BÀI 8.
CÁC HỆ THỐNG PHÒNG CHỐNG VÀ NGĂN CHẶN TẤN CÔNG

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1

1

Nội dung

- Hệ thống tường lửa
- Hệ thống phát hiện và ngăn chặn tấn công (IDPS)

2

2

1. HỆ THỐNG TƯỜNG LỬA

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

3

3

Giới thiệu chung

- Là hệ thống có khả năng ngăn chặn các truy cập không hợp lệ và **đã biết** từ bên ngoài và trong khu vực tài nguyên cần bảo vệ
- Tường lửa có thể triển khai ở nhiều vị trí, tùy thuộc cách thức định nghĩa, phạm vi tài nguyên cần bảo vệ:
  - Mạng ngoại vi
  - Mạng nội bộ

  } Network-based firewall
  - Nút mạng(Host-based firewall)
  - Ứng dụng(Application-based firewall)

4

4

Tường lửa có thể làm gì?

- Thi hành các chính sách an toàn bảo mật: hoạt động như một hệ thống cảnh vệ(traffic cop) cho phép/từ chối lưu lượng mạng nào đó **đi qua** tường lửa dựa trên các đặc điểm(giao thức, địa chỉ, nội dung…) **đã xác định**
- Hạn chế các hành vi tấn công vào mạng
  - Từ mạng bên ngoài(Internet) vào mạng nội bộ
  - Từ phân vùng mạng nội bộ này tới những phân vùng mạng nội bộ khác
- Lưu nhật ký các lưu lượng mạng

5

5

Tường lửa không thể làm gì?

- Không bảo vệ được tài nguyên trước các mối nguy cơ từ bên trong
- Không kiểm soát được các lưu lượng mạng không đi qua
- Không kiểm soát đầy đủ đối với các lưu lượng đã được mã hóa
- Không ngăn chặn được các truy cập tấn công chưa biết
- Không chống lại được hoàn toàn các nguy cơ từ phần mềm độc hại
- Do đó cần được:
  - Triển khai ở nhiều vị trí khác nhau
  - Kết hợp với các giải pháp khác: phòng chống phần mềm độc hại, IDS/IPS, điều khiển truy cập, kiểm toán(auditing)
  - Cập nhật liên tục các chính sách mới

6

6

Các kiến trúc tường lửa(1)

- Network-based firewall: Kiểm soát lưu lượng mạng giữa các phân vùng mạng
- Ưu điểm: Phạm vi kiểm soát rộng
- Nhược điểm:
  - Không kiểm soát được lưu lượng trong từng phân vùng
  - Không kiểm soát đầy đủ lưu lượng đã được mã hóa

7

7

Các kiến trúc tường lửa(2)

- Host-based firewall: Kiểm soát lưu lượng mạng đến và đi từ một nút mạng
- Ưu điểm: Kiểm soát được lưu lượng tới nút mạng từ những nguồn trong cùng phân vùng mạng
- Nhược điểm:
  - Chỉ bảo vệ được cho một mục tiêu đơn lẻ
  - Không kiểm soát đầy đủ lưu lượng đã được mã hóa

8

8

Các kiến trúc tường lửa(3)

- Application firewall: Kiểm soát lưu lượng mạng của một dịch vụ cụ thể
- Ưu điểm: Kiểm soát được toàn bộ lưu lượng mạng tới dịch vụ, kể cả lưu lượng đã mã hóa
- Nhược điểm:
  - Bộ luật phức tạp
  - Cần phải cài đặt nhiều phần mềm tường lửa nếu trên máy chủ cung cấp các dịch vụ khác nhau

9

9

Các công nghệ tường lửa

- Thế hệ 1(1985) – Packet filter: kiểm soát lưu lượng dựa trên các thông tin trong phần tiêu đề
- Thế hệ 2(1989) – Proxy server: có thể ngăn chặn lưu lượng tấn công dựa trên sự hiểu biết về các giao thức chuẩn của tầng ứng dụng
- Thế hệ 3(1991) – Stateful inspector firewall: kiểm soát thêm trạng thái của luồng dữ liệu
- Thế hệ 4(1994) – Dynamic packet filter: giao tiếp với hệ thống phát hiện tấn công để cung cấp các cơ chế phản ứng với tấn công
- Thế hệ 5(1996) – Kiểm soát quá trình xử lý gói tin dựa trên toàn bộ chồng giao thức TCP/IP
- Hiện nay: tích hợp với các giải pháp an toàn bảo mật khác

