**PHẦN II : CÁC CHÍNH SÁCH BẢO MẬT**

**CHƯƠNG 3: TỔNG QUAN VỀ BẢO MẬT**

**3.1 Định nghĩa bảo mật mạng:**

Bảo mật mạng là sự đảm bảo an toàn của toàn bộ hệ thống mạng trước những hoạt động nhằm tấn công phá hoại hệ thống mạng cả từ bên trong như bên ngoài.

Hoạt động phá hoại là những hoạt động như xâm nhập trái phép sử dụng tài nguyên trái phép ăn cắp thông tin, các hoạt động giả mạo nhằm phá hoại tài nguyên mạng và cơ sở dữ liệu của hệ thống.

Vấn đề bảo mật mạng luôn là một vấn đề bức thiết khi ta nghiên cứu một hệ thống mạng. Hệ thống mạng càng phát triển thì vấn đề bảo mật mạng càng được đạt lên hàng đầu.

Khi nguyên cứu một hệ thống mạng chúng ta cần phải kiểm soát vấn đề bảo mật mạng ở các cấp độ sau:

* Mức mạng: Ngăn chặn kẻ xâm nhập bất hợp pháp vào hệ thống mạng.
* Mức server: Kiểm soát quyền truy cập, các cơ chế bảo mật, quá trình nhận dạng người dùng, phân quyền truy cập, cho phép các tác vụ
* Mức cơ sở dữ liệu: Kiểm soát ai? được quyền như thế nào? với mỗi cơ sở dữ liệu.
* Mức trường thông tin: Trong mỗi cơ sở dữ liệu kiểm soát được mỗi trường dữ liệu chứa thông tin khác nhau sẽ cho phép các đối tượng khác nhau có quyền truy cập khác nhau.
* Mức mật mã: Mã hoá toàn bộ file dữ liệu theo một phương pháp nào đó và chỉ cho phép người có “ chìa khoá” mới có thể sử dụng được file dữ liệu.

Theo quan điểm hệ thống, một xí nghiệp (đơn vị kinh tế cơ sở) được thiết lập từ ba hệ thống sau:

* Hệ thống thông tin quản lý.
* Hệ thống trợ giúp quyết định.
* Hệ thống các thông tin tác nghiệp.

Trong đó hệ thống thông tin quản lý đóng vai trò trung gian giữa hệ thống trợ giúp quyết định và hệ thống thông tin tác nghiệp với chức năng chủ yếu là thu thập, xử lý và truyền tin.



*Hình 3.1 Sơ đồ mạng thông dụng hiện nay.*

* + 1. **Các yếu tố cần quan tâm khi phân tích bảo mật mạng:**

+ Vấn đề con người: Trong bảo mật mạng yếu tố con người cũng rất quan trọng. Khi nghiên cứu đến vấn đề bảo mật mạng cần quan tâm xem ai tham gia vào hệ thống mạng, họ có tránh nhiệm như thế nào. Ở mức độ vật lý khi một người không có thẩm quyền vào phòng máy họ có thể thực hiện một số hành vi phá hoại ở mức độ vật lý.

+ Kiến trúc mạng: Kiến trúc mạng cũng là một vấn đề mà chúng ta cần phải quan tâm khi nghiên cứu, phân tích một hệ thống mạng. Chúng ta cần nghiên cứu hiện trạng mạng khi xây dựng và nâng cấp mạng đưa ra các kiểu kiến trúc mạng phù hợp với hiện trạng và cơ sở hạ tầng ở nơi mình đang định xây dựng….

+ Phần cứng & phần mềm:

Mạng được thiết kế như thế nào. Nó bao gồm những phần cứng và phần mềm nào và tác dụng của chúng. Xây dựng một hệ thống phần cứng và phần mềm phù hợp với hệ thống mạng cũng là vấn đề cần quan tâm khi xây dựng hệ thống mạng. Xem xét tính tương thích của phần cứng và phần mềm với hệ thống và tính tương thích giữu chúng.

