

AN TOÀN MẠNG MÁY TÍNH

NỘI DUNG MÔN HỌC

1. Tổng quan
2. Các phần mềm gây hại – Trojan
3. Các phần mềm gây hại – Virus
4. Các giải thuật mã hoá dữ liệu
5. Mã hoá khoá công khai và quản lý khoá
6. Chứng thực dữ liệu
7. Một số giao thức bảo mật mạng
8. Bảo mật mạng không dây
9. Bảo mật mạng ngoại vi
10. Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

BÀI 10

HỆ THỐNG TÌM KIẾM,
PHÁT HIỆN VÀ
NGĂN NGỪA XÂM NHẬP

Nội dung

1. TỔNG QUAN VỀ IDS/IPS
2. PHẦN CỨNG VÀ PHẦN MỀM HỖ TRỢ IDS/IPS

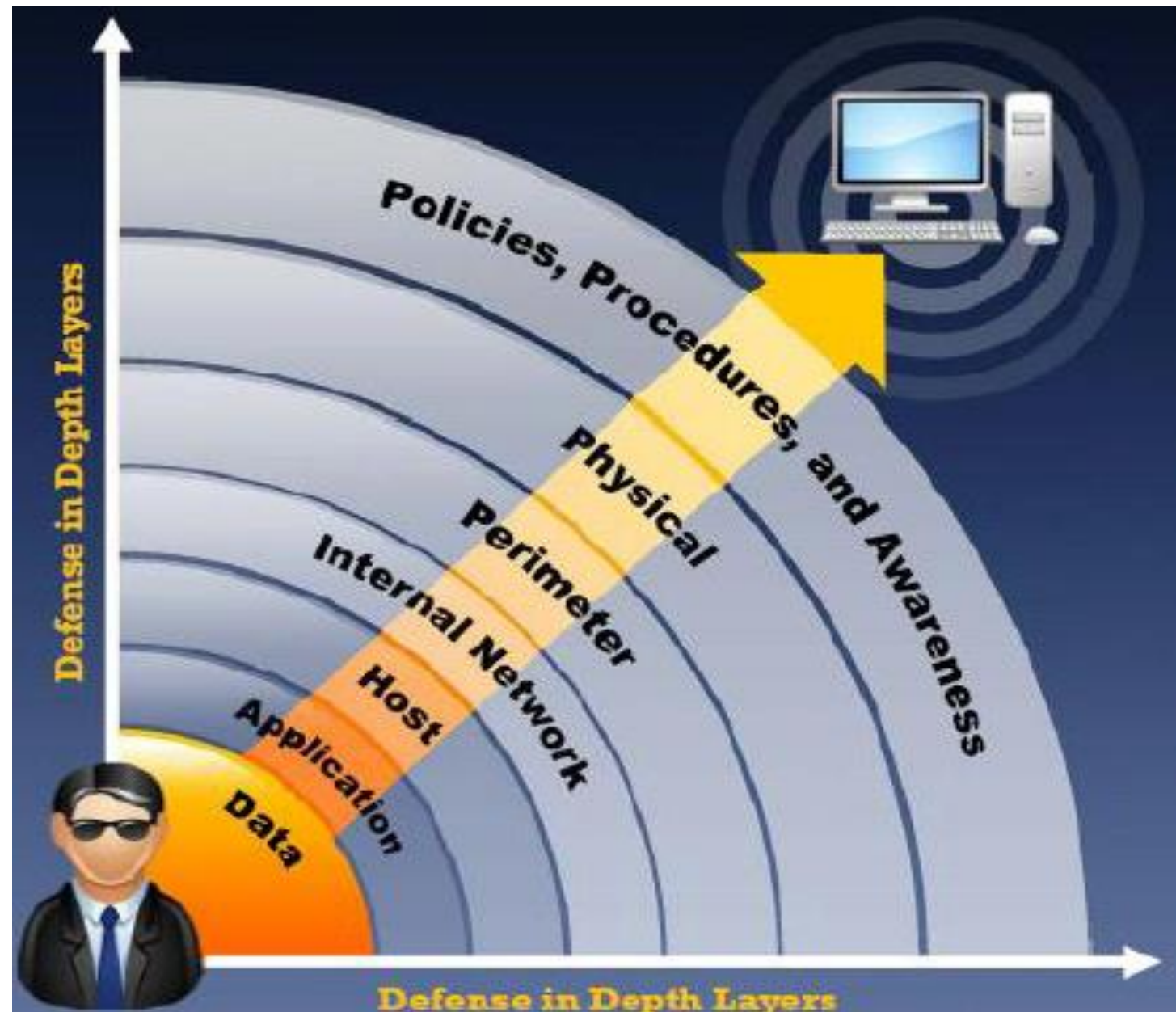
TỔNG QUAN VỀ IDS/IPS

- Giới thiệu
- Tường lửa và vị trí tường lửa trong hệ thống
- Phân loại
- Chế độ Promiscuous và Inline
- Sử dụng IDS hay IPS?
- Các kỹ thuật phát hiện
- Thành phần chính
- Triển khai IDS/IPS

Giới thiệu

Slide 3 có giải thích hình này

Physical: Port Security



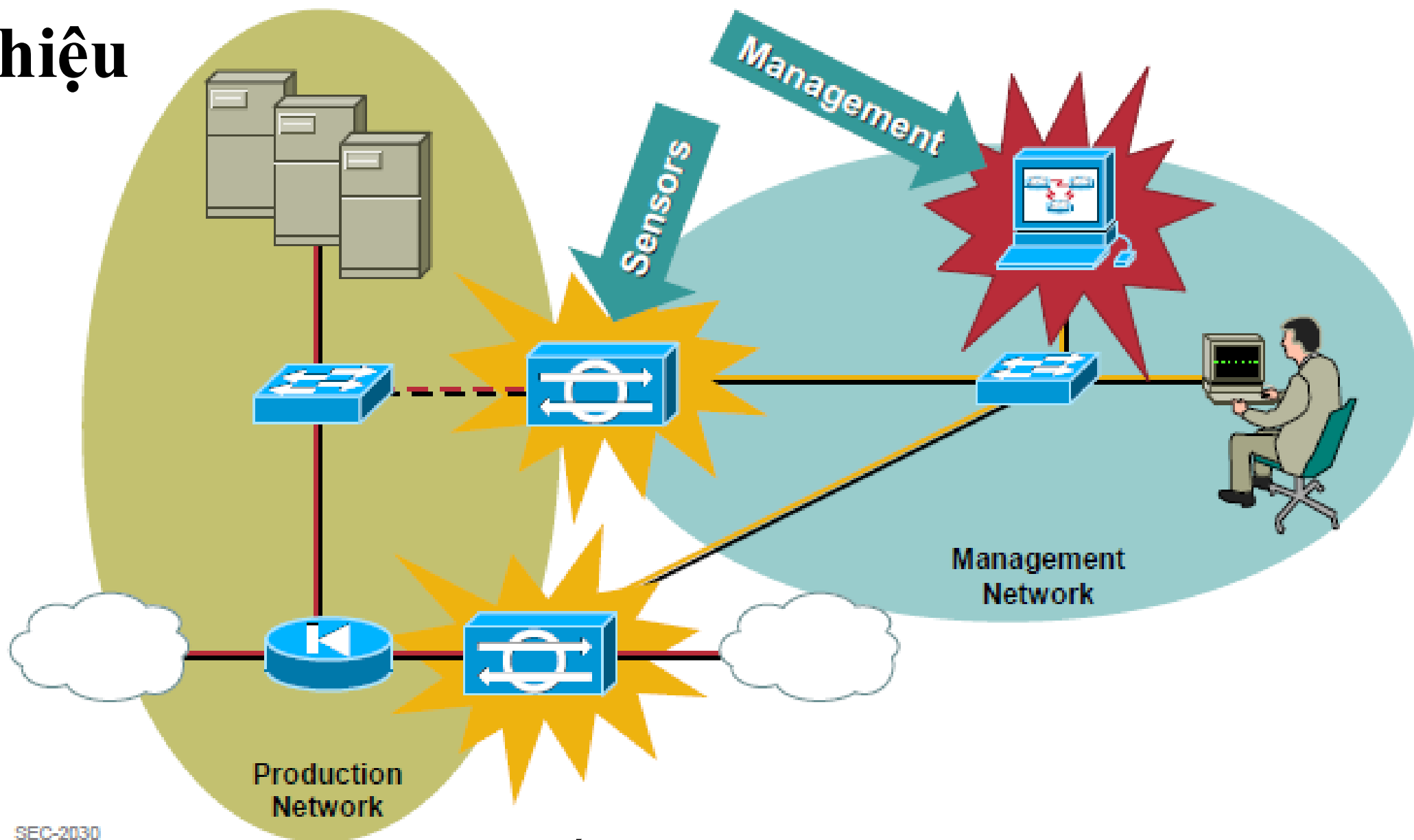
Hệ thống phòng thủ theo chiều sâu

Giới thiệu

Hệ thống phát hiện xâm nhập (Intrusion Detection System – IDS)

- Là hệ thống tìm kiếm, theo dõi nhằm phát hiện một cách kịp thời các hoạt động bất thường bao gồm việc tấn công, xâm nhập không mong muốn từ bên ngoài hoặc truy cập trái phép vào tài nguyên của hệ thống mạng.
- Dựa trên việc xây dựng các tập luật nhằm phân tích bản sao của lưu lượng mạng.
- Khi phát hiện các hoạt động bất thường, IDS sẽ đưa ra các cảnh báo (alert) để người quản trị đưa ra các quyết định đối phó.

Giới thiệu



Hệ thống IDS/IPS trong mạng

Giới thiệu

- **Hệ thống IDS có thể phát hiện các cuộc tấn công:**
 - Tấn công lớp Ứng dụng (Application layer): quét cây thư mục, tràn bộ đệm...
 - Quét mạng (Network scans)
 - Tấn công từ chối dịch vụ (DoS – DDoS)
 - Các bất thường của mạng được phát hiện bởi IDS: IP datagram không hợp lệ, TCP packet không hợp lệ, yêu cầu hoặc đáp ứng ARP không hợp lệ.

Giới thiệu

- Ưu và nhược điểm của IDS
 - Ưu điểm:

Về ưu điểm thì đối ngược lại vs firewall

 - Không tác động lên toàn mạng (ít gây ra độ trễ).
 - Khi một bộ cảm biến bị lỗi hoặc quá tải sẽ không làm ảnh hưởng nhiều đến hệ thống mạng.
 - Nhược điểm:
 - Attacker có thể sử dụng các kỹ thuật tránh né để đánh lừa IDS.

Giới thiệu

Hệ thống ngăn ngừa xâm nhập (Intrusion Prevention System – IPS)

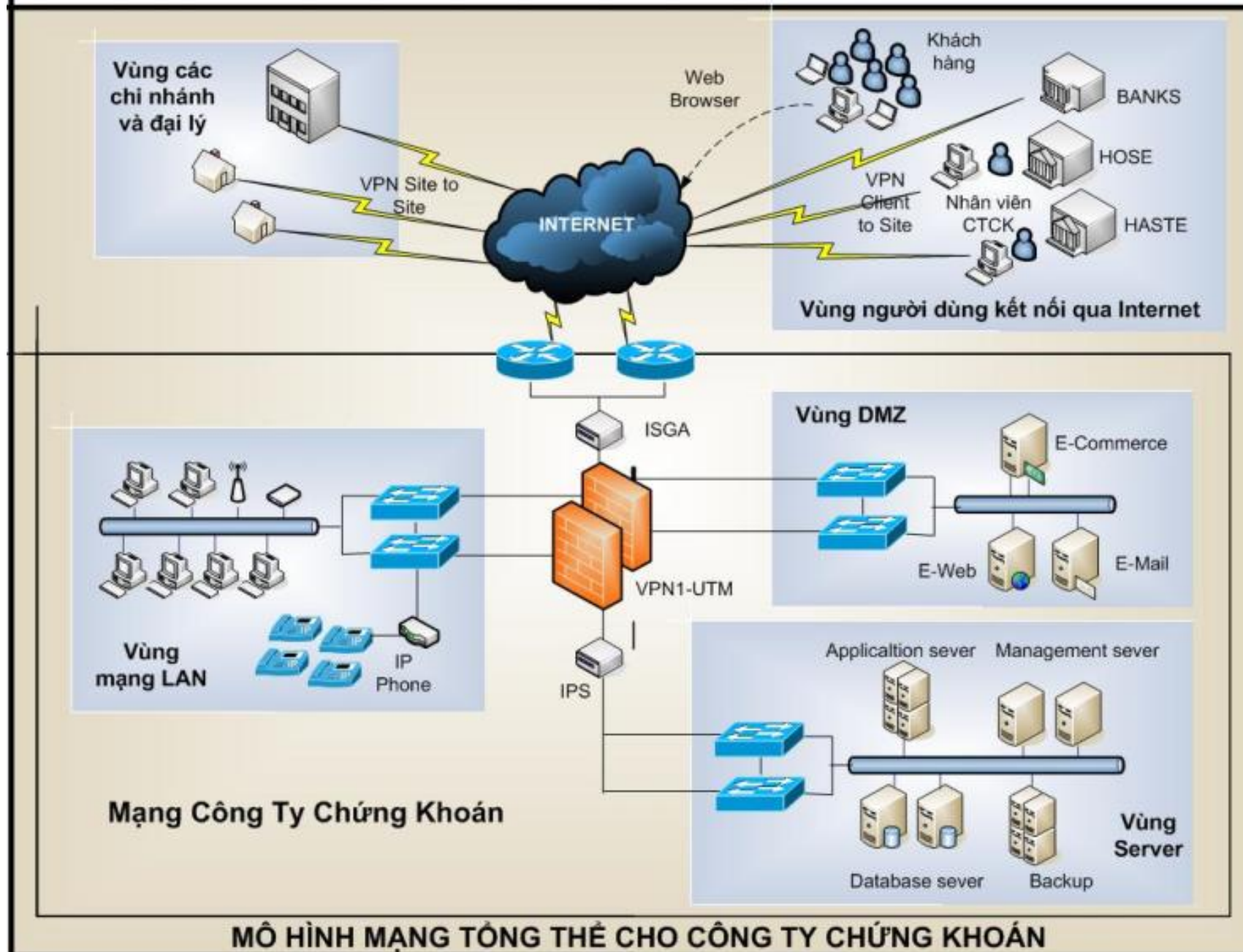
- Là hệ thống theo dõi, ngăn ngừa một cách kịp thời các hoạt động xâm nhập không mong muốn từ bên ngoài vào.
- Chức năng chính của IPS là xác định những hoạt động nguy hại, lưu giữ các thông tin này, kết hợp với tường lửa để ngăn chặn chúng và đưa ra các báo cáo chi tiết cho quá trình này.
- Được xem như một hệ thống IDS mở rộng có thêm chức năng ngăn ngừa và sử dụng tập luật tương tự IDS.

Giới thiệu

- **IPS thực hiện phân tích lưu lượng mạng như sau:**
 - Tập hợp lại các session ở tầng 4 và phân tích nội dung của chúng.
 - Theo dõi, giám sát tỷ lệ giữa packet và session để phát hiện và ngăn chặn sự sai lệch so với mạng cơ bản.
 - Phân tích nhóm các packet để xác định xem chúng có phải dùng để do thám hệ thống mạng hay không.
 - Giải mã các giao thức lớp Ứng dụng và phân tích nội dung của chúng.
 - Phân tích các packet để đối phó với hoạt động xấu được chứa trong một gói đơn.

Giới thiệu

Vị trí đặt của IPS nằm ở sau firewall
Vị trí đặt có thể linh hoạt không bị phụ thuộc



Vị trí của IPS trong hệ thống mạng

Giới thiệu

- **Vai trò của hệ thống IDS/IPS**
 - Cung cấp khả năng điều khiển truy cập mạng.
 - Nâng cao mức độ kiểm soát lưu lượng trên mạng, bao gồm việc kiểm soát, sao lưu dữ liệu, kiểm tra các điều kiện dựa vào tập luật.
 - Đưa ra cảnh báo về các cuộc tấn công và ngăn chặn những cuộc tấn công này.

Giới thiệu

- **Ưu nhược của IDS/IPS**
 - **Ưu điểm**
 - Cung cấp giải pháp bảo vệ toàn diện đối với tài nguyên hệ thống.
 - Ngăn chặn kịp thời các cuộc tấn công vào hệ thống mạng.
 - **Nhược điểm**
 - Có thể đưa ra cảnh báo nhầm dẫn đến không cho phép các truy cập hợp lệ vào hệ thống.

