HỆ THỐNG PHÁT HIỆN XÂM (IDS)

1. Khái niệm
2. Phân loại
3. Snort và cách tạo rules

Một số khái niệm

Các yêu cầu về cấu hình Rules:

- **Positives: dương tính – có tấn công**
- **Negatives: âm tính – ko có tấn công**
- **False positives**: Cảnh báo sai - có tấn công

=> Đưa ra cảnh báo bị tấn công, nhưng thực tế không có

- **True positives:** cảnh báo đúng khi có tấn công

=> Có tấn công và đã đưa ra cảnh báo

- **False negatives**: Sai trong trường hợp ko có tấn công

=> Có tấn công nhưng đã bỏ qua, ko đưa ra cảnh báo

- **True negatives:** hoạt động đúng khi ko có tấn công là gì?

=> Không có tấn công và không đưa ra cảnh báo

=> Cần cấu hình IDS để hạn chế hai nhược điểm trên

Khái niệm

- IDS - Intrusion Detection System: Là hệ thống thực hiện việc thu thập thông tin, phân tích sự kiện và phát hiện các vấn đề an ninh trong hệ thống
- Có thể là thiết bị cứng hoặc phần mềm

- Một số IDS mã nguồn mở phổ biến
  - Snort
  - Suricata
  - Wazuh
  - Zeek
  - OSSEC
  - Security Onion

Phương thức hoạt động

IDS phát hiện sự cố tấn công dựa trên hai phương thức:

- Signature recognition (NIDS)
  - Dựa trên dấu hiệu (đã đc biết trước) của các tấn công để nhận dạng
  - Nhận dạng một số gói tin hoặc là một mẫu dữ liệu trong gói tin
  - Nhanh chóng và tin cậy
- Protocal Anomaly detection (phát hiện bất thường)
  - Dựa trên đặc tả về các giao thức TCP/IP
    - Vd, TCP packet with both SYN and RST => bất thường của giao thức
    - Đăng nhập quá số lần quy định …

PHÂN LOẠI IDS

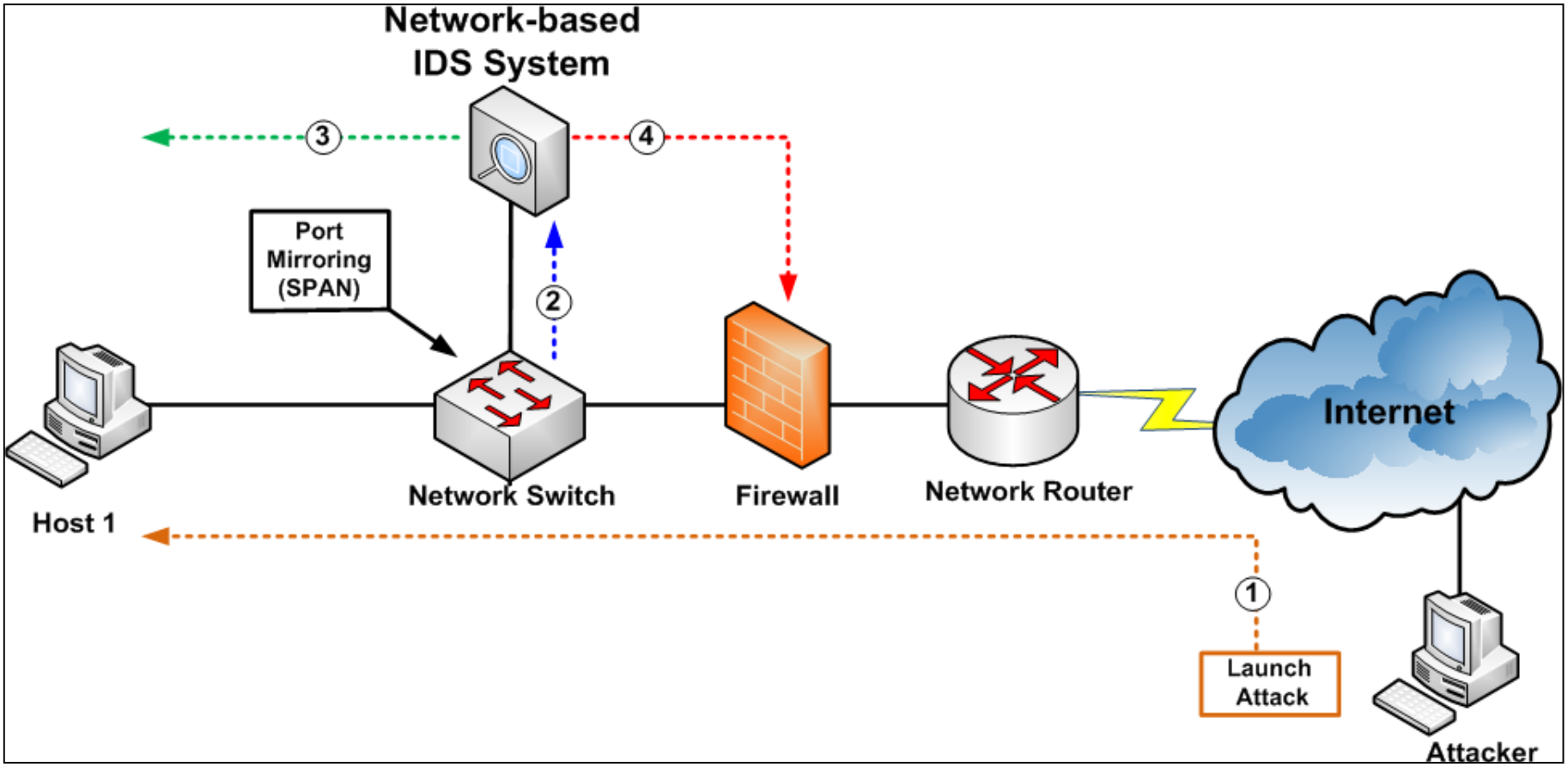
Phân loại IDS (1)