10

10

Packet filter(stateless)

- Loại tường lửa đơn giản nhất
- Dựa trên việc kiểm tra một số giá trị trong phần tiêu đề để xác định gói tin được chấp nhận hoặc chặn:
  - Địa chỉ MAC
  - Địa chỉ IP nguồn, đích
  - Số hiệu cổng nguồn, đích
  - Giao thức
- Ví dụ:

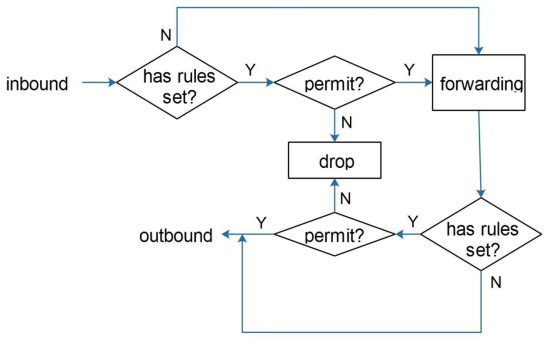
Rule	Source IP	Source port	Destination IP	Destination port	Action
1	Any	Any	192.168.120.0	Above 1023	Allow
2	192.168.120.1	Any	Any	Any	Deny
3	Any	Any	192.168.120.1	Any	Deny
4	192.168.120.0	Any	Any	Any	Allow
5	Any	Any	192.168.120.2	25	Allow
6	Any	Any	192.168.120.3	80	Allow
7	Any	Any	Any	Any	Deny

11

11

Packet filter – Nguyên lý hoạt động

- Mỗi firewall có một tập các luật định nghĩa cách thức xử lý gói tin(cho phép đi qua hoặc chặn).
- Tập các luật có thể áp dụng trên luồng dữ liệu đi vào(inbound) hoặc đi ra(outbound) của giao tiếp mạng trên firewall

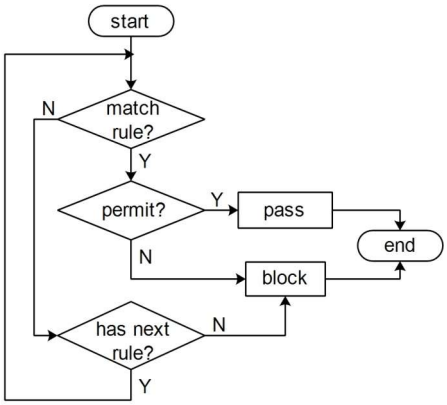


12

12

Packet filter – So khớp luật

- Thông tin trên phần tiêu đề của gói tin được so khớp với các giá trị định nghĩa trong luật
- Các luật được so khớp theo thứ tự sắp đặt trong tập luật
- Nếu phù hợp với luật nào, gói tin được xử lý theo cách thức đã chỉ ra trong luật đó
  - Không tiếp tục so khớp với các luật còn lại
- Nếu không có luật nào được so khớp: xử lý theo luật mặc định
  - Thông thường: luật mặc định là chặn



13

13

Packet filter(stateless)

- Ưu điểm:
  - Đơn giản
  - Tốc độ xử lý nhanh
- Hạn chế:
  - Có quá ít lựa chọn xử lý(drop, accept, forward)
  - Không kiểm soát được nội dung gói tin
  - Khả năng hỗ trợ ghi nhật ký hạn chế
  - Dễ dàng vượt qua bằng các kỹ thuật giả mạo thông tin trên phần tiêu đề
  - Không hỗ trợ tính năng xác thực

