

CƠ SỞ AN TOÀN THÔNG TIN

Bài 9. An toàn mạng máy tính

Tài liệu tham khảo

1. Lê Đình Thích, Hoàng Sỹ Tương, **An toàn mạng máy tính**, Học viện KTMM, 2013
2. Whitman, Mattord, **Principles of Information Security** (5e), Cengage Learning, 2014
3. Mark Ciampa, **Security+ Guide to Network Security Fundamentals**, Cengage Learning, 2009
4. Anonymous, **Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network**

1

Hiểm họa an toàn
mạng máy tính

2

Các hình thức tấn
công mạng máy tính

3

Giải pháp đảm bảo an
toàn mạng máy tính

1

Hiểm họa an toàn
mạng máy tính

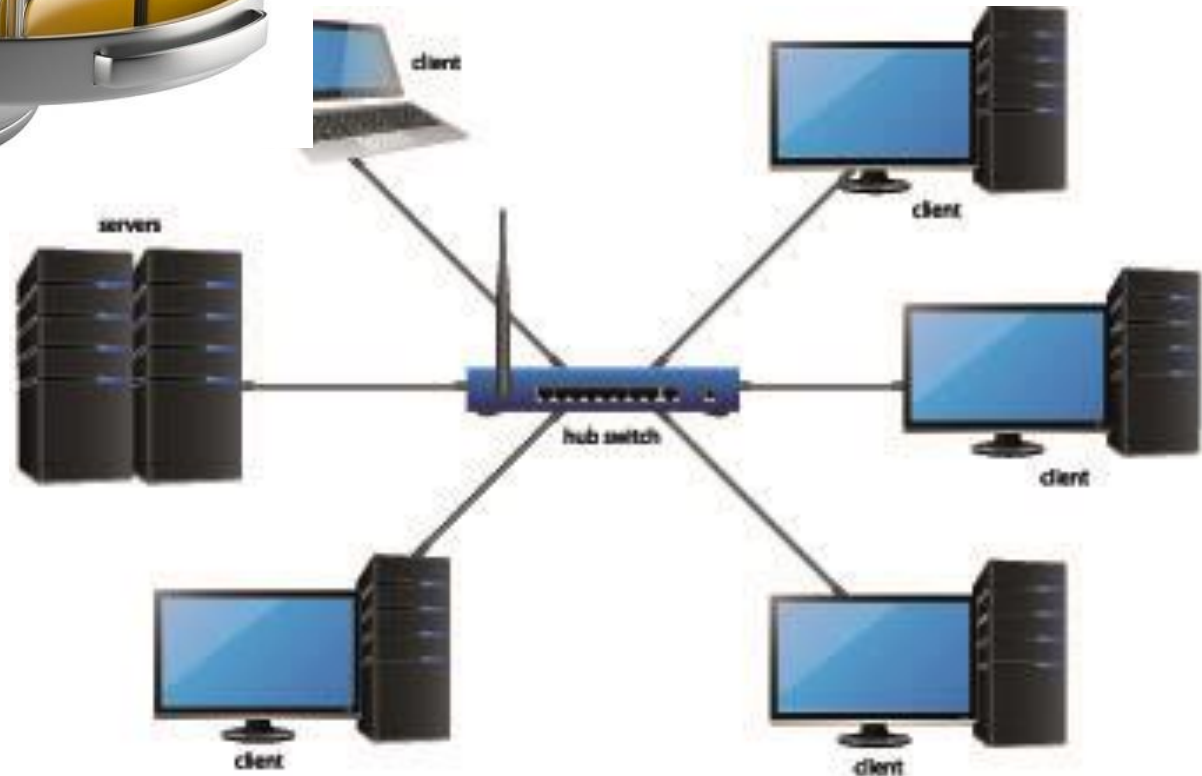
2

Các hình thức tấn
công mạng máy tính

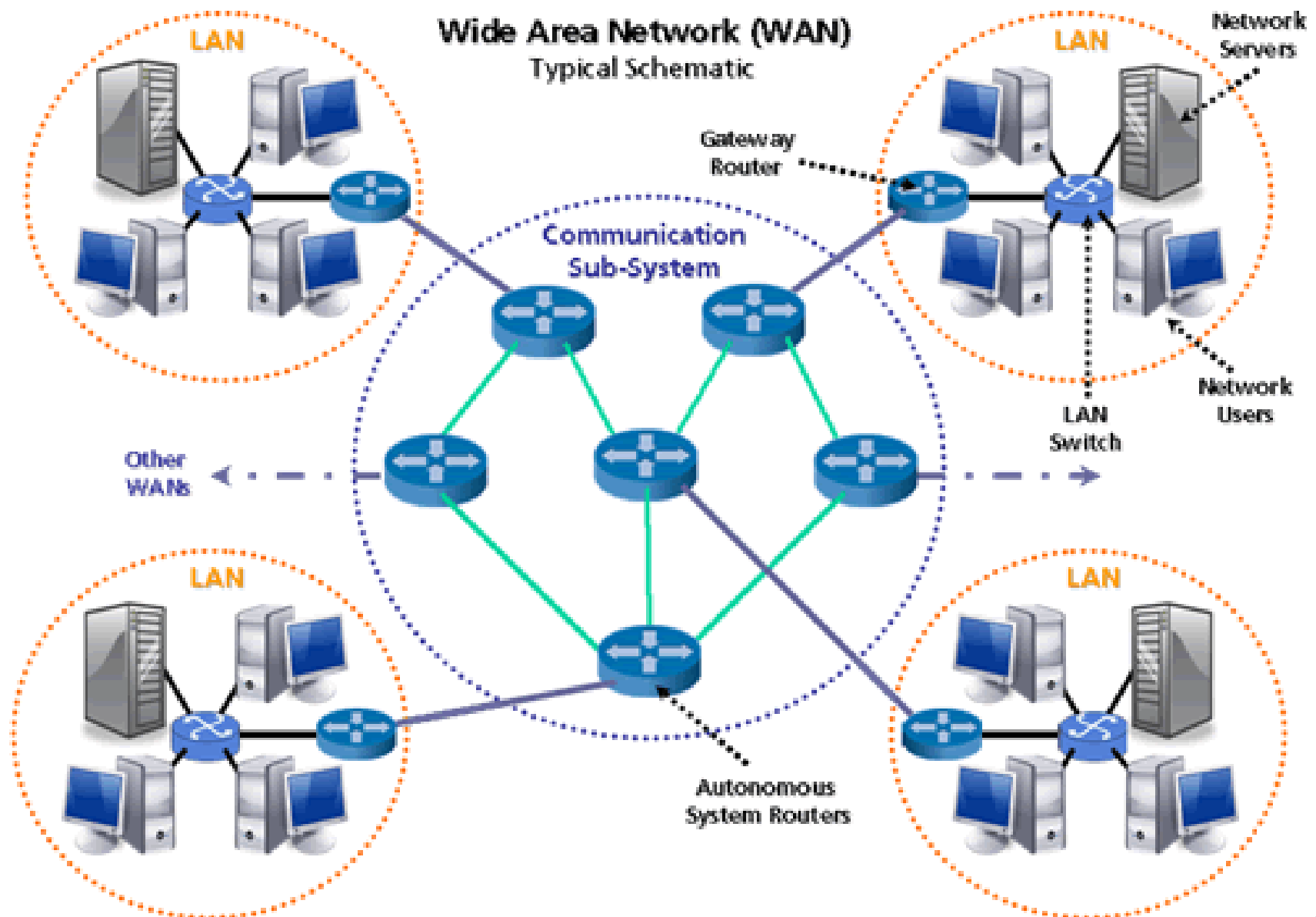
3

Giải pháp đảm bảo an
toàn mạng máy tính

Mạng máy tính - LAN



Mạng máy tính - WAN



Mạng máy tính - Internet



Khái niệm hiểm họa

- **Hiểm họa ATTT** là những **khả năng tác động** lên TT, HTTT dẫn tới sự thay đổi, hư hại, sao chép, sự ngăn chặn tiếp cận tới TT; tới sự phá huỷ hoặc sự ngừng trệ hoạt động của vật mang TT.
- **Ví dụ:** virus, động đất, tấn công mạng

Khái niệm tấn công

- ❑ Hiểm họa = Sự vật, hiện tượng tự nhiên + Hành vi vô ý + Hành vi cố ý
- ❑ **Tấn công HTTT** là hành vi có chủ ý của con người nhằm phá vỡ tính an toàn của thông tin và HTTT
- ❑ Tấn công \subset Hiểm họa
- ❑ Phân loại: rất không thống nhất

Phân loại tấn công theo Microsoft

1. Eavesdropping
2. Data Modification
3. Identity Spoofing (IP Address Spoofing)
4. Password-Based Attacks
5. Denial-of-Service Attack
6. Man-in-the-Middle Attack
7. Compromised-Key Attack
8. Sniffer Attack
9. Application-Layer Attack

Phân loại theo CompTIA

1. Denial of Service (DoS)
2. Spoofing
3. Man-in-the-Middle
4. Replay

Phân loại đề xuất (1/2)

□ Tấn công từ trong hệ thống

- Leo thang đặc quyền
- Chiếm quyền điều khiển
- Truy cập trái phép thông tin
- Sao chép, phát tán trái phép thông tin được tiếp cận

Phân loại đề xuất (2/2)

❑ Tấn công từ ngoài hệ thống

- Thăm dò hệ thống
- Chặn thu thông tin
- Tấn công ứng dụng, dịch vụ web
- Tấn công ứng dụng, dịch vụ mạng
- Tấn công ứng dụng cục bộ
- Tấn công DoS, DDoS

1

Hiểm họa an toàn
mạng máy tính

2

Tấn công mạng máy
tính điển hình

3

Công nghệ an toàn
mạng máy tính

Tấn công mạng

- 1 Tấn công sniffing
- 2 Tấn công DoS
- 3 Tấn công DDoS
- 4 Tấn công giao thức mạng
- 5 Tấn công khác