- Có hai loại IDS:
  - Network-based Intrusion Detection (NIDS)
  - Host-based Intrusion Detection (HIDS)
- NIDS
  - Được đặt trên hệ thống mạng, hoạt động ở chế độ promiscous nhằm lắng nghe và phân tích các thông tin qua mạng
  - Giám sát các traffic mạng
  - Cung cấp hệ thống cảnh báo sớm các cuộc tấn công

Phân loại IDS (3)

- Ưu điểm
  - Chi phí thấp (chỉ đặt ở những vị trí trọng yếu)
  - Sử dụng các traffic hiện hành và kiểm tra các header của các gói tin nên kẻ tấn công không thể xoá dấu vết các cuộc tấn công, HIDS thường bị lợi dụng điểm này
  - Phát hiện tấn công ngay khi xảy ra, do đó việc cảnh báo nhanh hơn HIDS
  - Có tính độc lập cao, vì NIDS chạy trên máy chuyên dụng, dễ cấu hình
- Hạn chế
  - Hạn chế hiệu năng mạng
  - Khó khăn trong việc xử lý các phiên được mã hoá như: Ipsec VPN, SSH, SSL, …

Mô hình triển khai NIDS



Phân loại IDS (4)

❖ HIDS

- Được đặt trên một host, kiểm soát các sự kiện xảy ra trên hệ thống đó.
- Log File Monitoring: Giám sát, thu thập log, phát hiện các sự kiện đã xảy ra.
- File integrity Checking: Kiểm tra các file nhiễm mã độc, các file bị sửa đổi.

❖ Ưu điểm HIDS

- Độ chính xác cao hơn NIDS
- Có thể giám sát được các hành động cụ thể (trên 1 máy) mà NIDS không thực hiện được, như truy nhập file, số lần đăng nhập, thay đổi quyền…
- Không yêu cầu thêm thiết bị, được cài đặt trực tiếp trên các máy chủ

Phân loại IDS (5)

❖ Nhược điểm HIDS

- Khó quản trị
- Chiếm tài nguyên trên hệ thống => vì phải lưu nhiều tt
- Nếu HIDS bị thoả hiệp nó sẽ dẫn đến bị vô hiệu hoá hoặc bị thay đổi để hệ thống cảnh báo sai
- Trong trường hợp Hacker không tấn công hoặc không thể tấn công, chúng có thể chọn cách tấn công hệ thống cảnh báo (email, syslog, SNMP, kết nối…), đồng thời gửi tin thông báo giả mạo “Every is OK”
- Để kiểm tra tính toàn vẹn (Checksum), H-IDS cần chiếm hiệu năng rất lớn của máy.
- Hacker thay đổi Update mode

