AN TOÀN MẠNG

**Nhóm 4:**

|  |  |
| --- | --- |
| NGUYỄN MINH HẬU | N18DCAT019 |
| TRƯƠNG VĂN NAM | N18DCAT051 |
| NGUYỄN ĐỨC QUỲNH | N18DCAT065 |
| NGUYỄN MẠNH THÌN | N18DCAT085 |
| MAI XUÂN Ý | N18DCAT105 |

1. **FIREWALL**

Top 5 Open Source firewall và các chức năng chính:

**1. Untangle Firewall :**

Spam Blocker Lite

Phishing blocker

Virus blocker

OpenVPN

Phòng chống xâm nhập

Adblocker

Restricted portal

Web monitor

**2.OPNsense Firewall:**

Forward Proxy Caching

Capital portal

Traffic Shaper

Virtual Private Network

Tính khả dụng cao và chuyển đổi dự phòng phần cứng

Support For Plugins

DNS Server DNS Forwarder

Công cụ Giám sát và Báo cáo Tích hợp

DHCP server and relay

Intrusion Exposure and Inline Prevention

**3.IPFire:**

Time server

DHCP server

Dynamic DNS

Catching name server

Intrusion Detection system

Wake-on-LAN

**4. IPCop Firewall**

VLAN available

Indirect installation to a flash device

Web interface

Stateful Firewall

**5.Shorewall**

Multiple interfaces per zone

Multiple zones per interface permitted

Different rules for proper access

Không giới hạn số lượng network interfaces

Completely customizable

Top 5 Commercial firewall và các chức năng chính:

**1.** **Check Point Next Generation Firewalls (NGFW)**

- Application and user control

- Integrated intrusion prevention

- Phát hiện phần mềm độc hại nâng cao như sandboxing và tận dụng nguồn cấp dữ liệu thông minh về mối đe dọa.

- Network address translation (NAT)

- Hỗ trợ giao thức định tuyến động

**2. Cisco Secure Firewall**

Các khả năng dựa trên phần cứng để kiểm tra lưu lượng được mã hóa trên quy mô lớn

Khả năng hiển thị và kiểm soát ứng dụng động thông qua tích hợp Khối lượng công việc bảo mật của Cisco

Tích hợp Khối lượng Công việc Bảo mật của Cisco cho phép khả năng hiển thị và thực thi chính sách cho các ứng dụng động và phân tán trên toàn mạng và khối lượng công việc.

**3. Palo Alto Networks’ PA-7000 Series**

Machine learning-enabled firewall

Highest Security Effectiveness score in the 2019 NSS Labs firewall test report with 100% of evasions blocked

Bảo mật gốc 5G được xây dựng để bảo vệ nhà cung cấp dịch vụ và sự chuyển đổi 5G của doanh nghiệp

Hỗ trợ tính khả dụng cao với các chế độ chủ động / tích cực và chủ động / thụ động

**4. Fortinet**

Bảo vệ khỏi phần mềm độc hại, khai thác và các trang web độc hại trong cả lưu lượng truy cập được mã hóa và không được mã hóa

Độ trễ cực thấp thông qua công nghệ SPU

Tích hợp với bảo mật lớp 7 và miền ảo (VDOM)

Tích hợp Zero Touch với Ngăn quản lý kính đơn của Fortinet’s Security Fabric.

