Project Proposal

1. Tên đồ án:

Triển khai và đánh giá Zero Trust Architecture trên môi trường Hybrid Cloud (OpenStack + AWS) với micro-segmentation & identity-aware proxies.

2. Thông tin sinh viên:

Trương Đức Hào (22520407) – Hồng Huy Hoàng (23520517)

3. Mục tiêu của đồ án:

- Thiết lập môi trường Hybrid Cloud: Xây dựng kết nối an toàn giữa OpenStack (Private Cloud) và môi trường AWS (Public Cloud).
- Xây dựng nền tảng danh tính hợp nhất (Identity Fabric): Triển khai hệ thống quản lý danh tính trung tâm (Keycloak) và cấp phát định danh tự động, ngắn hạn cho các ứng dụng (SPIFFE/SPIRE).
- Triển khai Phân đoạn vi mô (Micro-segmentation): Sử dụng Service Mesh (Istio) để thực thi mã hóa và xác thực lẫn nhau (mTLS) giữa các dịch vụ, kết hợp với các chính sách mạng (Security Groups) để cô lập các ứng dụng, ngăn chặn sự di chuyển ngang của kẻ tấn công.
- Thực thi Chính sách dưới dạng mã (Policy-as-Code): Sử dụng Open Policy Agent (OPA) để định nghĩa và thực thi các quy tắc truy cập một cách tập trung, tự động dựa trên danh tính, vai trò và ngữ cảnh.
- Đánh giá hiệu quả An ninh: Mô phỏng các kịch bản tấn công thực tế (Tấn công leo thang đặc quyền, đánh cắp danh tính,...) để đo lường và định lượng hiệu quả của kiến trúc ZTA so với mô hình truyền thống.

4. Kế hoạch triển khai chi tiết:

Xây dựng nền tảng Hybrid Cloud:

- Hạ tầng AWS: Công cụ Terraform, viết mã Terraform để tự động tạo một Virtual Private Cloud (VPC), các Subnet (private/public), Security Groups, Internet Gateway, và một cụm Amazon EKS (Kubernetes). Kết quả: Một cụm K8s sẵn sàng hoạt động trên AWS.
- Hạ tầng OpenStack: Công cụ Ansible để tự động cài đặt và cấu hình một cụm Kubernetes trên các VM này bằng kubeadm. Kết quả: Một cụm K8s tự host trên OpenStack.
- Kết nối mạng: Công cụ: OpenSwan/StrongSwan hoặc dịch vụ AWS VPN. Triển khai: Cấu hình một kết nối Site-to-Site VPN giữa VPC trên AWS và mạng ảo trên

OpenStack. Việc này đảm bảo các ứng dụng trên hai môi trường có thể giao tiếp với nhau qua địa chỉ IP nội bộ.

Thiết lập Trục Danh tính (Identity Fabric):

- Danh tính cho Người dùng (Keycloak): Triển khai Keycloak lên cụm K8s trên AWS bằng Helm Chart. Tạo một realm mới cho đồ án, định nghĩa các OIDC clients cho ứng dụng mẫu, và thiết lập liên kết (Federation) với AWS IAM qua giao thức SAML.
- Danh tính cho Ứng dụng (SPIFFE/SPIRE): Triển khai SPIRE Server vào control plane của cả hai cụm K8s. Cài đặt SPIRE Agent dưới dạng DaemonSet để nó chạy trên mọi node. Đăng ký các workload với SPIRE Server. Khi một ứng dụng khởi động, SPIRE Agent sẽ tự động cung cấp cho nó một định danh duy nhất và một chứng chỉ X.509 ngắn hạn (SVID) để chứng minh danh tính.

Triển khai Lớp Thực thi Chính sách:

- Lớp Mạng Dịch vụ (Service Mesh - Istio): Cài đặt Istio vào cả hai cụm K8s, kích hoạt chế độ STRICT mTLS để mọi giao tiếp giữa các dịch vụ đều phải được mã hóa và xác thực hai chiều. Bật tính năng tự động tiêm (Sidecar Injection) để mọi pod ứng dụng đều có một Envoy proxy đi kèm. Envoy sẽ xử lý toàn bộ traffic vào/ra.
- Công cụ Chính sách (OPA - Open Policy Agent): Triển khai OPA Gatekeeper trên K8s để kiểm soát các tài nguyên, tích hợp OPA với Envoy proxy thông qua bộ lọc ext_authz.

Kiểm thử, Đánh giá và Tinh chỉnh:

- Xây dựng một ứng dụng microservices đơn giản (ví dụ: frontend, backend, database) và triển khai một phần trên AWS, một phần trên OpenStack để kiểm tra luồng giao tiếp xuyên cloud.
- Mô phỏng tấn công: Atomic Red Team, thí nghiệm 1: Từ một pod đã bị chiếm, dùng lệnh curl để cố gắng truy cập một dịch vụ khác không được phép. Ghi nhận lỗi từ chối từ Envoy mTLS và OPA, thí nghiệm 2: Từ một ứng dụng trên OpenStack, cố gắng gọi API của một tài nguyên trên AWS mà không có danh tính hợp lệ.
- Thu thập và phân tích: Thiết lập Prometheus để thu thập metrics về độ trễ của Envoy và OPA. Sử dụng Fluentd/Loki để thu thập logs từ Istio và OPA, tạo dashboard trên Grafana để trực quan hóa các yêu cầu bị chặn.