



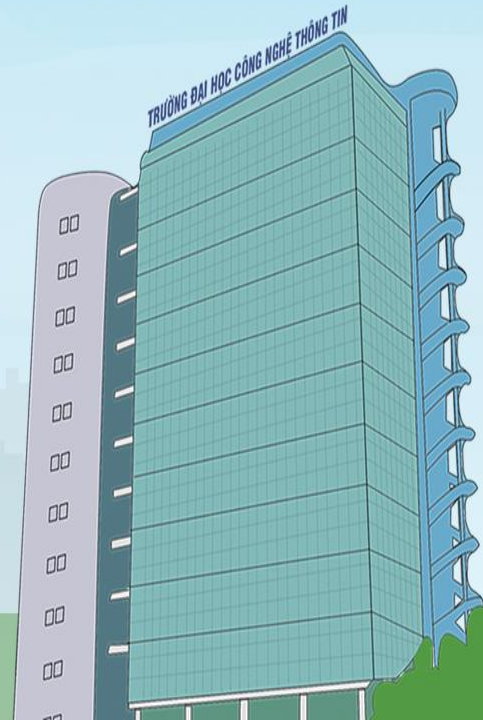
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM
Khoa Mạng máy tính & Truyền thông

Network-based IDS

NT204 – Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

GV: Đỗ Hoàng Hiễn

hiendh@uit.edu.vn





Nội dung hôm nay...

Network-based IDPS

Hôm nay có gì? Network-based IDPS

Tài liệu:

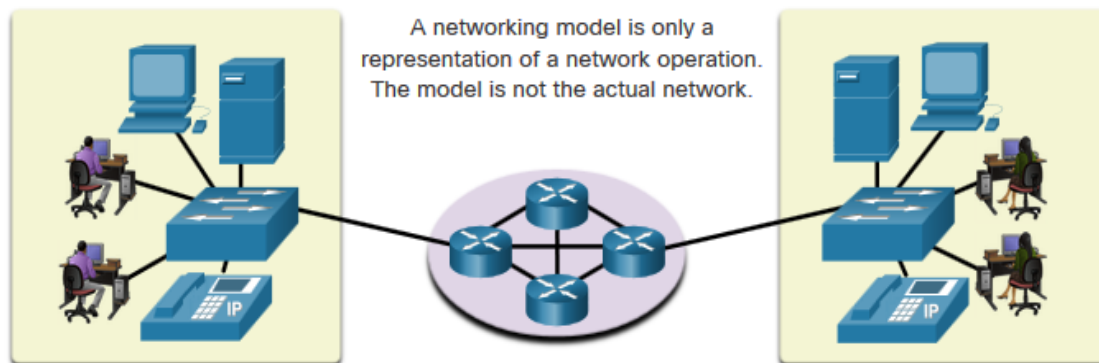
- NIST - Chapter 4
- Các paper, tài liệu liên quan

Tổng quan

Ôn tập: TCP/IP stack

Tại sao phải chia các tầng?

Các khái niệm phức tạp như cách 1 mạng máy tính hoạt động có thể khó giải thích. Do đó, mô hình chia tầng được sử dụng.

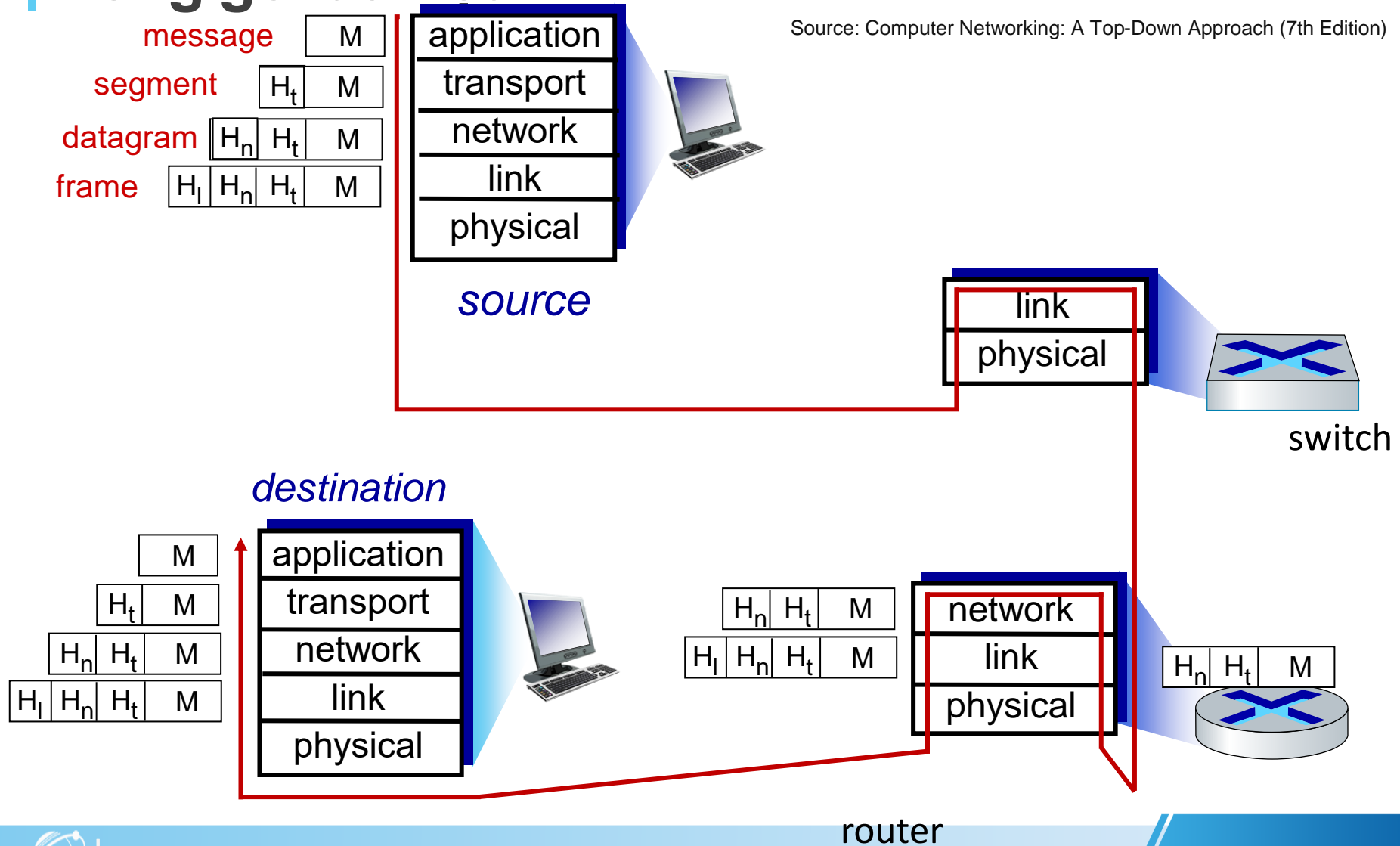


OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application	HTTP, DNS, DHCP, FTP	Application
Presentation		
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	Ethernet, WLAN, SONET, SDH	Network Access
Physical		

Nhắc lại

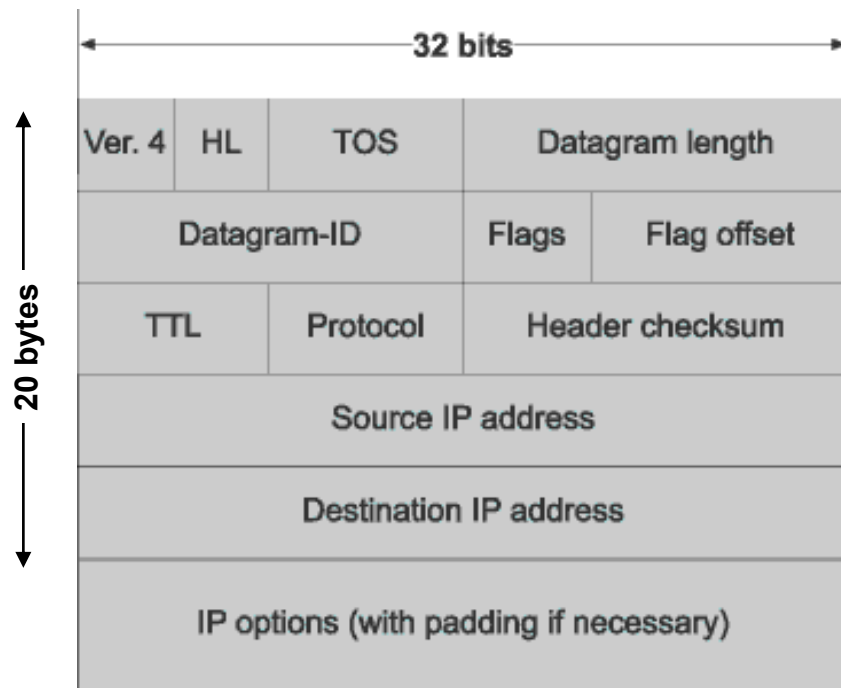
Đóng gói dữ liệu

Source: Computer Networking: A Top-Down Approach (7th Edition)