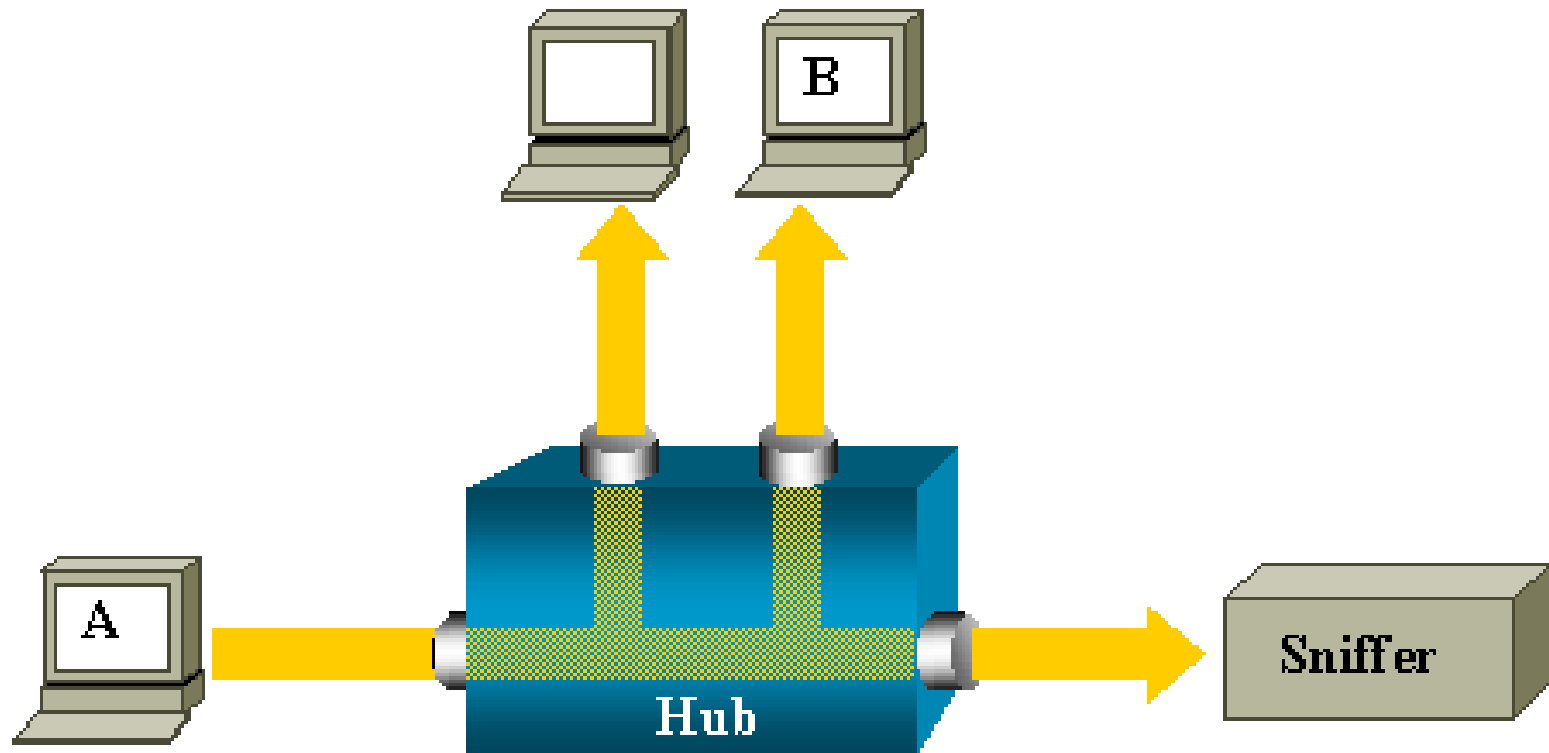
Tấn công chặn bắt thông tin

TẤN CÔNG CHẶN BẮT THÔNG TIN

- Lắng nghe thông tin trên đường truyền
- Điều hướng thông tin đi qua nút nhất định