14

14

Stateful Inspector/Filter

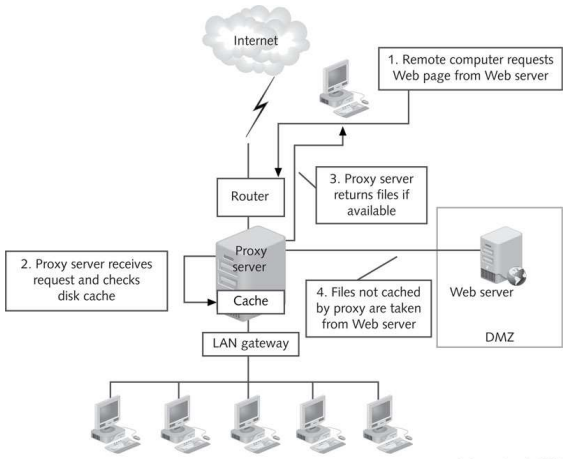
- Hạn chế của Packet filter: chỉ xử lý độc lập từng gói tin, không có cơ chế theo dõi trạng thái của liên kết
  - Ví dụ: Cho phép các gói tin từ External network vào Internal network nếu nút mạng trong Internal network đã khởi tạo liên kết
- Stateful Inspector
  - Sử dụng bảng lưu thông tin trạng thái của các liên kết đã được thiết lập
  - Cho phép dữ liệu đi vào(inbound) trong khu vực tài nguyên được bảo vệ khi và chỉ khi liên kết đã được thiết lập
  - Vẫn hỗ trợ các giao thức hướng không liên kết: chỉ cho phép dữ liệu đi vào nếu trước đó đã có dữ liệu đi ra tương ứng

15

15

Proxy server

- Tường lửa hoạt động ở tầng ứng dụng
- Chuyển tiếp dữ liệu đến và đi ra khỏi mạng
- VD: Web proxy



16

16

Proxy server – Ưu điểm

- Kiểm soát được nội dung của dữ liệu: URL filtering, MIME filtering, Content filtering
- Kiểm soát được trạng thái của phiên
- Che giấu được địa chỉ IP riêng
- Tách thông tin tiêu đề cũ, thay thế bằng tiêu đề mới → ngăn chặn các kỹ thuật tấn công dựa trên tiêu đề của gói tin tới mạng bên trong
- Chống lại việc giả mạo thông tin của tiêu đề
- Có thể định tuyến cho dịch vụ
- Hỗ trợ tốt các cơ chế nhật ký, kiểm toán

17

17

Proxy server – Hạn chế

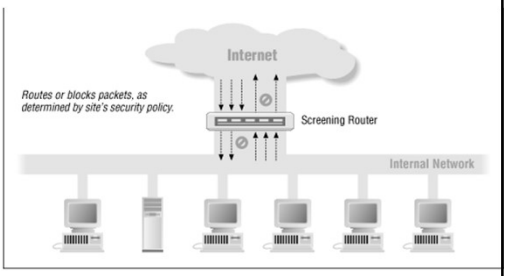
- Làm chậm quá trình cung cấp dịch vụ
- Các dịch vụ hỗ trợ bị hạn chế
- Không trong suốt với người dùng cuối:
  - Cần cấu hình để client kết nối tới proxy server
- Hiện nay proxy server có thể thay thế bằng các sản phẩm tường lửa có tính năng Deep Packet Inspection

18

18

Screening router

- Tích hợp bộ lọc với trên router kết nối mạng cần bảo vệ với mạng công cộng
- Ưu điểm:
  - Đơn giản
  - Chi phí thấp
- Nhược điểm:
  - Không có khả năng chịu lỗi
  - Mức độ an ninh thấp, dễ bị vượt qua



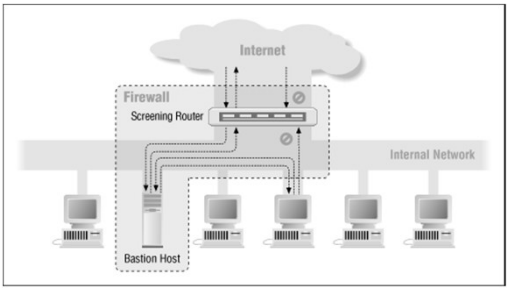
- Sử dụng khi nào?
  - Hệ thống đã có các lớp bảo vệ an toàn hơn ở bên trong
  - Số lượng giao thức cần kiểm soát ít

19

19

Screened-host

- Bastion Host đặt trên phân vùng mạng bên trong, là nút mạng duy nhất có thể truy cập từ mạng công cộng
- Bastion Host cần được bảo vệ ở mức cao nhất có thể
- Hạn chế: khi Bastion Host bị chiếm quyền quyền điều khiển, mạng bên trong không còn được bảo vệ