Tường lửa và vị trí tường lửa trong hệ thống

- Một số tường lửa phần cứng thông dụng

1. Cisco Route



2. FortiNet



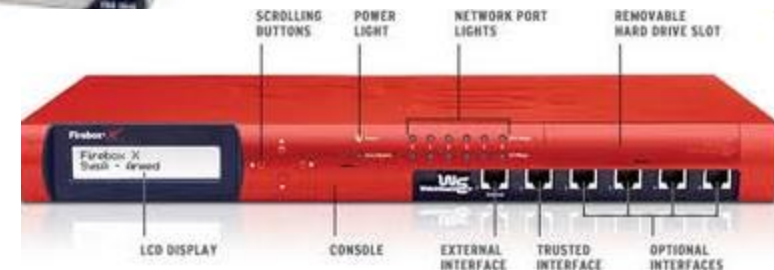
3. CheckPoint Safe@Office



4. Sonicwall PRO



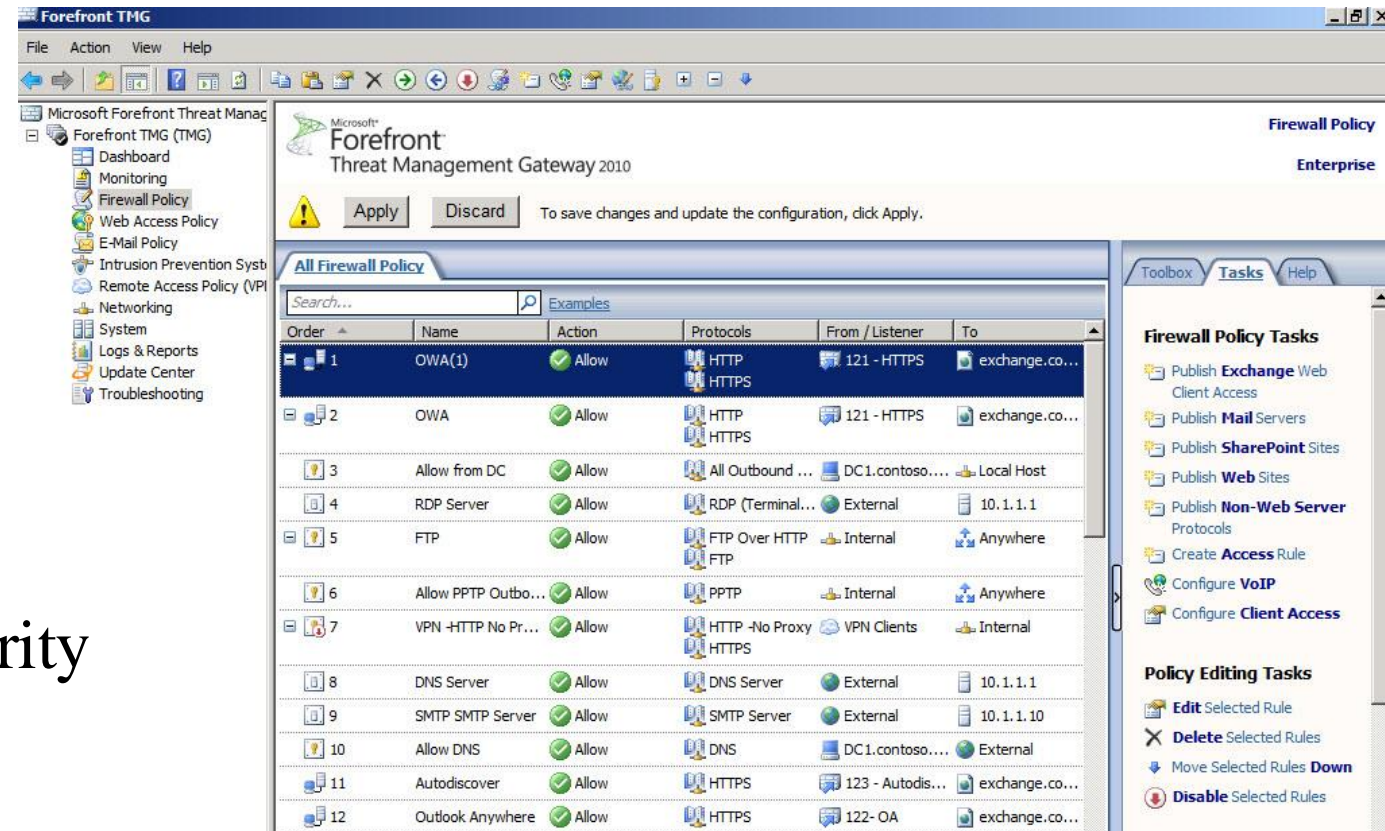
5. WatchGuard Firebox



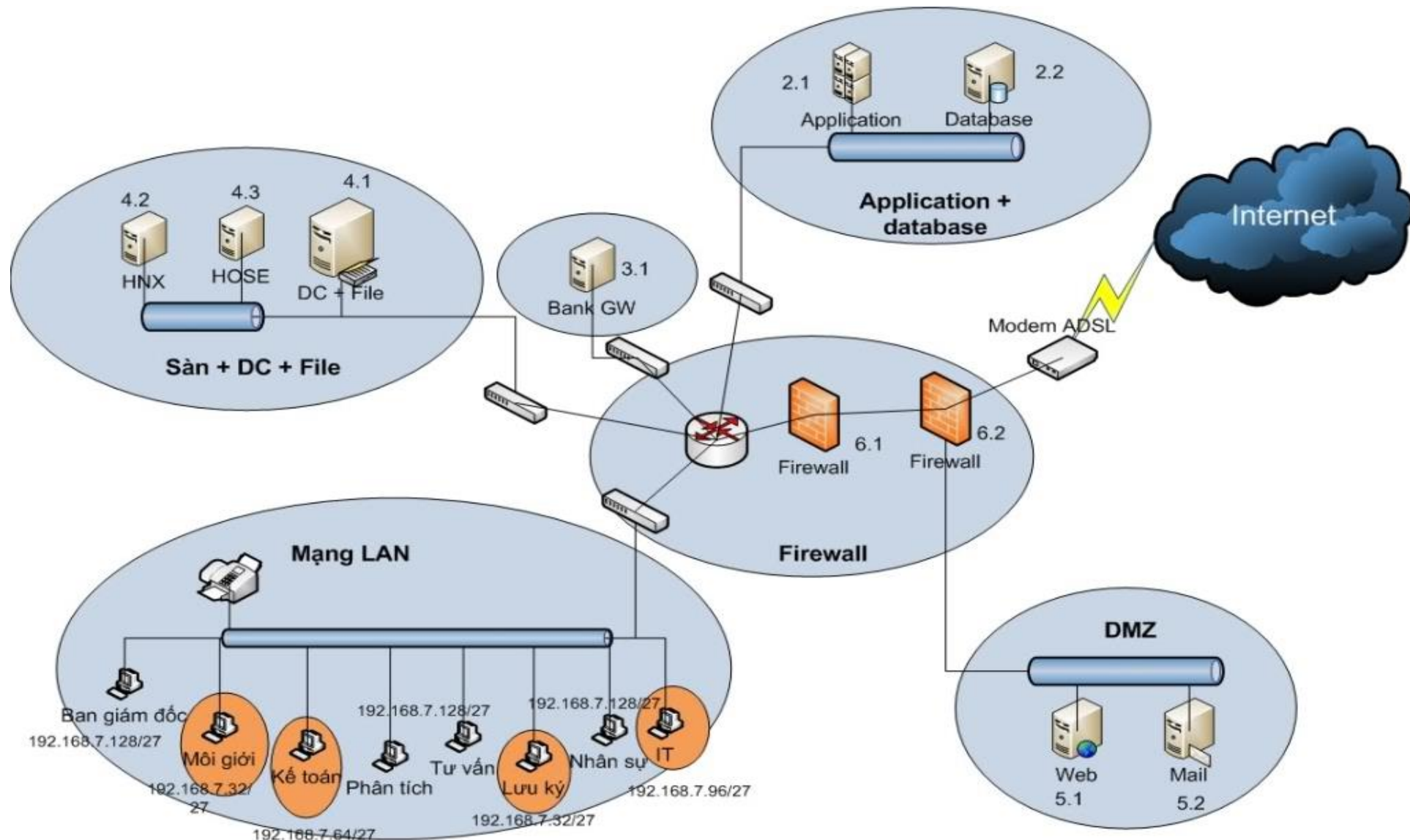
Tường lửa và vị trí tường lửa trong hệ thống

- Một số tường lửa phần mềm thông dụng

1. Comodo Firewall
2. ESET Smart Security
3. ZoneAlarm
4. Outpost Firewall Pro
5. F-Secure Internet Security
6. TMG

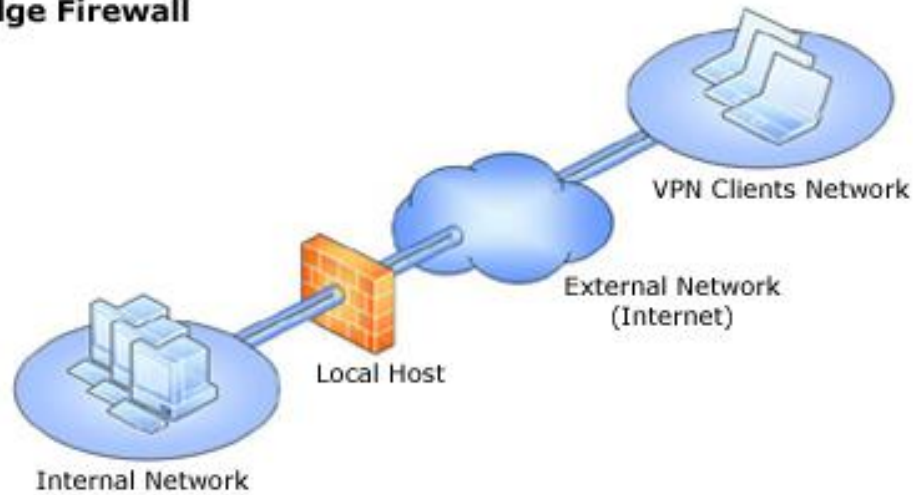


Tường lửa và vị trí tường lửa trong hệ thống

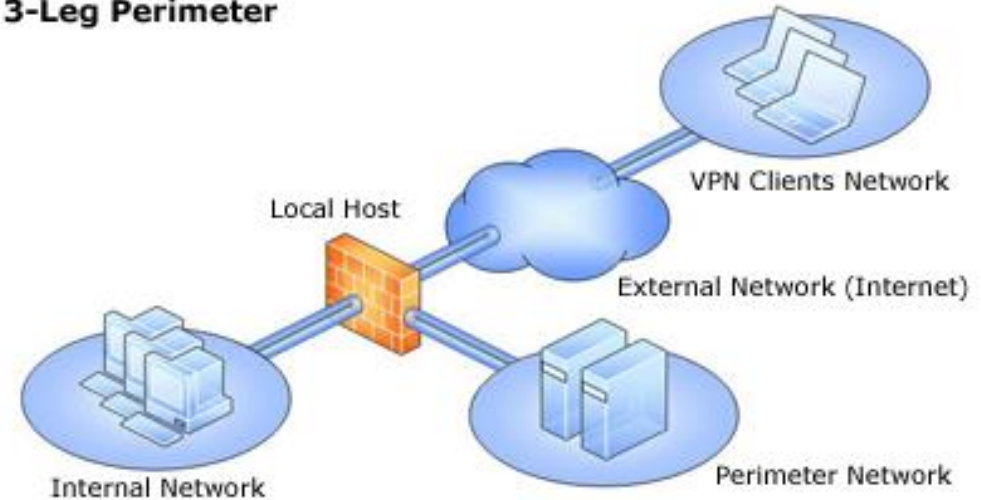


Tường lửa và vị trí tường lửa trong hệ thống

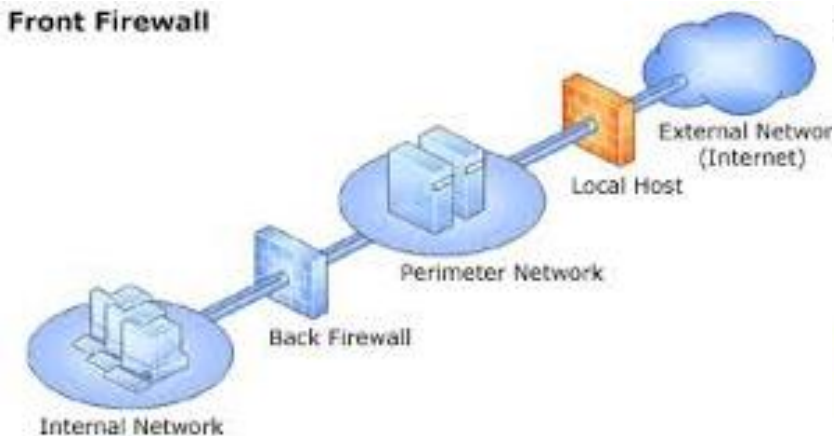
Edge Firewall



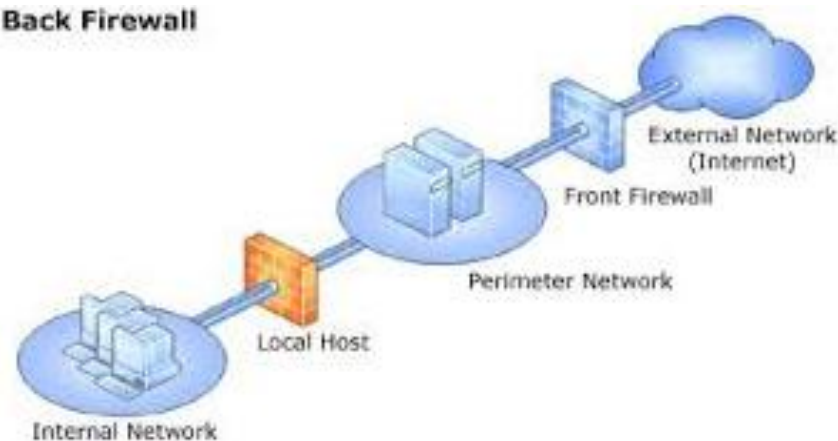
3-Leg Perimeter



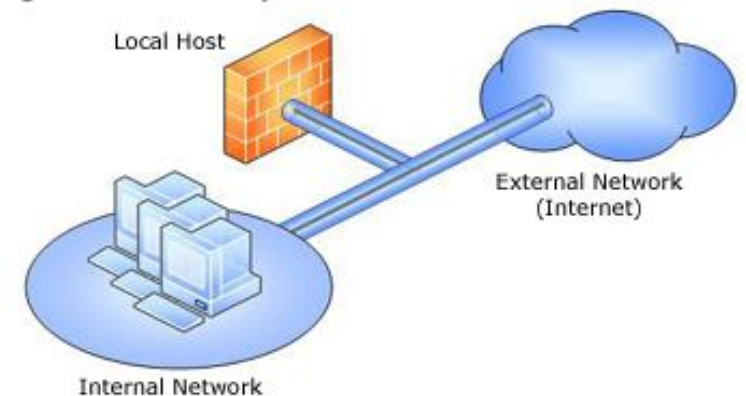
Front Firewall



Back Firewall



Single Network Adapter



Phân loại

- Hệ thống IDS/IPS dựa trên mạng (**NIDS/NIPS** – Network-based Intrusion Detection / Network-based Intrusion Prevention)

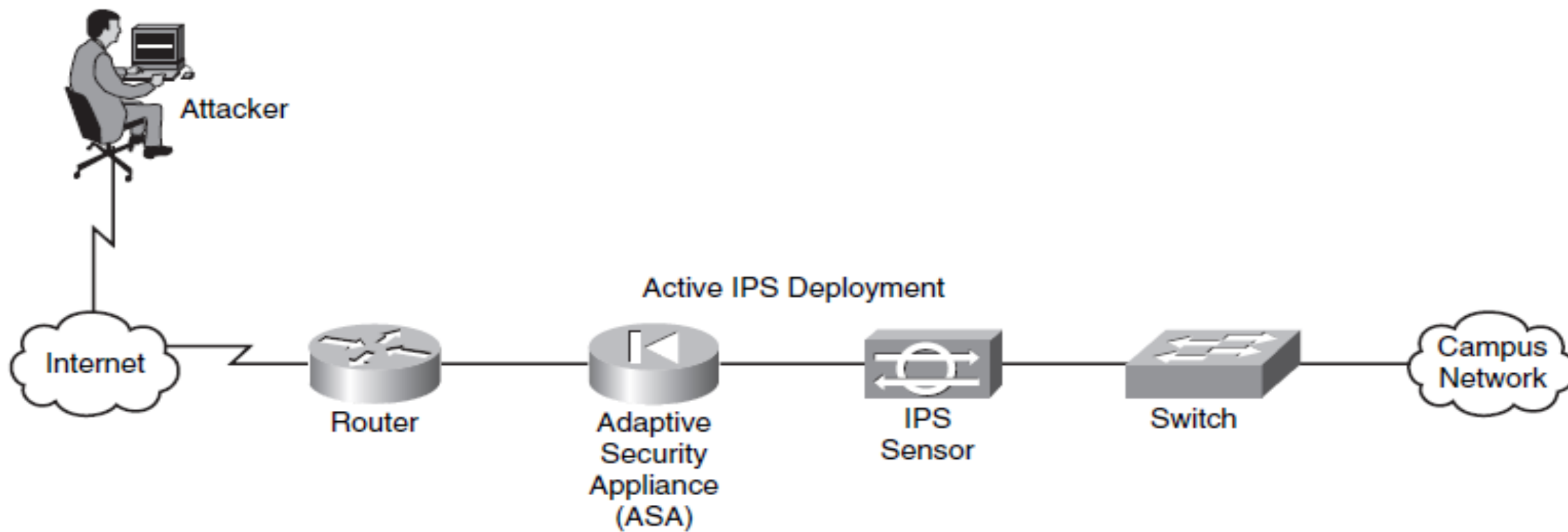
Có thể triển khai trước hoặc sau tường lửa.

- Hệ thống IDS/IPS dựa trên host (**HIPS/NIPS** – Host-based Intrusion Detection / Host-based Intrusion Prevention)

Được triển khai trên hệ thống đầu cuối nhằm ngăn chặn kịp thời các hoạt động xâm nhập trên các host.