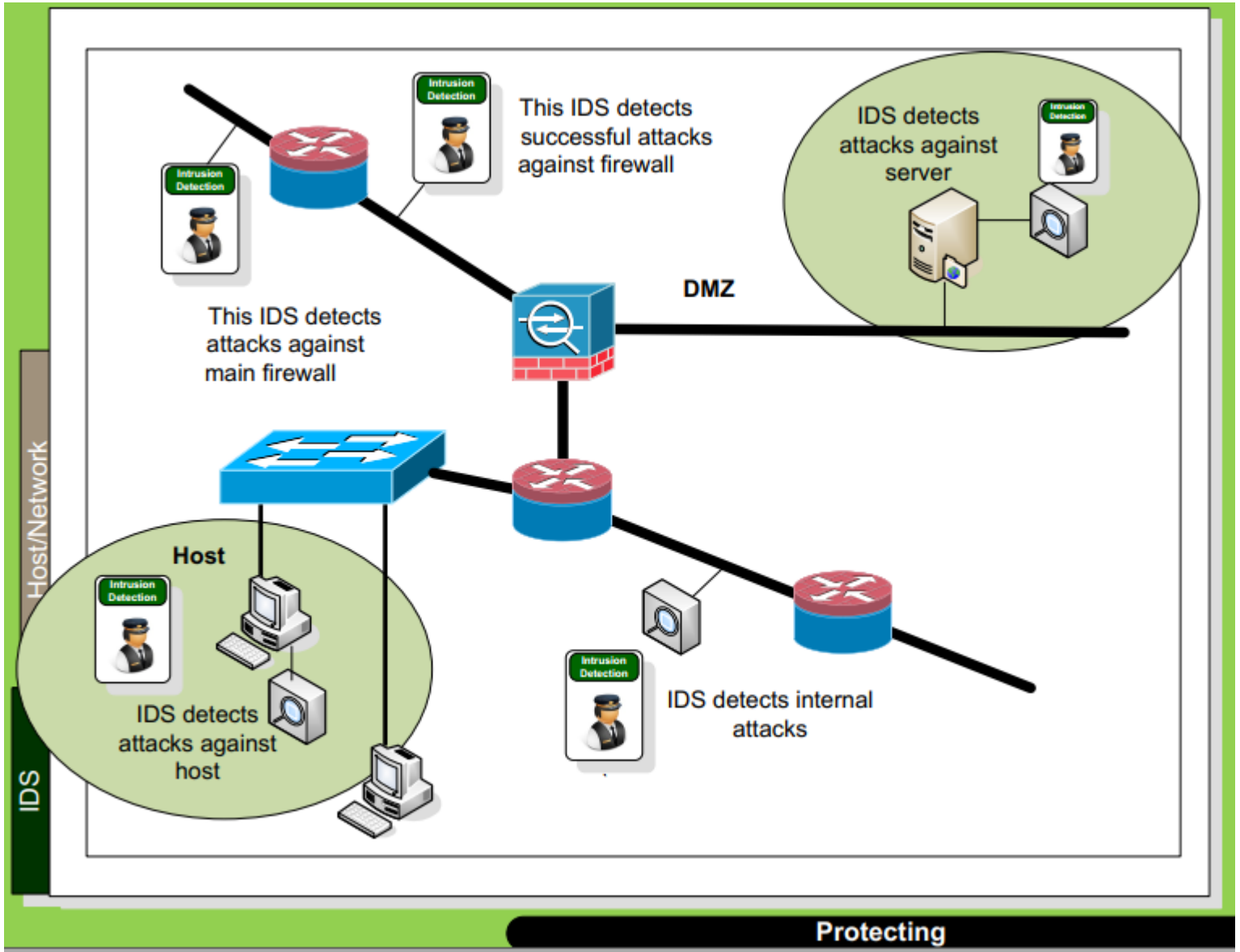
❖ HIDS phát hiện tấn công dựa vào các dấu hiệu sau:

- Xuất hiện các file lạ, chương trình mới
- Thay đổi quyền
- Thay đổi file size
- Các file giả mạo không tương ứng với các file đã được đánh dấu trên hệ thống
- Những tên file có tên lạ trong các thư mục
- Mất file hoặc hỏng file
- Hành động thăm dò các dịch vụ trên máy
- Kết nối từ những khu vực lạ

❖ Phản ứng của HIDS sau khi phát hiện tấn công

- Cấu hình firewall để lọc địa chỉ IP của kẻ xâm nhập
- Thông báo tới user/admin (sound/e-mail/sms...)
- Tạo event log
- Ghi lại thông tin tấn công (thời gian,ip attacker,ip victim,port...)
- Ghi các packets dưới dạng thô để phân tích về sau
- Chạy một chương trình riêng để xử lý event log
- Bắt buộc chấm dứt TCP session

Mô hình triển khai HIDS



Một số sản phẩm IDS

- Snort 2.x (www.snort.org)
- BlackICE Defender (NetworkICE)
- Check Point RealSecure (Check Point Software Technologies)
- Cisco Secure IDS (Cicso Systems)
- Dragon Sensor (Network Security Wizards)
- eTrust Internet Defense (Computer Associates)
- HP Openview Node Sentry (Hewlett-Packard)
- Lucent RealSecure (Lucent Technologies)
- Network Flight Recorder (Network Flight Recorder)
- RealSecure (ISS)
- SilentRunner (SilentRunner)
- Vanguard Enforcer (Vanguard Integrity Professionals)