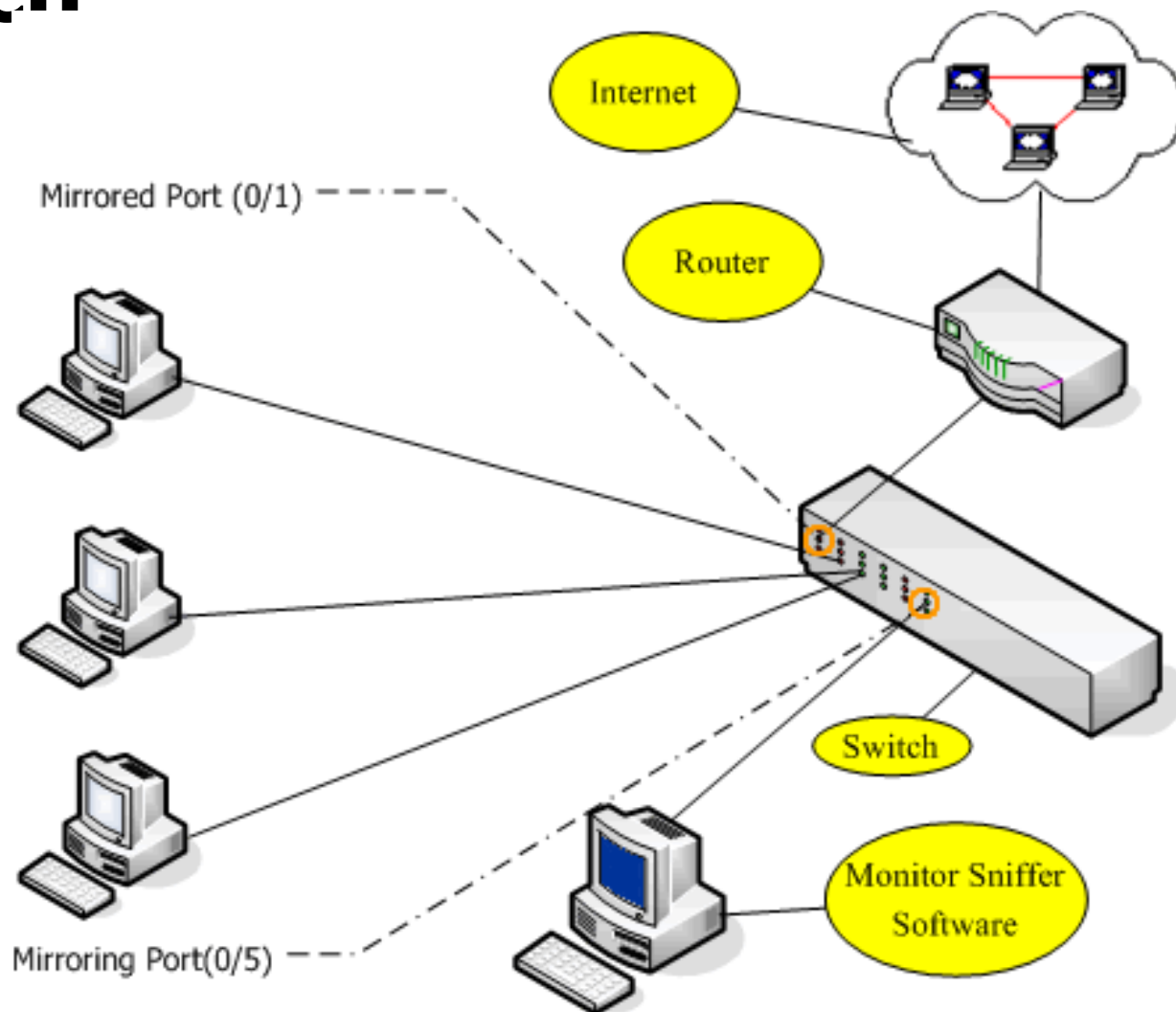
Tấn công chặn bắt thông tin

❖ Lắng nghe thông tin qua Hub



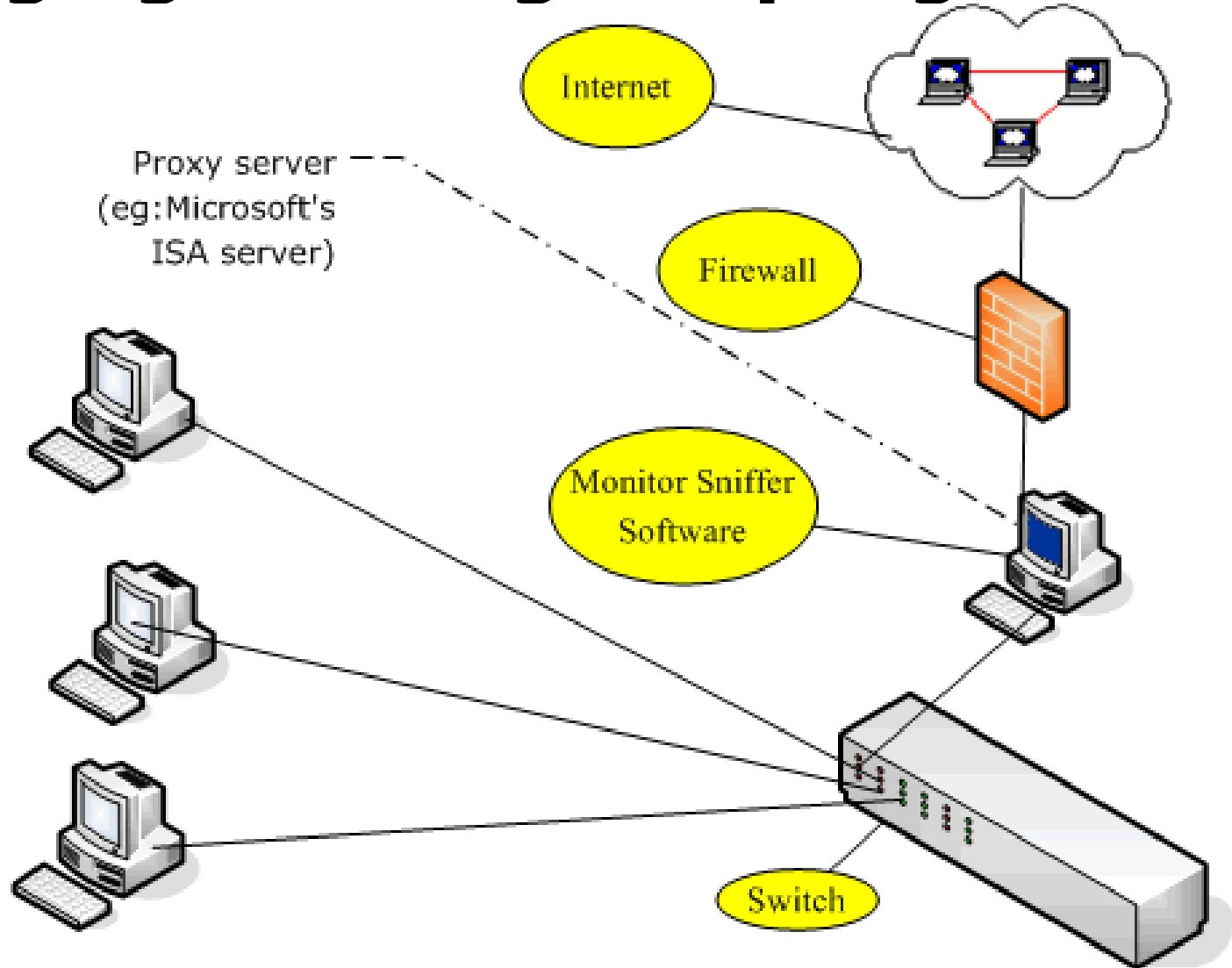
Tấn công chặn bắt thông tin

❖ Lắng nghe thông tin qua Span port trên switch



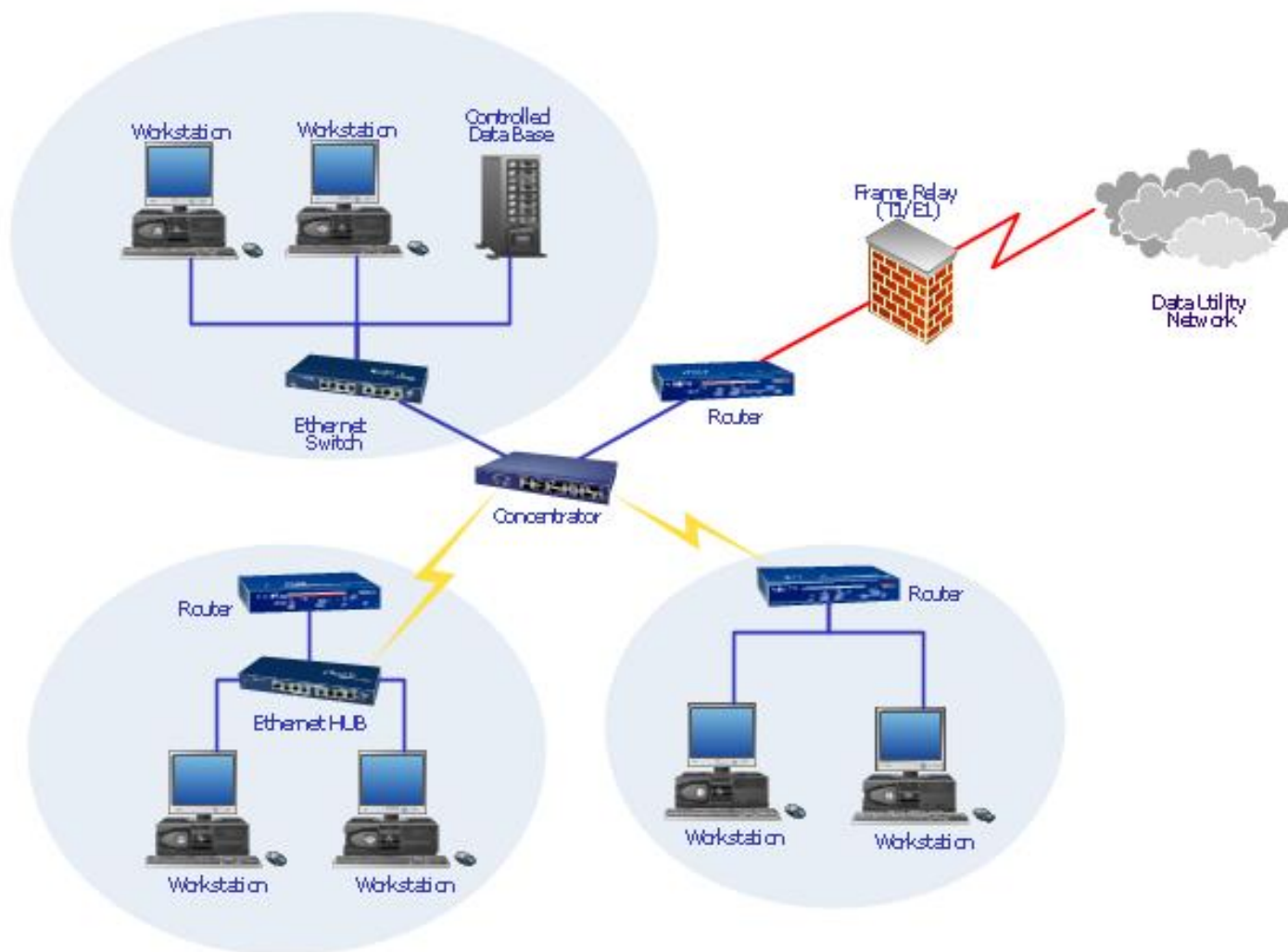
Tấn công chặn bắt thông tin

❖ Lắng nghe thông tin qua gateway



Tấn công chặn bắt thông tin

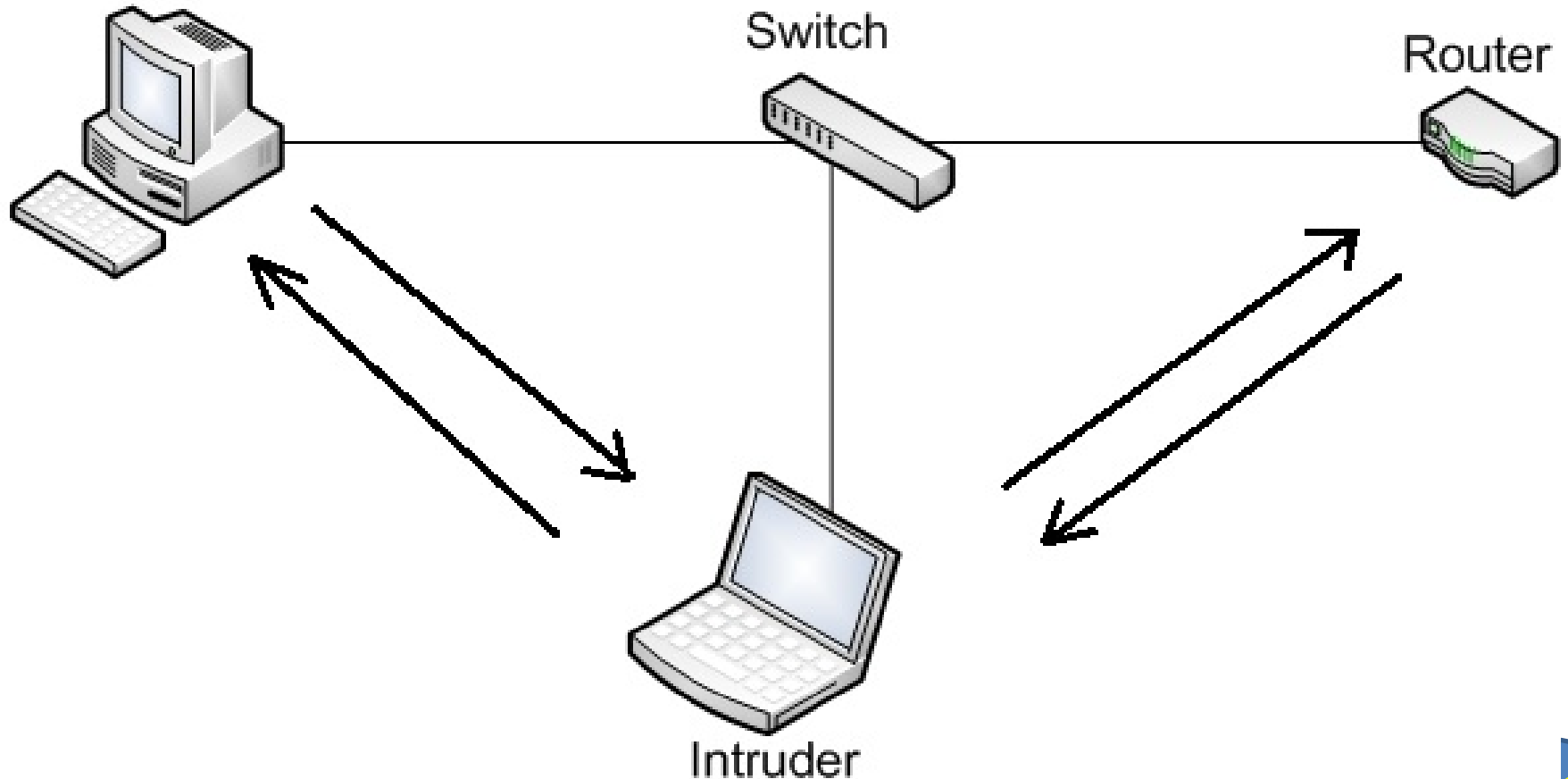
❖ Lắng nghe thông tin qua nút trung gian



Tấn công chặn bắt thông tin

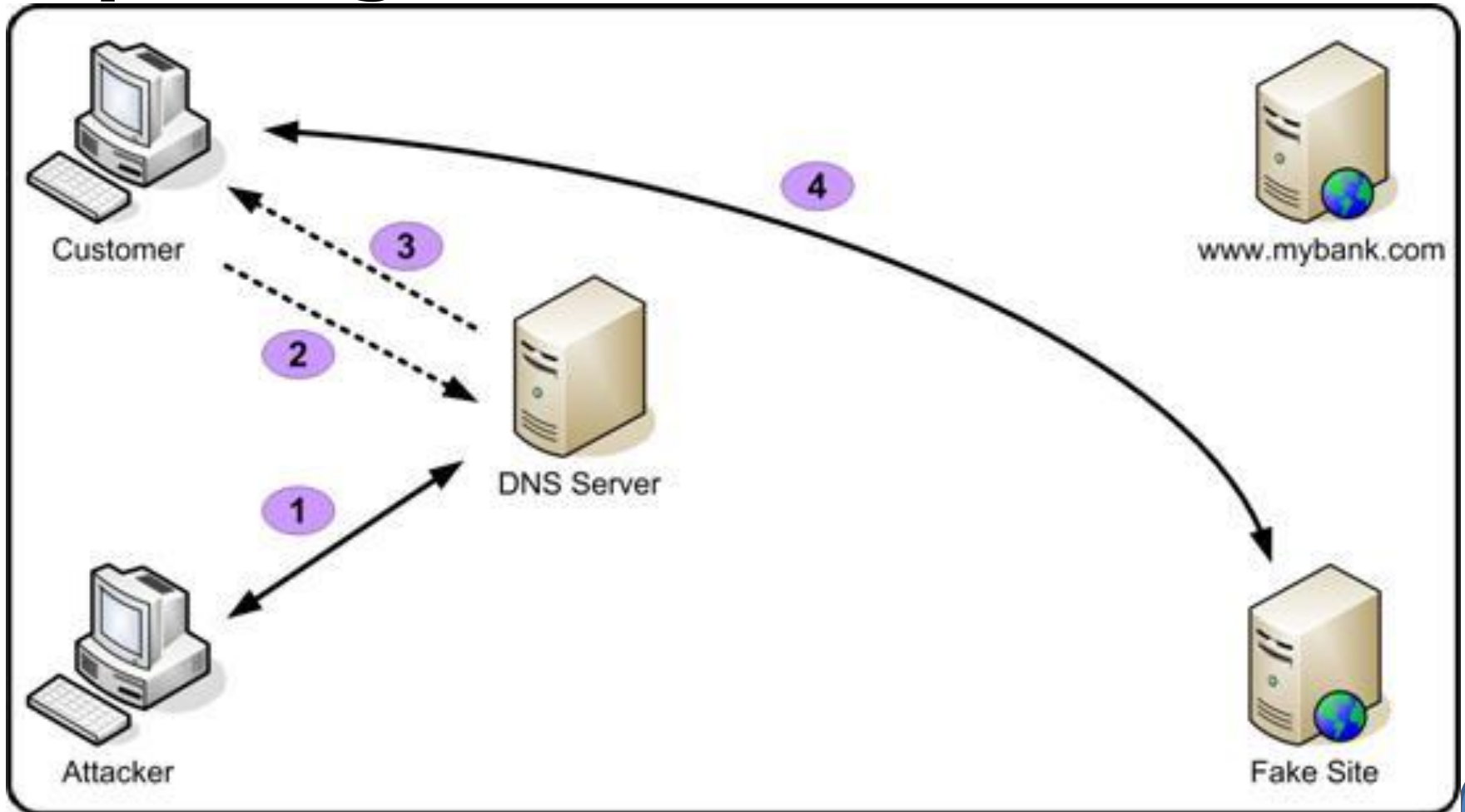
❖ Chặn bắt thông tin dùng ARP-poisoning

Target Computer



Tấn công chặn bắt thông tin

❖ Chặn bắt thông tin dùng DNS-Spoofing



Tấn công chặn bắt thông tin

□ Công cụ

- WireShark
- Ettercap
- Social Engineering Toolkit (SET)
- +++

Tấn công mạng

- 1 Tấn công sniffing
- 2 Tấn công DoS
- 3 Tấn công DDoS
- 4 Tấn công giao thức mạng
- 5 Tấn công khác

Tấn công từ chối dịch vụ

- ❑ Denial of Service (NOT “Deny”)
- ❑ Là tấn công nhằm phá vỡ tính khả dụng của thông tin, hệ thống thông tin
- ❑ Phân loại
 - Băng thông thấp
 - Băng thông cao
 - Đơn lẻ
 - Phân tán

Tấn công DoS

❑ Bảng thông thấp

- Ping of Death
- Teardrop
- +++

❑ Bảng thông cao (máy đơn)