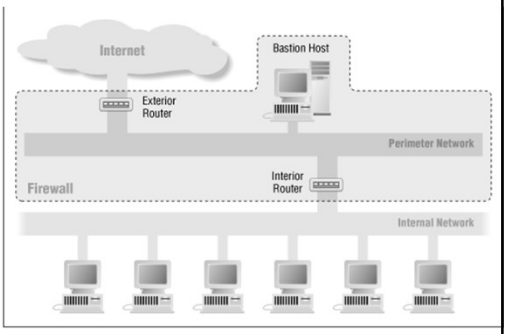
- Sử dụng khi nào?
  - Lưu lượng mạng thấp
  - Các nút của phân vùng mạng bên trong đã có lớp bảo vệ an toàn hơn

20

20

Screen-subnet

- Perimeter network: Phân vùng mạng vành đai nằm giữa phần vùng bên trong (internal network) và phần vùng bên ngoài (external network)
- Cài đặt packet filter trên cả 2 router
- Bastion Host có thể hoạt động như một proxy
- An toàn hơn do Bastion Host được tách biệt khỏi phân vùng bên trong



21

21

2. HỆ THỐNG PHÁT HIỆN VÀ NGĂN CHẶN TẤN CÔNG

Nguyễn Đức Toàn,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

22

22

Vấn đề phát hiện tấn công

- Không thể tạo ra một hệ thống hoàn toàn an toàn bảo mật
- Giải pháp chung: phát hiện và ngăn chặn các hành vi tấn công, khai thác lỗ hổng an toàn bảo mật
  - Bao gồm cả vấn đề phục hồi sau tấn công, truy vết tấn công, ngăn chặn tấn công kế tiếp
  - Bảo vệ đa tầng (Defense in depth)
  - Chú ý: khai thác lỗ hổng đối với cả tài nguyên cũng như chính sách an toàn bảo mật
- Các vấn đề:
  - Không có mô hình cụ thể và các nguyên lý để giải quyết
  - Rất nhiều vấn đề khi triển khai (vị trí giám sát, phát hiện các lỗ hổng thể nào, độ chính xác, khả năng vượt qua của kẻ tấn công)

23

23

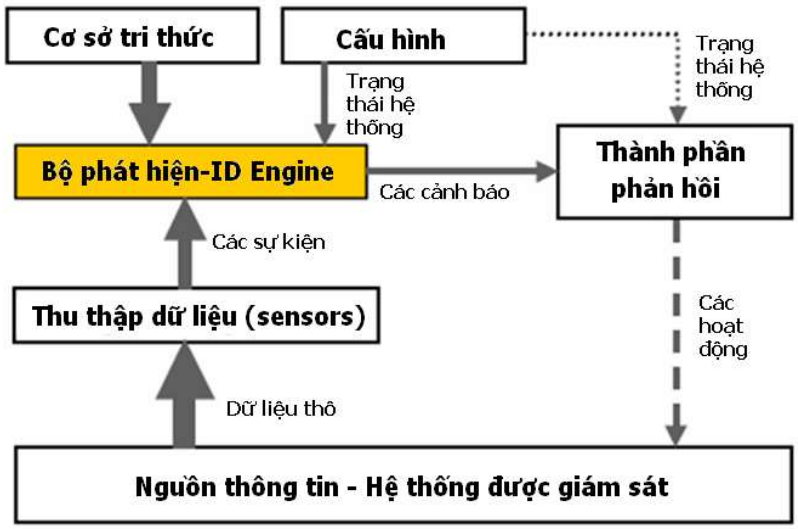
Khái niệm cơ bản

- Intrusion Detection and Preventation System: hệ thống có khả năng theo dõi, giám sát, phát hiện và ngăn chặn các hành vi tấn công, khai thác trái phép tài nguyên được bảo vệ
- IDPS vs tường lửa:
  - Tường lửa: xử lý từng gói tin trên lưu lượng mạng
  - IDPS: có khả năng theo dõi, giám sát chuỗi các gói tin, hành vi để xác định có phải là hành vi tấn công hay xâm nhập hay không
  - Các thiết bị tường lửa thế hệ mới thường trang bị tính năng IDPS

