I. Netflows

**\* Khái niệm**

+ Là 1 giao thức thu thập (collecting), tổng hợp (aggregating) và ghi lại (recording) dữ liệu luồng lưu lượng trong 1 mạng

+ Dữ liệu NetFlow cung cấp chi tiết về băng thông (bandwidth) và lưu lượng mạng (network traffic) đang được sử dụng

**\* Các thành phần chính trong Netflow:**

+ NetFlow Exporter: thu thập dữ liệu mạng đi qua, tạo ra các bản ghi luồng lưu thông tin (IP, port…)

+ NetFlow Cache: Lưu trữ các bản ghi luồng trước khi được xuất ra hoặc hết hạn

+ NetFlow Collector: Thu thập các bản ghi luồng, lưu trữ chúng trong hệ thống tập tin hoặc cơ sở dữ liệu

+ NetFlow Analyzer: Công cụ hoặc phần mềm sử dụng dữ liệu từ Collector để phân tích lưu lượng mạng. Có thể tạo báo cáo, biểu đồ, cảnh báo hiệu suất mạng, …

**\* Cách hoạt động:**

A diagram of a cloud computing system

Description automatically generated

A screenshot of a computer

Description automatically generated

A diagram of a network traffic system

Description automatically generated

1. Thu thập dữ liệu:

\* NetFlow Exporter: Là thiết bị mạng (router, switch) có hỗ trợ NetFlow. Khi 1 gói tin đi qua thiết bị này, nó sẽ thu thập các thông tin tiêu đề của gói tin:

+ Địa chỉ IP nguồn (Source IP)

+ Địa chỉ IP đích (Destination IP)

+ Cổng nguồn (Source Port)

+ Cổng đích (Destination Port)

+ Giao thức tầng 3 (Layer 3 Protocol)

+ TOS Byte (Type of Service)

+ Input Interface

1. Tạo luồng + bản ghi luồng

\* “flow” – Luồng: Khi một gói tin có cùng thông tin tiêu đề (các trường ở trên) được phát hiện, NetFlow sẽ nhóm chúng thành cùng một flow.

\* Bất kỳ giá trị nào (ở trường trên) thay đổi cũng sẽ tạo ra một luồng mới

\* NetFlow sẽ tạo ra một bản ghi cho mỗi luồng, bản ghi này chứa thông tin về: số lượng gói tin, tổng kích thước byte, thời gian bắt đầu và kết thúc của luồng và một số tiêu đề khác

\* NetFlow Cache: Là bộ nhớ tạm thời, dùng để lưu trữ các bản ghi luồng. Các bản ghi này vẫn sẽ được tồn tại cho đến khi được xuất ra hoặc hết han (timeout)

1. Xuất bản ghi NetFlow

\* Khi một luồng kết thúc hoặc đạt đến một ngưỡng thời gian nhất định, NetFlow Exporter sẽ xuất bản ghi của luồng đến Net Flow Collector

\* Bản ghi thường được gửi qua giao thức UDP hoặc SCTP đến IP của NetFlow Collector

1. Thu thập và phân tích dữ liệu

\* NetFlow Collector: Là máy chủ hoặc phần mềm được thiết kế để nhận, lưu trữ và phân tích các bản ghi NetFlow

**\* Ứng dụng của NetFlow:**

+ Giám sát mạng

+ Lập kế hoạch mạng

+ Phân tích bảo mật

\* Ở giai đoạn 3 của hoạt động NetFlow, giao thức được sử dụng là UDP/SCTP phổ biến do:

+ Hiệu suất cao độ trễ thấp:

* UDP: không cần thiết lập kết nối trước khi gửi dữ liệu
* SCTP: Thiết kế truyền tải thời gian thực và cần độ tin cậy (nhưng yêu cầu về độ tin cậy không phức tạp như TCP)

+ Đơn giản, tiêu thụ ít tài nguyên:

* UDP: là giao thức nhẹ, không có cơ chế kiểm soát lỗi hay đảm bảo trật tự gói tin => không cần duy trì nhiều trạng thái trên thiết bị gửi và nhận
* SCTP: cung cấp giải pháp trung gian giữa TCP và UDP nhưng không phức tạp về độ tin cậy

+ Không yêu cầu truyền tải chính xác:

* Các bản ghi luồng không yêu cầu đảm bảo truyền tải cao như dữ liệu nhạy cảm

+ Tính khả dụng trong hệt thống mạng

- UDP: phổ biến, dễ triển khai, cấu hình không phức tạp

- SCTP: nhẹ hơn TCP

\* Có 2 cách triển khái NetFlow:

1. TFF (Traditional NetFlow):

+ Đề cập đến việc thực hiện ban đầu của NetFlow, trong đó xác định 1 flow là kết hợp của 7 lĩnh vực:

- IP nguồn/đích (2 lĩnh vực)

- Cổng nguồn/đích (2 lĩnh vực)

- Giao thức layer 3

- TOS (Type of Service) byte

- Input logical interface

2. FNF (Flexible NetFlow):

+ Cho phép điều chỉnh và tập trung vào thông tin cụ thể ⬄Sử dụng một tập con hoặc nhỏ hơn trong 7 lĩnh vực trọng điểm truyền thống để xác định 1 flow

+ FNF cũng có nhiều lĩnh vực khác => xác định thông tin cụ thể hơn, giảm luồng traffic