- SYN flood
- Ping flood
- HTTP POST DoS
- +++

Local DoS attacks

❑ File Locking Local Denial of Service

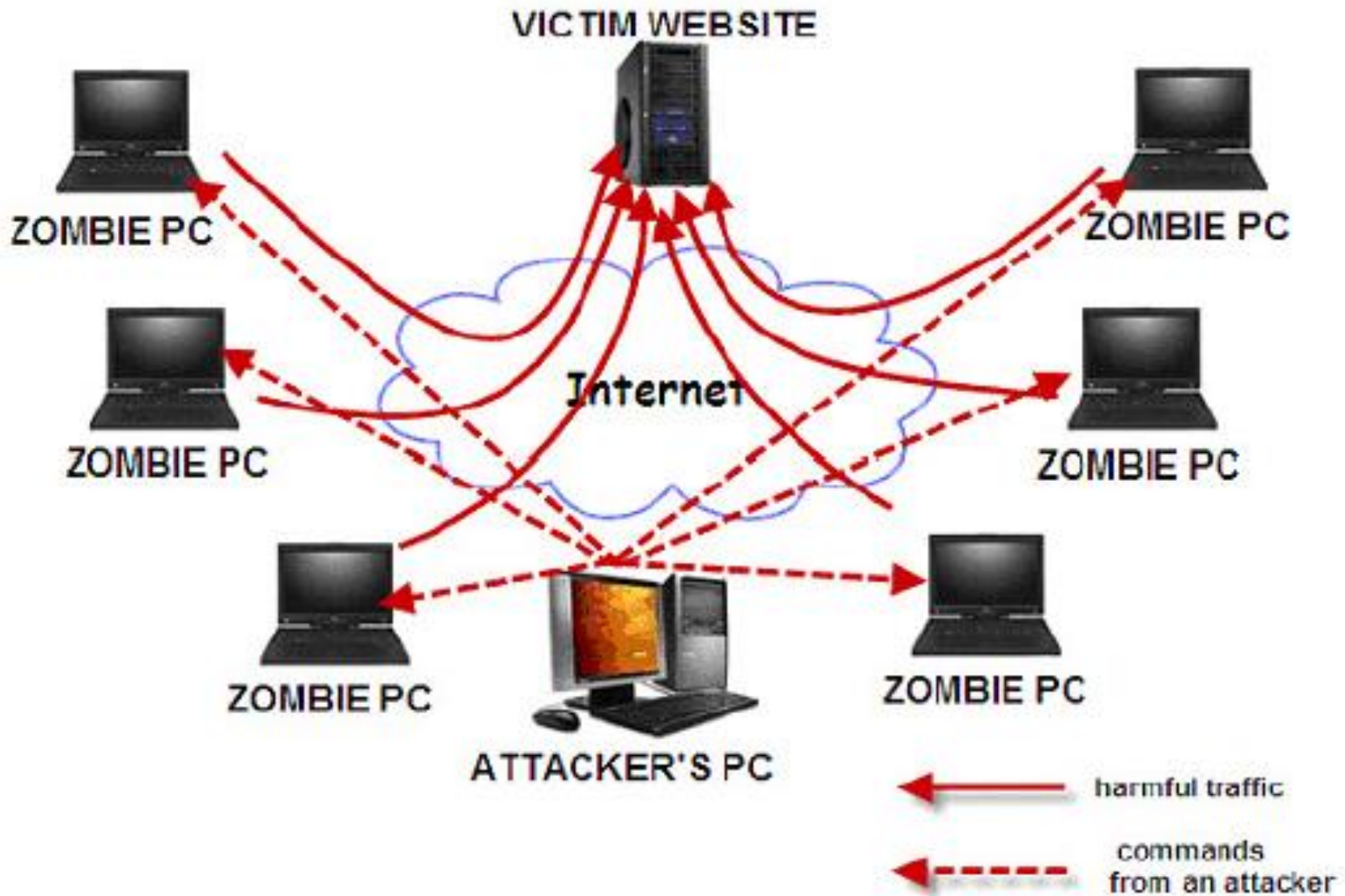
- Hàm chống xung đột truy cập file: flock(), fcntl()
- Ngăn chặn việc truy cập file trong thời gian tùy ý bởi bất kỳ tiến trình, người dùng nào

Tấn công mạng

- 1 Tấn công sniffing
- 2 Tấn công DoS
- 3 Tấn công DDoS
- 4 Tấn công giao thức mạng
- 5 Tấn công khác

Tấn công DDoS

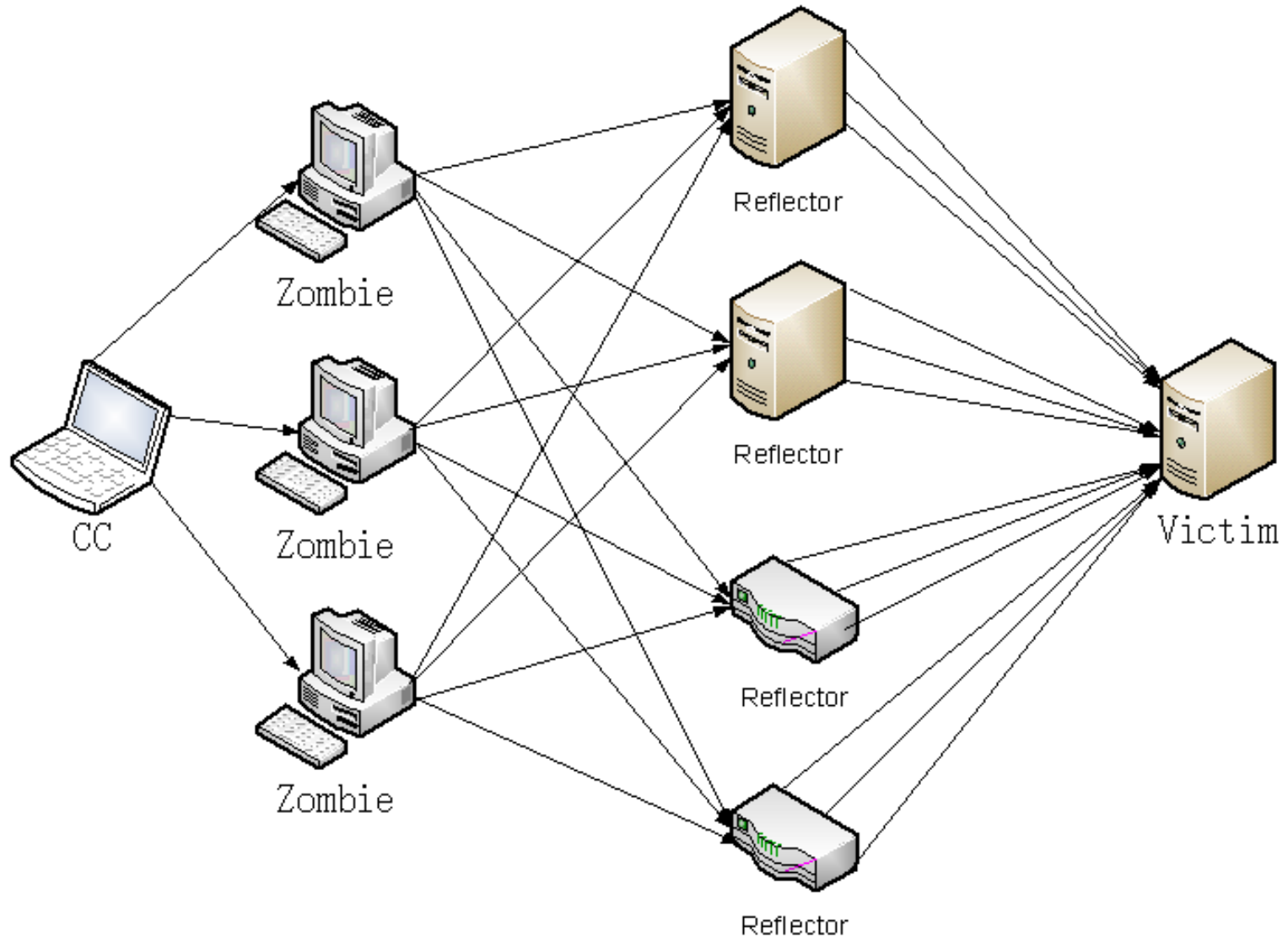
Tấn công từ chối dịch vụ phân tán



Tấn công DDoS

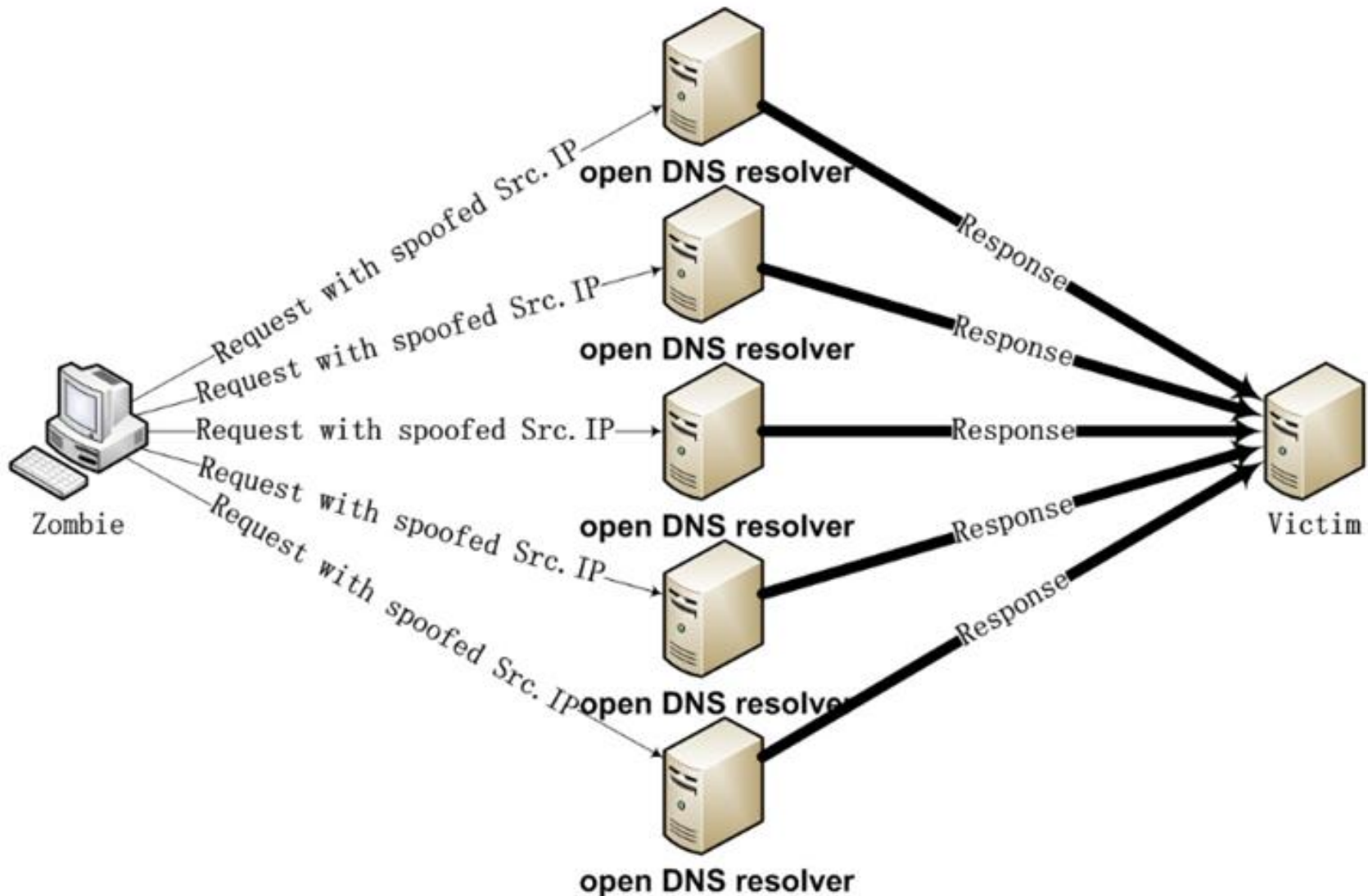
Tấn công DDoS

Reflected/Spoofed DDoS Attack



Tấn công DDoS

DNS Amplification DDoS Attack



Tấn công mạng

- 1 Tấn công sniffing
- 2 Tấn công DoS
- 3 Tấn công DDoS
- 4 Tấn công giao thức mạng
- 5 Tấn công khác