24

24

Kiến trúc chung



25

25

Kiến trúc chung (tiếp)s

- **Bộ cảm biến (Sensor):** thu thập dữ liệu từ hệ thống được giám sát.
- **Bộ phát hiện** : Thành phần này phân tích và tổng hợp thông tin từ dữ liệu thu được của bộ cảm biến dựa trên cơ sở tri thức của hệ thống
- **Bộ lưu trữ :** Lưu trữ tất cả dữ liệu của hệ thống IDS, bao gồm: dữ liệu của bộ cảm biến, dữ liệu phân tích của bộ phát hiện, cơ sở tri thức, cấu hình hệ thống … nhằm phục vụ quá trình hoạt động của hệ thống IDS.
- **Bộ phản ứng :** Thực hiện phản ứng lại với những hành động phát hiện được.
- **Giao diện người dùng**

26

26

Tính chính xác

- Đánh giá qua 2 giá trị:
  - FPR (False Positive Rate): tỉ lệ phát hiện nhầm
  - FNR (False Negative Rate): tỉ lệ bỏ sót
- $\mathcal{I}$: sự kiện có tấn công xảy ra
- $\mathcal{A}$: sự kiện hệ thống IDS phát ra cảnh báo
- FPR = P($\mathcal{A}$ | not $\mathcal{I}$)
- FNR = P(not $\mathcal{A}$ | $\mathcal{I}$)

27

27

FNR = 0 hay FPR = 0 ?

- Trong ví dụ về công ty FooCorp, để phát hiện các URL độc hại:

```
void my_detector_that_never_misses(char *URL)
  {
       printf("yep, it's an attack!\n");
  }
```

  - Nhận xét: FNR = 0 (Woo-hoo!)
- Để FPR = 0

```
void my_detector_that_never_mistakes(char *URL)
  {
       printf("nope, not an attack!\n");
  }
```

28

28

Tính chính xác (tiếp)

- Cần cân bằng giữa FPR và FNR
- Nên lựa chọn hệ thống có FPR thấp hay FNR thấp?
  - Phụ thuộc vào sự mức độ thiệt hại của hệ thống với mỗi dạng lỗi xảy ra
  - Phụ thuộc vào tỉ lệ tấn công trên thực tế
- Ví dụ: Giả sử hệ thống có FPR = 0.1% và FNR = 2%
  - Trường hợp 1: mỗi ngày hệ thống có 1000 truy cập, trong đó có 5 truy cập là tấn công:
    - ✓ Phát hiện nhầm: 995 x 0.1% ~ 1 truy cập hợp lệ/1 ngày
    - ✓ Bỏ sót: 5 x 2% ~ 0.1 (bỏ sót <1 tấn công/1 tuần)
  - Trường hợp 2: 1.000.000 truy cập mỗi ngày, trong đó 5 truy cập là tấn công:
    - ✓ Phát hiện nhầm: 999995 x 0.1% ~ 1000 truy cập hợp lệ/1 ngày ☹

29

29

Phát hiện lạm dụng(misuse detection)

- Đặc điểm: sử dụng dữ liệu về các dạng tấn công đã biết
  - Phát hiện dựa trên dấu hiệu (signature-based)
  - Phát hiện dựa trên lỗ hổng (vulnerability signature)
- Ưu điểm?
- Nhược điểm?

30

30

Phát hiện bất thường(anomaly detection)

- Đặc điểm: xây dựng mô hình các hành vi bình thường. Đánh dấu nghi ngờ và đo lường các hành vi nằm ngoài mô hình.
  - Phát hiện dựa trên ngưỡng (threshold-based)
  - Phát hiện dựa trên đặc điểm (specification-based)
  - Phát hiện dựa trên hành vi (behavioral-based)
- Ưu điểm?
- Nhược điểm?

31

31

NIDS và HIDS

- NIDS: Network-based IDS
- Một số thành phần chức năng trong bộ phát hiện:
  - Bộ phân tích giao thức
  - Bộ phân tích dấu hiệu: phát hiện các dạng tấn công đã biết
  - *Shadow execution*
  - Trình ghi nhật ký
- Ưu điểm
- Nhược điểm

32

32

NIDS và HIDS (tiếp)

- Host-based IDS
- Một số thành phần của bộ phát hiện:
  - Bộ quét gói tin
  - Bộ quét file
  - Bộ quét bộ nhớ chính
  - Phân tích thời gian thực
  - *Sandbox execution*
- Ưu điểm?
- Nhược điểm?

33

33