* + 1. **Các yếu tố cần được bảo vệ :**

+ Bảo vệ dữ liệu (tính bảo mật tính toàn vẹn và tính kíp thời).

+ Bảo vệ tài nguyên sử dụng trên mạng để tránh sử dụng tài nguyên này vào mục đính tấn công của kẻ khác.

+ bảo vệ danh tiếng.

* 1. **Các kiểu tấn công mạng:**

Cùng với sự phát triển nhanh chóng của mạng thì nó cũng để lại nhiều lỗ hổng để hacker có thể tấn công. Các thủ đoạn tấn công ngày càng trở nên tinh vi hơn. Các phương pháp tấn công thường gặp là :

* + 1. **Thăm dò(reconnaissance):**

Đó chính là hình thức hacker gửi vài thông tin truy vấn về địa chỉ IP hoặc domain name bằng hình thức này hacker có thể lấy được thông tin về địa chỉ IP và domain name từ đó thực hiện các biện pháp tấn công khác…

* + 1. **Packet sniffer:**

Packet sniffer là phần mềm sử dụng NIC card ở chế độ “promisscuous” để bắt tất cả các gói tin trong cùng miền xung đột. Nó có thể khai thác thông tin dưới dạng clear Text.

* + 1. **Đánh lừa (IP spoofing):**

Kỹ thuật này được sử dụng khi hacker giả mạo địa chỉ IP tin cậy trong mạng nhằm thực hiện việc chèn thông tin bất hợp pháp vào trong phiên làm việc hoặc thay đổi bản tin định tuyến để thu nhận các gói tin cần thiết.

* + 1. **Tấn công từ chối dịch vụ (Denial of services):**

Kiểu tấn công này nhằm tắc nghẽn mạng bằng cách hacker gửi các gói tin với tốc độ cao và liên tục tới hệ thống bảo mật nhằm làm tê liện hệ thống chiếm hết băng thông sử dụng.

* + 1. **Tấn công trực tiếp password:**

Đó là kiểu tấn công trực tiếp vào username và password của người sử dụng nhằm ăn cắp tài khoải sử dụng vào mục đích tấn công. Hacker dùng phần mềm để tấn công (vị dụ như Dictionary attacks).

* + 1. **Thám thính(agent):**

Hacker sử dụng các các phần mềm vius, trojan thường dùng để tấn công vào máy trạm làm bước đệm để tấn công vào máy chủ và hệ thống. Kẻ tấn công có thể nhận được các thông tin hữu ích từ máy nạn nhân thông qua các dịch vụ mạng.

* + 1. **Tấn công vào yếu tố con người:**

Hacker có thể tấn công vào các lỗ hổng do lỗi nhà quản trị hệ thống hoặc liên lạc với nhà quản trị hệ thống giả mạo là người sủ dụng thay đổi username và password.

* 1. **Các mức độ bảo mật:**

Khi phân tích hệ thống bảo mật mạng người ta chia ra làm các muác độ an toàn sau:

**Bức tường lửa (Firewall)**

**Bảo vệ vật lý (Physical Protect)**

**Mã hóa dữ liệu(Data Encryption)**

**Đăng nhập/Mật khẩu (Login/Password)**

**Quyền truy nhập (Access Right)**

**Thông tin (Information)**

*Hình 3.3 Các mức độ bảo mật mạng.*

*Hình 3.3 Các mức độ bảo mật.*

* + 1. **Quyền truy nhập:**

Đây là lớp bảo vệ sâu nhất nhằm kiểm soát tài nguyên mạng kiểm soát ở mức độ file và việc xác định quyền hạn của người dùng do nhà quản trị quyết định như: chỉ đọc( only read), chỉ ghi (only write), thực thi(execute).

* + 1. **Đăng nhập/Mật khẩu(login/password):**

Đây là lớp bảo vệ mức độ truy nhập thông tin ở mức độ hệ thống. Đây là mức độ bảo vệ được sử dụng phổ biến nhất vì nó đơn giản và ít tốn kém. Nhà quản trị cung cấp cho mỗi người dùng một username và password và kiểm soát mọi hoạt động của mạng thông qua hình thức đó. Mỗi lần truy nhập mạng người dùng phải đăng nhập nhập username và password hệ thống kiểm tra thấy hợp lệ mới cho đăng nhập.