Phân loại

- NIPS



Triển khai NIPS

Phân loại

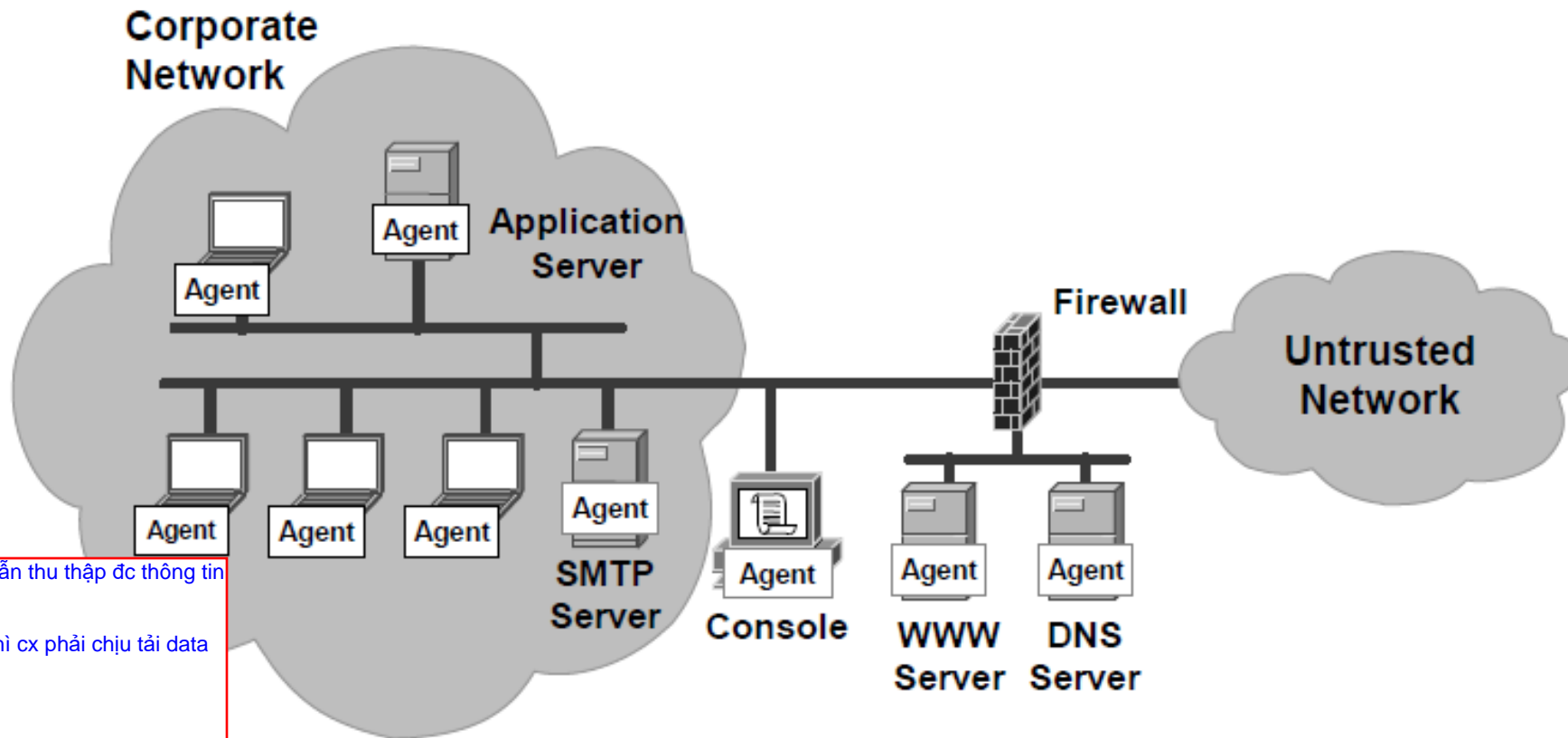
- **Đặc điểm của NIPS**
 - Có khả năng phát hiện các cuộc tấn công trên **các hệ điều hành và ứng dụng khác nhau.**
 - **Giảm chi phí** lắp đặt, thi công, bảo trì và triển khai hệ thống mạng do chỉ cần 1 thiết bị NIPS có thể phân tích lưu lượng của toàn mạng.
 - **Có cái nhìn tổng quan về hệ thống mạng.**
 - NIPS là **vô hình** với kẻ tấn công nhờ có Interface được dành riêng để giám sát mạng.

Phân loại

- **HIPS**
 - Phần mềm được cài đặt lên từng host
 - Phát hiện và bảo vệ từng máy
 - Không yêu cầu phần cứng chuyên dụng

Phân loại

- HIPS



ko có agent nhưng server vẫn thu thập đc thông tin thì sẽ sd

Ngoài phục vụ traffic trống thì cx phải chịu tải data

Triển khai HIPS

Phân loại

- **Sử dụng NIPS hay HIPS?**
 - Hỏi: NIPS có khả năng giám sát tất cả lưu lượng mạng đi qua nó, bao gồm cả lưu lượng mạng sẽ tới máy đích được thiết lập HIPS. **Như vậy việc cài đặt HIPS trên máy đích đó có dư thừa và thực sự cần thiết hay không?**

Có cần thiết và ko dư thừa vì lun cần đến sự xuất hiện của host

Phân loại

- **Sử dụng NIPS hay HIPS?**
 - **Đáp:** NIPS không thể phân tích các lưu lượng mạng được mã hóa ở lớp Ứng dụng (Application layer) với IPSec hoặc SSL. Điều gì sẽ xảy ra nếu dữ liệu độc hại được chứa trong lưu lượng đã được mã hóa? Do đó, giả sử có 1 kết nối SSL giữa máy tính đích đến server, thì lưu lượng SSL sẽ không thể được phân tích bởi cảm biến NIPS. Thay vào đó, HIPS sẽ thực hiện việc này thay cho NIPS. **HIPS sẽ phân tích dữ liệu chứa trong SSL sau khi lưu lượng SSL đã được giải mã.**

Phân loại

- **Sử dụng NIPS hay HIPS?**
 - Phân tích và phát hiện dữ liệu mã hoá tầng Application
 - Áp đặt chính sách (điều khiển tài nguyên)
 - Bảo vệ ứng dụng Web
 - Tràn bộ đệm
 - Phát hiện tấn công mạng và thăm dò mạng
 - Tấn công DoS/DDoS

Host-Focused
Technology

Network-Focused
Technology



Phân loại

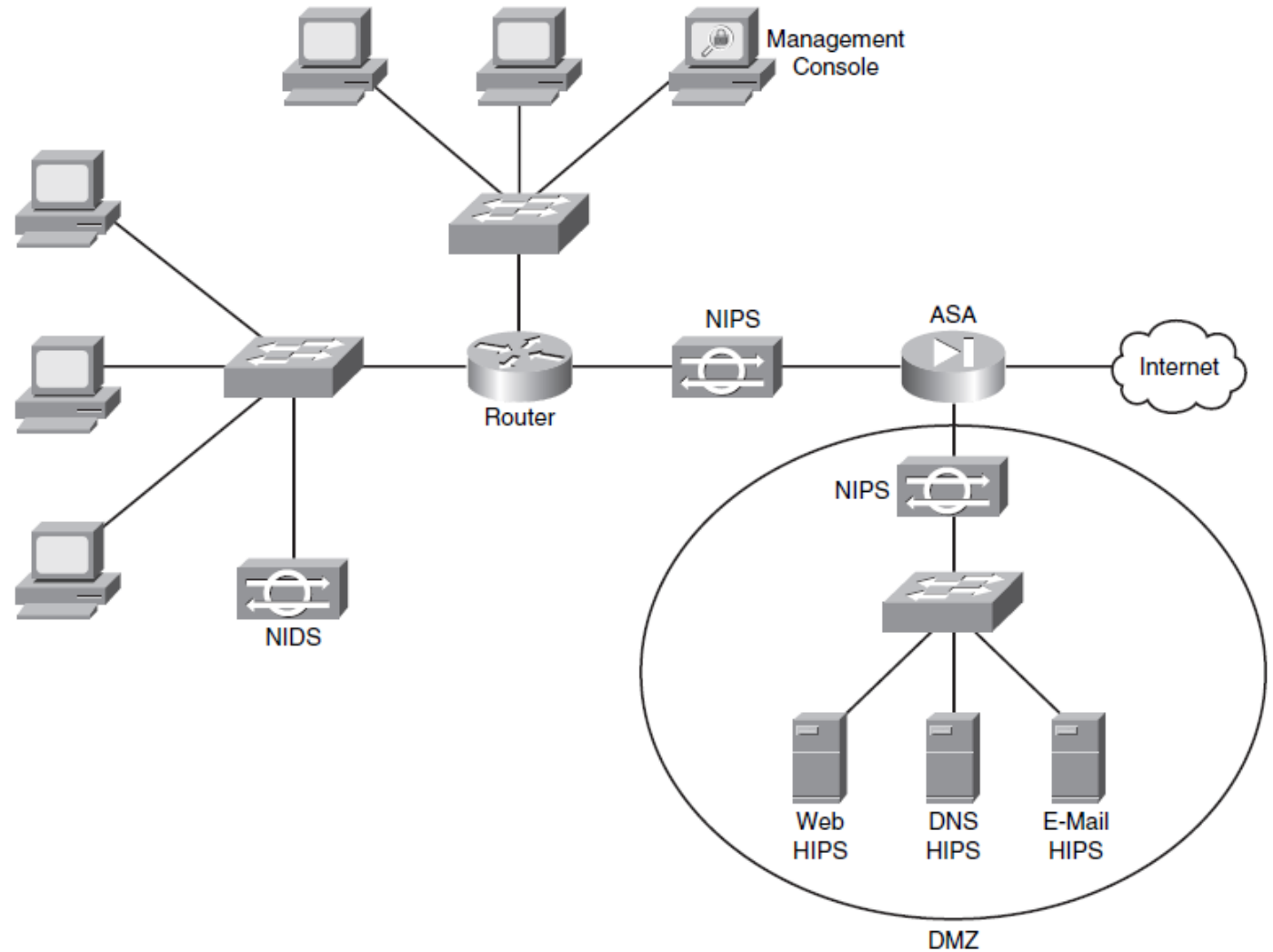
- **Sử dụng NIPS hay HIPS?**

Nên triển khai cả NIPS và HIPS để hỗ trợ cho nhau:

- NIPS có khả năng phân tích lưu lượng mạng để ngăn chặn tấn công DoS/DDoS hoặc các packet thăm dò mạng.
- HIPS có thể tập trung bảo vệ các ứng dụng và tài nguyên của máy chủ.

Phân loại

- Sử dụng NIPS hay HIPS?



Triển khai IDS, NIPS và HIPS

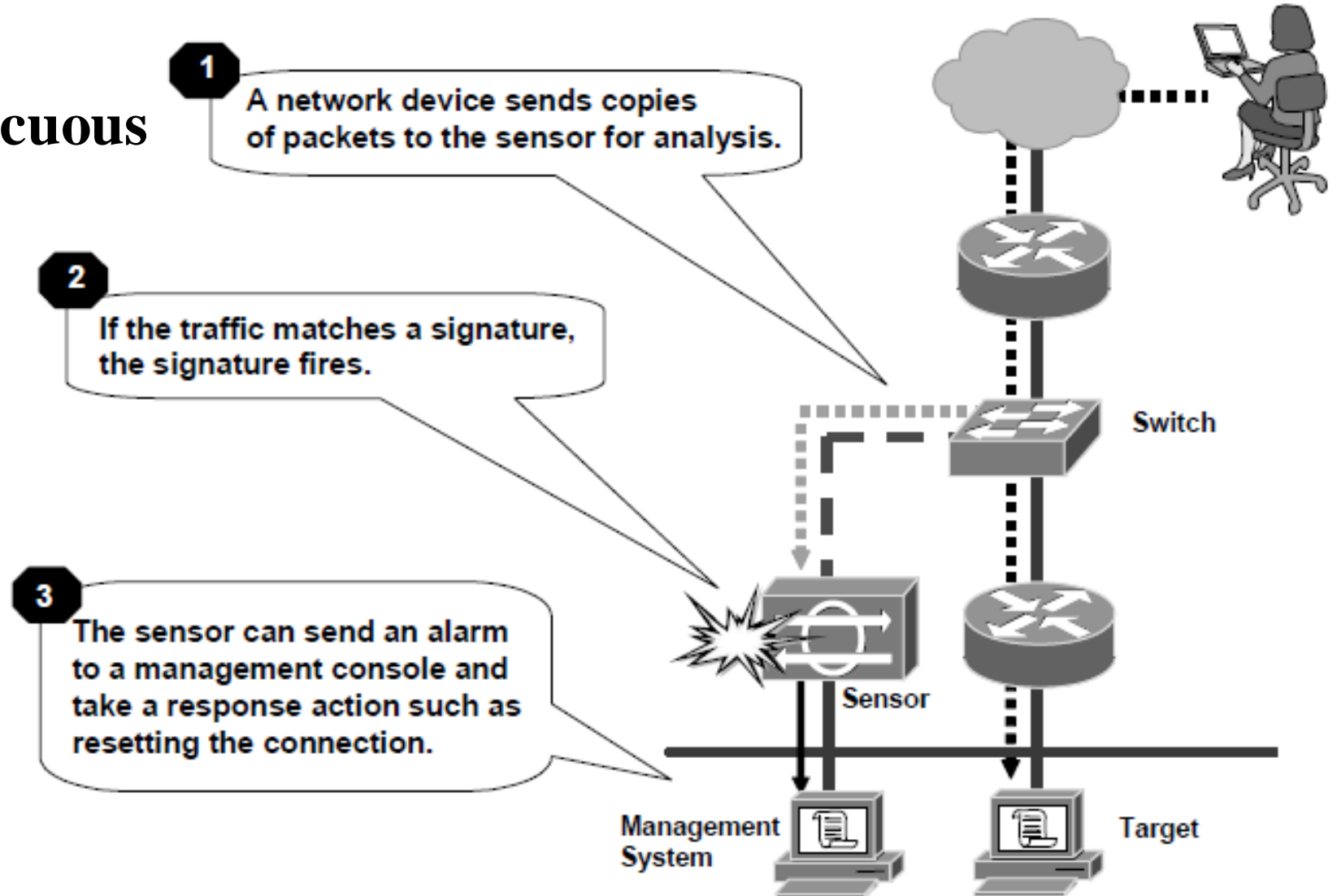
Chế độ Promiscuous và Inline

- **Chế độ Promiscuous**

Chỉ yêu cầu 1 cổng (interface) giám sát. Khi thực thi chế độ promiscuous, bộ cảm biến sẽ sao chép lưu lượng mạng. Sau đó, bộ cảm biến sẽ phân tích lưu lượng sao chép này và có thể phát hiện lưu lượng xấu.

Chế độ Promiscuous và Inline

- Chế độ Promiscuous



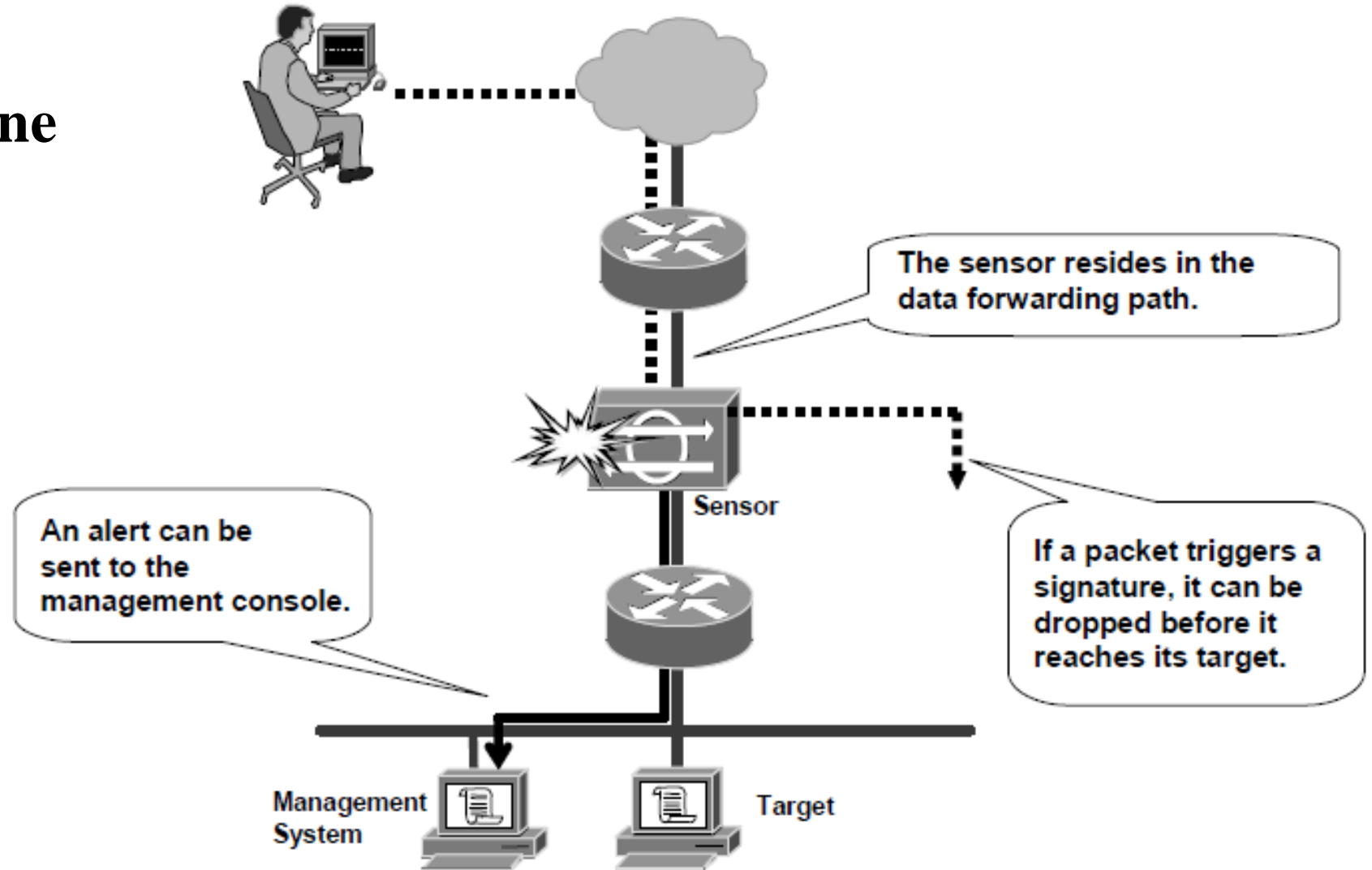
Chế độ Promiscuous và Inline

- **Chế độ Inline** phù hợp vs IPS hay firewall

Chế độ Inline yêu cầu ít nhất 2 cổng (interface) giám sát. Ở chế độ này, bộ cảm biến sẽ giám sát trực tiếp lưu lượng gốc đi qua nó. Vì vậy, bộ cảm biến có thể loại bỏ các lưu lượng xấu trước khi chúng tới được đích (kể cả trigger packet).

Chế độ Promiscuous và Inline

- Chế độ Inline



Sử dụng IDS hay IPS?

