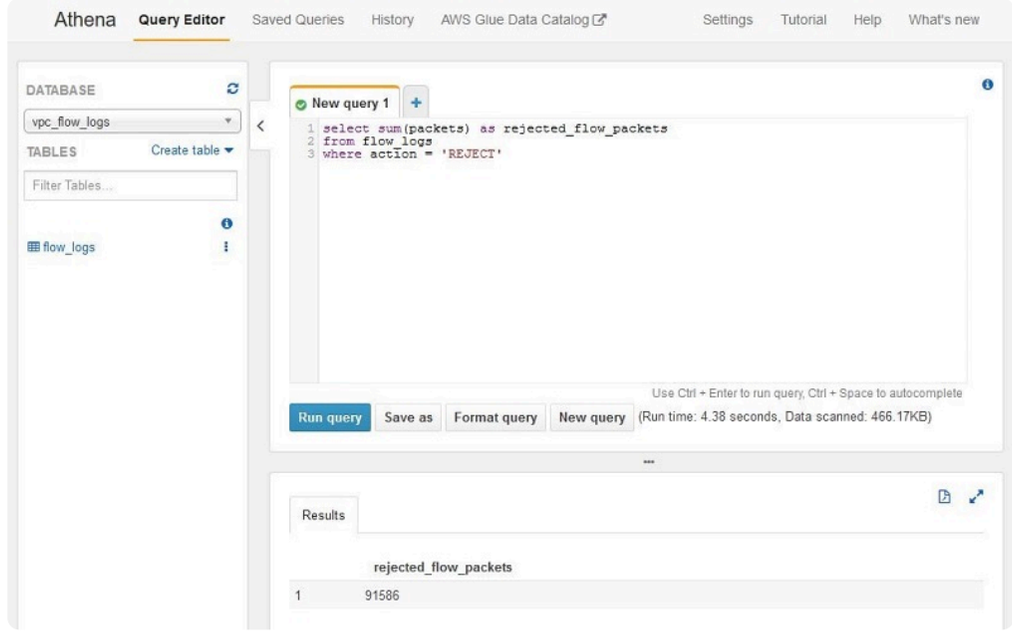
Bước 2

- Cấu hình VPC Flow Logs để gửi đến S3 ở định dạng **Parquet**
- Sử dụng **Athena với phân vùng** để tối ưu truy vấn
- Câu lệnh SQL để xác định **Top Talkers** và IP đáng ngờ
- QuickSight để trực quan hóa traffic và bản đồ nhiệt

Mẹo chuyên gia

Truy vấn các IP đích ngoài dải RFC1918 để tìm traffic Internet:

```
SELECT srcaddr, dstaddr, bytes FROM vpc_flow_logs
WHERE NOT (dstaddr LIKE '10.%' OR dstaddr LIKE
'172.16.%' OR dstaddr LIKE '192.168.%')
```



Kết quả truy vấn Athena cho phân tích traffic mạng

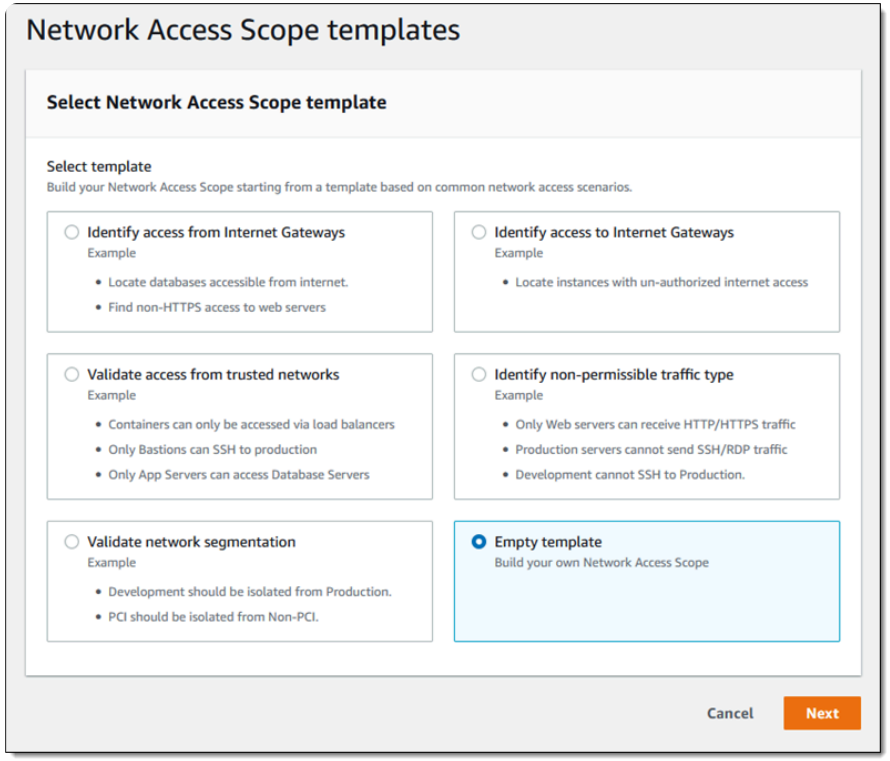
Xác định rủi ro bảo mật: Network Access Analyzer

Bước 3

- Sử dụng **Automated Reasoning** để phân tích cấu hình mạng
- Phân tích Security Groups, NACLs, Route Tables, Network Firewalls, và Gateways
- Tìm đáp án cho câu hỏi: "Có đường nào từ Internet Gateway đến Database của tôi không?"
- **Zero-overhead** - phân tích trên cấu hình Control Plane