* + 1. **Mã hóa dữ liệu(Data encryption):**

Đó là sử dụng các phương pháp mã hoá dữ liệu ở bên phát và thực hiện giải mã ở bên thu bên thu chỉ có thể mã hóa chính xác khi có khoá mã hóa do bên phát cung cấp.

* + 1. **Bảo vệ vật lý (Physical protect):**

Đây là hình thức ngăn chạn nguy cơ truy nhập vật lý bất hợp pháp vào hệ thống như ngăn cấm tuyệt đối người không phận sự vào phòng đặt máy mạng, dùng ổ khoá máy tính, hoặc cài đặt cơ chế báo động khi có truy nhập vào hệ thống ...

* + 1. **Bức tường lửa (firewall):**

Đây là hình thức ngăn chặn sự xâm nhập bất hợp pháp vào mạng nội bộ thông qua firewall. ). Chức năng của tường lửa là ngăn chặn các truy nhập trái phép (theo danh sách truy nhập đã xác định trước) và thậm chí có thể lọc các gói tin mà ta không muốn gửi đi hoặc nhận vào vì một lý do nào đó. Phương thức bảo vệ này được dùng nhiều trong môi trường liên mạng Internet.

* 1. **Các biện pháp bảo vệ an toàn hệ thống:**

Đối với mỗi hệ thống mạng, không nên cài đặt và chỉ sử dụng một chế độ an toàn cho dù nó có thể rất mạnh, mà nên lắp đặt nhiều cơ chế an toàn khác nhau để chúng có thể hỗ trợ lẫn nhau và có thể đẳm bảo an toàn ở mức độ cao.

* + 1. **Quyền hạn tối thiểu (Least Privilege):**

Một nguyên tắc cơ bản nhất của an toàn nói chung là trao quyền tối thiểu. Có nghĩa là: Bất kỳ một đối tượng nào trên mạng chỉ nên có những quyền hạn nhất định mà đối tượng đó cần phải có để thực hiện các nhiệm vụ của mình và chỉ có những quyền đó mà thôi. Như vậy, mọi người sử dụng đều không nhất thiết được trao quyền truy nhập mọi dich vụ Internet, đọc và sửa đổi tất cả các file trong hệ thống… Người quản trị hệ thống không nhất thiết phải biết các mật khẩu root hoặc mật khẩu của mọi người sử dụng …

Nhiều vấn đề an toàn trên mạng Internet bị xem là thất bại khi thực hiện nguyên tắc Quyền hạn tối thiểu. Vì vậy, các chương trình đặc quyền phải được đơn giản đến mức có thể và nếu một chương trình phức tạp, ta phải tìm cách chia nhỏ và cô lập từng phần mà nó yêu cầu quyền hạn.

* + 1. **Bảo vệ theo chiều sâu (Defense in Depth):**

Đối với mỗi hệ thống, không nên cài đặt và chỉ sử dụng một chế độ an toàn cho dù nó có thể rất mạnh, mà nên lắp đặt nhiều cơ chế an toàn để chúng có thể hỗ trợ lẫn nhau.

* + 1. **Nút thắt (choke point):**

Một nút thắt bắt buộc những kẻ đột nhập phải đi qua một lối hẹp mà chúng ta có thể kiểm soát và điều khiển được. Trong cơ chế an toàn mạng, Firewall nằm giữa hệ thống mạng của ta và mạng Internet, nó chính là một nút thắt. Khi đó, bất kỳ ai muốn truy nhập vào hệ thống cũng phải đi qua nó, vì vậy, ta có thể theo dõi, quản lý được.