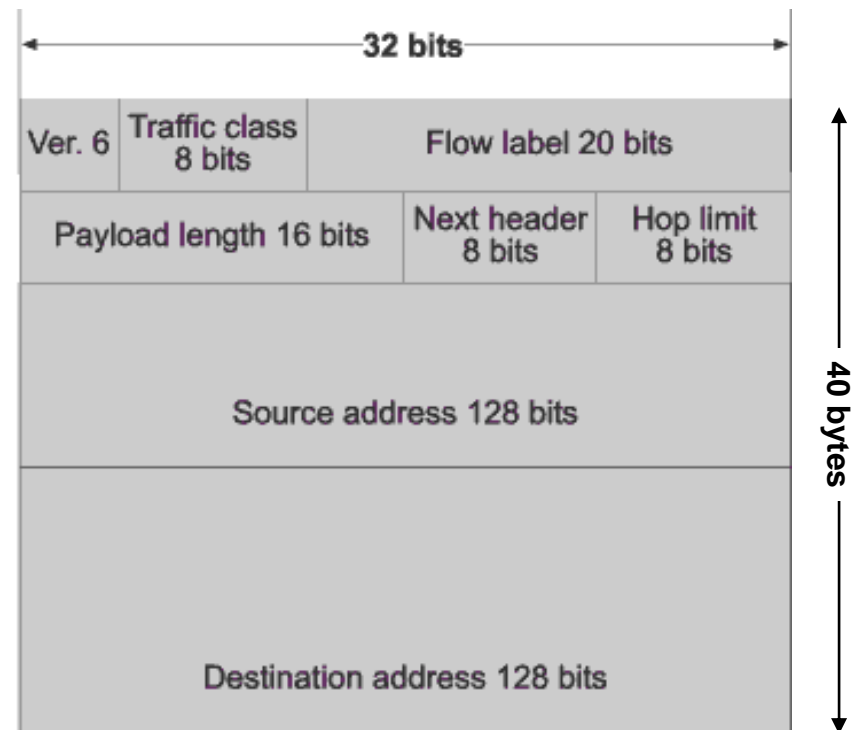


Nhắc lại IP packet header

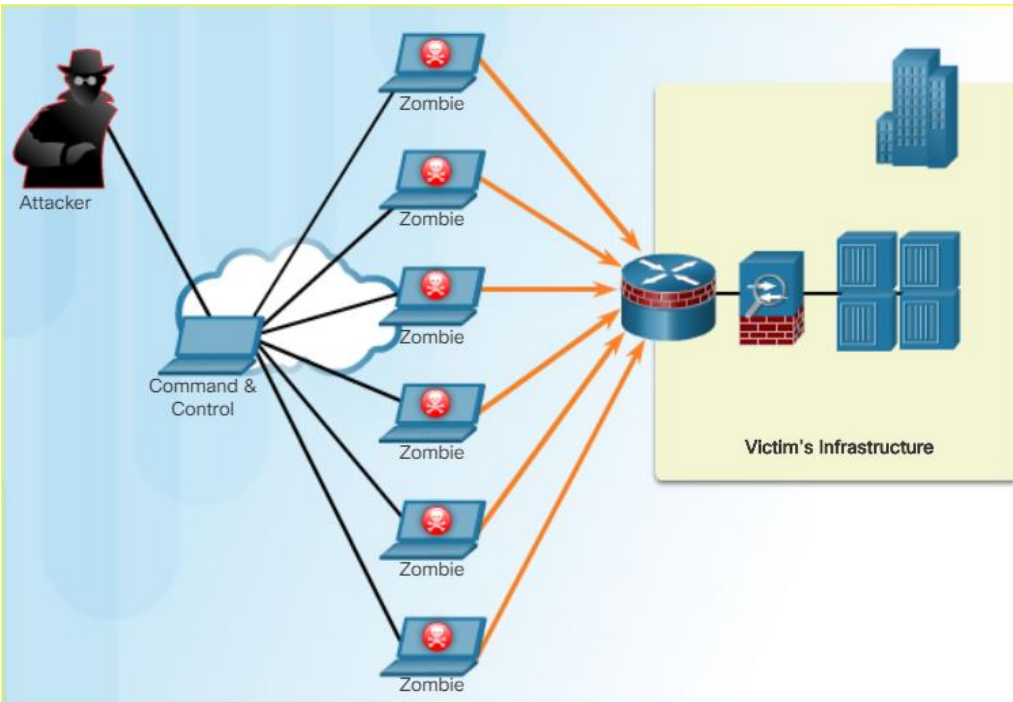
IPv4 header



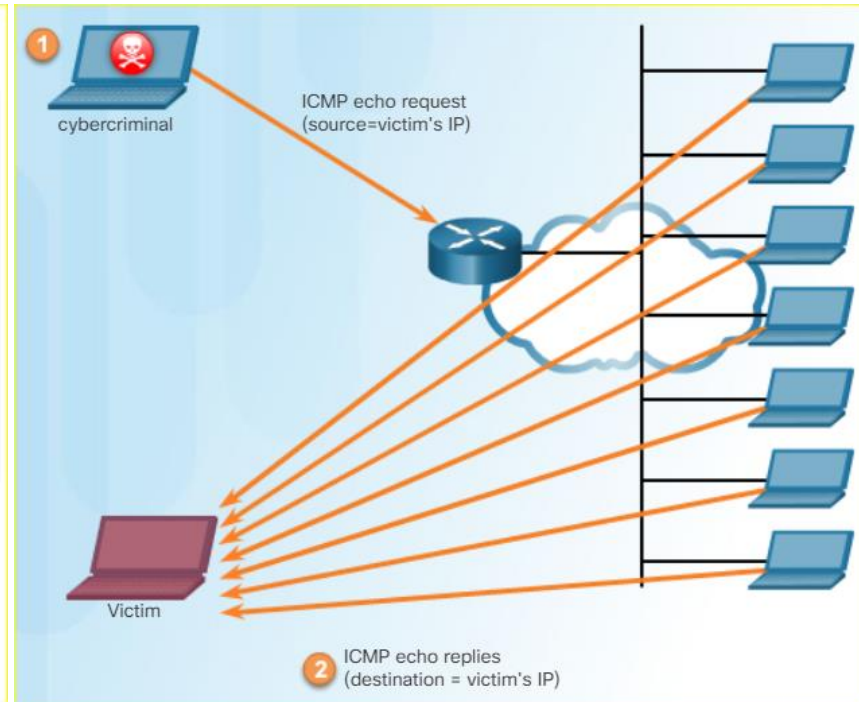
IPv6 header



DoS/DDoS attacks



DDoS attack

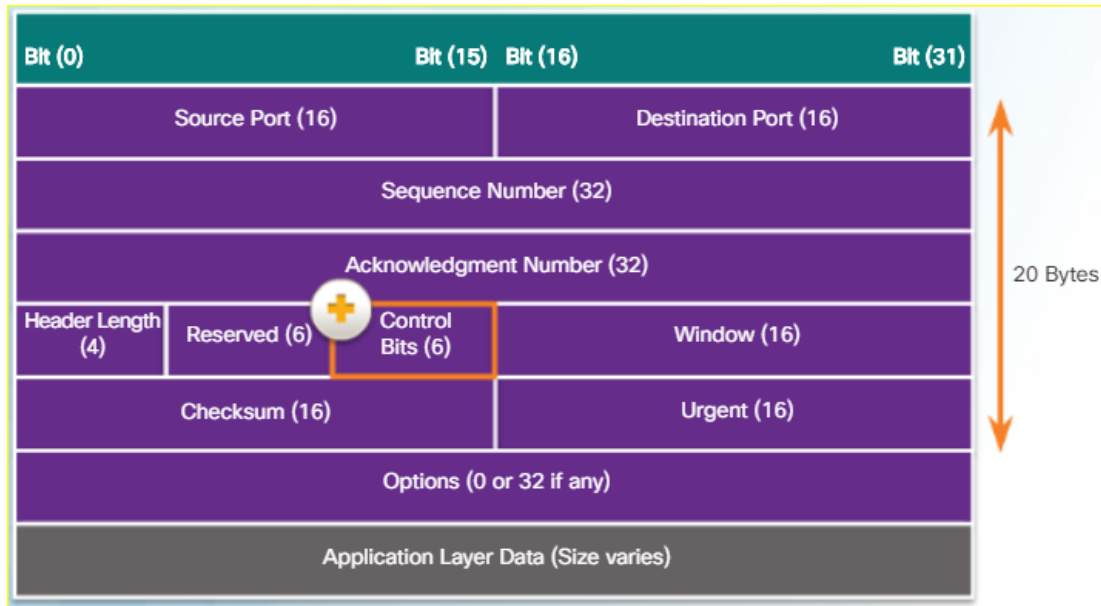


Smurf attack (DoS)

(sử dụng kỹ thuật khuếch đại (amplification) và phản xạ (reflection) technique)

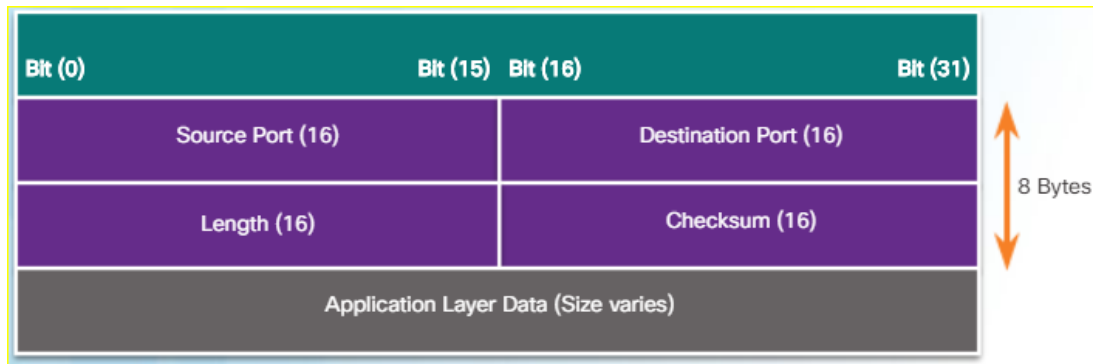
Nhắc lại