Tấn công giao thức mạng

❑ Tấn công giao thức xác thực

- WPA/WPS pincode bruteforce

❑ Tấn công giao thức bảo mật dữ liệu

- CBC Padding Oracle

❑ Tấn công giao thức khác

- Heartbleed



Tấn công mạng

- 1 Tấn công sniffing
- 2 Tấn công DoS
- 3 Tấn công DDoS
- 4 Tấn công giao thức mạng
- 5 Tấn công khác

Tấn công mạng khác

- Tấn công ứng dụng web
- Chiếm quyền điều khiển hệ thống
- Lừa đảo
- +++

1

Hiểm họa an toàn
mạng máy tính

2

Tấn công mạng máy
tính điển hình

3

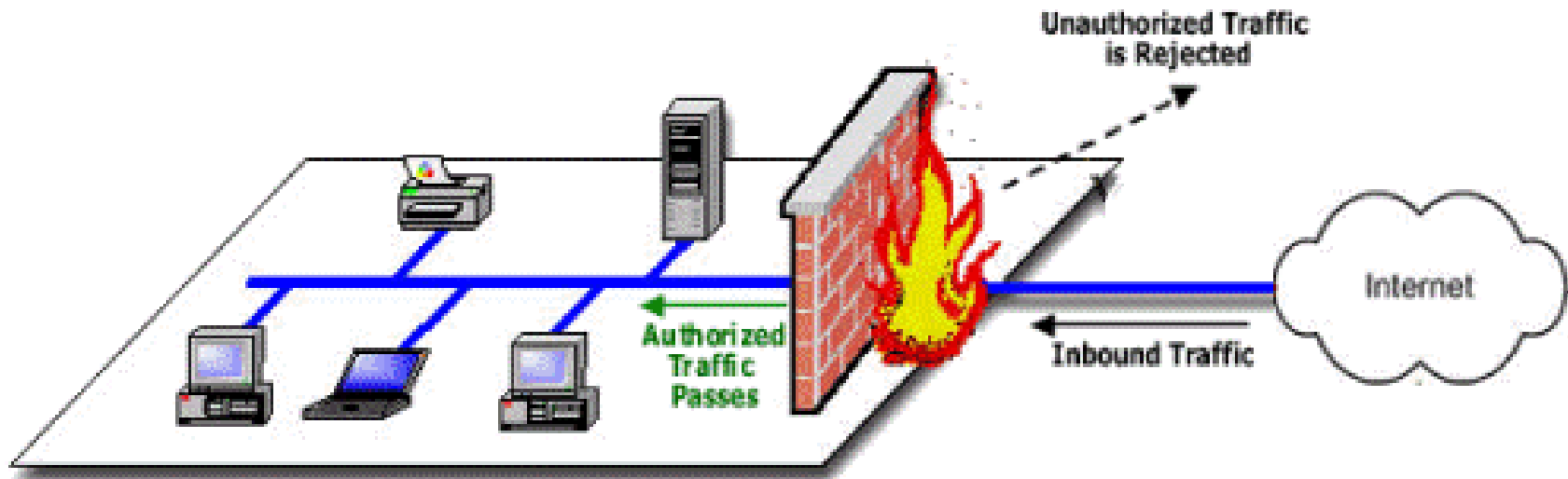
Công nghệ an toàn
mạng máy tính

Công nghệ an toàn mạng

- Chống mã độc và thư rác (Antivirus, Antispam)
- Tường lửa (Firewall)
- Phát hiện và ngăn chặn xâm nhập (IDPS)
- Hệ thống bẫy (Honeypot, Honeyynet)
- Mạng riêng ảo (VPN)
- Chống rò rỉ dữ liệu (DLP)
- Giám sát an toàn mạng (SIEM)

Tường lửa (Firewall)

❑ **Tường lửa** (Firewall) là hệ thống ngăn chặn việc truy nhập trái phép từ bên ngoài vào mạng cũng như những kết nối không hợp lệ từ bên trong ra.



Phân loại tường lửa

□ Theo vị trí

- Tường lửa cá nhân
- Tường lửa mạng

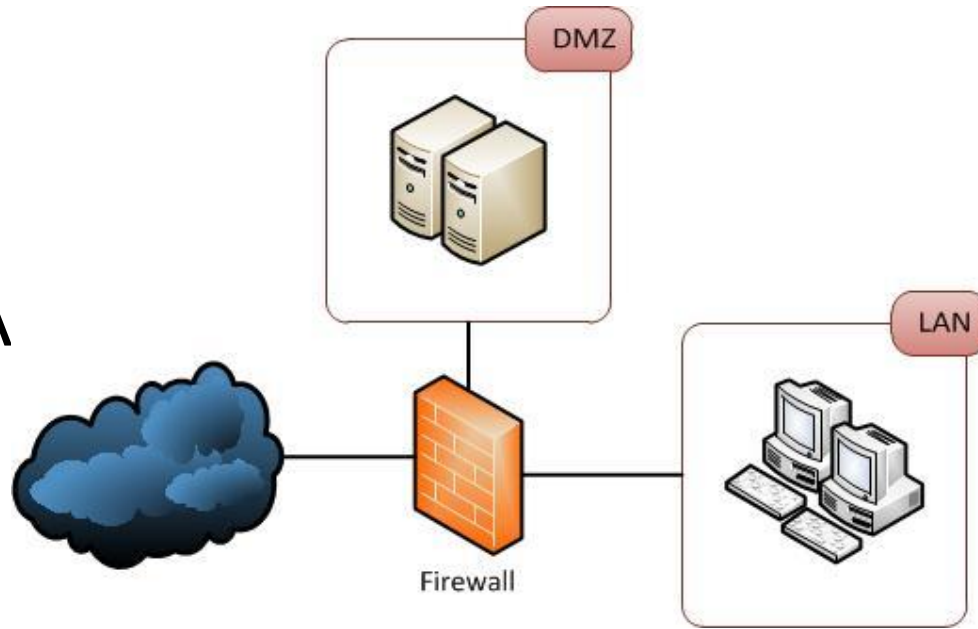
□ Theo khả năng xử lý

- Tầng mạng: packet filter
- Tầng giao vận: stateful packet inspection
- Tầng ứng dụng: application level firewall

Tường lửa mạng và Tường lửa cá nhân

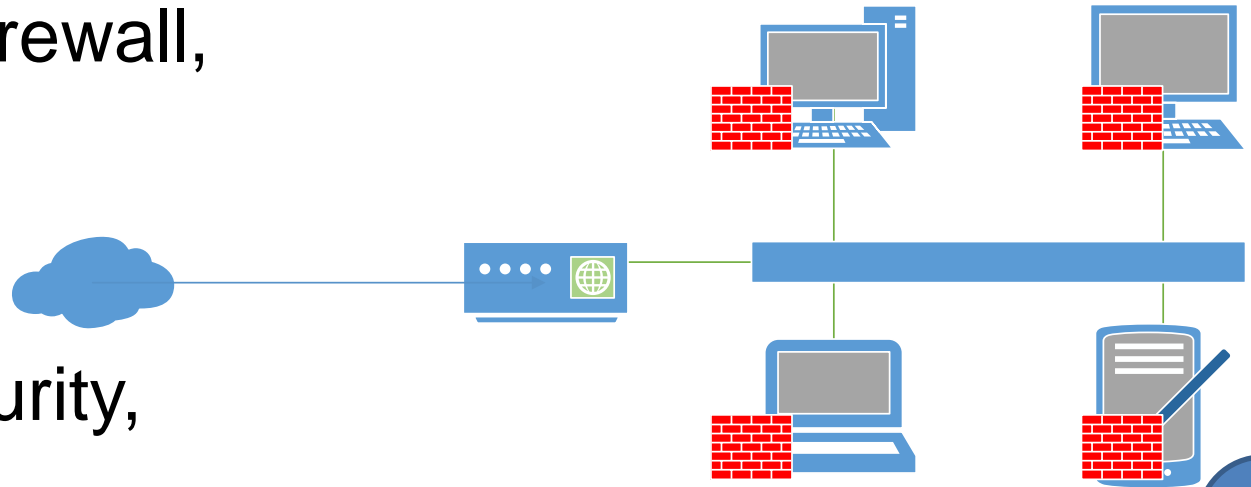
Cisco ASA,
Checkpoint,
Microsoft ISA

...