Nhưng một nút thắt cũng sẽ trở nên vô dụng nếu có một đường khác vào hệ thống mà không cần đi qua nó (trong môi trường mạng, còn có những đường Dial–up không được bảo vệ khác có thể truy nhập được vào hệ thống)

* + 1. **Điểm xung yếu nhất (Weakest point):**

Một nguyên tắc cơ bản khác của an toàn là: “Một dây xích chỉ chắc chắn khi mắt nối yếu nhất được làm chắc chắn”. Khi muốn thâm nhập vào hệ thống của chúng ta, kẻ đột nhập thường tìm điểm yếu nhất để tấn công vào đó. Do vậy, với từng hệ thống, cần phải biết điểm yếu nhất để có phương án bảo vệ.

* + 1. **Hỏng trong an toàn (Fail–Safe Stance):**

Nếu một hệ thống chẳng may bị hỏng thì nó phải được hỏng theo một cách nào đó để ngăn chặn những kẻ lợi dụng tấn công vào hệ thống hỏng đó. Đương nhiên, việc hỏng trong an toàn cũng hủy bỏ sự truy nhập hợp pháp của người sử dụng cho tới khi hệ thống được khôi phục lại.

Nguyên tắc này cũng được áp dụng trong nhiều lĩnh vực. Chẳng hạn, cửa ra vào tự động được thiết kế để có thể chuyển sang mở bằng tay khi nguồn điện cung cấp bị ngắt để tránh giữ người bên trong.

Dựa trên nguyên tắc này, người ta đưa ra hai quy tắc để áp dụng vào hệ thống an toàn:

- Default deny Stance: Chú trọng vào những cái được phép và ngăn chặn tất cả những cái còn lại.

- Default permit Stance: Chú trọng vào những cái bị ngăn cấm và cho phép tất cả những cái còn lại. Những gì không bị ngăn cấm thì được phép.

Theo quan điểm về vấn đề an toàn trên thì nên dùng quy tắc thứ nhất, còn theo quan điểm của các nhà quản lý thì lại là quy tắc thứ hai.

* + 1. **Sự tham gia toàn cầu:**

Để đạt được hiệu quả an toàn cao, tất cả các hệ thống trên mạng toàn cầu phải tham gia vào giải pháp an toàn. Nếu tồn tại một hệ thống có cơ chế an toàn kém, người truy nhập bất hợp pháp có thể truy nhập vào hệ thống này và sau đó dùng chính hệ thống này để truy nhập vào các hệ thống khác.

* + 1. **Kết hợp nhiều biện pháp bảo vệ:**

Trên liên mạng, có nhiều loại hệ thống khác nhau được sử dụng, do vậy, phải có nhiều biện pháp bảo vệ để đảm bảo chiến lược bảo vệ theo chiều sâu. Nếu tất cả các hệ thống của chúng ta đều giống nhau và một người nào đó biết cách thâm nhập vào một hệ thống thì cũng có thể thâm nhậo được vào các hệ thống khác.

* + 1. **Đơn giản hóa:**

Nếu ta không hiểu một cái gì đó, ta cũng không thể biết được liệu nó có an toàn hay không. Chính vì vậy, ta cần phải đơn giản hóa hệ thống để có thể áp dụng các biện pháp an toàn một cách hiệu quả hơn.

* 1. **Các chính sách bảo mật:**

Kế hoạch an toàn thông tin phải tính đến các nguy cơ từ bên ngoài và từ trong nội bộ, đồng thời phải kết hợp cả các biện pháp kỹ thuật và các biện pháp quản lý. Sau đây là các bước cần tiến hành:

• Xác định các yêu cầu và chính sách an toàn thông tin: Bước đầu tiên trong kế hoạch an toàn thông tin là xác định các yêu cầu truy nhập và tập hợp những dịch vụ cung cấp cho người sử dụng trong và ngoài cơ quan, trên cơ sở đó có được các chính sách tương ứng.

• Thiết kế an toàn vòng ngoài: Việc thiết kế dựa trên các chính sách an toàn được xác định trước. Kết quả của bước này là kiến trúc mạng cùng với các thành phần phần cứng và phần mềm sẽ sử dụng. Trong đó cần đặc biệt chú ý hệ thống truy cập từ xa và cơ chế xác thực người dùng.