TCP – UDP Segments



TCP:

- Connection-oriented
- Reliable delivery
- Flow control
- Stateful communication



UDP:

- connectionless transport

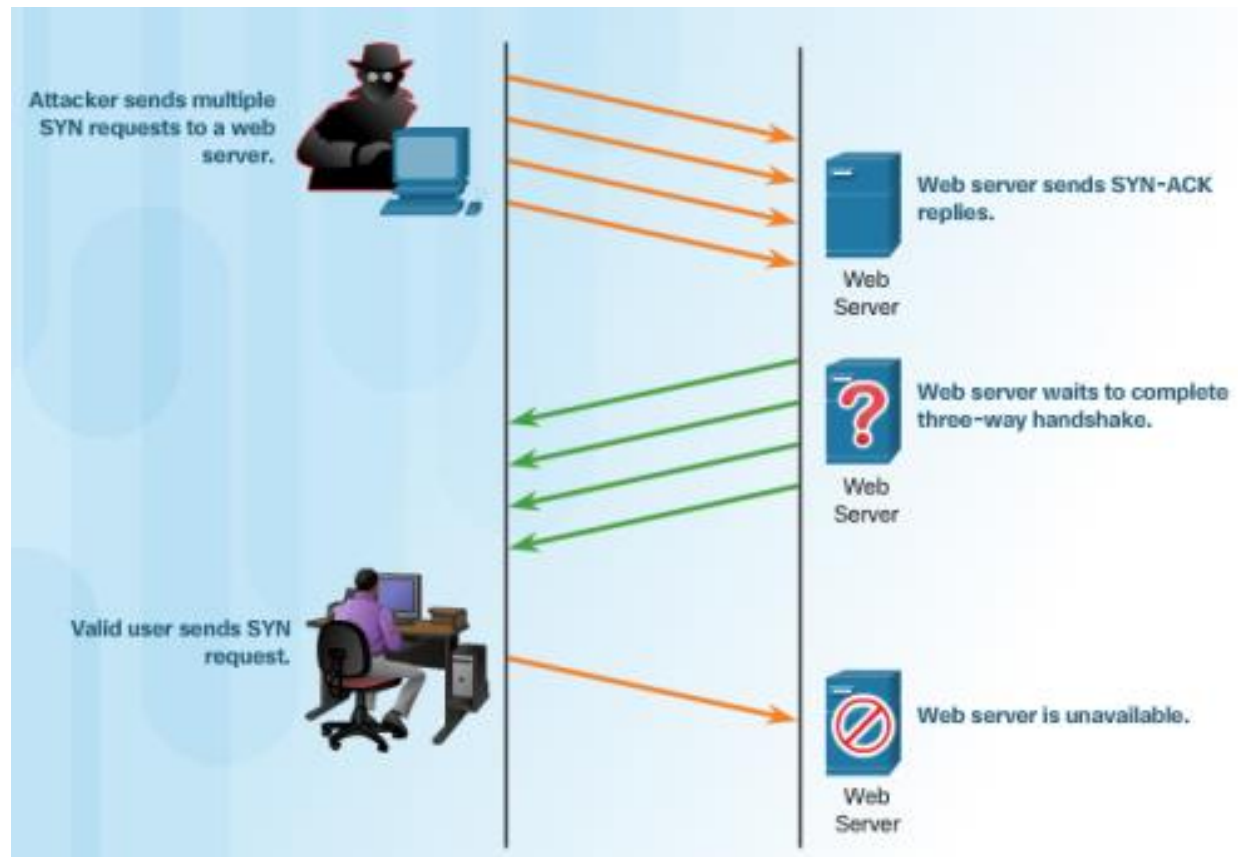
Lỗ hổng trong TCP – UDP

TCP attacks:

- TCP SYN flood attack
- TCP reset attack
- TCP session hijacking

UDP attacks:

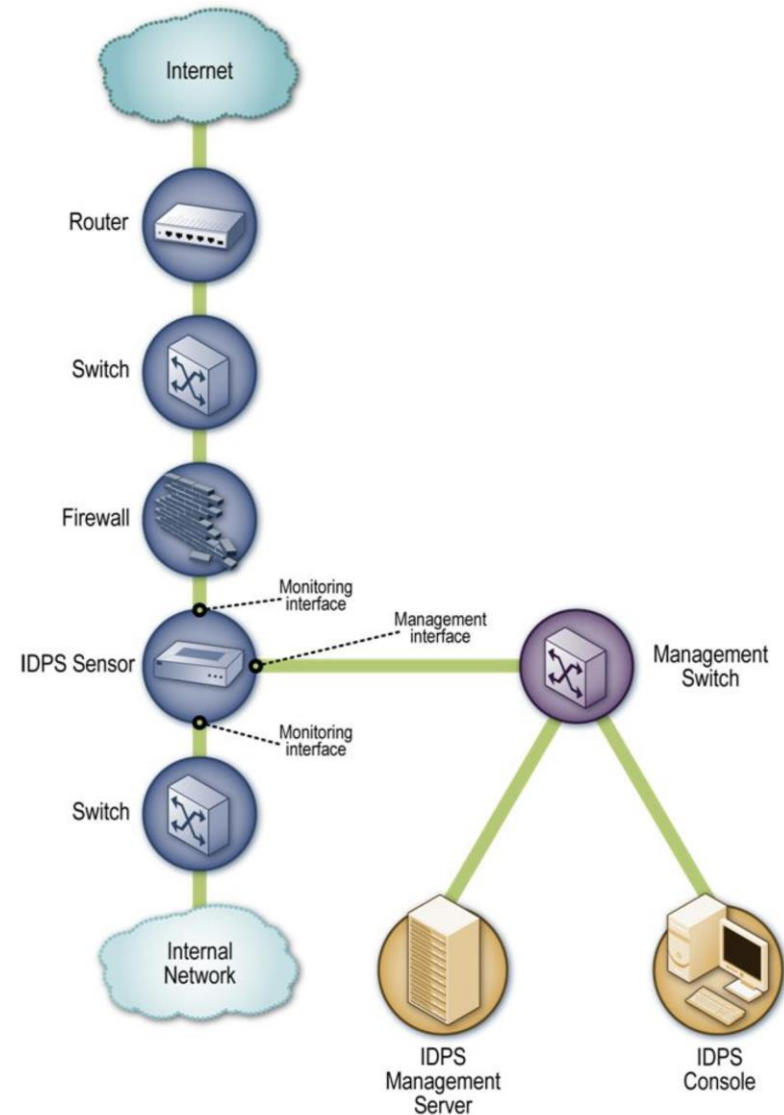
- UDP ping-pong attack
- UDP amplification attack
- UDP DoS attacks