Snort và cách tạo rules

Giới thiệu SNORT

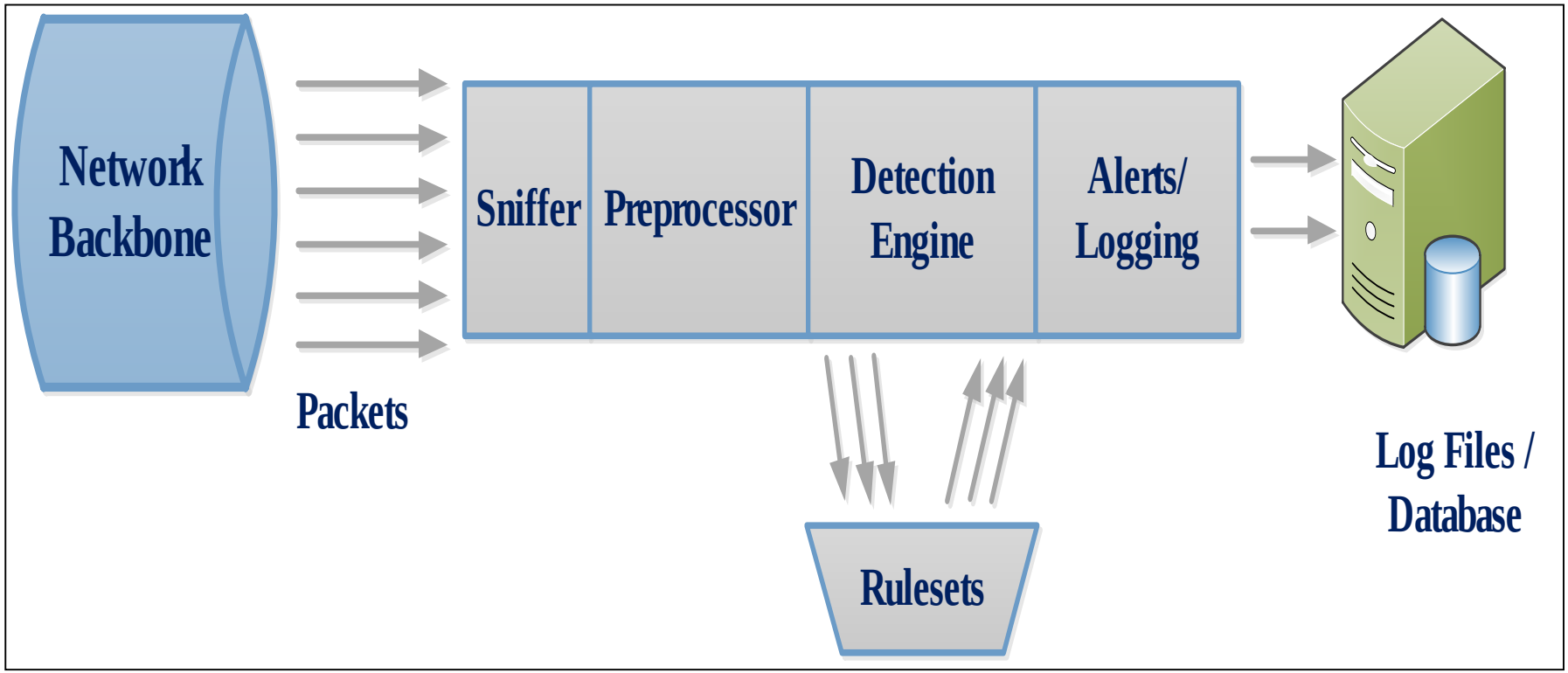
❖ Giới thiệu Snort

- Là công cụ phân tích gói tin ở nhiều chế độ
- Là sp mã nguồn mở, dùng miễn phí, có thể cấu hình trở thành IPS.
- Có thể chạy trên Windows, Linux, MacOS …

❖ Một số thành phần chính của Snort

- Packet Decoder (modul giải mã gói tin) => (sử dụng các thư viện Pcap để bắt gói tin, phụ hồi => DL hoàn chỉnh)
- Preprocessors (tiền xử lý)
- Detection Engine (phát hiện)
- Logging and Alerting System (nhật ký và cảnh báo)
- Output module (kết xuất thông tin)

Kiến trúc Snort



Modul Decoder & Preprocessors

Decoder

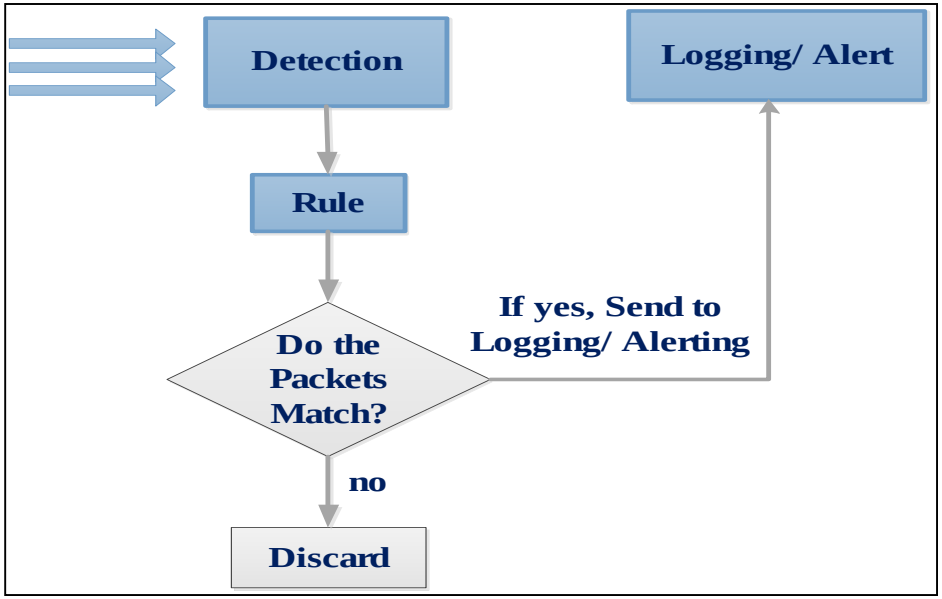
- Bắt gói tin (từ các card mạng khác nhau)
- Phục hồi thành gói dữ liệu hoàn chỉnh,
- Là đầu vào cho tiền xử lý