• Biện pháp an toàn cho các máy chủ và máy trạm: Các biện pháp an toàn vòng ngoài, dù đầy đủ đến đâu, cũng có thể không đủ để chống lại sự tấn công, đặc biệt là sự tấn công từ bên trong. Cần phải kiểm tra các máy chủ và máy trạm để phát hiện những sơ hở về bảo mật. Đối với Filewall và các máy chủ ở ngoài cần kiểm tra những dạng tấn công (denial of service).

• Kiểm tra thường kỳ: Cần có kế hoạch kiểm tra định kỳ toàn bộ hệ thống an toàn thông tin, ngoài ra cần kiểm tra lại mỗi khi có sự thay đổi về cấu hình.

* + 1. **Kế hoạch bảo mật mạng:**

Có một chính sách bảo mật mạng đúng đắn và hiệu quả để có thể bảo vệ các thông tin, các tài nguyên của một công ty, tổ chức nói riêng hay của một bộ, ngành, của một quốc gia nói chung là vấn đề hết sức quan trọng. Nếu như các tài nguyên và thông tin mà công ty đó có trên mạng là đáng được bảo vệ thì một chính sách bảo mật mạng là đáng được thực hiện. Hầu hết các cơ quan đều có các thông tin nhạy cảm và các bí mật cạnh tranh trên mạng máy tính của họ, vì vậy chúng ta sẽ cần một chính sách bảo mật mạnng đề bảo vệ tài nguyên và thông tin của công ty.

Để có một chính sách bảo mật mạng hiệu quả thì chúng ta phải trả lời được câu hỏi: loại dịch vụ nào, loại tài nguyên nào người dùng được phép truy nhập và loại nào thì bị cấm?

* + 1. **Chính sách bảo mật nội bộ:**

Một tổ chức có thể có nhiều bộ phận ở nhiều nơi, mỗi bộ phận có mạng riêng. Nếu tổ chức lớn thì mỗi mạng phải có ít nhất một người quản trị mạng. Nếu các nơi không nối với nhau thành mạng nội bộ thì chính sách an ninh cũng có những điểm khác nhau.

Thông thường thì tài nguyên mạng ở mỗi nơi bao gồm:

• Các trạm làm việc

• Các thiết bị kết nối: Gateway, Router, Bridge, Repeater

• Các Server

• Phần mềm mạng và phần mềm ứng dụng

• Cáp mạng

• Thông tin trong các tệp và các CSDL

Chính sách an ninh tại chỗ phải cân nhắc đến việc bảo vệ các tài nguyên này. Đồng thời cũng phải cân nhắc giữa các yêu cầu an ninh với các yêu cầu kết nối mạng bởi vì một chính sách bảo vệ tốt cho mạng này lại bất lợi cho mạng khác.

* + 1. **Phương thức thiết kế:**

Tạo ra một chính sách mạng có nghĩa là lập lên các thủ tục và kế hoạch bảo vệ tài nguyên của chúng ta khỏi mất mát và hư hại. Một hướng tiếp cận khả thi là trả lời các câu hỏi sau :

• Chúng ta muốn bảo vệ tài nguyên nào ?

• Chúng ta cần bảo vệ tài nguyên trên khỏi những người nào ?

• Có các mối đe doạ như thế nào ?

• Tài nguyên quan trọng tới mức nào ?

• Chúng ta sẽ dùng cách nào để bảo vệ tài nguyên theo cách tiết kiệm và hợp lý nhất

• Kiểm tra lại chính sách theo chu kỳ nào để phù hợp với các thay đổi về mục đích cũng như về hiện trạng của mạng ?

* + 1. **Thiết kế chính sách bảo mật mạng:**
       1. **Phân tích nguy cơ mất an ninh:**

Trước khi thiết lập chính sách ta cần phải biết rõ tài nguyên nào cần được bảo vệ, tức là tài nguyên nào có tầm quan trọng lớn hơn để đi đến một giải pháp hợp lý về kinh tế. Đồng thời ta cũng phải xác định rõ đâu là nguồn đe doạ tới hệ thống. Nhiều nghiên cứu cho thấy rằng, thiệt hại do những kẻ “đột nhập bên ngoài” vẫn còn nhỏ hơn nhiều so với sự phá hoại của những “người bên trong”. Phân tích nguy cơ bao gồm những việc :

• Ta cần bảo vệ những gì ?