Các công nghệ IDPS

Network-based (NIDPS)

- **Network-based IDPS (NIDPS)** theo dõi lưu lượng mạng cho một phần của mạng (network segment) hoặc các thiết bị, phân tích các hoạt động mạng và các giao thức ứng dụng để xác định các hành vi bất thường.
 - Thường triển khai ở **biên mạng**, như gần tường lửa hoặc router biên, server VPN, server remote access và mạng không dây.
- Network-based IDPS thường chủ yếu phân tích tại **tầng application**, tầng **transport** và **network**, tuy nhiên, ít phân tích ở tầng network access.



NIDPS: Các thành phần

- **Các thành phần chủ yếu:** sensor, server quản lý, console, server cơ sở dữ liệu (optional)
- Card mạng (Network interface card - NIC) được đặt ở ***promiscuous mode*** – mode dùng để theo dõi lưu lượng mạng.
- Sensor:
 - **Dựa trên thiết bị:** gồm một **phần cứng chuyên dụng** (NICs hay driver NIC để bắt gói tin, bộ xử lý và các thành phần phần cứng khác cho việc phân tích), **phần mềm** sensor (firmware), và một **hệ điều hành** (OS) được tùy chỉnh.
 - **Chỉ gồm phần mềm:** có thể bao gồm cả hệ điều hành (OS) được tùy chỉnh, hoặc có thể được cài đặt trên OS chuẩn của các host.

Promiscuous Mode

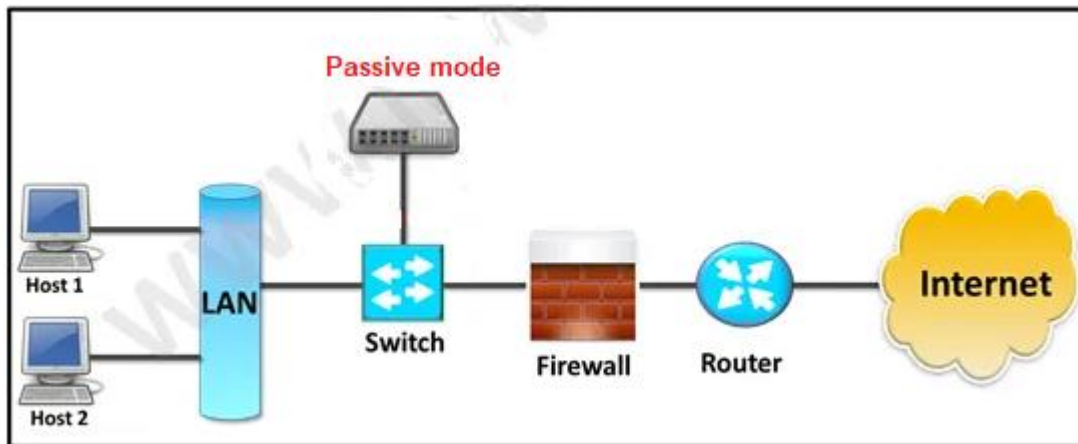
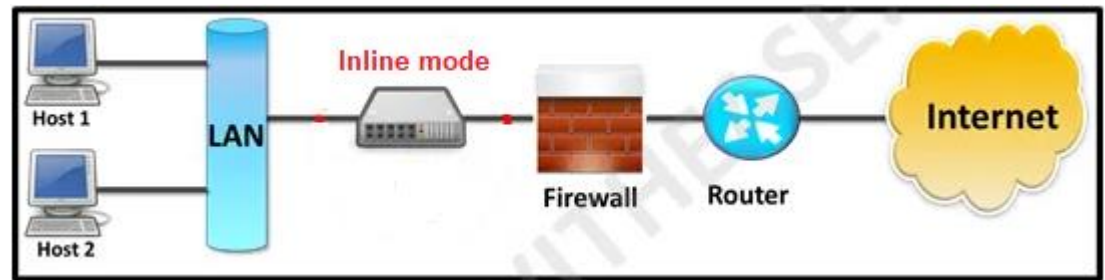
Bắt và xử lý mọi gói tin

- Thông thường, card mạng (NIC) sẽ bỏ qua các gói tin không gửi đến nó (khác địa chỉ MAC).
- Khi **hoạt động ở promiscuous mode**, NIC chuyển tất cả các frame nhận được từ mạng đến kernel.
- Nếu một sniffer đã có đăng ký với kernel, nó có thể thấy tất cả các gói tin (frame) đó.
- Trong Wi-Fi được gọi là **Monitor Mode**.



NIDPS: Kiến trúc và Vị trí các sensor

- Nên cân nhắc sử dụng **mạng quản lý** để triển khai NIDPS hoặc sử dụng **VLAN** để bảo vệ các giao tiếp IDPS.
- Các sensor có thể được triển khai ở 2 mode:
 - **Inline sensor**
 - **Passive sensor**