Lợi ích chính

Xác định rủi ro tiềm ẩn trước khi chúng trở thành vấn đề



AWS Network Access Analyzer - Xác định quyền truy cập mạng không mong muốn

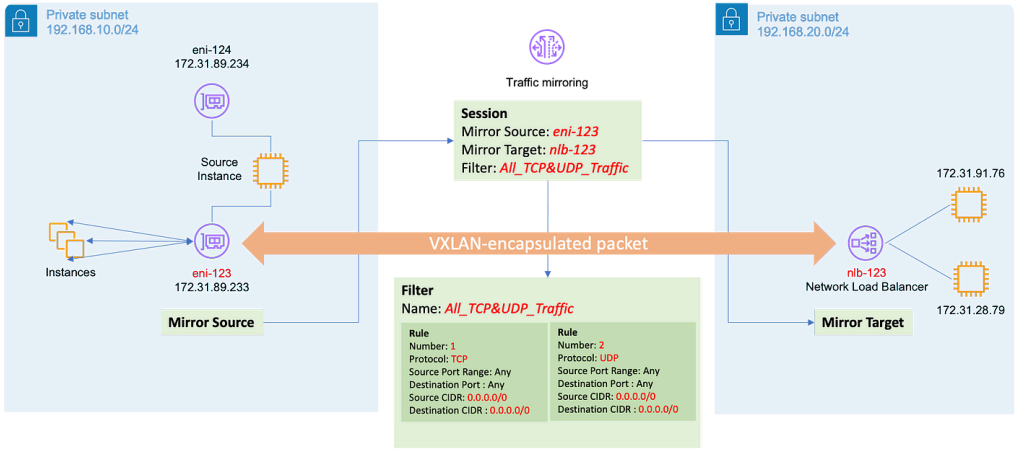
Kiểm tra gói tin chi tiết: AWS Traffic Mirroring

Bước 4

- Sao chép traffic từ ENI của server "gốc" đến **Security VPC**
- Sử dụng công cụ như **Suricata** hoặc **Zeek** để phân tích gói tin
- **Giám sát out-of-band** với độ trễ bằng không
- Cho phép kiểm tra chi tiết nội dung Layer 7

Sử dụng hiệu quả về chi phí

Chỉ kích hoạt khi cần điều tra thay vì giám sát 24/7



Kiến trúc AWS Traffic Mirroring cho việc kiểm tra gói tin chi tiết

Luồng triển khai

Lưu ý quan trọng

- **Định dạng Parquet** giảm chi phí lưu trữ và cải thiện hiệu suất truy vấn
- Lên lịch **quét định kỳ** với Network Access Analyzer
- Sử dụng **trường metadata** để lọc traffic nội bộ AWS
- Kích hoạt Traffic Mirroring **khi cần** để kiểm soát chi phí

Lợi ích & Thực hành tốt nhất

Lợi ích chính

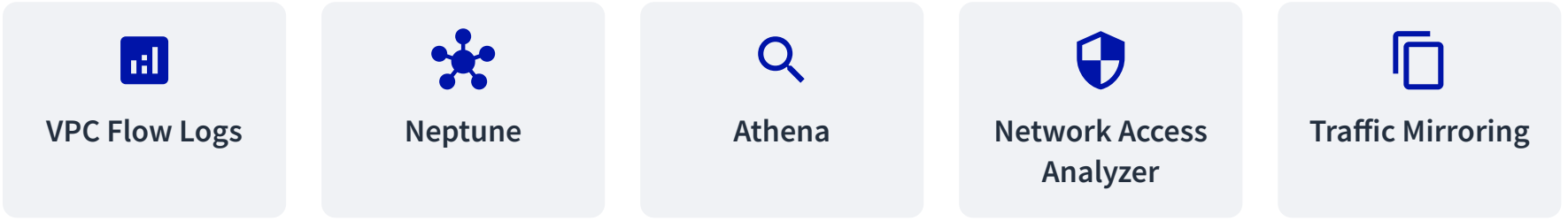
- **Zero agent overhead** - Không ảnh hưởng hiệu năng server
- **Quan sát mạng toàn diện** - Lập bản đồ mạng đầy đủ
- **Phát hiện rủi ro tự động** - Đánh giá bảo mật chủ động
- **Có khả năng mở rộng & hiệu quả về chi phí** - Chỉ trả tiền khi sử dụng

Mẹo chuyên gia

- Kích hoạt các trường Flow Log bổ sung: **pkt-src-aws-service**, traffic-path, flow-direction
- Sử dụng **phân vùng và định dạng Parquet** để tối ưu truy vấn Athena
- Kích hoạt Traffic Mirroring **chỉ khi cần** để kiểm soát chi phí
- Thường xuyên xem xét các phát hiện của Network Access Analyzer

Kết luận

Cách tiếp cận AWS-native này cung cấp việc **network topology toàn diện** và **đánh giá rủi ro bảo mật** mà không cần cài đặt agent trên server. Bằng cách tận dụng các dịch vụ AWS Native, tổ chức có thể quan sát toàn diện mạng của mình trong khi duy trì hiệu suất tối ưu và tránh gián đoạn dịch vụ.



NTD Cybersecurity Team - hung.nguyen17@ntq-solution.com.vn