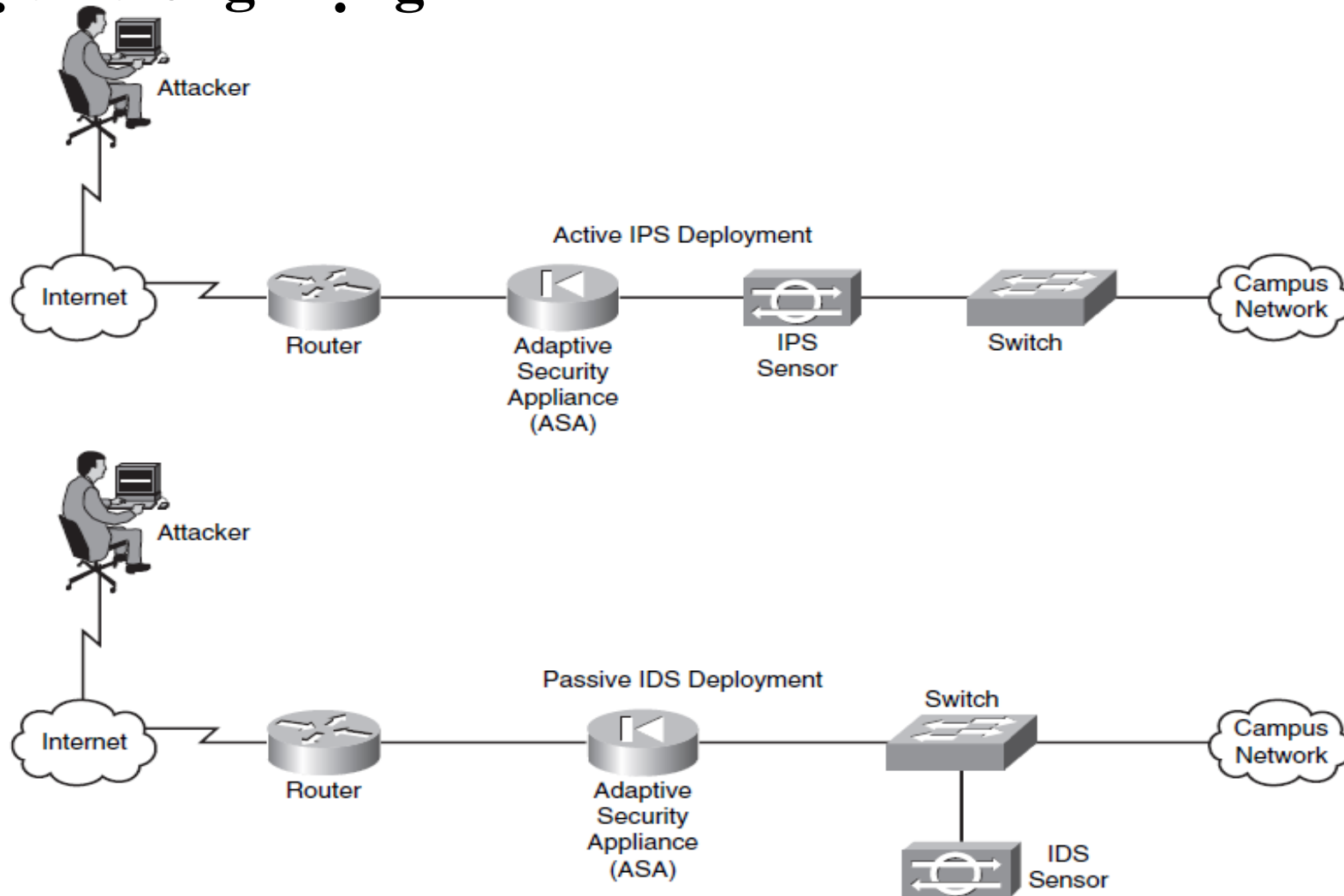
- **Đặc điểm chung của IDS và IPS:**
 - Cả 2 kỹ thuật đều sử dụng các **cảm biến (sensor)**.
 - Cả 2 kỹ thuật đều sử dụng các **signature** để phát hiện các dạng bất thường của lưu lượng trong hệ thống mạng.
 - Cả 2 đều có thể phát hiện các dạng **atomic** (packet đơn) hoặc dạng **composite** (nhiều packet).

Sử dụng IDS hay IPS?

- Sự khác biệt cơ bản của IDS và IPS là cách thức hoạt động và vị trí trong mạng.
 - Cách hoạt động
 - IDS hoạt động ở chế độ **promiscuous**. Ở chế độ này IDS sẽ sao chép lưu lượng để phân tích. IDS không phân tích trực tiếp lên lưu lượng gốc.
 - IPS hoạt động ở chế độ **inline**. Ở chế độ này, IPS trực tiếp phân tích lên lưu lượng gốc. Điều này sẽ giúp cho IPS có thể ngăn chặn kịp thời lưu lượng có hại, kể cả những trigger packet.

Sử dụng IDS hay IPS?

- Vị trí trong mạng



Sử dụng IDS hay IPS?

- Sử dụng IDS hay IPS tùy thuộc vào quy mô, tính chất, chính sách an ninh của hệ thống mạng.
 - Với quy mô nhỏ, có thể sử dụng IPS nhằm phát hiện và ngăn chặn trực tiếp cuộc tấn công.
 - Với quy mô lớn, có thể kết hợp cả IDS lẫn IPS để hỗ trợ cho nhau. Trong đó thiết bị IDS dùng để kiểm tra sự hoạt động của IPS.

Các kỹ thuật phát hiện (detection)

- Phát hiện dựa trên dấu hiệu (Signature)
- Phát hiện dựa trên chính sách (Policy)
- Phát hiện dựa trên sự bất thường (Anomaly)
- Phát hiện dựa trên Honey pot

Các kỹ thuật phát hiện (detection)

- **Phát hiện dựa trên dấu hiệu (Signature)**
 - Lưu lượng mạng được phân tích và so sánh dữ liệu đó với các dấu hiệu (signatures) tấn công đã được biết trước.

Ví dụ: Tấn công web server thường ở dạng URL. Vì vậy, các chuỗi trong URL sẽ được xác định xem có phải là chuỗi dùng để tấn công máy chủ hay không.

Các kỹ thuật phát hiện (detection)

- **Phát hiện dựa trên dấu hiệu (Signature)**
 - Ưu điểm:
 - Dạng đơn giản nhất để triển khai IDS/IPS.
 - Dễ dàng cập nhật dấu hiệu mới, tùy chỉnh và mở rộng dấu hiệu.
 - Nhận dạng các dấu hiệu tấn công (đã được biết trước) với tỷ lệ chính xác cao.

Các kỹ thuật phát hiện (detection)

- **Phát hiện dựa trên dấu hiệu (Signature)**
 - Nhược điểm:
 - Phải liên tục cập nhật các dấu hiệu tấn công mới.
 - Cần có kiến thức sâu về IDP/IPS nếu muốn điều chỉnh dấu hiệu một cách hiệu quả trong môi trường phức tạp và có tính không ổn định.
 - Các kỹ thuật trốn tránh (evasion) có thể vượt qua IPS dùng kỹ thuật này.
 - Không thể phát hiện các loại tấn công chưa được biết đến.

Các kỹ thuật phát hiện (detection)

- **Phát hiện dựa trên bất thường (Anomaly-based Detection)**

Phương pháp này phân tích và quan sát lưu lượng mạng. Sau đó, so sánh định nghĩa của những hoạt động bình thường và đối tượng được quan sát nhằm xác định độ lệch. Có một vài phương pháp để phát hiện sự bất thường:

- *Phát hiện bất thường theo thống kê (Statistical anomaly detection):* phương pháp này sẽ giám sát các mẫu lưu lượng mạng trong một khoảng thời gian và tự động xây dựng đường cơ sở (baseline).
- *Phát hiện bất thường không dựa theo thống kê (Nonstatistical anomaly detection):* phương pháp này cho phép người quản trị định nghĩa đường baseline cho các mẫu lưu lượng.

Các kỹ thuật phát hiện (detection)

- **Phát hiện dựa trên bất thường (Anomaly-based Detection)**
 - Ưu điểm: có khả năng phát hiện cả mối nguy hiểm đã biết và chưa được biết tới.
 - Nhược điểm:
 - Các kỹ thuật trốn tránh (evasion) có thể vượt qua IPS dùng kỹ thuật này
 - Phương pháp này yêu cầu một khoảng thời gian để thiết lập hồ sơ (profile) mạng ở trạng thái bình thường

Các kỹ thuật phát hiện (detection)

- **Phát hiện dựa trên Policy (Policy-based Detection)**

Lưu lượng mạng được phân tích. IDS/IPS sẽ xử lý đối tượng được quan sát nếu đối tượng này vi phạm chính sách về lưu lượng. Chính sách này sẽ cho phép (permit) hoặc từ chối (deny) lưu lượng mạng.

Ví dụ: Chính sách về truy cập mạng: Chính sách này quy định cụ thể các mạng nào có thể truyền thông với các host cụ thể nào. IDP/IPS có thể nhận ra các lưu lượng không được quy định trong profile và sau đó sẽ ghi nhận lại các hoạt động này.

Các kỹ thuật phát hiện (detection)

- **Phát hiện dựa trên Policy (Policy-based Detection)**
 - Ưu điểm: có khả năng phát hiện cả mối nguy hiểm đã biết và chưa được biết tới.
 - Nhược điểm: phải được xây dựng từ đầu theo chính sách an ninh mạng.

Các kỹ thuật phát hiện (detection)

- **Phát hiện dựa trên Honey pot**

Phương pháp này dựa trên nguyên lý Honey pot để hấp dẫn những kẻ tấn công tập trung vào các Honey pot. Từ đó máy chủ thực sự sẽ không phải là mục tiêu cuộc tấn công và người quản trị mạng sẽ dùng các dữ liệu thu thập được từ Honey pot để phân tích kỹ thuật tấn công.

Thành phần chính của IDS/IPS

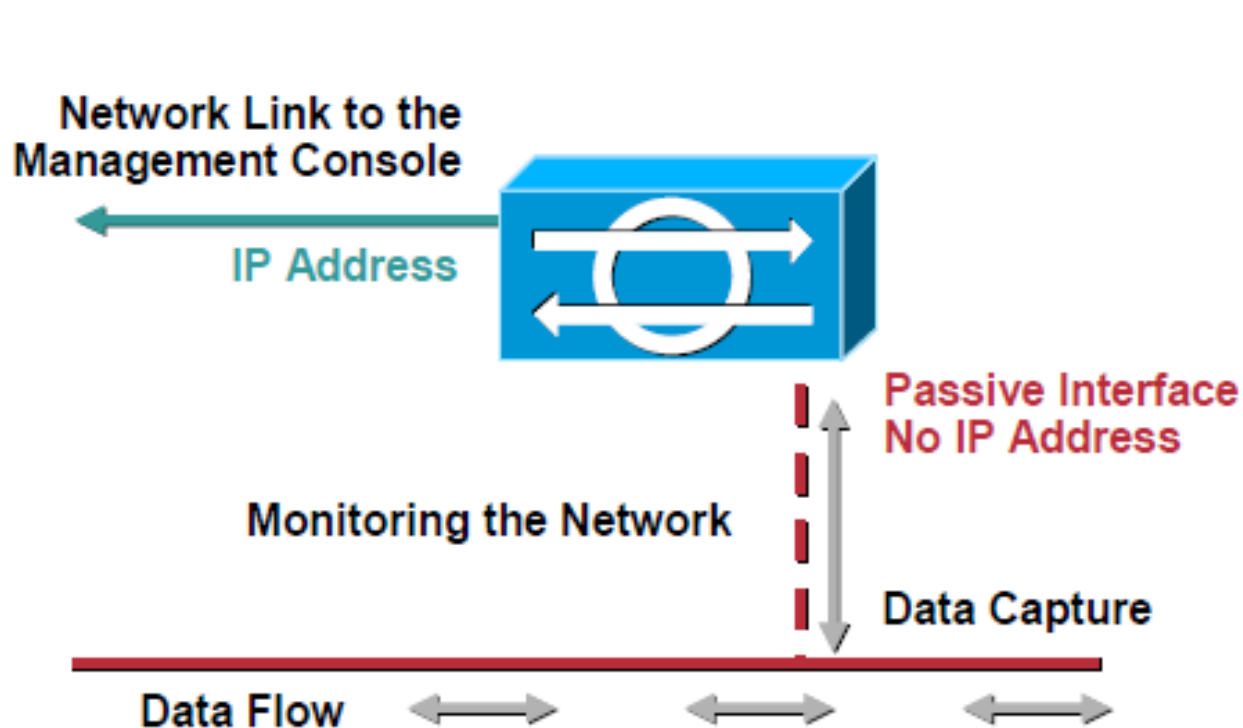
- Bộ cảm biến: giám sát và phân tích các hoạt động.
- Server quản lý (management server): là thiết bị tập trung để nhận thông tin từ các bộ cảm biến và quản lý chúng.
- Database server: là một kho lưu trữ thông tin sự kiện được ghi bởi bộ cảm biến và/ hoặc server quản lý
- Console: là chương trình cung cấp giao diện cho người quản trị quản lý thiết bị IDP/IPS.

Thành phần chính của IDS/IPS

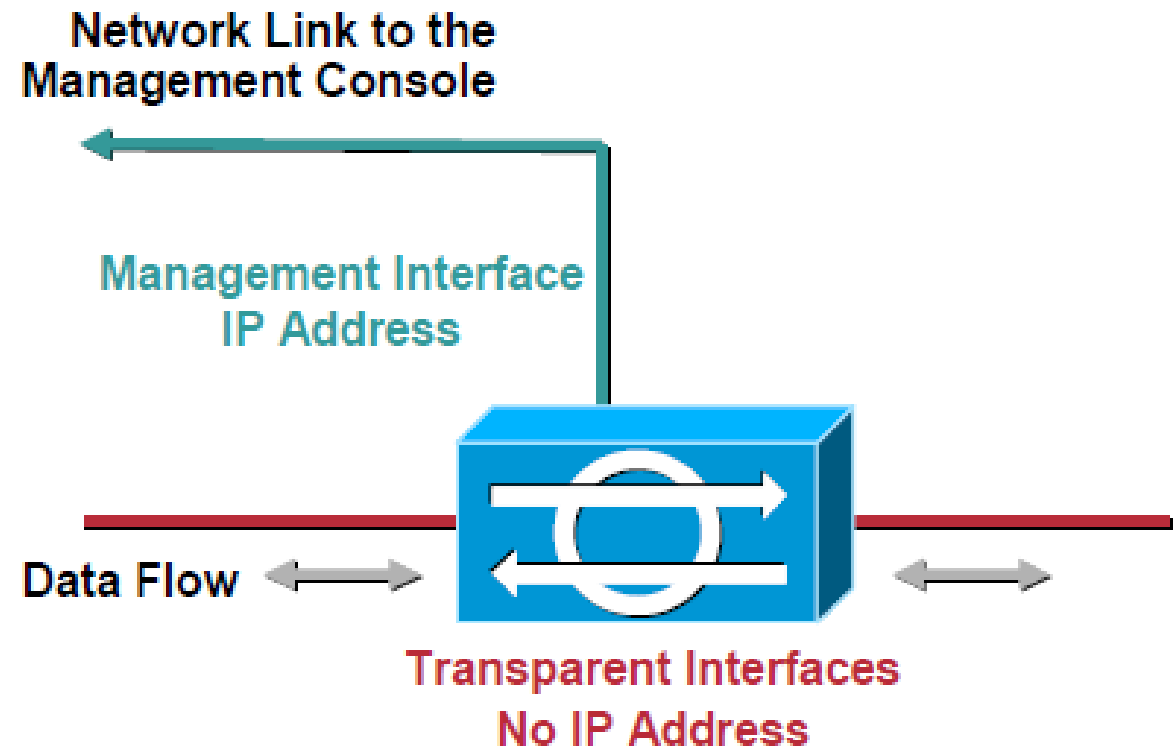
- **Bộ cảm biến IPS (Sensor)**
 - Cảm biến IPS phân tích các packet khi chúng đi vào cổng (interface) của cảm biến.
 - Cảm biến so sánh lưu lượng xấu với các signature của IPS để đưa ra các phản ứng thích hợp: ngưng lưu lượng, gửi cảnh báo cho người quản trị mạng.

Thành phần chính của IDS/IPS

- Bộ cảm biến (Sensor)



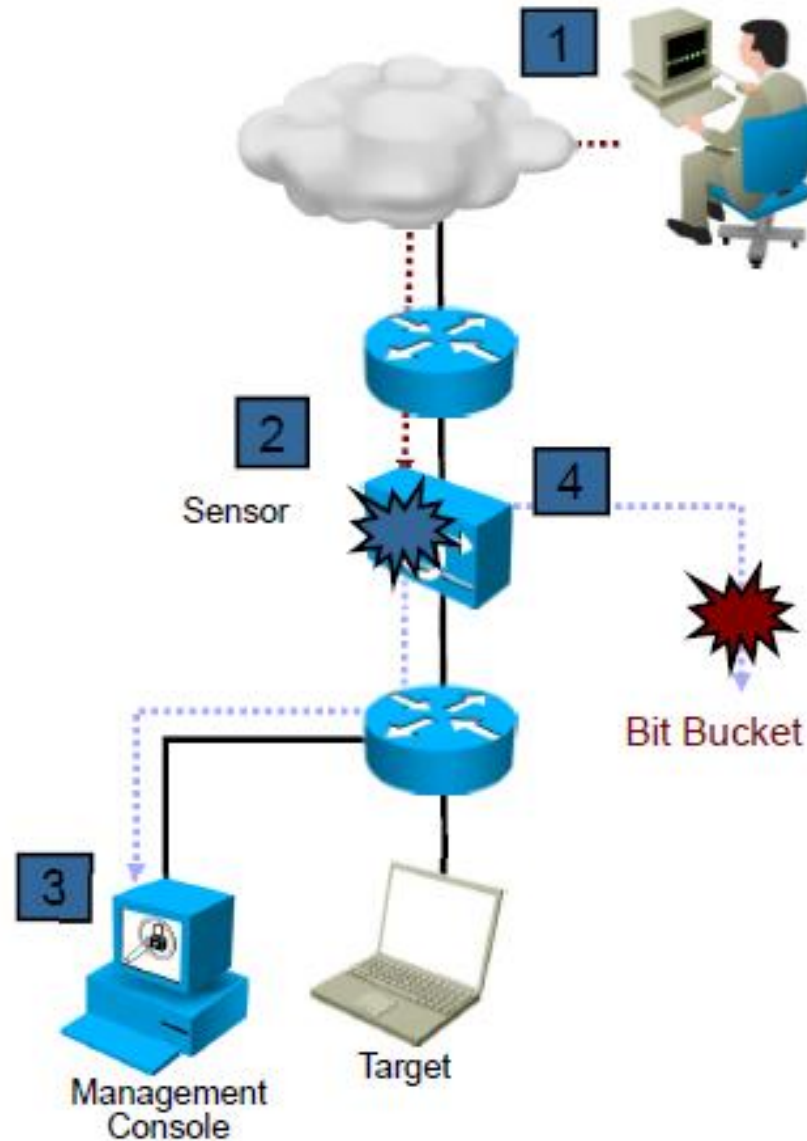
Network-based IDS: The Sensor



Network-based IPS: The Sensor

Thành phần chính của IDS/IPS

- Bộ cảm biến (Sensor)