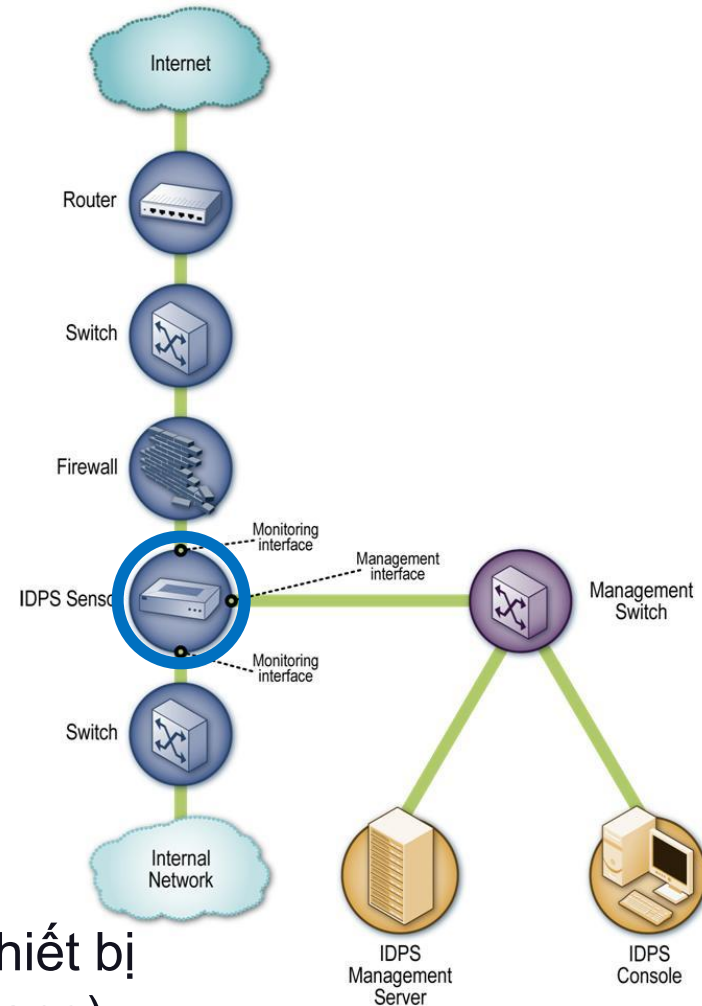


Nguồn: ipwithease.com

Inline Sensor

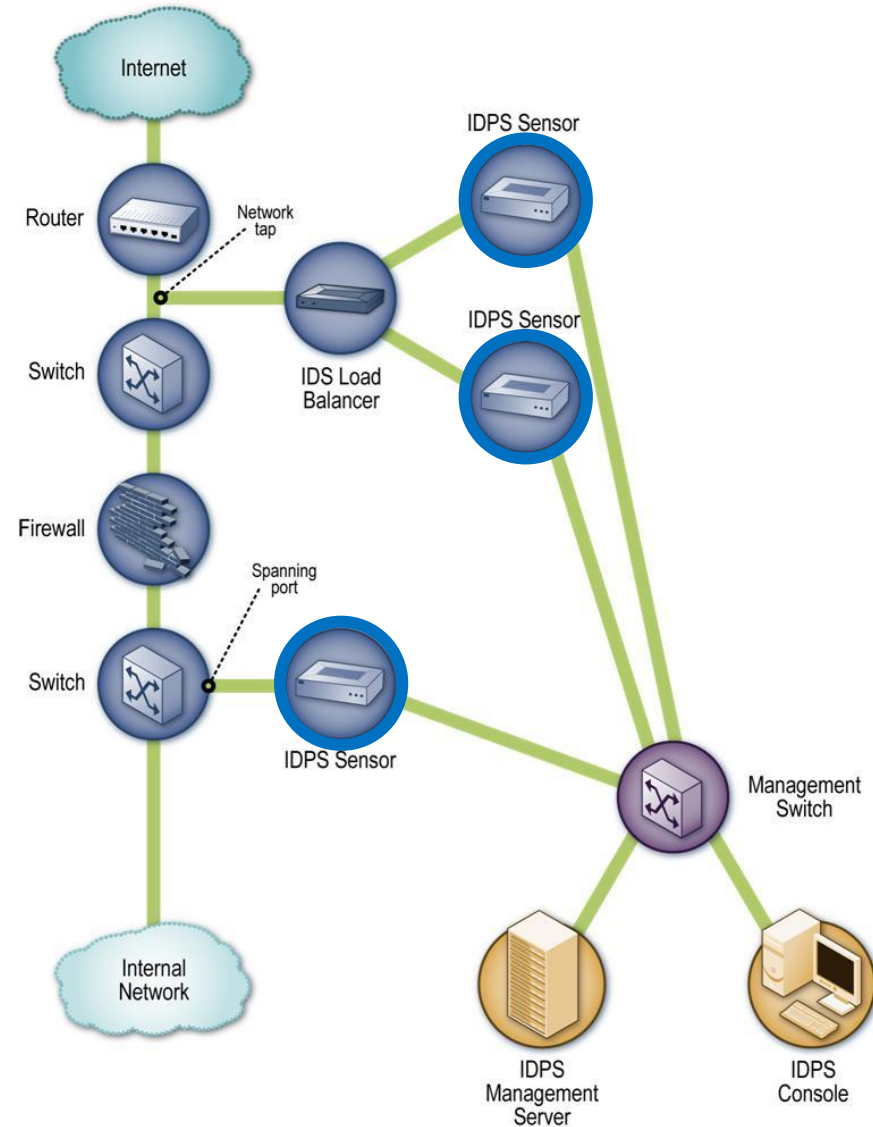
○ *Inline sensor:*

- Lưu lượng mạng được theo dõi **đều phải đi qua** sensor đó, tương tự như lưu lượng đi qua tường lửa.
- ***Cho phép ngăn chặn tấn công bằng cách chặn lưu lượng mạng.***
- Một vài inline sensor là thiết bị **lai firewall/IDPS (A)** hoặc chỉ là **IDPS (B)**
- **Đặt ở đâu?**
 - **A:** Đặt tại vị trí của tường lửa mạng và các thiết bị bảo mật mạng khác (giữa các mạng, biên mạng)
 - **B:** Đặt ở một phía an toàn hơn của phần mạng để có ít traffic phải xử lý hơn.



Passive sensor

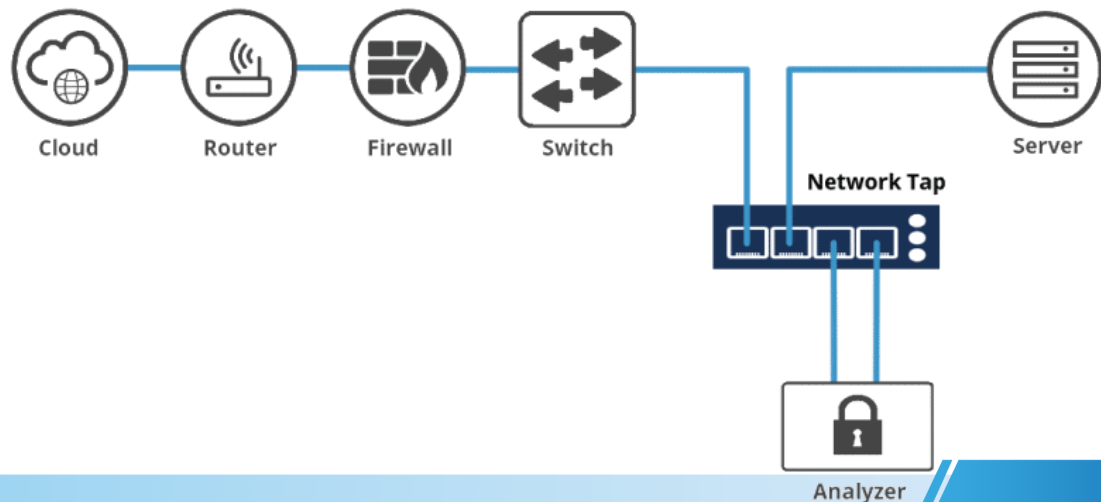
- **Passive sensor:**
 - Theo dõi **bản sao của lưu lượng mạng**; không có lưu lượng thực tế nào đi qua sensor
- **Vị trí?**
 - **Vị trí quan trọng trong mạng** (như vị trí chia giữa các mạng)
 - **Các segment mạng quan trọng** (như vùng DMZ)



Các phương pháp theo dõi mạng

Network TAPs (Terminal Access Point):

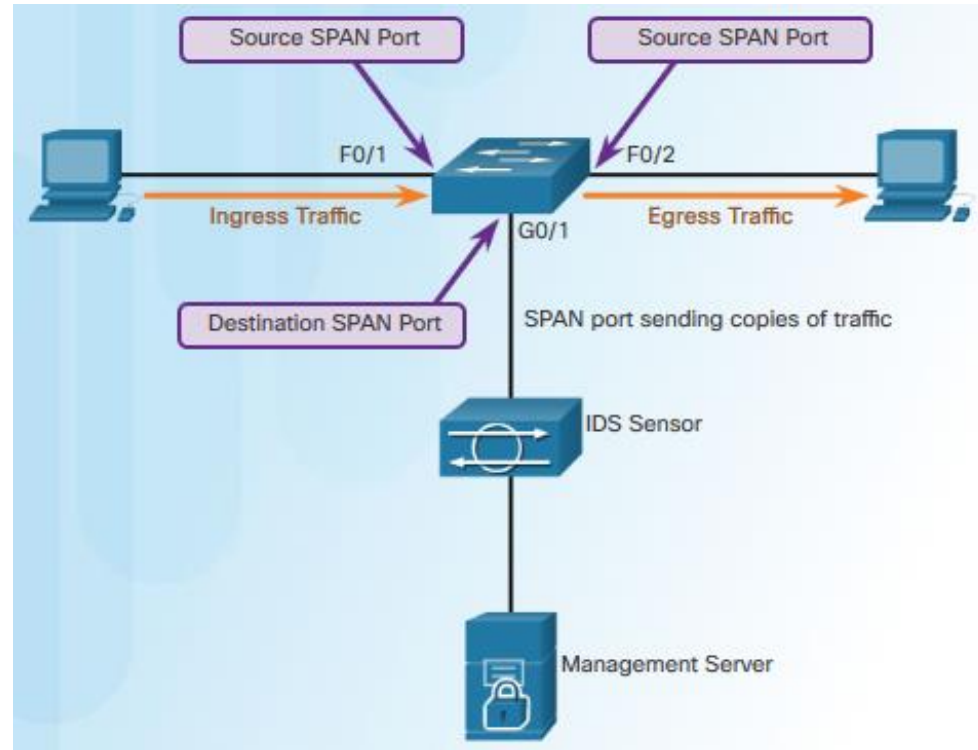
- Kết nối trực tiếp giữa sensor và đường truyền vật lý
- Cung cấp bản sao các lưu lượng mạng trên đường truyền
- **Fail-safe**
- Nhược điểm: cần thêm chi phí trang bị