• Ta cần bảo vệ những tài nguyên khỏi những gì ?

• Làm thế nào để bảo vệ ?

* + - 1. **Xác định tài nguyên cần bảo vệ:**

Khi thực hiện phân tích ta cũng cần xác định tài nguyên nào có nguy cơ bị xâm phạm. Quan trọng là phải liệt kê được hết những tài nguyên mạng có thể bị ảnh hưởng khi gặp các vấn đề về an ninh.

* Phần cứng: Vi xử lý, bản mạch, bàn phím, terminal, trạm làm việc, máy tính các nhân, máy in, ổ đĩa, đường liên lạc, server, router
* Phần mềm: Chương trình nguồn, chương trình đối tượng, tiện ích, chương trình khảo sát, hệ điều hành, chương trình truyền thông.
* Dữ liệu: Trong khi thực hiện, lưu trữ trực tuyến, cất giữ off–line, backup, các nhật ký kiểm tra, CSDL truyền trên các phương tiện liên lạc.
* Con người: Người dùng, người cần để khởi động hệ thống.
* Tài liệu: Về chương trình , về phần cứng, về hệ thống, về thủ tục quản trị cục bộ.

- Nguồn cung cấp: giấy in, các bảng biểu, băng mực, thiết bị từ.

* + - 1. **Xác định các mối đe dọa bảo mật mạng:**

Sau khi đã xác định những tài nguyên nào cần được bảo vệ, chúng ta cũng cần xác định xem có các mối đe doạ nào nhằm vào các tài nguyên đó. Có thể có những mối đe dọa sau:

* **Truy nhập bất hợp pháp:**

Chỉ có những người dùng hợp pháp mới có quyền truy nhập tài nguyên mạng, khi đó ta gọi là truy nhập hợp pháp. Có rất nhiều dạng truy nhập được gọi là bất hợp pháp chẳng hạn như dùng tài khoản của người khác khi không được phép. Mức độ trầm trọng của việc truy nhập bất hợp pháp tuỳ thuộc vào bản chất và mức độ thiệt hại do truy nhập đó gây nên.

* **Để lộ thông tin:**

Để lộ thông tin do vô tình hay cố ý cũng là một mối đe dọa khác. Chúng ta nên định ra các giá trị để phản ánh tầm quan trọng của thông tin. Ví dụ đối với các nhà sản xuất phần mềm thì đó là: mã nguồn, chi tiết thiết kế, biểu đồ, thông tin cạnh tranh về sản phẩm... Nếu để lộ các thông tin quan trọng, tổ chức của chúng ta có thể bị thiệt hại về các mặt như uy tín, tính cạnh tranh, lợi ích khách hàng ...

* **Từ chối cung cấp dịch vụ:**

Mạng thường gồm những tài nguyên quý báu như máy tính, CSDL ... và cung cấp các dịch vụ cho cả tổ chức. Đa phần người dùng trên mạng đều phụ thuộc vào các dịch vụ để thực hiện công việc được hiệu quả.

Chúng ta rất khó biết trước các dạng từ chối của một dịch vụ. Có thể tạm thời liệt kê ra một số lỗi mạng bị từ chối: do một gói gay lỗi, do quá tải đường truyền, router bị vô hiệu hóa, do virus..

* + - 1. **Xác định trách nhiệm người sử dụng mạng:**
  + **Ai được quyền dùng tài nguyên mạng:**

Ta phải liệt kê tất cả người dùng cần truy nhập tới tài nguyên mạng. Không nhất thiết liệt kê toàn bộ người dùng. Nếu phân nhóm cho người dùng thì việc liệt kê sẽ đơn giản hơn. Đồng thời ta cũng phải liệt kê một nhóm đặc biệt gọi là các người dùng bên ngoài, đó là những người truy nhập từ một trạm đơn lẻ hoặc từ một mạng khác.