**5.** **Forcepoint**

Giải mã lưu lượng truy cập trong khi bảo vệ quyền riêng tư

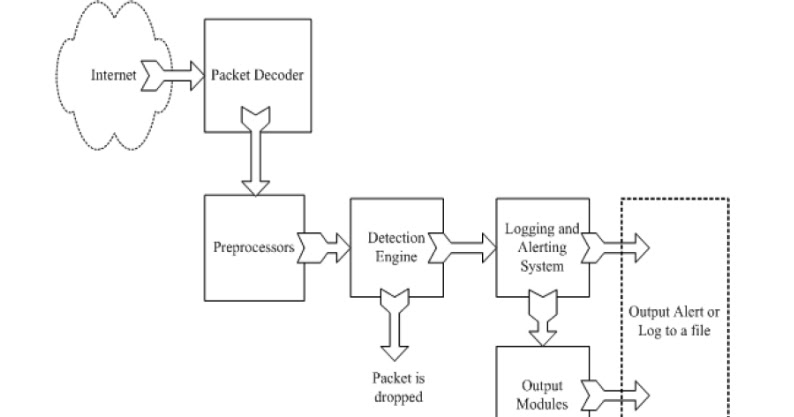
Kết nối đa liên kết cho SD-WAN

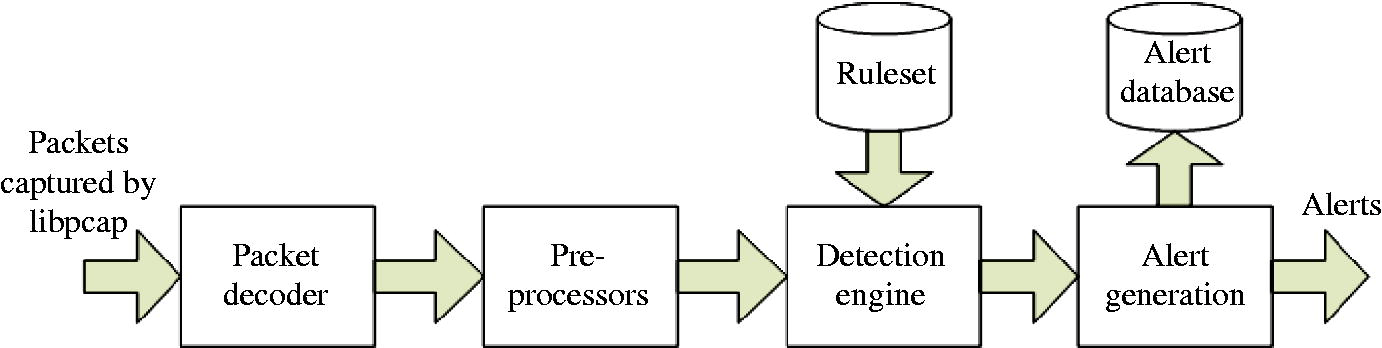
1. **IDS/IPS**

**Snort**

Snort là một hệ thống phát hiện xâm nhập mạng mã nguồn mở miễn phí (IDS) và hệ thống ngăn chặn xâm nhập (IPS) được tạo ra vào năm 1998 bởi Martin Roesch, người sáng lập và là cựu CTO của Sourcefire. Snort hiện được phát triển bởi Cisco, công ty đã mua Sourcefire vào năm 2013.

**Mô hình kiến trúc của Snort**





Trong mô hình kiến trúc trên, hệ thống Snort được chia thành 4 phần:

Module Decoder: Xử lý giải mã các gói tin

Module Preprocessors: Tiền xử lý

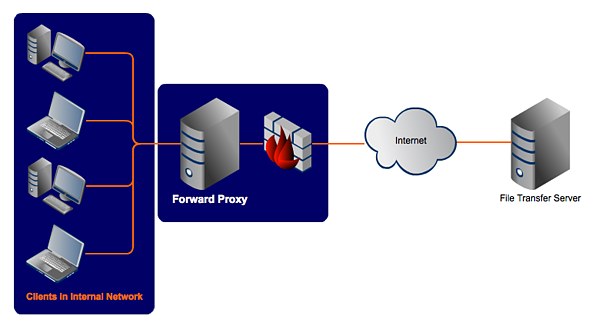
Module Detection Engine: Phát hiện

Module Logging and Alerting System: Lưu log và cảnh báo

**Top 5 commercial IDS/IPS**

1. Cisco NGIPS
2. Corelight and Zeek
3. Fidelis Network
4. FireEye Intrusion Prevention System
5. Hillstone S-Series
6. **PROXY**

**Forward Proxy**



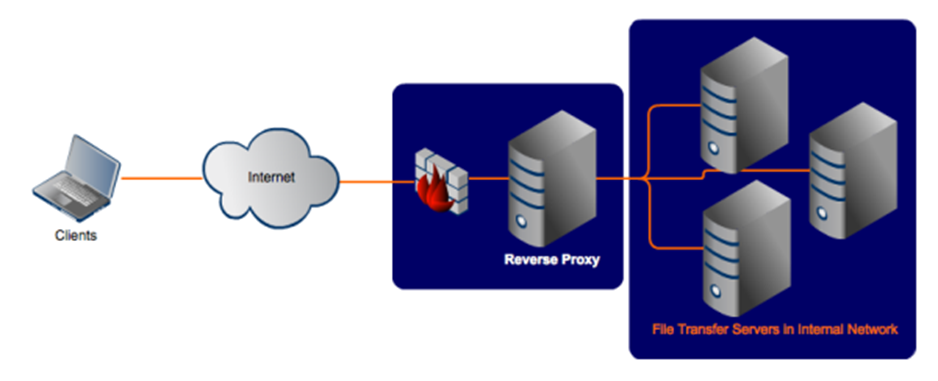
Client có thể sử dụng Forward proxy để ẩn danh trực tuyến(stay anonymous online) hoặc vượt qua bộ lọc tường lửa(bypass firewall restrictions) để truy cập các trang web bị chặn. Nếu một website bị chặn trong một dải IP, thì người dùng trong dải IP đó có thể sử dụng Forward proxy để ẩn IP thực của họ để có thể truy cập website bị cấm.

Tuy nhiên, Forward proxy vẫn có thể bị phát hiện. Có một số dịch vụ proxy trả phí có nhiều hệ thống proxy trên khắp thế giới có thể thay đổi địa chỉ IP của bạn mỗi lần truy cập.

Có nhiều Proxy miễn phí được xây dựng bởi những hackers vì mục đích không mấy tốt đẹp. Nếu bạn tình cờ sử dụng chúng, mọi nhật ký hoạt động của bạn trên Internet sẽ bị lưu lại. Vì vậy, đó là cái kết của dùng đồ miễn phí (There ain't no such thing as a free lunch).

Việc sử dụng Forward proxy để duyệt Internet thường làm chậm tốc độ truy cập Internet. Điều đó phụ thuộc vào vị trí giữa bạn và Forward proxy và số lượng người đang sử dụng Forward proxy đó.

**Reverse Proxy**

****

Reverse proxy chủ yếu được sử dụng ở phía Server để cân bằng tải(Load balancing) và đạt tính sẵn sàng cao(High Availability), ủy quyền(Authorize), chặn truy cập, etc... Một website có thể có nhiều web server đằng sau Reverse proxy.

Máy chủ Reverse proxy nhận các requests từ Internet và chuyển tiếp(forwarding) các requests này đến một trong các web server.

Reverse proxy thêm tính bảo mật(security) và tính linh hoạt(flexibility) cho một website. Vì clients chỉ có thể truy cập mạng thông qua Reverse proxy, nên tránh được các rủi ro.

Reverse proxy cũng cho phép owners thay đổi cấu hình máy chủ mà không ảnh hưởng đến người dùng. Reverse proxy cũng có thể giúp tăng tốc độ web bằng cách cache lại dữ liệu nên có thể giảm tải cho các máy chủ back-end.