Các phương pháp theo dõi mạng (tt)

Switch Port mirroring: switch sao chép các frame của một hoặc nhiều port gửi đến SPAN (Switch Port Analyzer) port, có thể kết nối với thiết bị phân tích

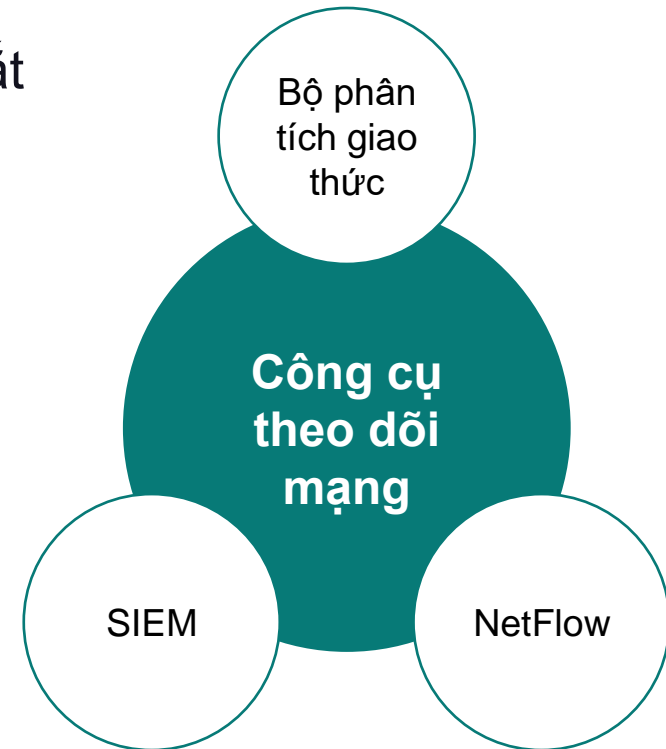
- **Nhược điểm:** SPAN port có thể không thấy được tất cả lưu lượng nếu cấu hình sai hoặc đang quá tải



Công cụ theo dõi mạng

○ Các công cụ theo dõi mạng:

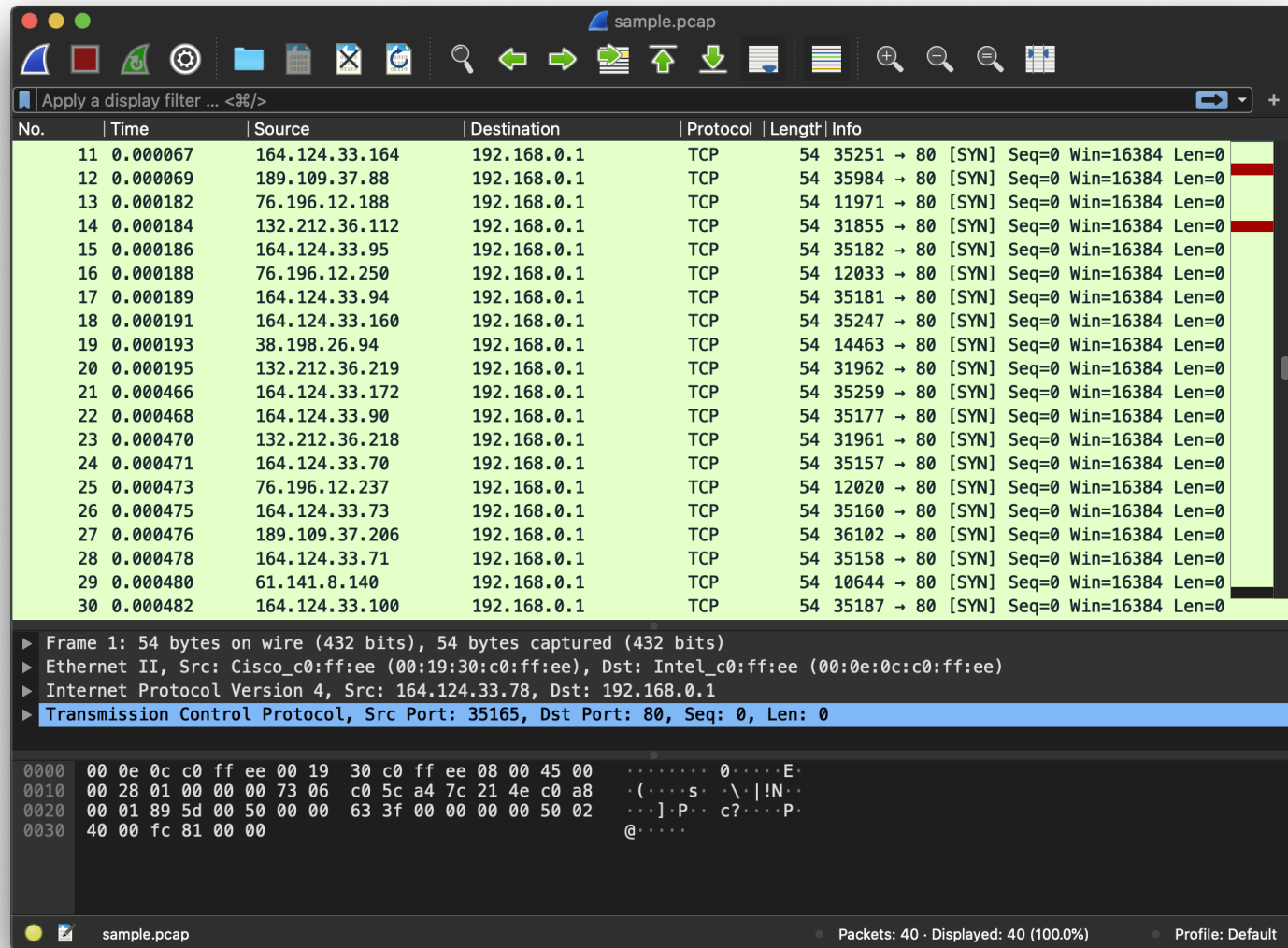
- **Bộ phân tích giao thức** – Chương trình bắt lưu lượng mạng. Vd: *Wireshark* và *Tcpdump*
 - **NetFlow** – Cung cấp đầy đủ các thông tin cơ bản về tất cả luồng IP chuyển tiếp trên 1 thiết bị
 - **SIEM** – Security Information Event Management hỗ trợ báo cáo theo thời gian thực và phân tích các sự kiện bảo mật
- **SNMP** – Simple Network Management Protocol cho phép yêu cầu và thu thập thông tin (thụ động) trên tất cả các thiết bị mạng



Ví dụ về Công cụ theo dõi mạng

Bộ phân tích giao thức

Có thể dự đoán
tấn công gì đang
xảy ra???