Preprocessors

- Chuẩn bị dữ liệu cho hệ thống phân tích; cũng có thể phát hiện bất thường dựa vào header của gói tin (kích thước lạ) để đưa ra cảnh báo

Modul Detection

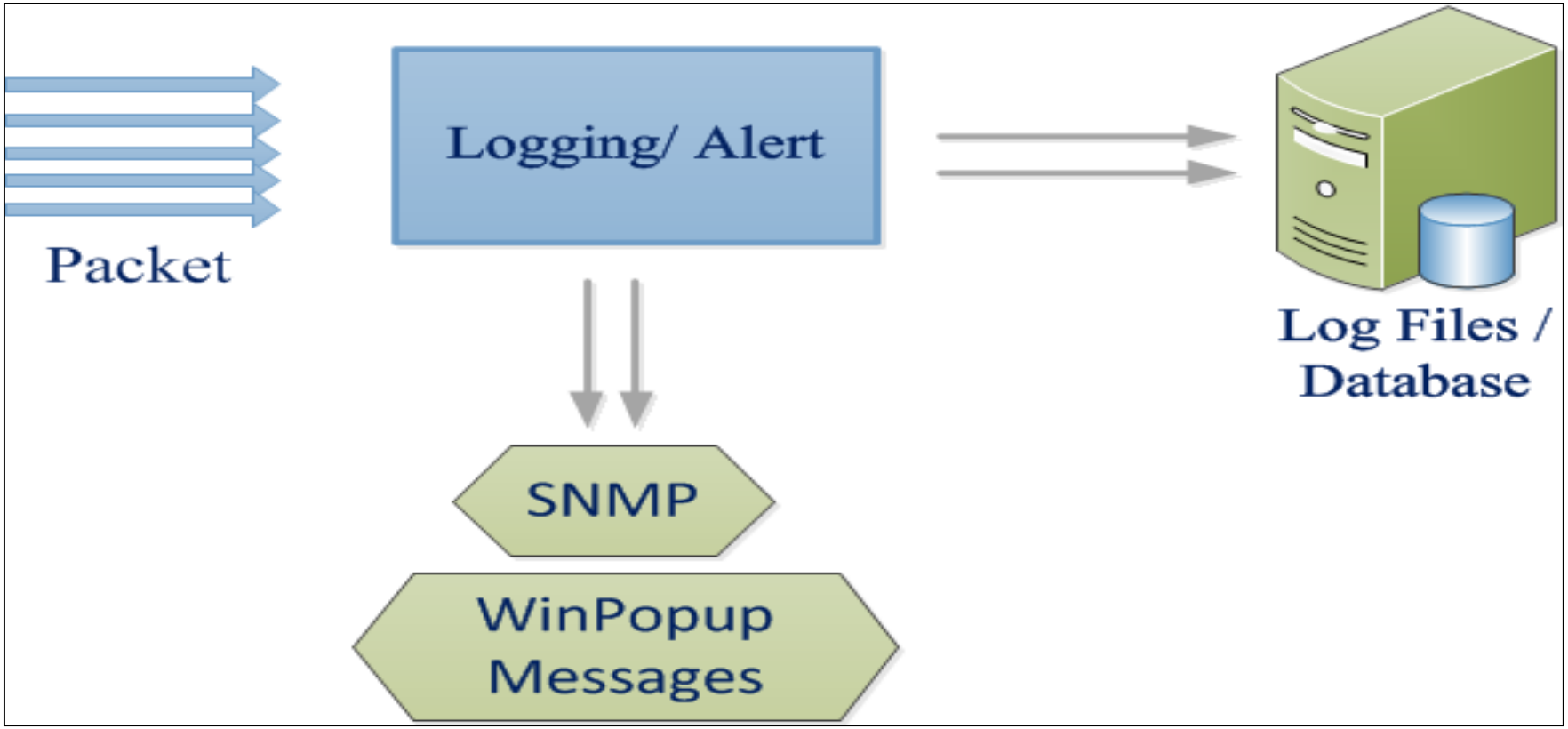
- Đây là modul quan trọng nhất
- Phát hiện dị thường (Dựa vào tập luật đã được định nghĩa) để đưa ra các cảnh báo;
- Nếu 1 gói tin bị phát hiện bởi nhiều luật thì nó sẽ đc xử lý theo luật được ưu tiên cao nhất
- Discard: Bỏ qua gói tin