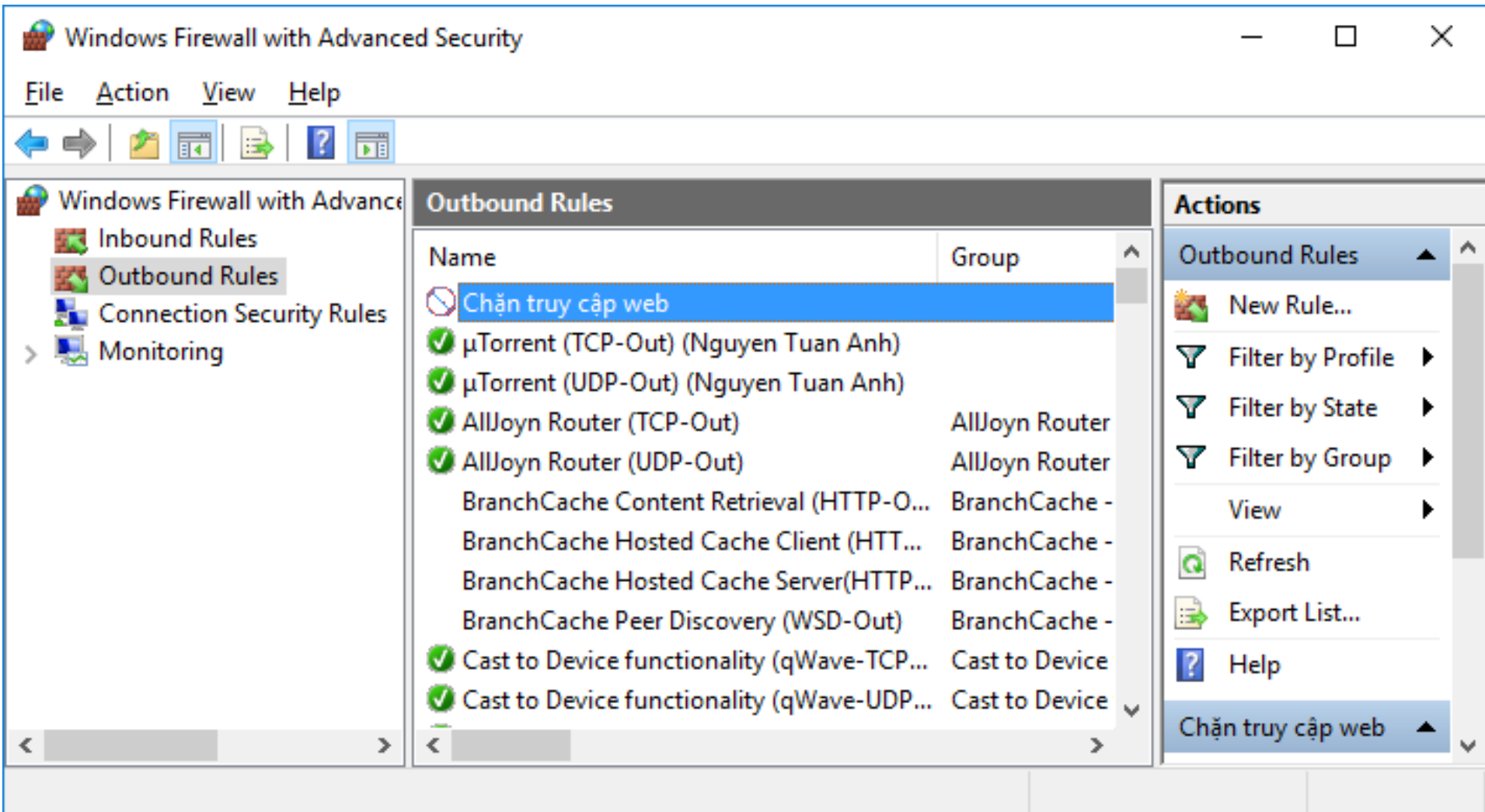


MS Windows Firewall,
iptables,
Comodo,
ZoneAlarm,
*** Internet Security,

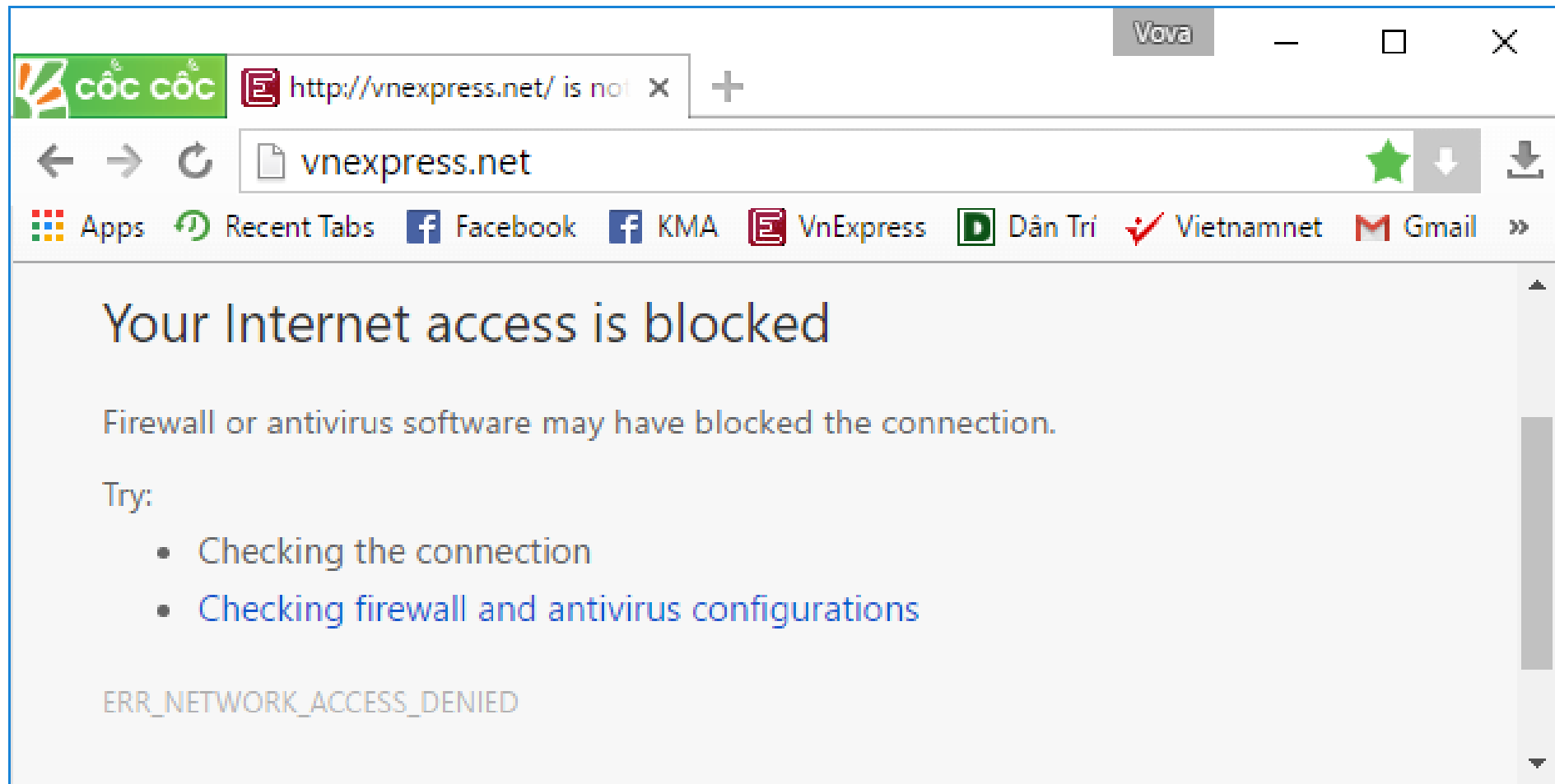
.....



Windows Personal Firewall



Windows Personal Firewall

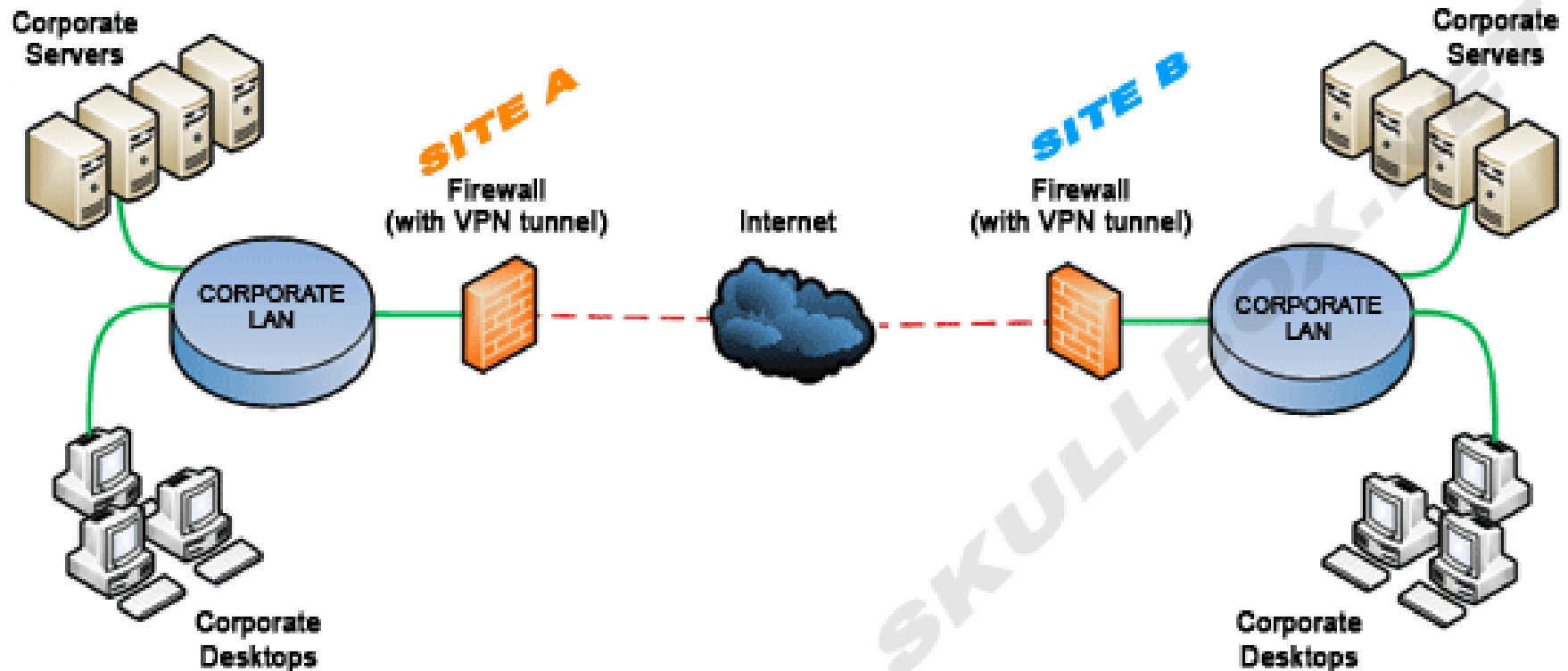


Mạng riêng ảo

- ❑ Virtual Private Network (VPN)
- ❑ **Mạng riêng ảo** là một mạng dữ liệu riêng được thiết lập qua một hạ tầng mạng dùng chung, trong đó tính riêng tư của dữ liệu được đảm bảo bằng cách sử dụng một giao thức tạo đường hầm và các cơ chế an toàn khác.