Thành phần chính của IDS/IPS

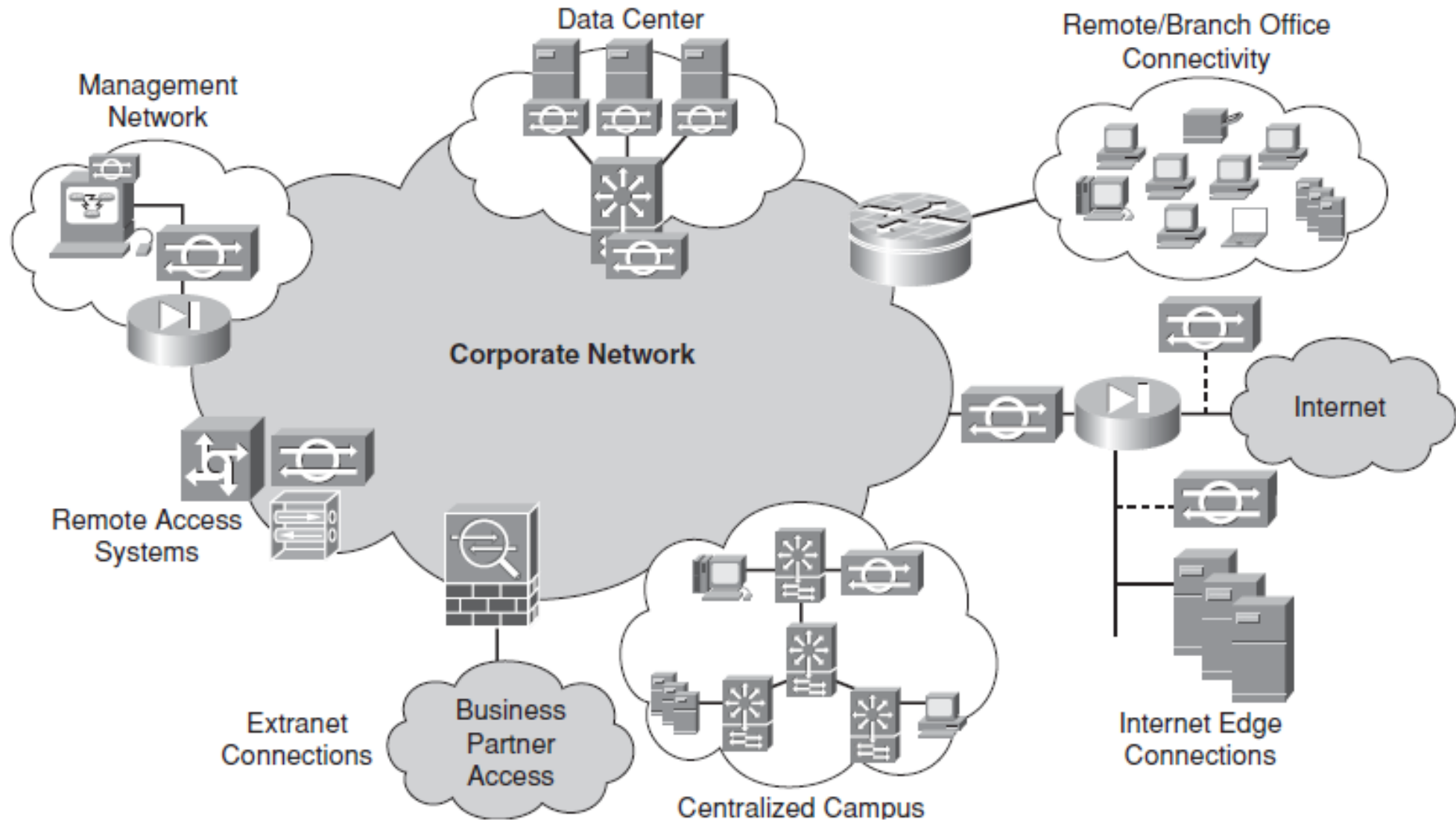
- **Bộ cảm biến (Sensor)**

Khi nào cần tăng số lượng cảm biến trong hệ thống mạng?

- Thực thi chính sách bảo mật: tăng số lượng cảm biến để thực thi các ranh giới bảo mật dựa trên chính sách bảo mật hoặc thiết kế của hệ thống mạng.
- Vượt quá khả năng lưu lượng mạng: yêu cầu thêm băng thông có thể làm tăng thêm các đường link trong hệ thống mạng. Do đó, tăng số lượng cảm biến để đáp ứng yêu cầu bảo mật.
- Khả năng hiệu suất của cảm biến: cảm biến hiện tại không đáp ứng được lưu lượng trong hệ thống mạng.

Triển khai IDS/IPS

- Vị trí triển khai?



PHẦN CỨNG VÀ PHẦN MỀM HỖ TRỢ IDS/IPS

- Các thiết bị Cisco hỗ trợ NIPS
- Các dòng cảm biến Cisco IPS 4200 series
- Cisco ASA AIP SSM và AIP SSC-5
- Cisco AIM-IPS và NME-IPS trên Cisco ISR routers
- Cisco Catalyst 6500 Series IDSM-2 Module
- Kiến trúc phần mềm của Cisco IPS
- Snort

Các thiết bị Cisco hỗ trợ NIPS

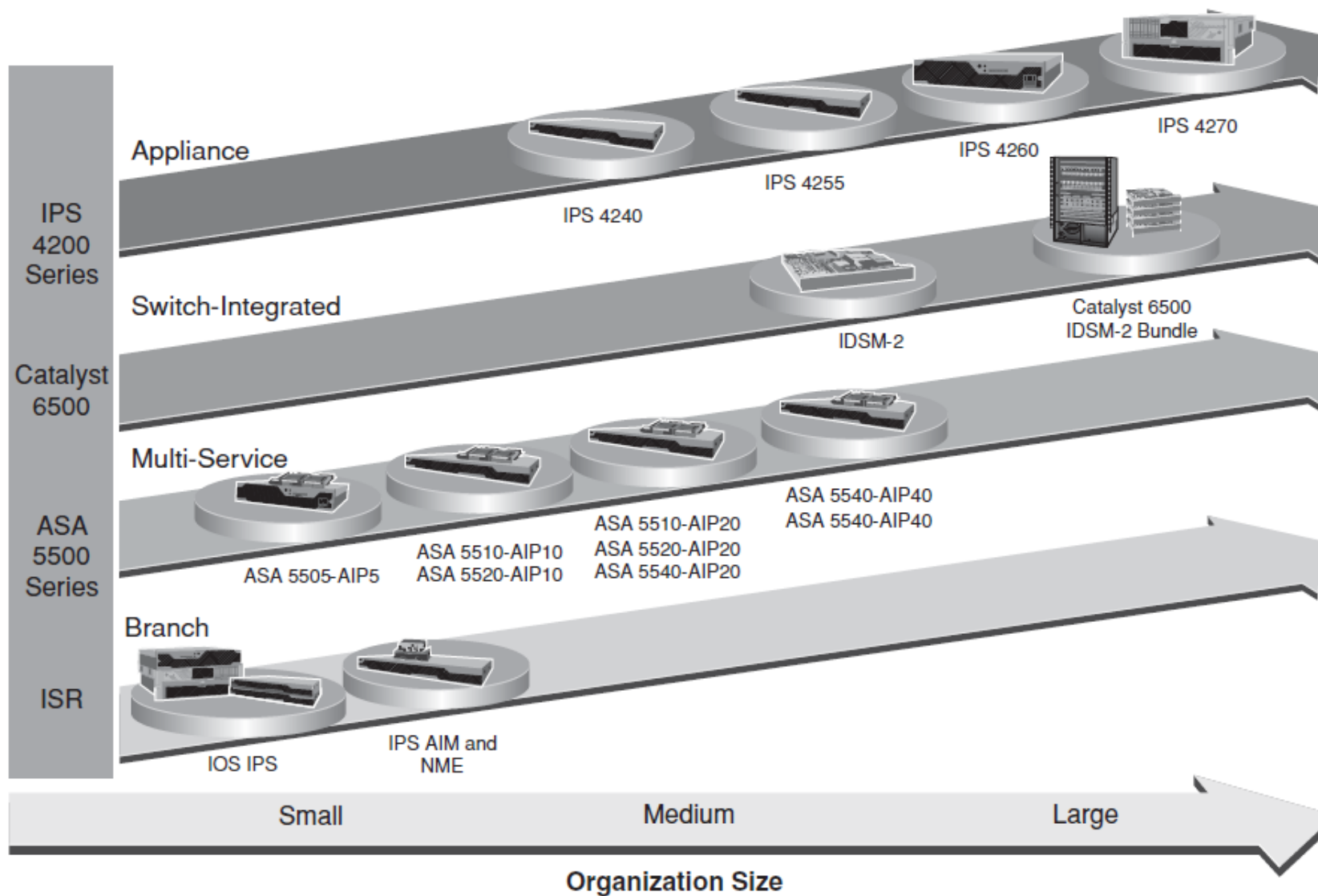
- Cisco có nhiều hệ thống cảm biến IPS đáp ứng các yêu cầu khác nhau.
- Cần phải đánh giá, lựa chọn các ứng dụng nền tảng, mô hình và cách quản lý phù hợp đáp ứng các yêu cầu này.

Các thiết bị Cisco hỗ trợ NIPS

Hệ thống sensor của Cisco chia thành các nhóm chính:

- Các thiết bị IPS độc lập như Cisco IPS 4200 series sensors.
- Các router Cisco tích hợp dịch vụ như Cisco AIM-IPS, NME-IPS.
- Các module của hệ thống tìm kiếm phát hiện xâm nhập như Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Modules.
- Tích hợp vào các mô đun dịch vụ an ninh và kiểm tra tiên tiến của Cisco ASA 5500 Series (AIP SSC-5, AIP SSM-10, AIP SSM-20 và AIP SSM-40).




Các thiết bị Cisco hỗ trợ NIPS



Các dòng cảm biến Cisco IPS 4200 series

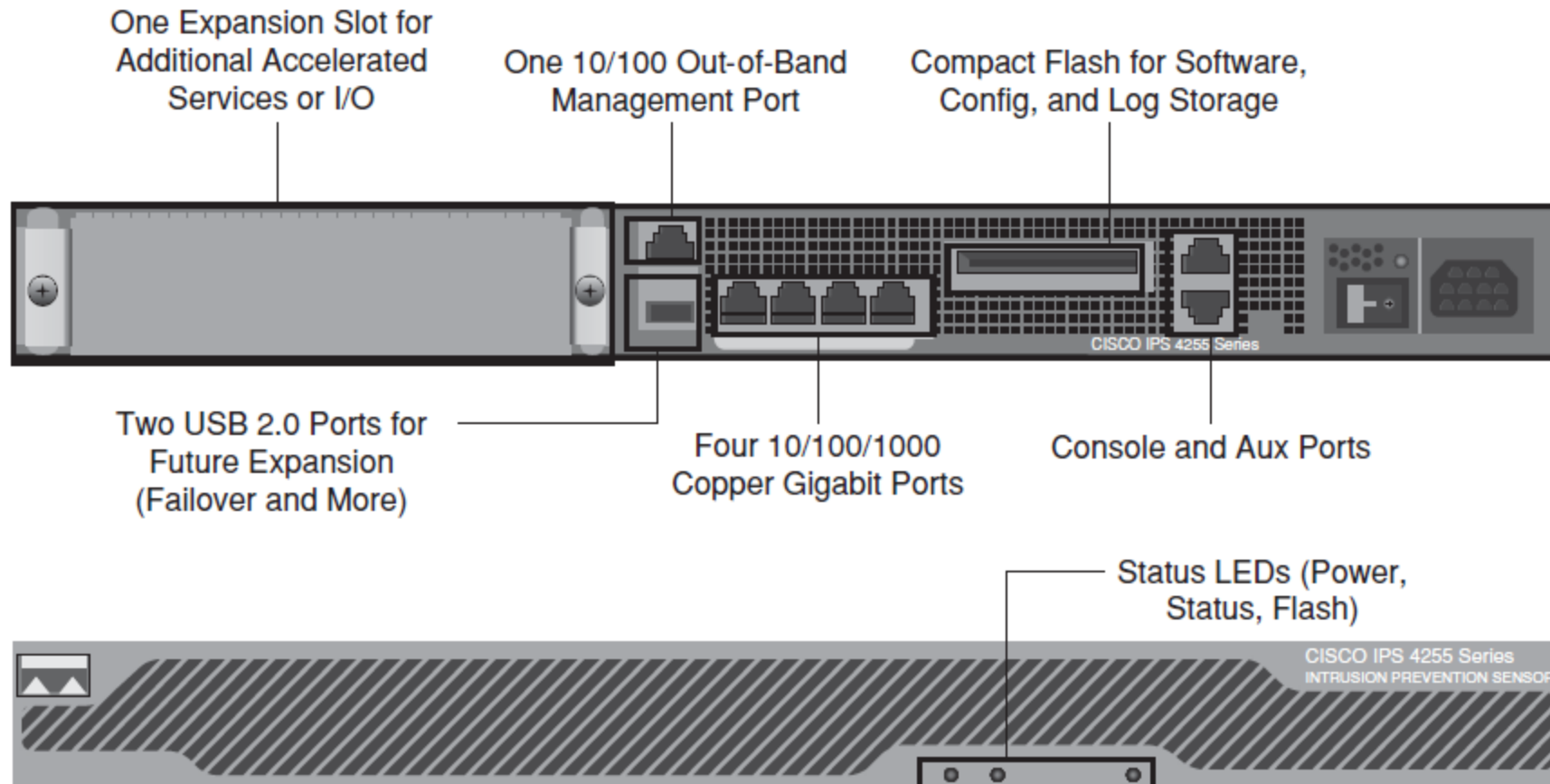
- Đây là các bộ cảm biến IPS độc lập và chuyên dụng.
- Các thiết bị này có thể vận chuyển thông lượng lên tới 4Gbps.

Các dòng cảm biến Cisco IPS 4200 series

Đặc điểm	Cảm biến Cisco IPS 4240	Cảm biến Cisco IPS 4255	Cảm biến Cisco IPS 4260	Cảm biến Cisco IPS 4270
				
Thông lượng	300 Mbps	600 Mbps	2 Gbps	4Gbps
Số lượng cổng cảm biến	4	4	1	4
Cổng điều khiển	10/100Base-TX	10/100Base-TX	10/1001000 Base-TX	10/1001000 Base-TX
Năng lượng nguồn dự phòng	không	không	Tùy chọn	có

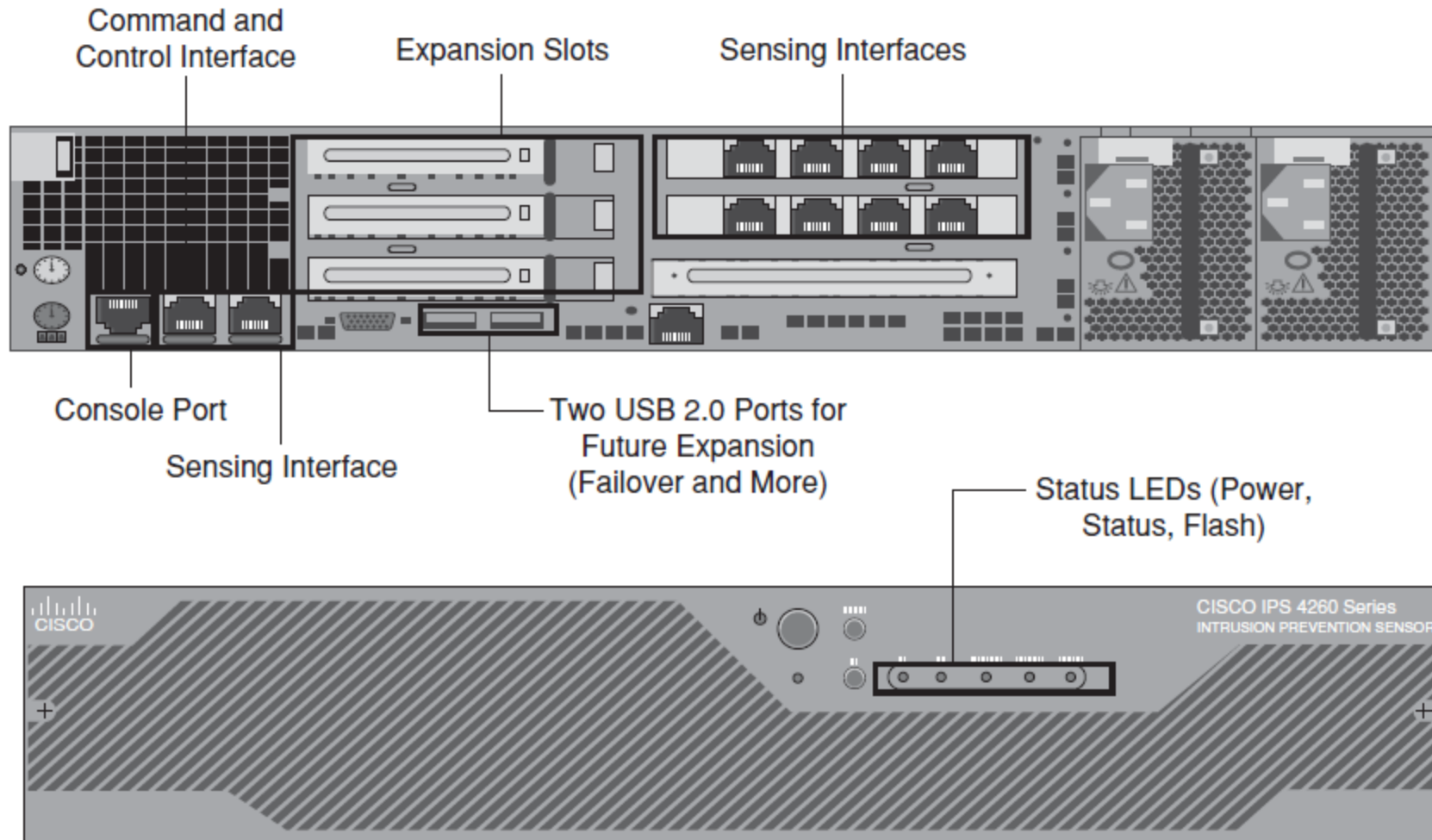
Các dòng cảm biến Cisco IPS 4200 series

4255



Các dòng cảm biến Cisco IPS 4200 series

4260



Cisco ASA AIP SSM và AIP SSC-5

- Các Mô-đun AIP SSM và AIP SSC được tích hợp vào các dòng Cisco ASA 5500 để cung cấp tính năng phát hiện và ngăn ngừa xâm nhập mạng.