Modul phát hiện

- Phát hiện dị thường trong header của gói tin
- Tách các phần của gói tin => áp dụng luật lên từng phần, dựa trên:
  - IP header
  - Header ở tầng giao vận: TCP, UDP
  - Header ở tầng ứng dụng: DNS header, HTTP header, FTP header, …
  - Nội dung gói tin

Module kết xuất thông tin



Rules

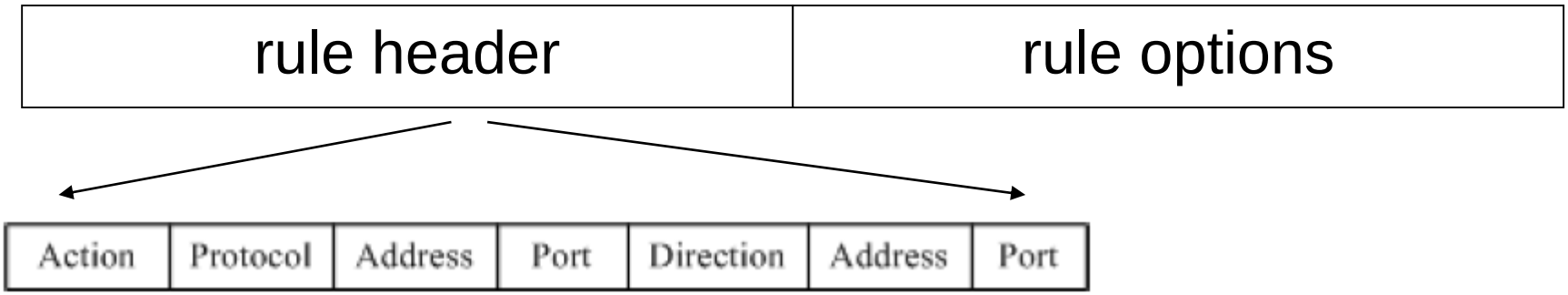
- Cấu trúc rules gồm 2 phần
  - Rule Header: Chứa các thông tin về hành động của luật sẽ thực hiện
  - Rule Option: chứa thông tin về cảnh báo, các thành phần của gói tin
- Rule Header

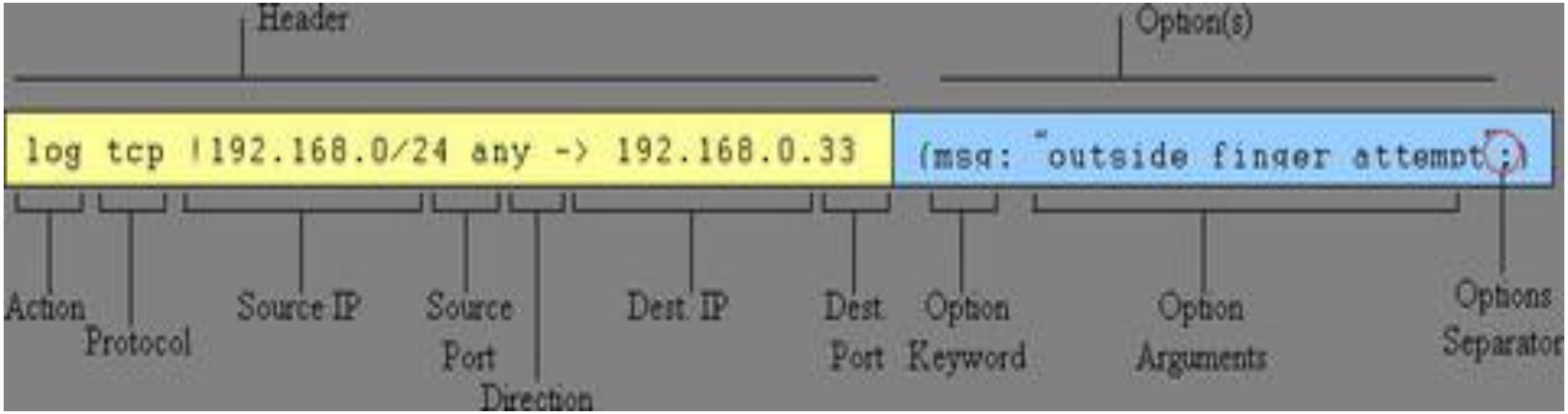
Action	Protocol	Address	Port	Direction	Address	Port