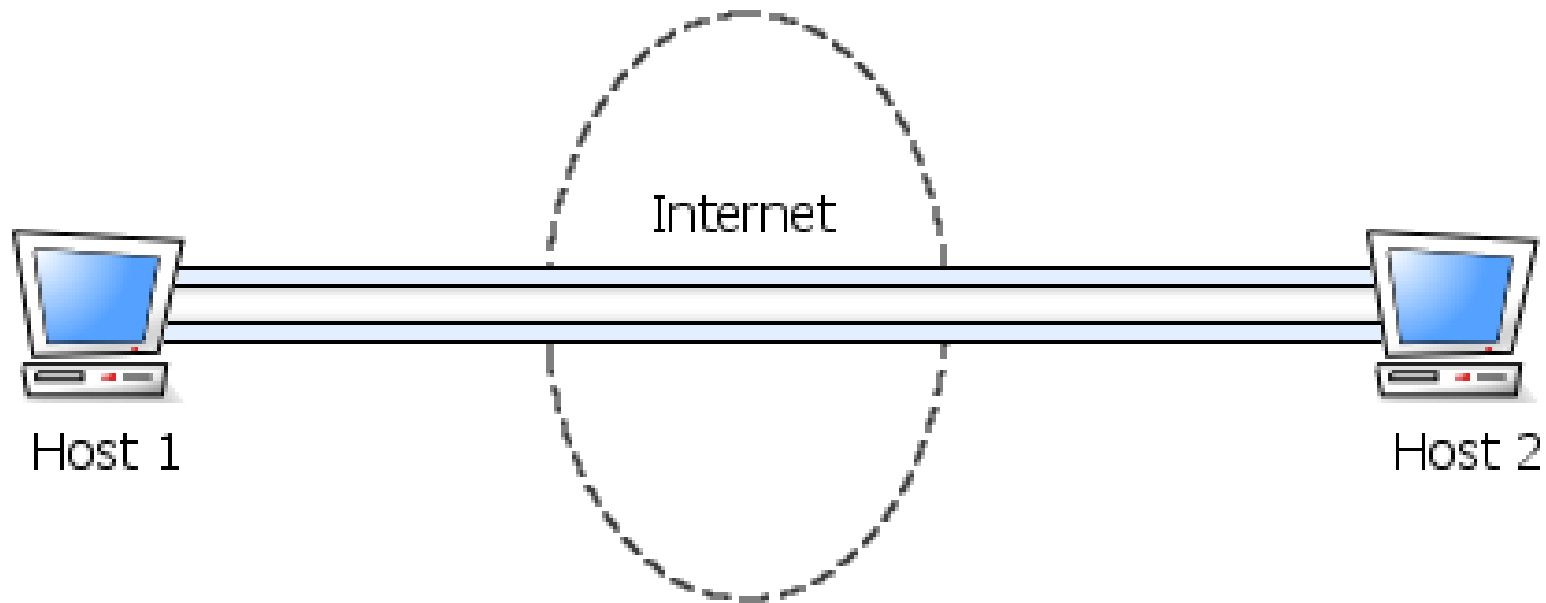
VPN

□ Site-to-Site (Tunnel Mode) VPN

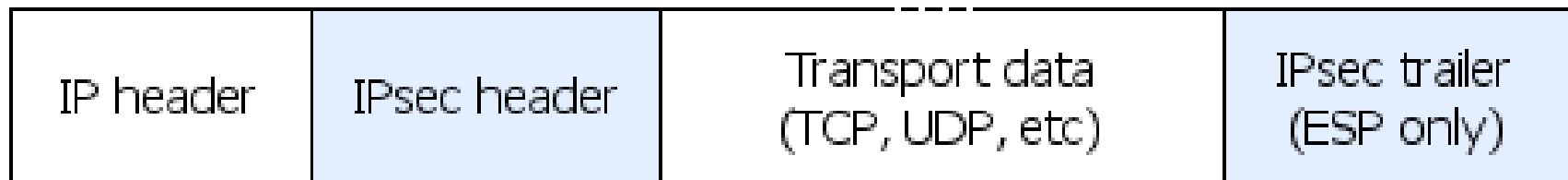


VPN

❑ Point-to-Point (Transport Mode) VPN

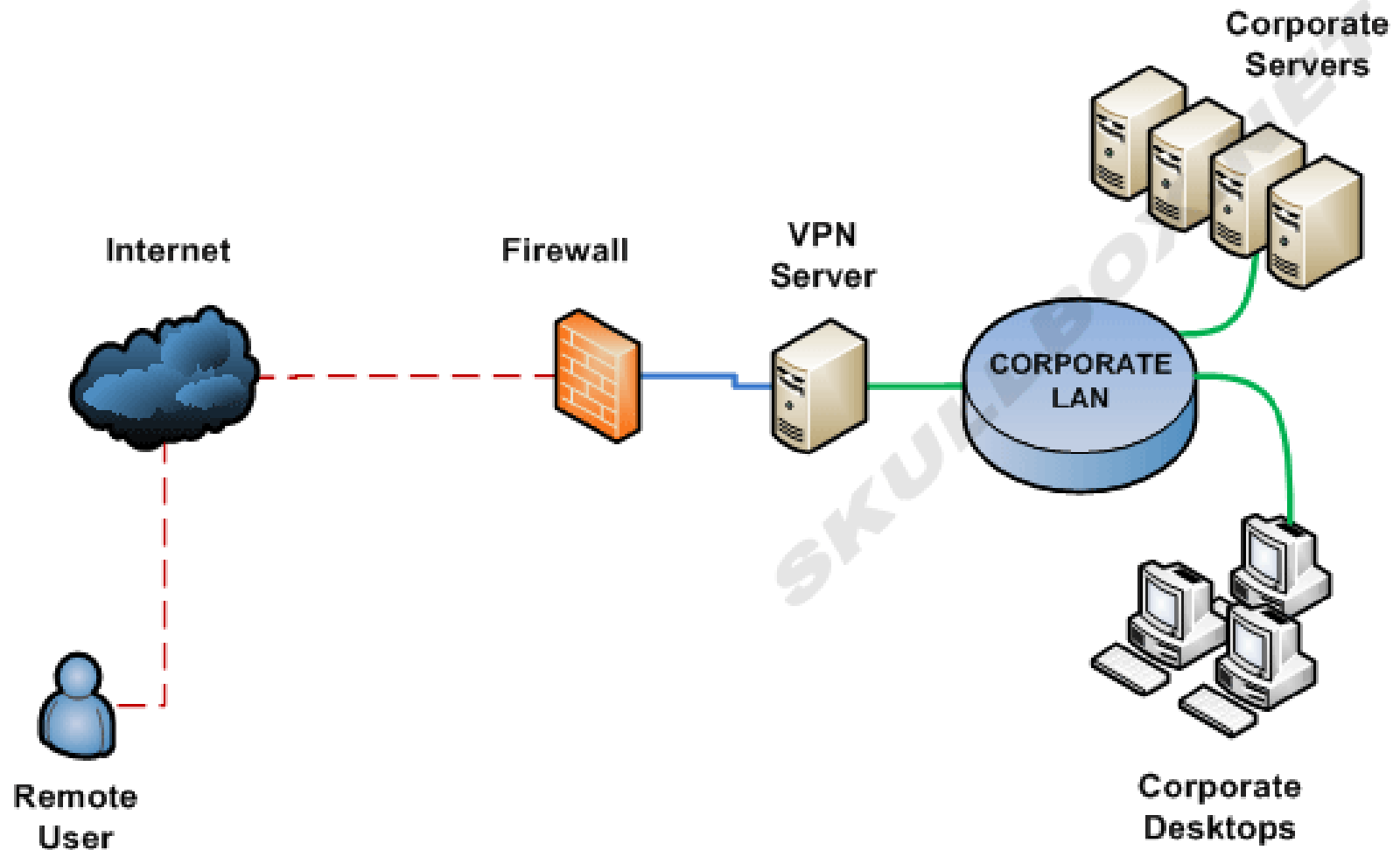


Transport-mode encapsulation:



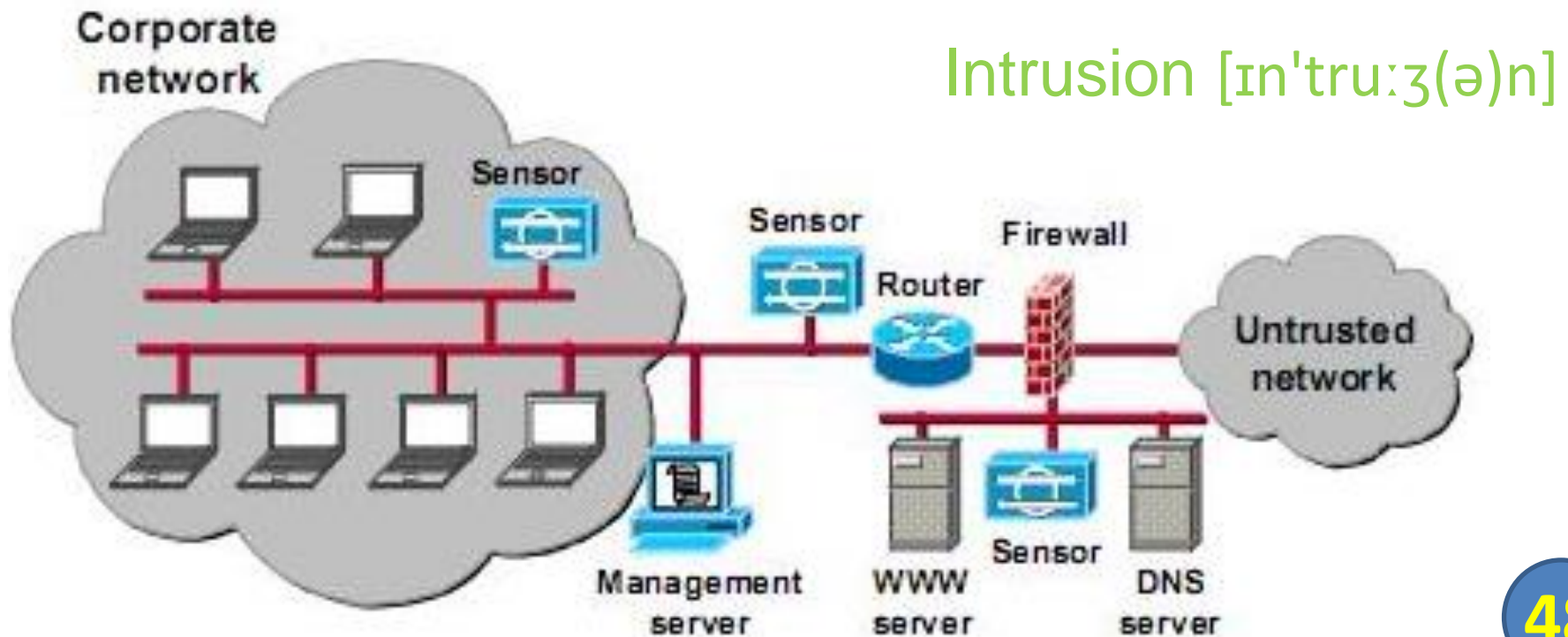
VPN

□ Point-to-Site (Remote Access) VPN



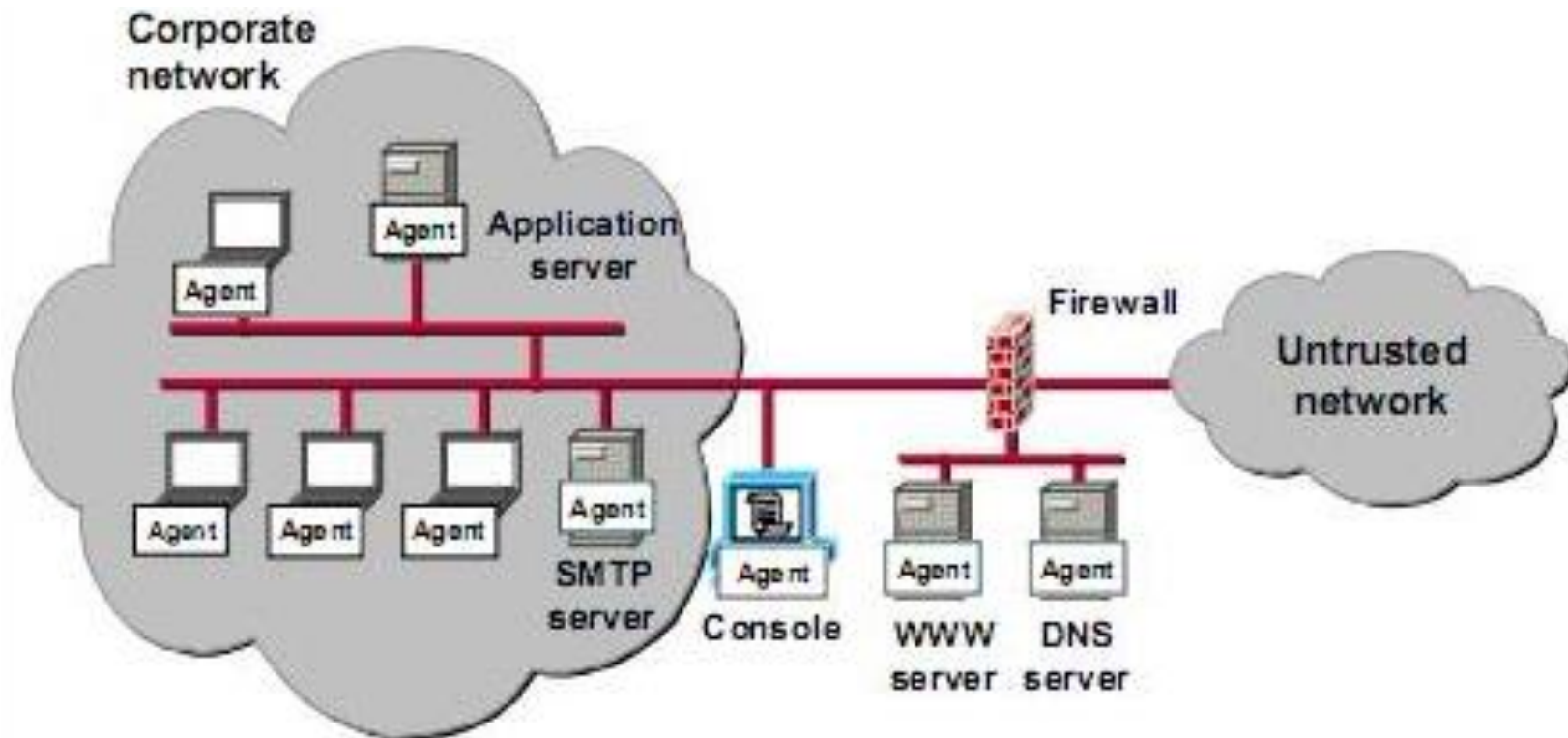
Phát hiện và ngăn chặn xâm nhập

Hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS) là hệ thống tự động theo dõi các sự kiện xảy ra trên mạng máy tính, phân tích để phát hiện ra các vấn đề an toàn.