Cisco ASA AIP SSM và AIP SSC-5

	Cisco ASA AIP SSC-5	Cisco ASA AIP SSM-10	Cisco ASA AIP SSM-10	Cisco ASA AIP SSM-20
Supported Platforms	ASA 5505	ASA 5510 ASA 5520	ASA 5520 ASA 5540	ASA 5520 ASA 5540
Maximum Traffic Throughput	75 Mbps (ASA 5505)	225 Mbps (ASA 5520)	500 Mbps (ASA 5540)	650 Mbps (ASA 5540)
Monitoring Interfaces	ASA backplane interface	ASA backplane interface	ASA backplane interface	ASA backplane interface
Command and Control Interface	Backplane VLAN	10/100BASE- TX	10/100BASE- TX	10/100/1000BASE- TX
Global Correlation	No	Yes	Yes	Yes
Anomaly Detection	No	Yes	Yes	Yes
Customer Signa- ture Support	No	Yes	Yes	Yes
Virtual Sensors	1	4	4	4

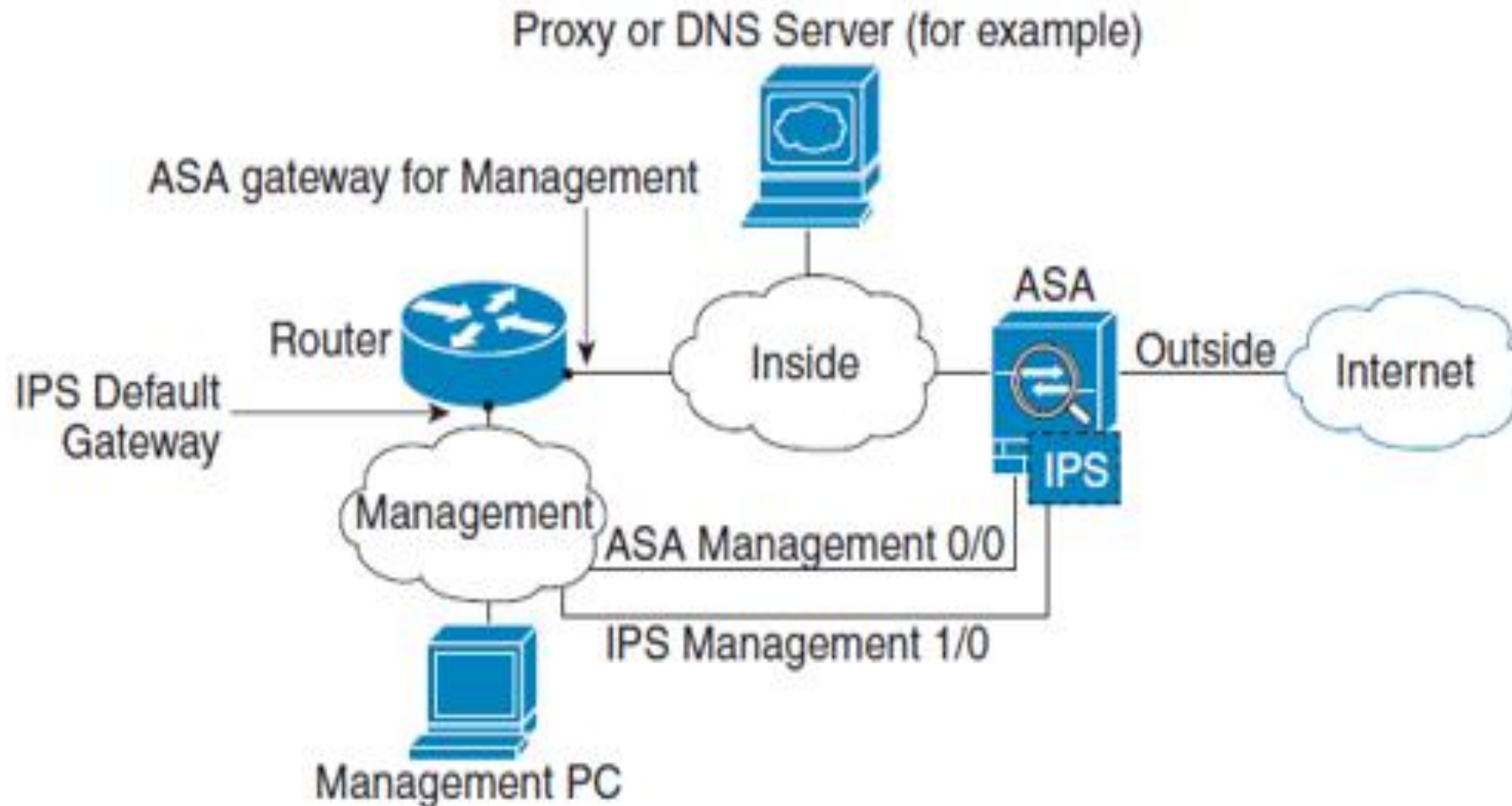
Cisco ASA AIP SSM và AIP SSC-5

Cisco ASA 5505



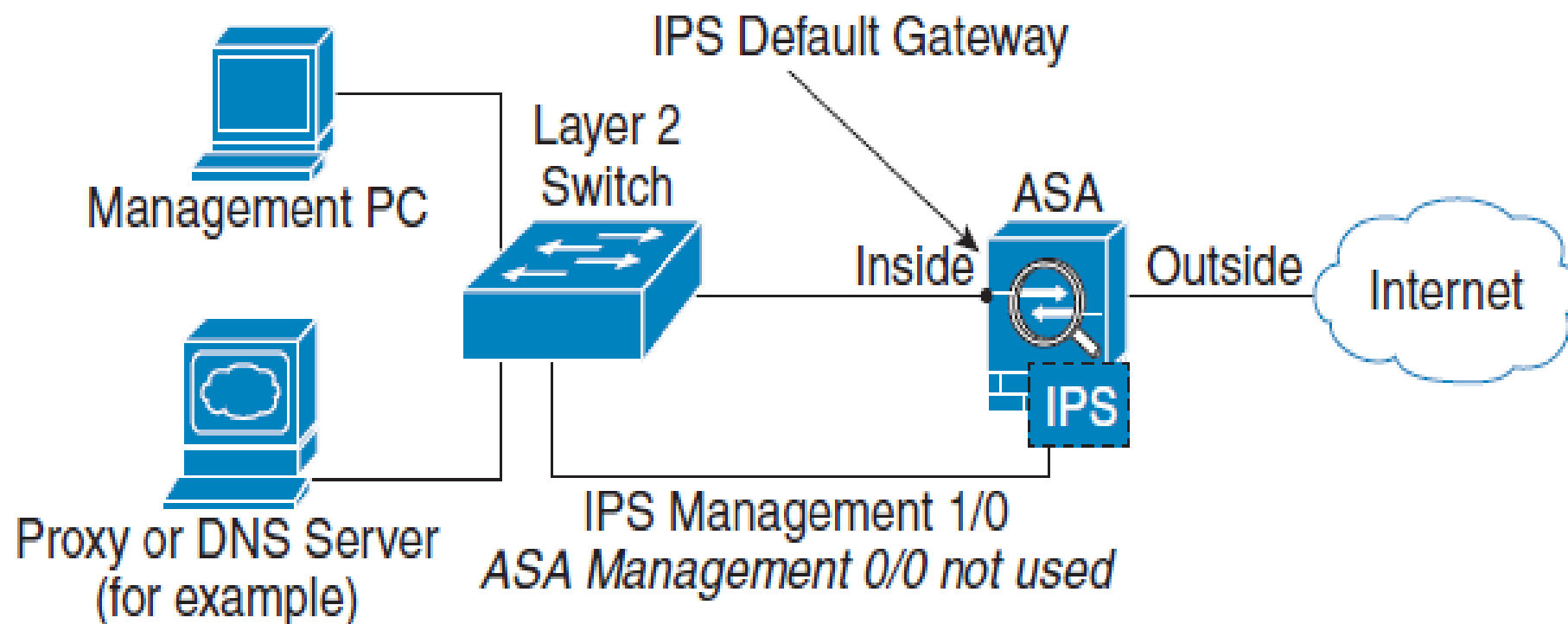
Cisco ASA AIP SSM và AIP SSC-5

Vị trí của ASA trong hệ thống mạng có bộ định tuyến



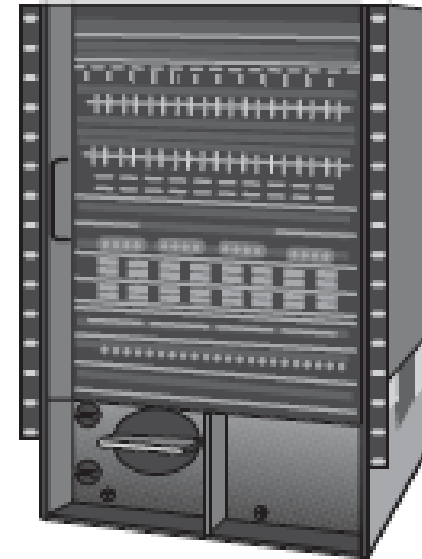
Cisco ASA AIP SSM và AIP SSC-5

Vị trí của ASA trong hệ thống mạng không có bộ định tuyến

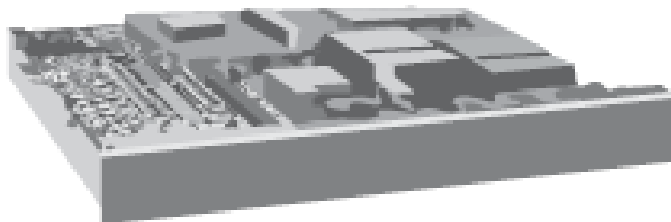


Cisco Catalyst 6500 Series IDSM-2 Module

- IDSM-2 has no physical interfaces (no console or LAN ports)
- Up to eight IDSM-2 per chassis scalable with etherchannel load balancing
- Catalyst 6500 backplane used for
 1. Initial console access (boot-strap)
 2. Management access via SSH, SDEE
 3. Data traffic IPS mode
 4. Data traffic IDS mode

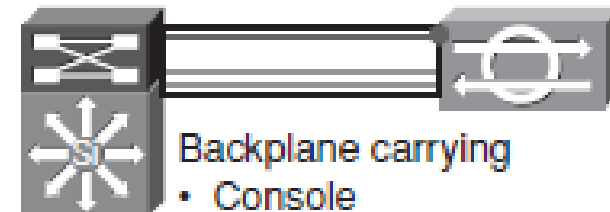


Physical View



No Physical Ports

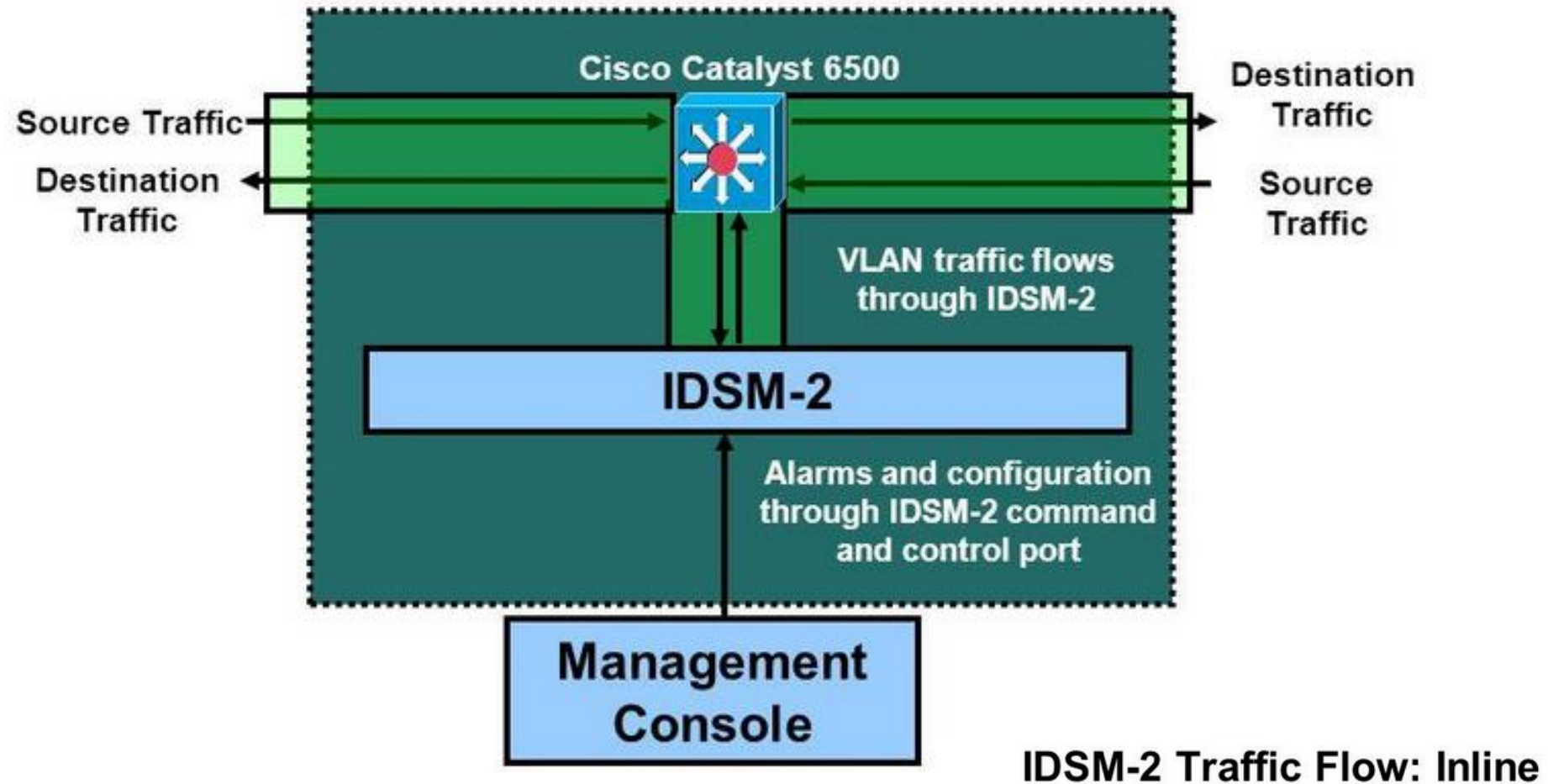
Logical View



Backplane carrying

- Console
- Management network
- Data VLANs (IDS)
- Data VLANs (IPS)

Cisco Catalyst 6500 Series IDSM-2 Module



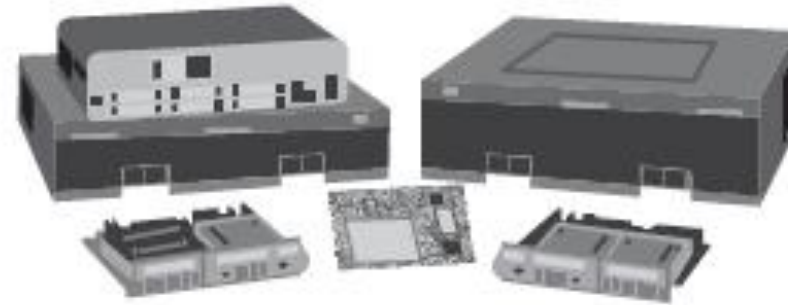
Cisco AIM-IPS và NME-IPS trên Cisco ISR routers

- **AIM:** Cisco IPS Advanced Integration Module
- **NME:** Network Module Enhanced
- **Các dòng router hỗ trợ AIM:** Cisco router 1841, 2801, 2811, 2821, 2851, 3825, 3845
- **Các dòng router hỗ trợ NME:** Cisco router 2811, 2821, 2851, 2911, 2921, 2951, 3825, 3845, 3925, 3945.