* + **Sử dụng tài nguyên thế nào cho đúng:**

Sau khi xác định những người dùng được phép truy nhập tài nguyên mạng, chúng ta phải tiếp tục xác định xem các tài nguyên đó sẽ được dùng như thế nào. Như vậy ta phải đề ra đường lối cho từng lớp người sử dụng như: Những nhà phát triển phần mềm, sinh viên, những người sử dụng ngoài.

* + **Ai có quyền cấp phát truy nhập:**

Chính sách an ninh mạng phải xác định rõ ai có quyền cấp phát dịch vụ cho người dùng. Đồng thời cũng phải xác định những kiểu truy nhập mà người dùng có thể cấp phát lại. Nếu đã biết ai là người có quyền cấp phát truy nhập thì ta có thể biết được kiểu truy nhập đó được cấp phát, biết được người dùng có được cấp phát quá quyền hạn không. Ta phải cân nhắc hai điều sau:

* Truy nhập dịch vụ có được cấp phát từ một điểm trung tâm không?
* Phương thức nào được dùng để tạo tài khoản mới và kết thúc truy nhập?

Nếu một tổ chức lớn mà không tập trung thì tất nhiên là có nhiều điểm trung tâm để cấp phát truy nhập, mỗi điểm trung tâm phải chịu trách nhiệm cho tất cả các phần mà nó cấp phát truy nhập.

* + **Người dùng có quyền hạn và trách nhiệm gì:**

Cần phải xác định rõ quyền lợi và nghĩa vụ của người sử dụng nhằm đảm bảo cho việc quản lý và hoạt động bình thường của mạng. Đảm bỏa tính minh bạch và riêng tư cho người dùng, cũng như người dùng phải có trách nhiệm bảo tài khoản của mình.

* + **Người quản trị hệ thống có quyền hạn và trách nhiệm gì:**

Người quản trị hệ thống thường xuyên phải thu thập thông tin về các tệp trong các thư mục riêng của người dùng để tìm hiểu các vấn đề hệ thống. Ngược lại, người dùng phải giữ gìn bí mật riêng tư về thông tin của họ. Nếu an ninh có nguy cơ thì người quản trị phải có khả năng linh hoạt để giải quyết vấn đề.

* + **Làm gì với các thông tin quan trọng:** Theo quan điểm an ninh, các dữ liệu cực kỳ quan trọng phải được hạn chế, chỉ một số ít máy và ít người có thể truy nhập. Trước khi cấp phát truy nhập cho một người dùng, phải cân nhắc xem nếu anh ta có khả năng đó thì anh ta có thể thu được các truy nhập khác không. Ngoài ra cũng phải báo cho người dùng biết là dịch vụ nào tương ứng với việc lưu trữ thông tin quan trọng của anh ta.
    - 1. **Kế hoạch hành động khi chính sách bị vi phạm:**

Mỗi khi chính sách bị vi phạm cũng có nghĩa là hệ thống đứng trước nguy cơ mất an ninh. Khi phát hiện vi phạm, chúng ta phải phân loại lý do vi phạm chẳng hạn như do người dùng cẩu thả, lỗi hoặc vô ý, không tuân thủ chính sách...

* + **Phản ứng khi có vi phạm:**

Khi vi phạm xảy ra thì mọi người dùng có trách nhiệm đều phải liên đới. Ta phải định ra các hành động tương ứng với các kiểu vi phạm. Đồng thời mọi người đều phải biết các quy định này bất kể người trong tổ chức hoặc người ngoài đến sử dụng máy. Chúng ta phải lường trước trường hợp vi phạm không cố ý để giải quyết linh hoạt, lập các sổ ghi chép và định kỳ xem lại để phát hiện các khuynh hướng vi phạm cũng như để điều chỉnh các chính sách khi cần.

* + **Phản ứng khi người dùng cục bộ vi phạm:**

Người dùng cục bộ có các vi phạm sau:

* Vi phạm chính sách cục bộ.
* Vi phạm chính sách của các tổ chức khác.