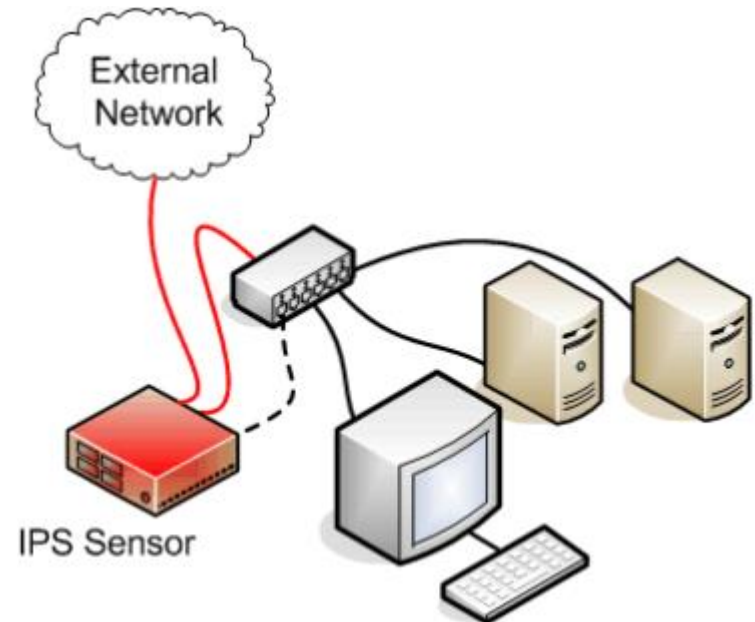
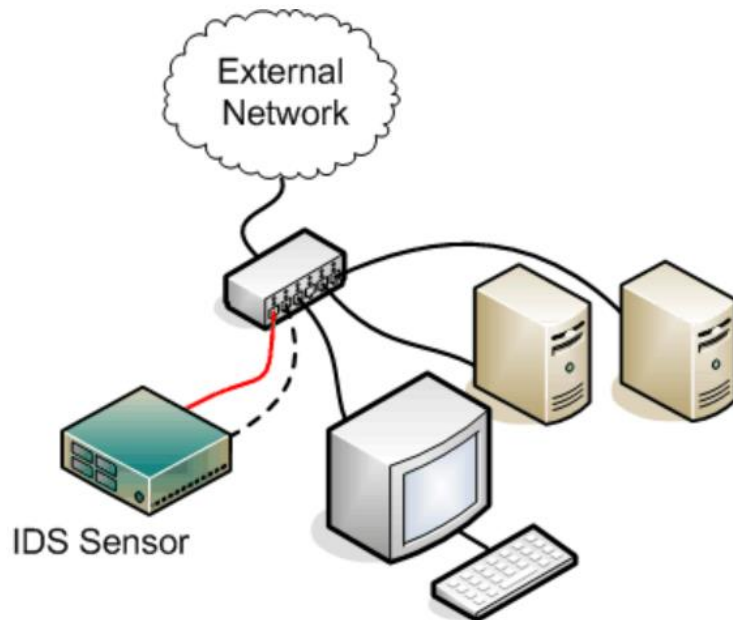
Phát hiện và ngăn chặn xâm nhập

- Network-based IDS
- Host-based IDS



Phát hiện và ngăn chặn xâm nhập

- IDS: Phát hiện xâm nhập
- IPS (Intrusion Protection System): Phát hiện và ngăn chặn xâm nhập



Phòng chống rò rỉ dữ liệu

❑ **Đã trình bày trong bài 6**

Giám sát an toàn mạng

- ❑ **Security Information and Event management (SIEM)** là hệ thống thu thập log từ các thiết bị đầu cuối, cho phép lưu trữ, phân tích tập trung và báo cáo về các sự kiện an toàn mạng của tổ chức.
- ❑ Kết quả phân tích có thể giúp phát hiện các cuộc tấn công mà không thể phát hiện được theo phương pháp thông thường.

Giám sát an toàn mạng

Dashboards

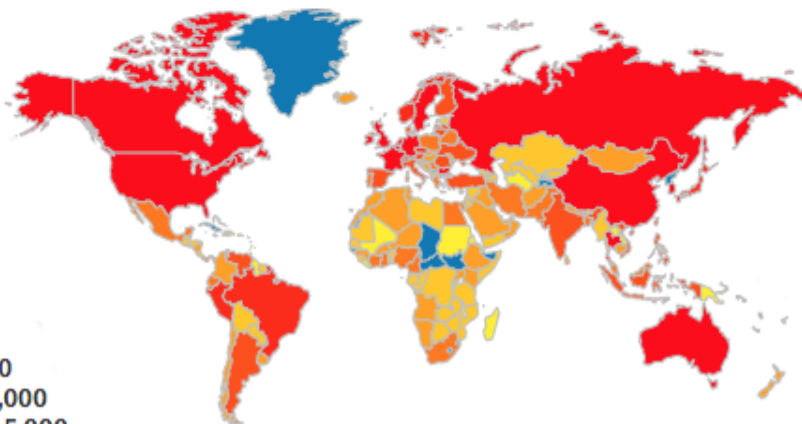
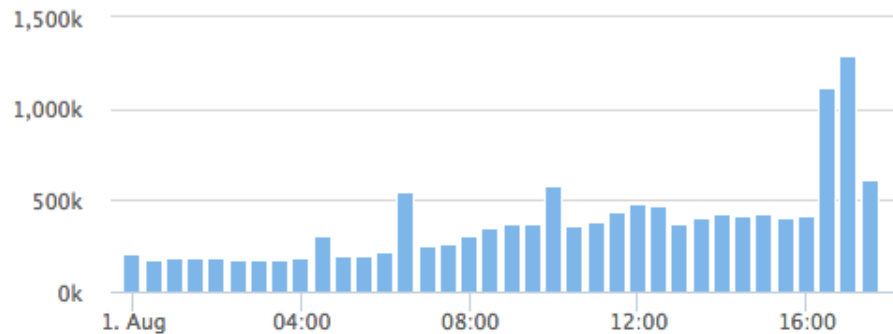
⌚ Past Hour Today Last Week Last Month

Alerts and Alarms

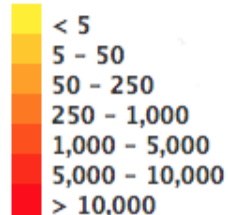
Viruses and Malware

Log Activity

Log Ingestion Rate



of Events

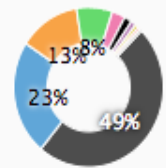


Top Countries

Country	Count
United States	4.1M
Netherlands	256.5K
Canada	67.1K
United Kingdom	57.2K
China	41.9K
Ireland	35.4K
Korea	34.3K
Singapore	25.7K
Germany	25.4K
Russian Federation	22.9K
Sweden	22K
France	19K
Australia	16.8K
Hong Kong	12.5K
Asia/Pacific Region	12.1K
Thailand	11.6K
Bulgaria	10.7K
Switzerland	9.6K
Peru	7.5K

Top Data Sources

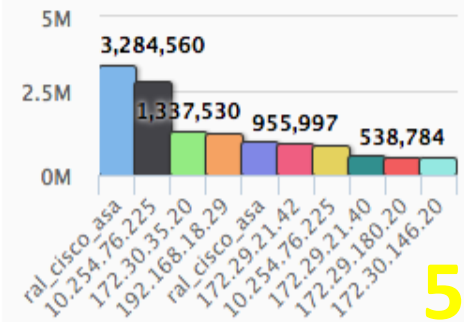
■ cisco-asa
■ winevtlog
■ iis
■ o365-exchange
■ suricata
■ windows-dhcp
■ sonicwall
■ iboss
■ juniper-vpn



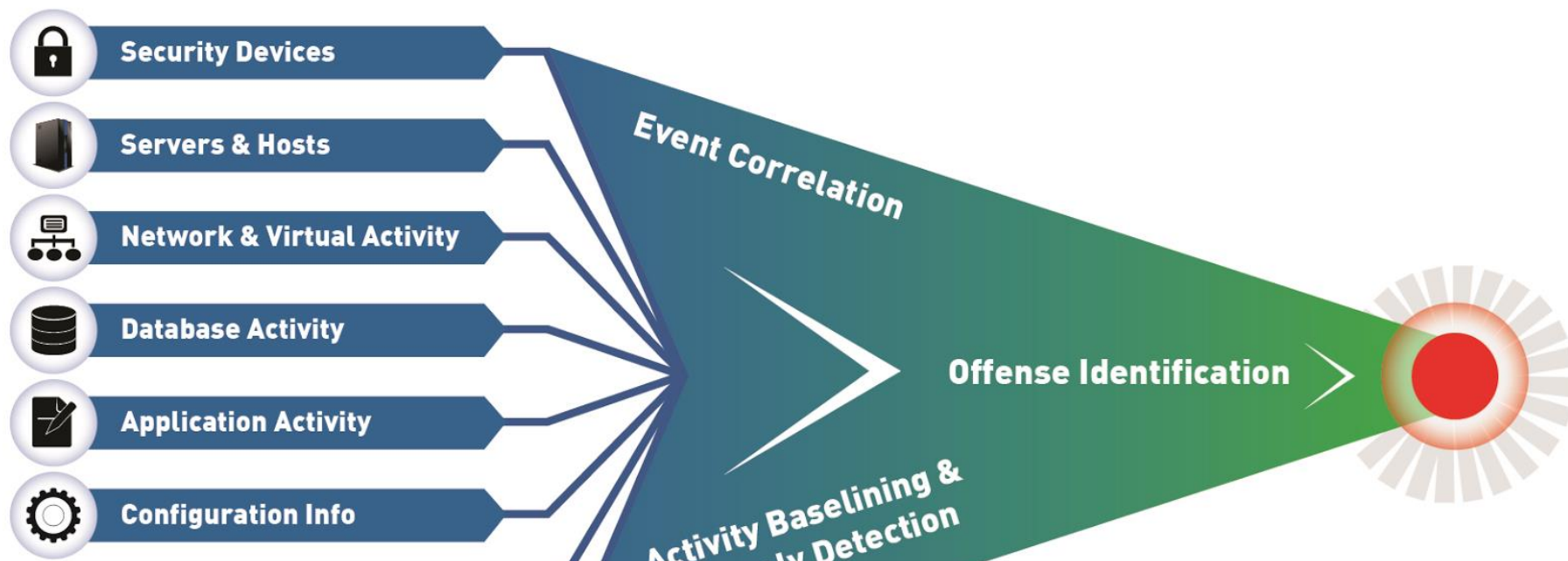
Perimeter Firewall Traffic



Top Agents













Giám sát an toàn mạng



- AlienVault Open Source SIEM (OSSIM),
- HP ArcSight Enterprise Security Manager (ESM),
- IBM Security QRadar SIEM
-

Giám sát an toàn mạng

Top SIEM Vendors								
SIEM VENDOR	<div> <div>●●●● BEST</div> <div>●●● VERY GOOD</div> <div>●● GOOD</div> <div>● FAIR</div> </div>							
	THREATS BLOCKED	SOURCES INGESTED	PERFORMANCE	VALUE	IMPLEMENTATION	MANAGEMENT	SUPPORT	SCALABILITY
 splunk > ES	●●●●	●●●	●●●	●●●	●●	●●●	●●	●●●
 LogRhythm ENTERPRISE	●●●	●●●●	●●●	●●	●●●	●●●	●●●	●●
 USM <small>ALIEN VAULT</small>	●●●	●●●	●●●	●●●●	●●●	●●	●●	●●●
 MICRO FOCUS ArcSight	●●	●●●	●●●	●●	●●●	●●●●	●●	●●●
 MICRO FOCUS Sentinel	●●	●●	●●	●●●	●●●	●●●	●●	●●●
 McAfee ESM	●●●	●●●	●●●	●●●	●●	●●	●●●	●●●
 Trustwave SIEM	●●●	●●●	●●●	●●●	●●	●●●	●●	●●●●
 IBM QRadar	●●●	●●●	●●●●	●●●	●●	●●●	●●●	●●●
 RSA NetWitness	●●	●●	●●●	●●	●●	●●	●●●	●●●
 solarwinds LEM	●●	●●●	●●	●●	●●●●	●●	●●●	●●