Cisco AIM-IPS và NME-IPS trên Cisco ISR routers



Physical View



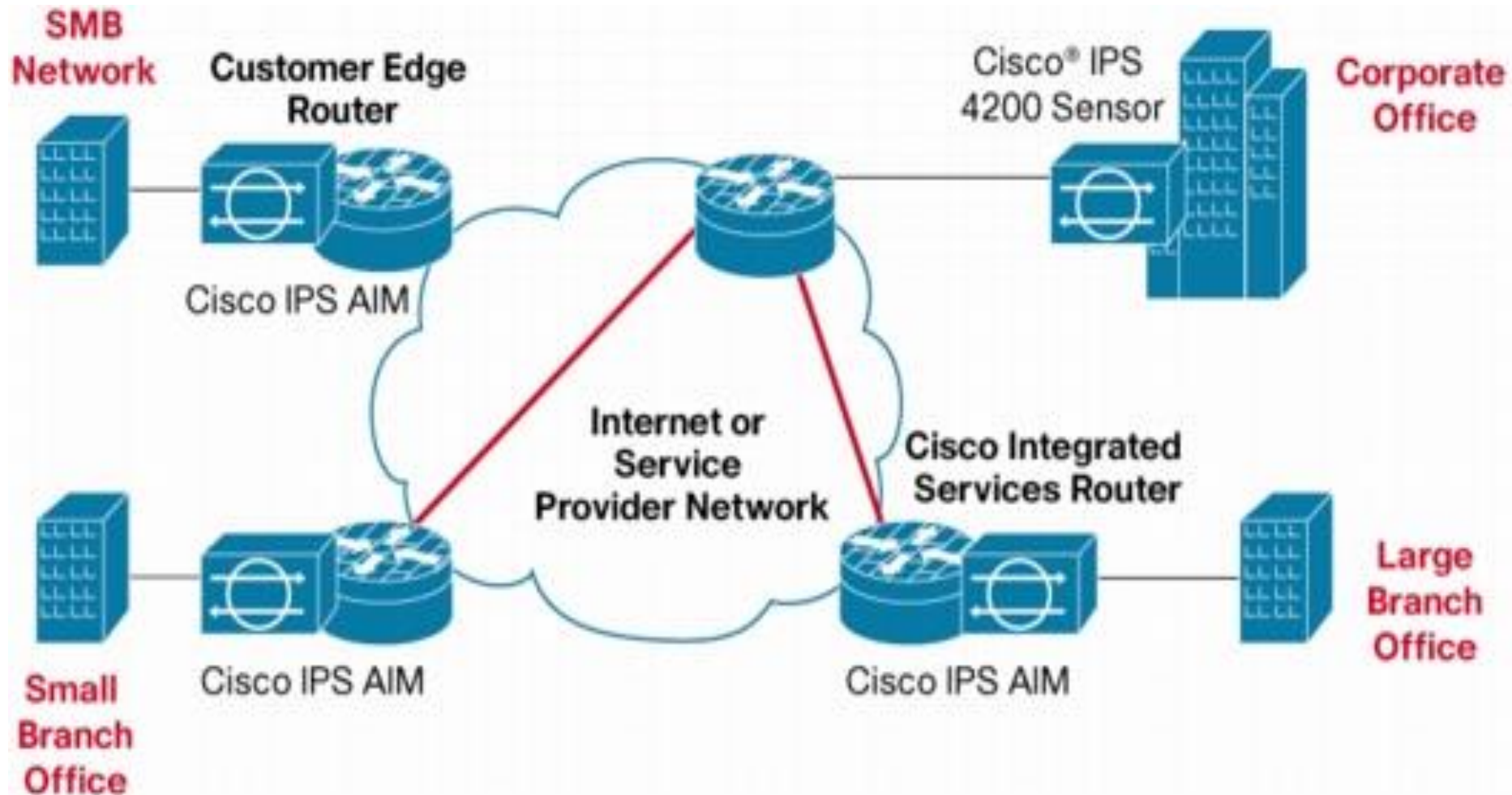
No Physical
Console

Management Port

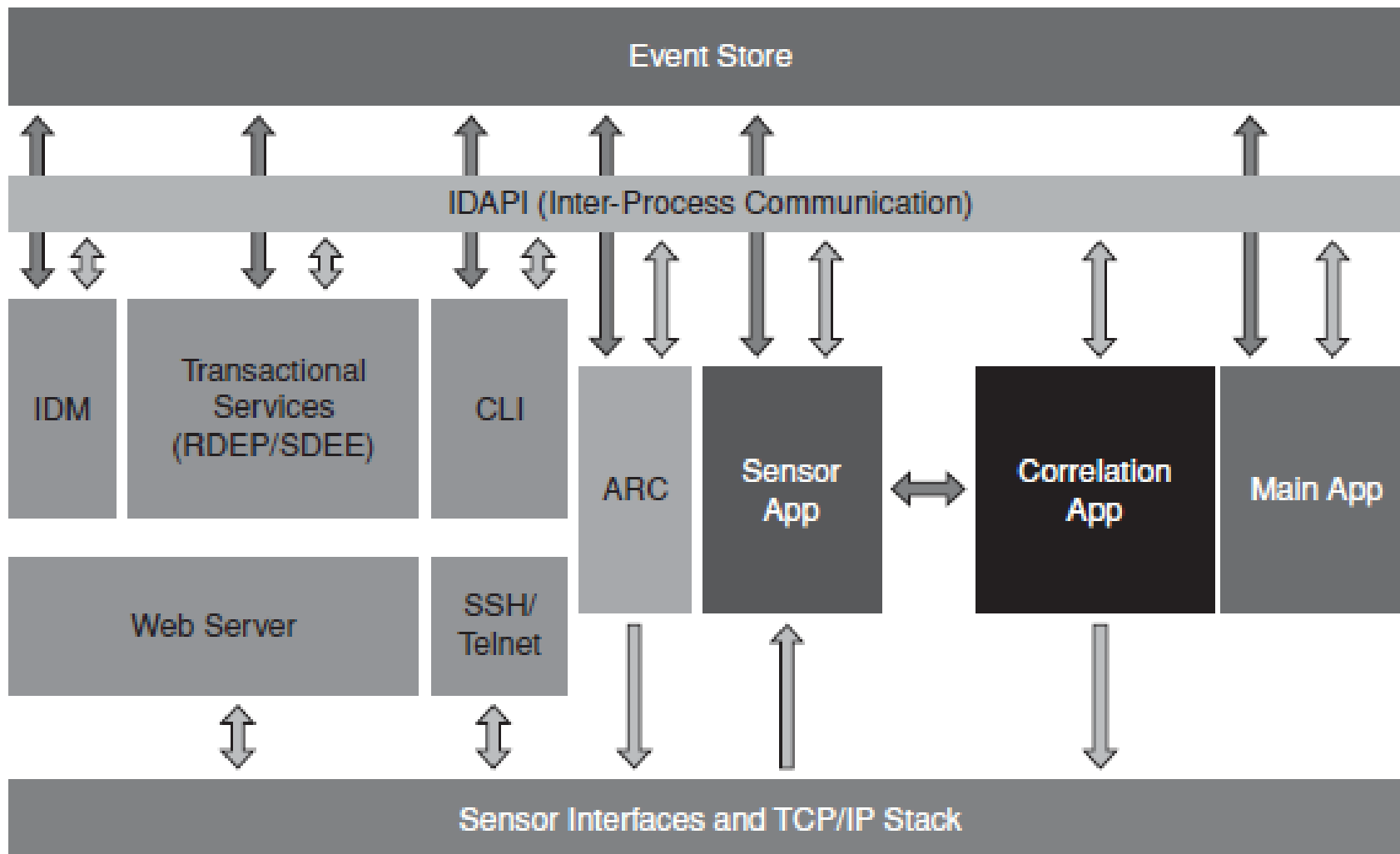
Logical View



Cisco AIM-IPS và NME-IPS trên Cisco ISR routers



Kiến trúc phần mềm của Cisco IPS



Kiến trúc phần mềm của Cisco IPS

Cisco IPS Manager Express (IME)

All-In-One IPS Management Application for up to 10 IPS Sensors

Startup Wizard: Gets you up and running in just minutes

Dashboard: Puts needed information at your finger tips

Configuration: Save time with intuitive interface

Reporting: Create and share security and compliance reports

Monitoring: See what's happening with real-time and historical security events

The screenshot displays the Cisco IPS Manager Express (IME) web interface. The top section shows the 'Dashboard' with two circular gauges for 'Sensor Health' and 'Network Security Health'. Below these, there's a table of sensors. The bottom section shows the 'Configuration' area with a list of sensors and a table of policies. The interface is clean and professional, with a blue header and a white background.

SNORT

- Snort là một chương trình NIDS (Network intrusion detection system) dùng để bảo vệ hệ thống bên trong, ngăn chặn và cảnh báo các cuộc tấn công từ bên ngoài.
- Snort được Martin Roesch phát triển dưới dạng mã nguồn mở nhằm kiểm tra các gói dữ liệu trên mạng bằng cách tạo các rule phát hiện các gói dữ liệu bất thường.
- Snort có thể chạy trên nhiều hệ thống như Windows, Linux, Solaris, MacOS...
- Snort hỗ trợ khả năng hoạt động trên nhiều giao thức như Ethernet, 802.11, Token ring, FDDI, SLIP, PPP, Cisco HDLC...

SNORT

Snort Setup Guides

Snort 2.9.8.x on CentOS 6.x and 7.x 

Snort 2.9.8.x on Fedora 22 

Snort 2.9.8.x on NetBSD 5.1.x 

Snort 2.9.9.x on Ubuntu 14 -16 

Snort 2.9.8.x on OpenSuSE 12x 

Snort 2.9.9.x on OpenSuSE Leap 42.2 

Snort 2.9.8.x on OpenSuSE 13x 

Snort 2.9.8.x on Fedora 17/18/19 

Snort 2.9.8.x on OpenBSD 5.x 

Snort 3 on Ubuntu 14 and 16 

Snort Setup Guides for Windows 

Snort 2.9.0.x with PF_RING inline
deployment 

William Parker

William Parker

William Parker

Noah Dietrich

William Parker

Boris Gamez

William Parker

William Parker

William Parker

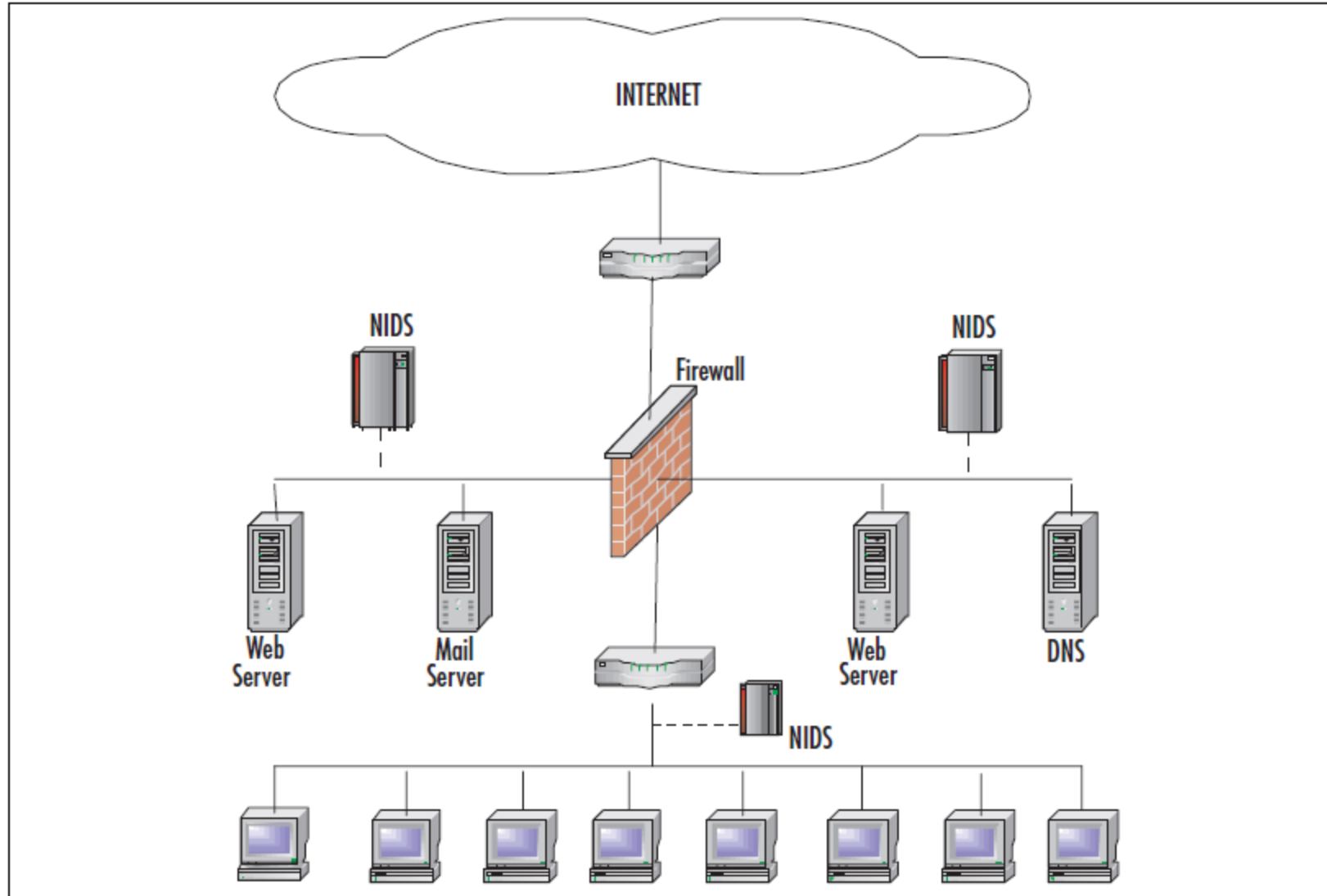
Noah Dietrich

WinSnort.com

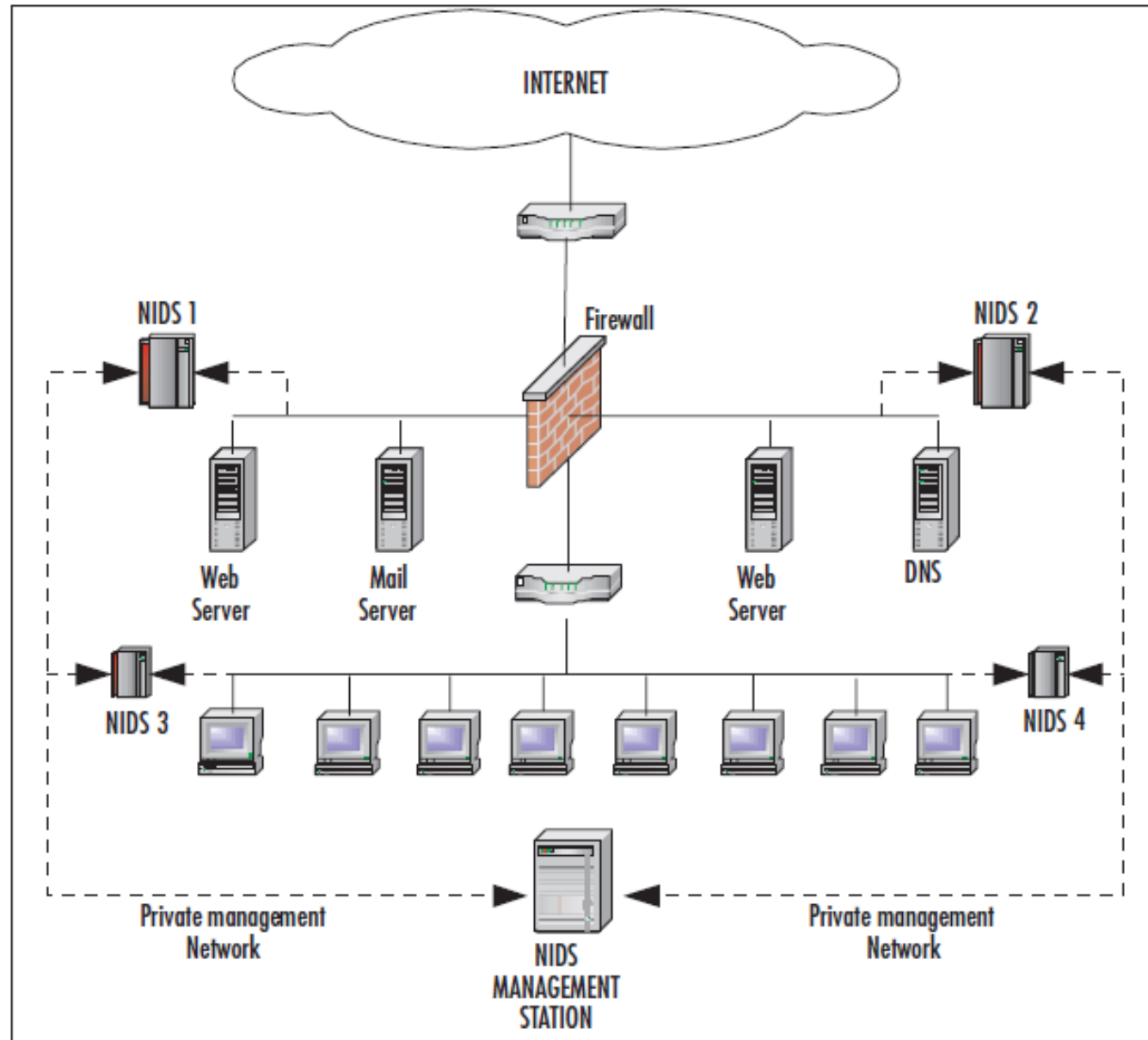
Metaflows Google

Group

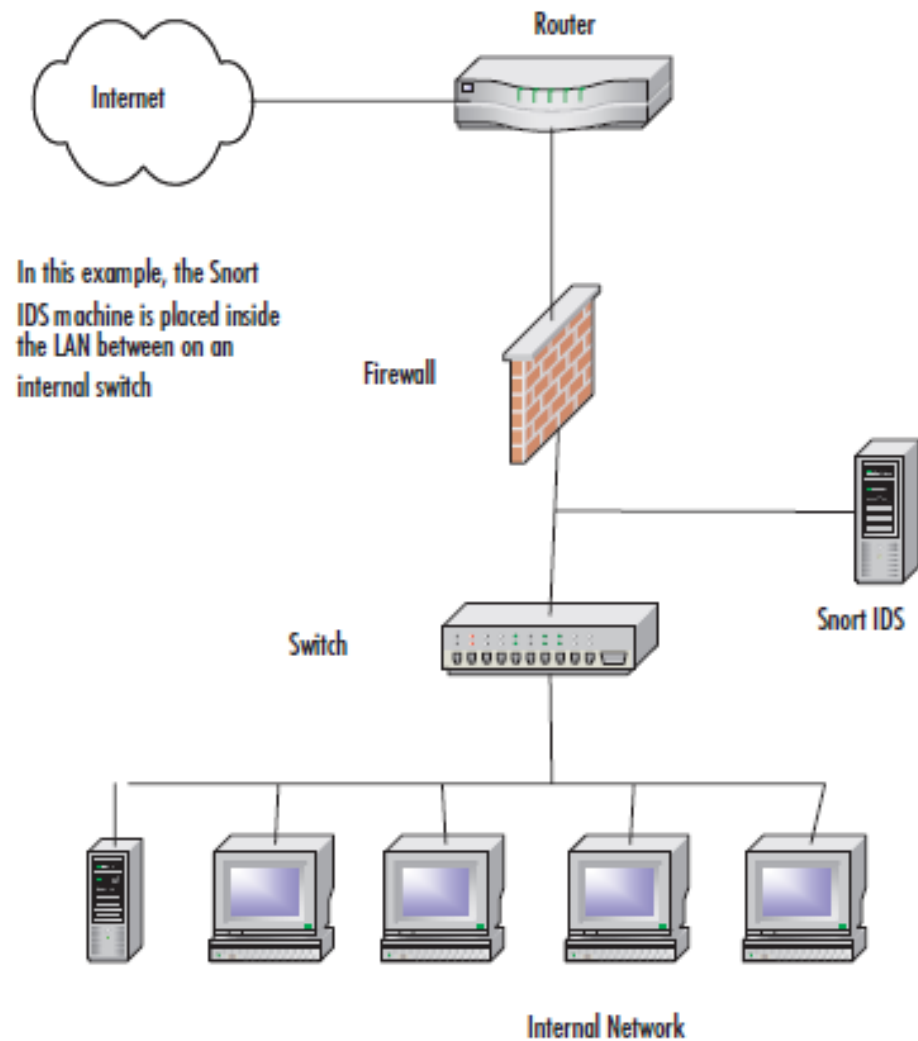
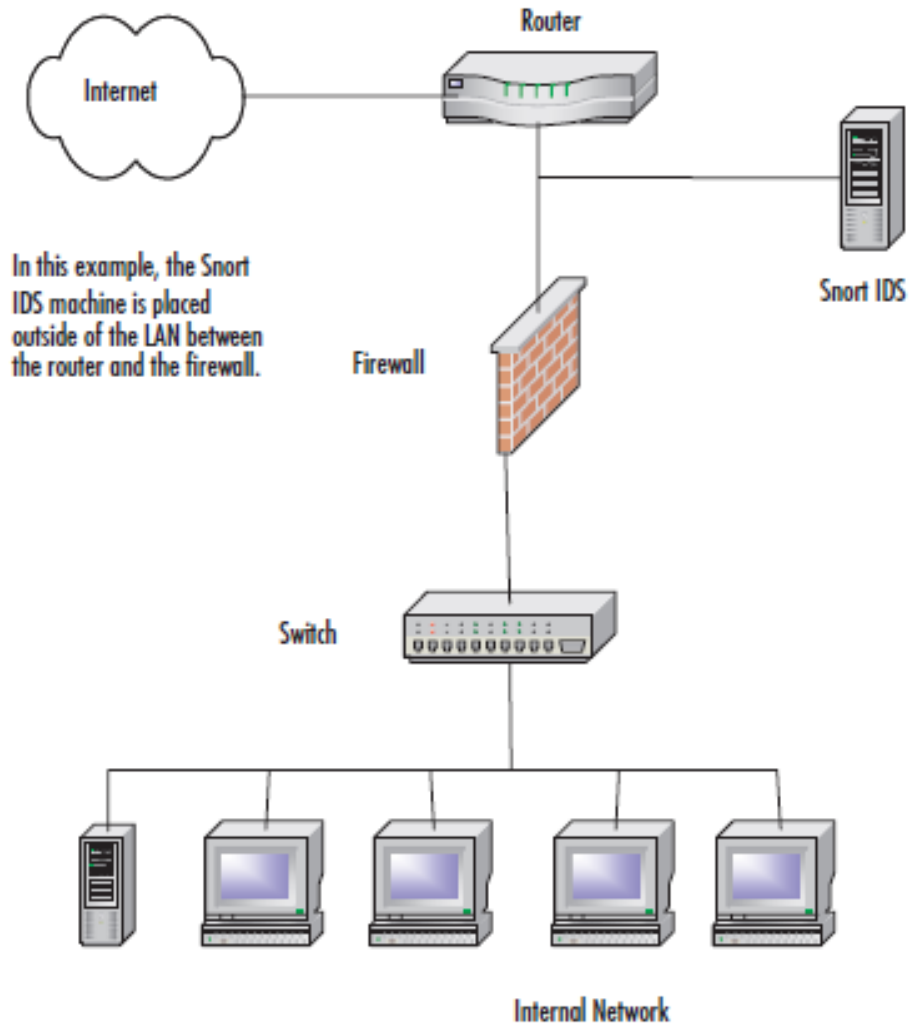
SNORT