sample.pcap

Apply a display filter ... <%%/>

No.	Time	Source	Destination	Protocol	Length	Info
11	0.000067	164.124.33.164	192.168.0.1	TCP	54	35251 → 80 [SYN] Seq=0 Win=16384 Len=0
12	0.000069	189.109.37.88	192.168.0.1	TCP	54	35984 → 80 [SYN] Seq=0 Win=16384 Len=0
13	0.000182	76.196.12.188	192.168.0.1	TCP	54	11971 → 80 [SYN] Seq=0 Win=16384 Len=0
14	0.000184	132.212.36.112	192.168.0.1	TCP	54	31855 → 80 [SYN] Seq=0 Win=16384 Len=0
15	0.000186	164.124.33.95	192.168.0.1	TCP	54	35182 → 80 [SYN] Seq=0 Win=16384 Len=0
16	0.000188	76.196.12.250	192.168.0.1	TCP	54	12033 → 80 [SYN] Seq=0 Win=16384 Len=0
17	0.000189	164.124.33.94	192.168.0.1	TCP	54	35181 → 80 [SYN] Seq=0 Win=16384 Len=0
18	0.000191	164.124.33.160	192.168.0.1	TCP	54	35247 → 80 [SYN] Seq=0 Win=16384 Len=0
19	0.000193	38.198.26.94	192.168.0.1	TCP	54	14463 → 80 [SYN] Seq=0 Win=16384 Len=0
20	0.000195	132.212.36.219	192.168.0.1	TCP	54	31962 → 80 [SYN] Seq=0 Win=16384 Len=0
21	0.000466	164.124.33.172	192.168.0.1	TCP	54	35259 → 80 [SYN] Seq=0 Win=16384 Len=0
22	0.000468	164.124.33.90	192.168.0.1	TCP	54	35177 → 80 [SYN] Seq=0 Win=16384 Len=0
23	0.000470	132.212.36.218	192.168.0.1	TCP	54	31961 → 80 [SYN] Seq=0 Win=16384 Len=0
24	0.000471	164.124.33.70	192.168.0.1	TCP	54	35157 → 80 [SYN] Seq=0 Win=16384 Len=0
25	0.000473	76.196.12.237	192.168.0.1	TCP	54	12020 → 80 [SYN] Seq=0 Win=16384 Len=0
26	0.000475	164.124.33.73	192.168.0.1	TCP	54	35160 → 80 [SYN] Seq=0 Win=16384 Len=0
27	0.000476	189.109.37.206	192.168.0.1	TCP	54	36102 → 80 [SYN] Seq=0 Win=16384 Len=0
28	0.000478	164.124.33.71	192.168.0.1	TCP	54	35158 → 80 [SYN] Seq=0 Win=16384 Len=0
29	0.000480	61.141.8.140	192.168.0.1	TCP	54	10644 → 80 [SYN] Seq=0 Win=16384 Len=0
30	0.000482	164.124.33.100	192.168.0.1	TCP	54	35187 → 80 [SYN] Seq=0 Win=16384 Len=0

► Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
► Ethernet II, Src: Cisco_c0:ff:ee (00:19:30:c0:ff:ee), Dst: Intel_c0:ff:ee (00:0e:0c:c0:ff:ee)
► Internet Protocol Version 4, Src: 164.124.33.78, Dst: 192.168.0.1
► Transmission Control Protocol, Src Port: 35165, Dst Port: 80, Seq: 0, Len: 0

```
0000  00 0e 0c c0 ff ee 00 19 30 c0 ff ee 08 00 45 00  .....0.....E.
0010  00 28 01 00 00 00 73 06 c0 5c a4 7c 21 4e c0 a8  .(....s..\.|N..
0020  00 01 89 5d 00 50 00 00 63 3f 00 00 00 00 50 02  ...]P..c?....P.
0030  40 00 fc 81 00 00                                @.....
```

sample.pcap Packets: 40 · Displayed: 40 (100.0%) Profile: Default



NIDPS: Các khả năng bảo mật

Gồm các khả năng đặc trưng của IDPS trong ngữ cảnh theo dõi và phát hiện tấn công trong một mạng:

- Thu thập thông tin
- Ghi log
- Phát hiện tấn công
- Ngăn chặn tấn công

Thu thập thông tin

- Thu thập cả thông tin trên các host và các hoạt động mạng chứa các host đó.
 - **Xác định các host** dựa trên địa chỉ IP và MAC
 - **Xác định thông tin hệ điều hành OS**
 - Theo dõi các port được sử dụng, phân tích header của packet, xác định phiên bản ứng dụng
 - **Xác định các ứng dụng**
 - Theo dõi các port đang được sử dụng, theo dõi các đặc điểm của các giao tiếp ứng dụng
 - **Xác định các đặc điểm của mạng**
 - Ví dụ số lượng hop giữa 2 thiết bị

Ghi log

○ Các trường thông tin điển hình:

- Thời gian
- ID của kết nối/session
- Sự kiện hoặc loại cảnh báo (thường liên kết đến lỗ hổng hoặc khai thác cụ thể, như CVE)
- Xếp hạng (ví dụ, mức ưu tiên, mức quan trọng, ảnh hưởng, độ tin cậy)
- Các giao thức ở tầng Network, Transport, và Application
- Địa chỉ IP nguồn và đích, port TCP hay UDP, hoặc loại và code ICMP
- Số byte đã được truyền qua kết nối
- Dữ liệu payload đã giải mã, ví dụ: yêu cầu (request) hoặc phản hồi của ứng dụng
- Các thông tin liên quan đến trạng thái của kết nối (ví dụ, username đã đăng nhập)
- Hoạt động ngăn chặn đã thực hiện (nếu có)

Phát hiện tấn công

○ Các dạng sự kiện có thể phát hiện

- **Do thám và tấn công ở tầng Application** (vd: banner grabbing, buffer overflows, format string, dò/đoán password, malware...)
- **Do thám và tấn công ở tầng Transport** (vd: port scanning, packet fragmentation, SYN floods...)
- **Do thám và tấn công ở tầng Network** (vd: giả mạo IP address, giá trị IP header không hợp lệ...)
- **Các dịch vụ ứng dụng bất thường** (vd: backdoor, host chạy các dịch vụ ứng dụng trái phép...)
- **Vi phạm chính sách** (vd: sử dụng website không phù hợp, sử dụng giao thức bị cấm...)

NIDPS: Các khả năng bảo mật

Phát hiện tấn công (tt)

Độ chính xác

- Các NIDPS trước đây sử dụng signature thường có tỷ lệ false positive thấp và false negative cao
- *Kỹ thuật mới* kết hợp nhiều phương pháp phát hiện -> tăng độ chính xác, phạm vi phát hiện và giảm tỷ lệ false positive và false negative
- False positive và false negative của NIDPS chỉ có thể **giảm một phần** nào đó, do sự phức tạp của các hoạt động được theo dõi (nhiều OS, ứng dụng đa dạng)
- Các tổ chức nên sử dụng NIDPS để một phần nào đó có thể chống lại một số **kỹ thuật qua mặt (evasion technique)** phổ biến

NIDPS: Các khả năng bảo mật

Phát hiện tấn công (tt)

Khả năng tùy chỉnh

- Cần **tùy chỉnh** để cải thiện độ chính xác trong phát hiện tấn công
 - Vd: ngưỡng cho port scan và số lần đăng nhập ứng dụng sai, blacklist và whitelist cho địa chỉ IP và username, thiết lập cảnh báo
- Một số NIDPS sử dụng kết quả quét lỗ hổng, và sử dụng chúng để xác định các tấn công có thể đã xảy ra thành công nếu không ngăn chặn
 - Quyết định hành động ngăn chặn tốt hơn và ưu tiên các cảnh báo chính xác hơn

Phát hiện tấn công (tt)