Rule Header

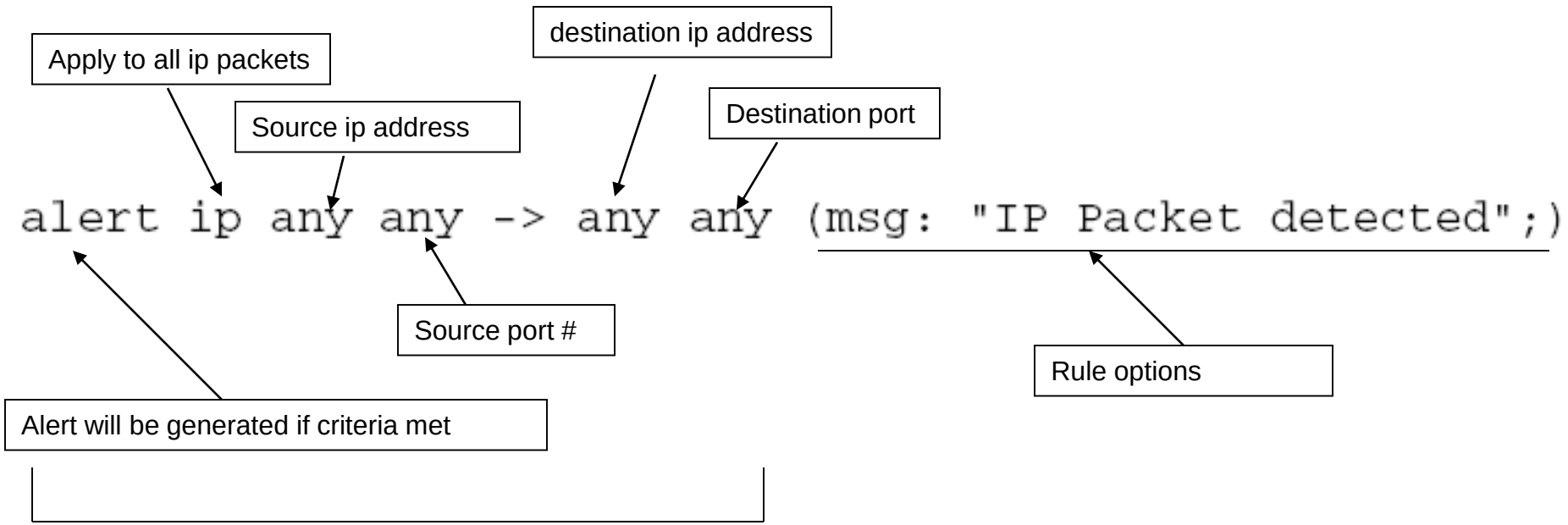
- Rule Action
  - Alert
  - Log
  - Pass
  - Drop
  - Activate
  - …
- Protocol (IP, ICMP, UDP, TCP)
- Source/Destination IP
- Port
- Điều hướng: -> (giám sát từ “trái qua phải”) ; <-; <> (giám sát cả client & SV)

Rules


rule header
rule options
Action
Protocol
Address
Port
Direction
Address
Port


Header
Option(s)
log tcp !192.168.0/24 any -> 192.168.0.33
(msg: "outside finger attempt";)
Action
Protocol
Source IP
Source Port
Direction
Dest IP
Dest Port
Option Keyword
Option Arguments
Options Separator

Ví dụ một số Rules




```
alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET any (msg:"TELNET
  Attempted SU from wrong group"; flow:
from_server,established; content:"to su root"; nocase;
  classtype:attempted-admin; sid:715; rev:6;)
```

- Cấu trúc threshold theo dõi hành vi: type threshold, track by_src/dst, count a, seconds b
- \x: câu lệnh cho biết chúng ta đang cung cấp nội dung dưới dạng mã Hexa, vd:
  - \x3d tương đương với dấu "=" trong bảng mã ascii
  - \x20 tương đương với khoảng trống
  - \x00 tương đương với null (giá trị rỗng)
- "^": nghĩa phủ định, ví dụ cho class: [^\x20\x3d\x00] nghĩa là PCRE match với các ký tự mà không có trong class trên
- Ví dụ tìm kiếm n lần/ký tự mà không có trong class trên: {n}
- pcre:"/[^A]{100}/" tìm kiếm 100 ký tự liên tiếp mà không có ký tự A
- Giám sát content: content: "|hexa|", ví dụ: content: "|47 45 54|" 47=G, 45=E, 54=T
  - (note: không nên lạm dụng quá nhiều option content trong 1 rule vì hệ thống xử lý khó khăn)
  - Giá trị content dưới dạng giá trị Hexa thì nằm trong dấu ||

- Một số tiêu chí để tìm kiếm trong content
  - offset keyword (bắt đầu tìm kiếm sau n bytes đầu tiên của Payload)
  - depth keyword (chỉ tìm kiếm n bytes đầu tiên của Payload). Giá trị n phải có độ dài lớn hơn hoặc bằng giá trị keyword định tìm kiếm. Giá trị n nằm trong đoạn [1,65535]
  - nocase keyword (không phục thuộc chữ hoa, chữ thường)
- VD offset keyword
  - Content:"A"; offset: n di chuyển vào n bytes của payload và tìm kiếm "A"
- VD depth keyword
  - Content:"A"; offset:n tìm kiếm "A" với n bytes tiếp theo của payload
- VD kết hợp depth và offset:
  - Content: "A"; offset n; depth m di chuyển n bytes của payload và tìm kiếm "A" với m bytes tiếp theo