SNORT



SNORT



SNORT

Snort có thể cấu hình để chạy trong 3 chế độ:

- Sniffer mode: đọc các gói tin trên mạng và hiển thị chúng ra màn hình.
- Packet logger mode: ghi các log của các gói tin lên đĩa cứng.
- Network intrusion detection system (NIDS) mode: thực hiện việc tìm kiếm và phân tích traffic trên mạng. Đây là chế độ phức tạp nhất và có thể cấu hình được.

SNORT

Các thành phần chính của Snort:

- Packet Decoder (module giải mã gói tin): Snort sử dụng thư viện pcap để bắt các gói tin trên hệ thống mạng và đưa vào module tiền xử lý.
- Preprocessors (module tiền xử lý):
 - chuẩn bị dữ liệu cho việc phân tích,
 - phân tích header của gói tin để phát hiện sự bất thường,
 - chống phân mảnh gói tin,
 - lắp ráp lại các gói TCP, UDP...

SNORT

Các thành phần chính của Snort:

- Detection Engine (module phát hiện): so sánh dữ liệu thu thập được với các rule đã được định nghĩa trước trên cả gói tin hoặc từng thành phần riêng biệt của gói tin như IP header, TCP header, UDP header, DNS header, HTTP header, FTP header, payload...

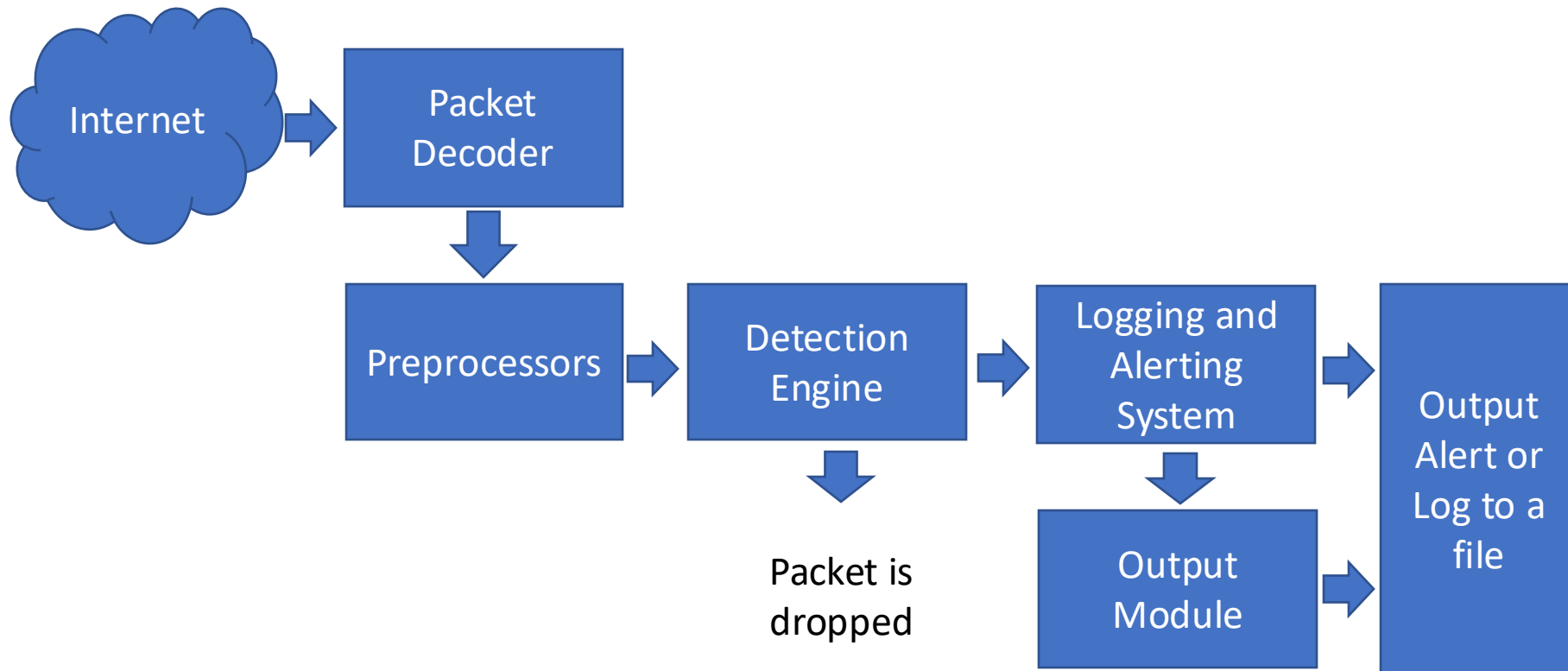
SNORT

Các thành phần chính của Snort:

- Logging and Alerting System (module log và cảnh báo): gói tin sau khi được phân tích có thể bị ghi vào file log hoặc đưa ra cảnh báo tùy kết quả phân tích ở module trước.
- Output Module (module kết xuất thông tin): xuất thông tin ra các định dạng khác nhau đã được cấu hình trước.

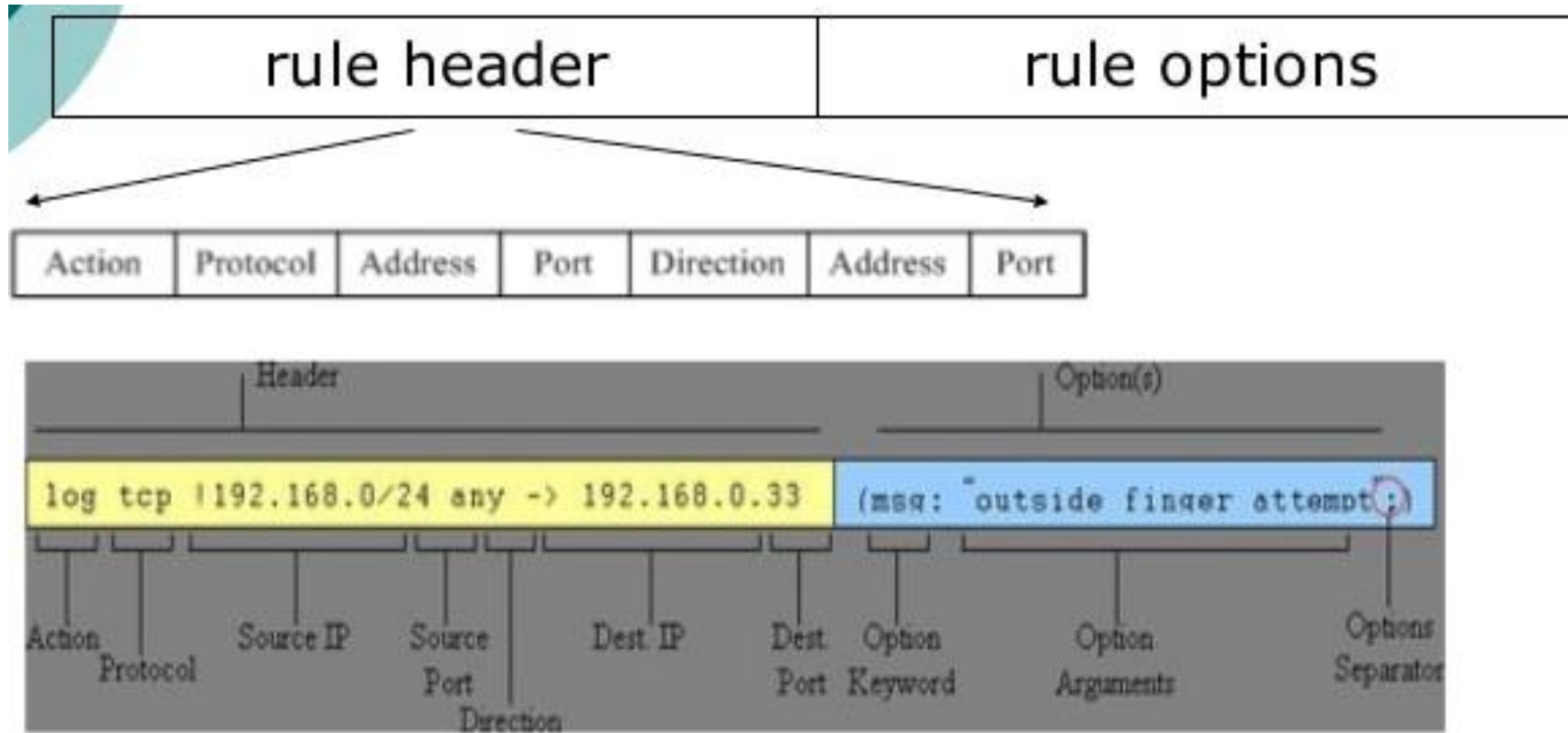
SNORT

Cơ chế hoạt động của Snort:



SNORT

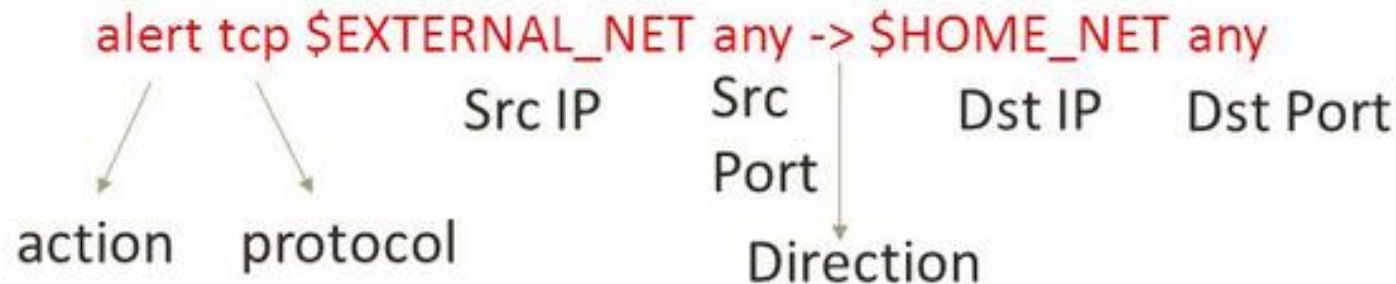
Nguyên tắc của các rule:



SNORT

Nguyên tắc của các rule:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any \  
  (msg:"SCAN SYN FIN";flags:SF; reference: arachnids,198; \  
  classtype:attempted-recon; sid:624; rev:1;)
```



1. **alert**: Alerts and logs the packet when triggered.
2. **log**: Only logs the packet when triggered.
3. **pass**: Ignores or drops the packet or traffic matching.
4. **activate**: Alerts then activates a dynamic rule or rules.
5. **dynamic**: Ignores, until started by the activate rule, at which time, acts as a log rule.
6. **drop**: block and log the packet
7. **reject**: block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
8. **sdrop**: block the packet but do not log it.

SNORT

Ví dụ:

- Detecting when root user is trying to send an email:

```
1 | alert tcp any any -> 192.168.1.0/24 25 (sid:1002345;rev:2;msg:  
"root users attempts to send an email"; content: "mail from:  
root";classtype:suspicious-login;)
```

TCP	Source Port		Dest Port		R	R	U	A	P	S	R	F	seq #	ack	offset	res	window	urg	checksum
	33663		25						X	X			248748397	2105662115	32	0	115	0	21778 = 0x5512
	[source] [target] [state]		[source] [target] [state]																
Options		code		length	data														
		#1	(1) NOP	0															
		#2	(1) NOP	0															
		#3	(8) TS	8	001103AA0EE5A649														
Payload																			
Plain Display		length = 27																	
Download of Payload		000 : 4D 61 69 6E 20 65 72 6F 6D 3A 20 72 6F 6F 74 40 mail from: root@ 010 : 6C 6F 63 61 6C 68 6F 73 74 6D 6A localhost..																	
Download in pcap format																			

SNORT

Ví dụ:

- Identifying the source of icmp traffic of a windows host:

```
alert icmp any any -> 192.168.1.0/24 any (sid:1002356;msg:"Hey!!  
A windows Host is pinging me!";itype:8;content:"|6566 6768 696a  
6b6c 6d6e 6f70 7172 7374 7576 7761 6263 6465 6667  
6869|";nocase;depth:32;classtype:icmp-event;)
```

IP	<table><tr><th>Source Address</th><th>Dest. Address</th><th>Ver</th><th>Hdr Len</th><th>TOS</th><th>length</th><th>ID</th><th>fragment</th><th>offset</th><th>TTL</th><th>checksum</th></tr><tr><td>192.168.1.131</td><td>192.168.1.250</td><td>4</td><td>20</td><td>0</td><td>60</td><td>4594</td><td>no</td><td>0</td><td>128</td><td>41905 = 0xa401</td></tr></table>											Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	fragment	offset	TTL	checksum	192.168.1.131	192.168.1.250	4	20	0	60	4594	no	0	128	41905 = 0xa401																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
	Source Address	Dest. Address	Ver	Hdr Len	TOS	length	ID	fragment	offset	TTL	checksum																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																								
	192.168.1.131	192.168.1.250	4	20	0	60	4594	no	0	128	41905 = 0xa401																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																								
<table><tr><td>Options</td><td>none</td></tr></table>											Options	none																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																							
Options	none																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
ICMP	<table><tr><th>type</th><th>code</th><th>checksum</th><th>ID</th><th>seq #</th></tr><tr><td>(8) Echo Request</td><td>(0) 0</td><td>19796 = 0x4d54</td><td>1</td><td>7</td></tr></table>											type	code	checksum	ID	seq #	(8) Echo Request	(0) 0	19796 = 0x4d54	1	7																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														
	type	code	checksum	ID	seq #																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														
	(8) Echo Request	(0) 0	19796 = 0x4d54	1	7																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														
Payload																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			
Plain Display	length = 32																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
	Download of Payload																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
	<table><tr><td>000</td><td>:</td><td>61</td><td>62</td><td>63</td><td>64</td><td>65</td><td>66</td><td>67</td><td>68</td><td>69</td><td>6A</td><td>6B</td><td>6C</td><td>6D</td><td>6E</td><td>6F</td><td>70</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>											000	:	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F	70																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						
000	:	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F	70																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		

SNORT

Ví dụ:

- Alert all SMTP traffic that contains a file virus.exe attached:

```
1 | alert tcp any any -> 192.168.1.0/24 25 (sid:1002311; rev:3;
msg:"Warning!! The virus.exe is included in one mail!!";
content:"filename=\"virus.exe\""; classtype:suspicious-filename-
detect;)
```

	Source Port			Dest Port			R	R	U	A	P	S	S	F	seq #	ack	offset	res	window	urp	chksum	
	[sane]	[proto]	[state]	[sane]	[proto]	[state]	1	0	G	K	H	T	N	N								
TCP	51005			25						X	X				2094453262	730853246	32	0	115	0	28797 = 0x707d	
Options		code	length	data																		
	#1	(1) NOP	0																			
	#2	(1) NOP	0																			
	#3	(0) TS	8	0020F3D7F1FE53D4																		
Payload	<p>Message-ID: <5086082F.80305608@bedamp.mooo.com> [2 non-ASCII characters] Date: Tue, 23 Oct 2012 19:30:19 +0200 [2 non-ASCII characters] From: usul <usul@bedamp.mooo.com> [2 non-ASCII characters] User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:16.0) Gecko/20121011 Thunderbird/16.0.1 [2 non-ASCII characters] MIME-Version: 1.0 [2 non-ASCII characters] To: root@bedamp.mooo.com [2 non-ASCII characters] Subject: Hi my virus!! [2 non-ASCII characters] Content-Type: multipart/mixed; [2 non-ASCII characters] boundary="-----370969040165020160940360" [4 non-ASCII characters] This is a multi-part message in MIME format.</p>																					