Hạn chế

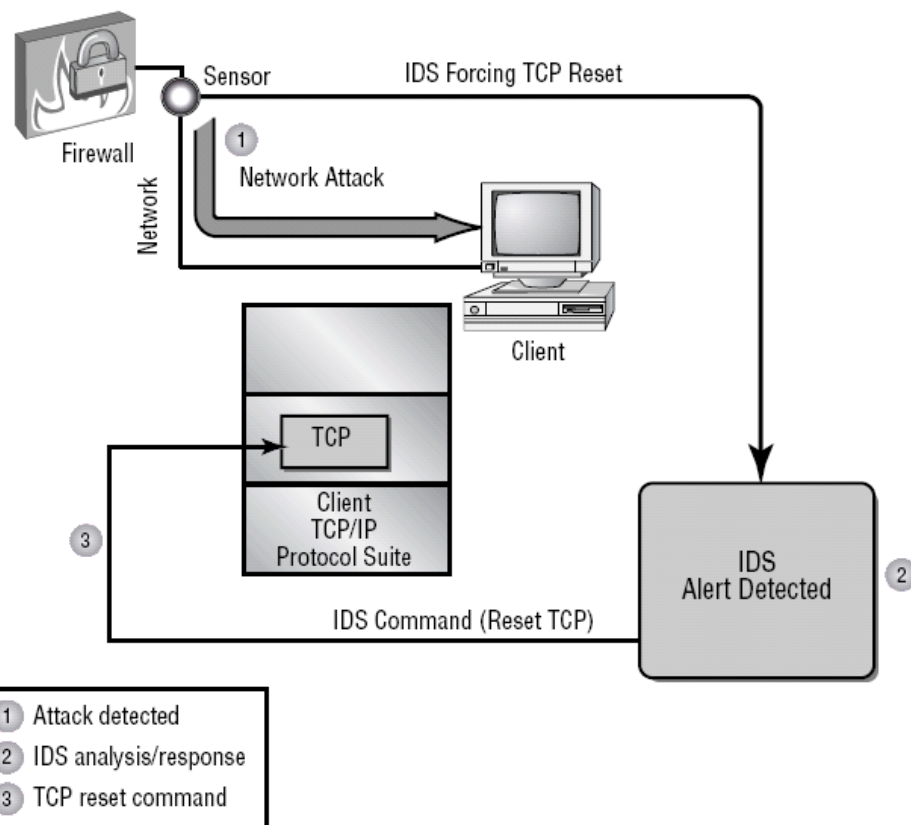
- **Bị giới hạn hoặc không thể phân tích lưu lượng mạng đã mã hoá**
 - Vd: kết nối VPN, (HTTPS), và session SSH
- **Xử lý tải lượng lưu lượng cao**
 - Passive IDPS sensor có thể drop 1 vài gói, khiến phát hiện sai tấn công, đặc biệt khi phân tích stateful protocol
 - Inline IDPS sensor drop gói tin sẽ khiến mạng bị gián đoạn; hoặc chậm xử lý gói tin dẫn đến độ trễ quá cao
- **Hứng chịu các tấn công vào chính NIDPS**
 - Attacker tạo lượng traffic lớn (vd: DDoS) hoặc các hoạt động bất thường (vd: gói tin bị fragment bất thường) để làm cạn kiệt tài nguyên của sensor và khiến sensor bị crash
 - Tạo lưu lượng mạng khiến NIDPS kích hoạt nhiều cảnh báo trong thời gian ngắn

NIDPS: Các khả năng bảo mật

Ngăn chặn tấn công

○ Chỉ Passive mode

- Kết thúc phiên session TCP hiện tại bằng cách gửi gói **TCP reset** đến cả 2 đầu kết nối (*session sniping*)
- Chỉ thích hợp với TCP, không sử dụng được với các tấn công sử dụng UDP và ICMP
- Không còn được sử dụng rộng rãi

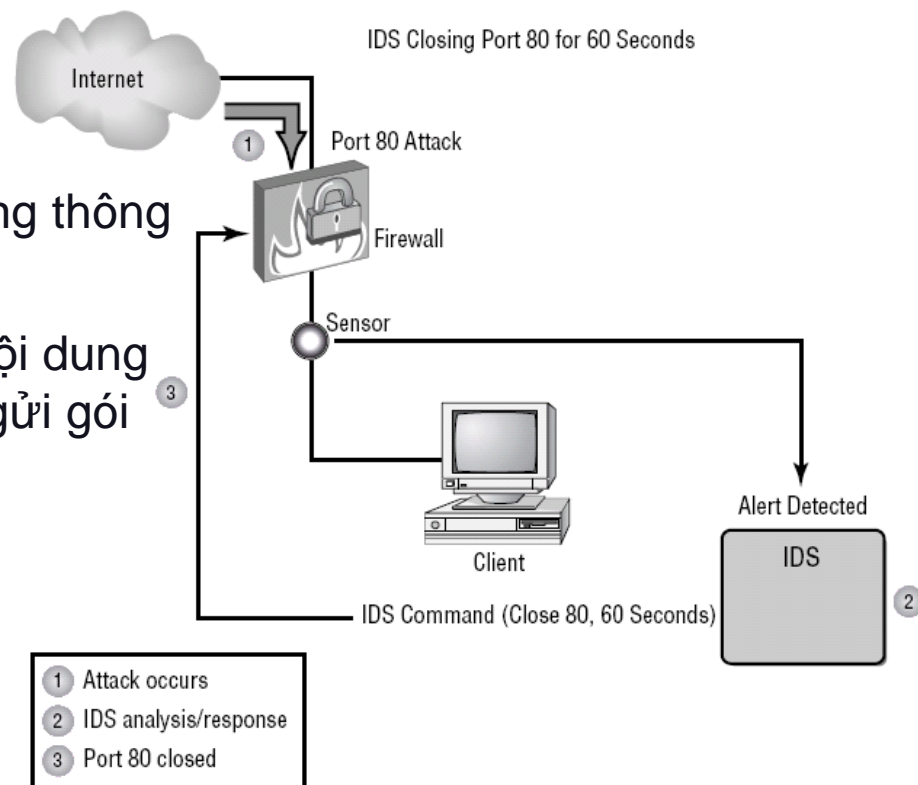


NIDPS: Các khả năng bảo mật

Ngăn chặn tấn công (tt)

Chỉ Inline mode

- Thực hiện chức năng tường lửa
- Giới hạn băng thông:** giới hạn tỉ lệ băng thông mạng mà giao thức có thể dùng
- Thay đổi nội dung độc hại:** thay thế nội dung độc hại bằng nội dung bình thường và gửi gói tin đã thay đổi đến host đích



Cả Passive và Inline mode

- Tái cấu hình các thiết bị mạng khác
- Chạy các chương trình hoặc script khác

NIDPS: quản lý

○ Triển khai

- **Thiết kế kiến trúc**

- Cần bao nhiêu sensor và đặt ở vị trí nào?
- Mỗi sensor nên hoạt động ở mode inline hay passive?
- Các sensor passive nên kết nối với mạng như thế nào? (vd., IDS load balancer, network tap, SPAN port)

- **Kiểm tra và triển khai các thành phần**

- **Bảo vệ các thành phần NIDPS**

- Stealth mode: không gán địa chỉ IP cho các monitoring interface của sensor

○ Vận hành và bảo trì:

- Tương tự như IDPS thông thường

Một số NIDPS phổ biến

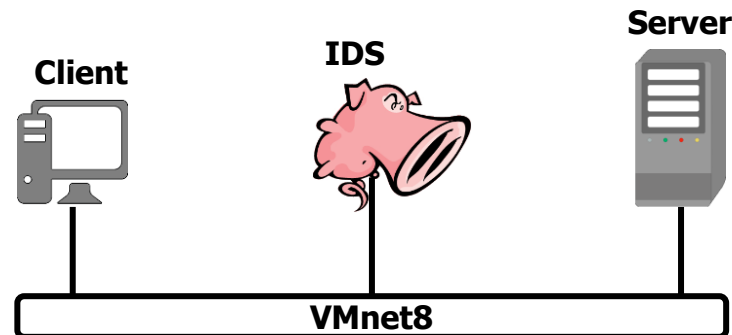
Các công cụ NIDPS

- Snort
- Zeek
- Suricata
- Security Onion



Assignment 1: Cài đặt Snort

- Tìm hiểu cách thức hoạt động của Snort
- Triển khai **Snort 2**
- Tìm hiểu cách viết rule của Snort
- Mô hình triển khai



Tham khảo: <https://snort.org/resources#documents>

Tóm lại...

- **Network-based IDPS (NIDPS)** theo dõi lưu lượng mạng cho các phần mạng hoặc các thiết bị, phân tích các giao thức tầng network, transport, application để phát hiện hành vi đáng ngờ
- NIDPS gồm các thành phần tương tự các loại IDPS khác, trừ các **sensor**
- Các **sensor** theo dõi và phân tích hoạt động mạng của một hoặc nhiều segment mạng, có thể **dựa trên thiết bị phần cứng** hoặc **chỉ là phần mềm**
- Có thể triển khai sensor ở mode **inline** hoặc **passive**
- NIDPS cung cấp đa dạng các khả năng bảo mật nhưng cũng có một số hạn chế đáng kể
- NIDPS sensor có khả năng ngăn chặn tấn công với nhiều phương pháp khác nhau

Tuần sau...

- Hôm nay: **Network-based IDPS**
 - **Assignment 1:** Cài đặt Snort
- Chuẩn bị cho buổi sau: **Network-based IDPS** (cont.)
 - Tài liệu: **Snort** (<https://snort.org/resources#documents> - <http://manual.snort.org/>)
 - Các thành phần của Snort
 - Snort Rules
 - Chuẩn bị đăng ký đề án môn học theo danh sách topic

Câu hỏi/thắc mắc nếu có?



Today end,
See you
next week!