- False Positive
- False Nagative
- True Positive
- True Nagative

Ví dụ một số Rules

❖ Phát hiện quét mạng với SYN/FIN :

- `Alert tcp any any -> 10.0.10.0/24 any (msg: "SYNFIN => scan detected"; flags: SF;)`

❖ Phát hiện Dictionary attack (SSH)

- `alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:“Co the dang tan cong dò tìm SSH!"; flags: S+; threshold: type both, track by_src, count 5, seconds 30; sid:10000002; rev: 1;)`
- Cấu trúc threshold theo dõi hành vi: type threshold, track by_src/dst, count a, seconds b

❖ Phát hiện tấn công SQL injection

- `alert tcp any any -> $HOME_NET any (msg:”SQL Injection Attempt”;pcre:”/w*((%27)|(‘))((%6F)|o|(%4F))((%72)|r|(%52))/ix”; sid:1000017; rev:1;)`

Ví dụ một số Rules

PCRE: cho phép tìm kiếm nhiều biến thể của nội dung

(%27)|’ : tìm kiếm dấu nháy đơn

(): nhóm các ký tự

❖ Phát hiện tấn công XSS

- `alert tcp any any -> any 80 (msg:"Tan cong Cross-site scripting"; flow:to_server, established; pcre:"/((\%3C)|<)((\%2F)|\/)*[a-z0-9\%]+((\%3E)|>)/i"; classtype:Web-application-attack; sid:9000; rev:5;)`

❖ Giám sát tải mã độc về máy victim:

- `alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Tai hotgirl.exe ve may"; flow:established,to_server; content:"GET"; http_method; content: “/hotgirl.exe"; http_uri; classtype:trojan-activity; sid:10000004; rev:1;)`

Ví dụ một số Rules

❖ Cảnh báo tấn công DoS - SYN Food

hping3 -c 100 -d 50 -S -w 64 -p 139 --flood 208.100.26.141

alert tcp any any -> any any (msg:"Co the dang bi DoS attack!";flags: SA; flow:stateless; threshold: type both, track by_src, count 70, seconds 10; sid:1000005;rev:1;)
flow:stateless => không quan tâm đến kết nối có thành công hay không

❖ alert tcp any any -> any any (msg:”SSN in Clear Text”; pcre:”/[0-9]{3,3}-[0-9]{2,2}-[0-9]{4,4}/”; sid:1000016; rev:1;)

- []: chỉ ra phạm vi số cần tìm
- {m,n}: khớp ít nhất m lần nhưng không quá n lần
- -: thoát khỏi dấu “–” để sẽ được đưa vào phần tìm kiếm

Một số rule mặc định trên SNORT

- bad-traffic.rules exploit.rules scan.rules
- finger.rules ftp.rules telnet.rules
- smtp.rules rpc.rules rservices.rules
- dos.rules ddos.rules dns.rules
- tftp.rules web-cgi.rules web-coldfusion.rules
- web-frontpage.rules web-iis.rules web-misc.rules
- web-attacks.rules sql.rules x11.rules
- icmp.rules netbios.rules misc.rules
- backdoor.rules shellcode.rules policy.rules
- porn.rules info.rules icmp-info.rules
- virus.rules local.rules attack-responses.rules

Rule Option

HƯỚNG DẪN CÀI ĐẶT SNORT TRÊN PFSENSE

HƯỚNG DẪN CÀI ĐẶT SNORT TRÊN PFSENSE

❖ Cài đặt snort

- System -> Package manager -> tìm snort -> install
- Chọn Tab Service -> snort
- Đăng ký **Oinkmaster Code**
  - Vào Global Settings
  - Enable Snort VRT
  - Sign Up for a free Registered User Rule Account
  - Đăng ký **Oinkmaster Code**
    - Chọn phần hiển thị email (click lên phần hiển thị user) đăng ký ở góc phải màn hình. Phía góc trái sẽ hiện Oinkmaster Code

HƯỚNG DẪN CÀI ĐẶT SNORT TRÊN PFSENSE

- Chọn Tab Updates
- Chọn Update Rules

❖ Chọn Snort interfaces

❖ Chọn iface rules

❖ Chọn iface categories => chọn cấu hình IPS

❖ WAN Settings/ Intrusion Detection System => Checksum

Tham khảo các rules:

- https://github.com/eldondev/Snort/tree/master/rules
- http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node36.html
- http://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm#nocase
- https://www.sbarjatiya.com/notes_wiki/index.php/Snort_general_rule_options
- https://doc.pfsense.org/index.php/Setup_Snort_Package
- https://paginas.fe.up.pt/~mgi98020/pgr/writing_snort_rules.htm#dsize
- https://asecuritysite.com/forensics/snort?fname=nmap.pcap&rulesname=rulesportscan.rules