Trường hợp thứ nhất chính chúng ta, dưới quan điểm của người quản trị hệ thống sẽ tiến hành việc xử lý. Trong trường hợp thứ hai phức tạp hơn có thể xảy ra khi kết nối Internet, chúng ta phải xử lý cùng các tổ chức có chính sách an ninh bị vi phạm.

* + **Chiến lược phản ứng:**

Chúng ta có thể sử dụng một trong hai chiến lược sau:

* Bảo vệ và xử lý.
* Theo dõi và truy tố.

Trong đó, chiến lược thứ nhất nên được áp dụng khi mạng của chúng ta dễ bị xâm phạm. Mục đích là bảo vệ mạng ngay lập tức xử lý, phục hồi về tình trạng bình thường để người dùng tiếp tục sử dụng được, như thế ta phải can thiệp vào hành động của người vi phạm và ngăn cản không cho truy nhập nữa. Đôi khi không thể khôi phục lại ngay thì chúng ta phải cách ly các phân đoạn mạng và đóng hệ thống để không cho truy nhập bất hợp pháp tiếp tục.

* + - 1. **Xác định các lỗi an ninh:**

Ngoài việc nêu ra những gì cần bảo vệ, chúng ta phải nêu rõ những lỗi gì gây ra mất an ninh và làm cách nào để bảo vệ khỏi các lỗi đó. Trước khi tiến hành các thủ tục an ninh, nhất định chúng ta phải biết mức độ quan trọng của các tài nguyên cũng như mức độ của nguy cơ.

1. **Lỗi điểm truy nhập:**

Lỗi điểm truy nhập là điểm mà những người dùng không hợp lệ có thể đi vào hệ thống, càng nhiều điểm truy nhập càng có nguy có mất an ninh.

1. **Lỗi cấu hình hệ thống:**

Khi một kẻ tấn công thâm nhập vào mạng, hắn thường tìm cách phá hoại các máy trên hệ thống. Nếu các máy được cấu hình sai thì hệ thống càng dễ bị phá hoại. Lý do của việc cấu hình sai là độ phức tạp của hệ điều hành, độ phức tạp của phần mềm đi kèm và hiểu biết của người có trách nhiệm đặt cấu hình. Ngoài ra, mật khẩu và tên truy nhập dễ đoán cũng là một sơ hở để những kẻ tấn công có cơ hội truy nhập hệ thống.

1. **Lỗi phần mềm:**

Phần mềm càng phức tạp thì lỗi của nó càng phức tạp. Khó có phần mềm nào mà không gặp lỗi. Nếu những kẻ tấn công nắm được lỗi của phần mềm, nhất là phần mềm hệ thống thì việc phá hoại cũng khá dễ dàng. Người quản trị cần có trách nhiệm duy trì các bản cập nhật, các bản sửa đổi cũng như thông báo các lỗi cho người sản xuất chương trình.

1. **Lỗi người dùng nội bộ:**

Người dùng nội bộ thường có nhiều truy nhập hệ thống hơn những người bên ngoài, nhiều truy nhập tới phần mềm hơn phần cứng do đó đễ dàng phá hoại hệ thống. Đa số các dịch vụ TCP/IP như Telnet, tfp, … đều có điểm yếu là truyền mật khẩu trên mạng mà không mã hoá nên nếu là người trong mạng thì họ có khả năng rất lớn để có thể dễ dàng nắm được mật khẩu với sự trợ giúp của các chương trình đặc biệt.

1. **Lỗi an ninh vật lý:**

Các tài nguyên trong các trục xương sống (backbone), đường liên lạc, Server quan trọng ... đều phải được giữ trong các khu vực an toàn về vật lý. An toàn vật lý có nghĩa là máy được khoá ở trong một phòng kín hoặc đặt ở những nơi người ngoài không thể truy nhập vật lý tới dữ liệu trong máy.

1. **Lỗi bảo mật:**

Bảo mật mà chúng ta hiểu ở đây là hành động giữ bí mật một điều gì, thông tin rất dễ lộ ra trong những trường hợp sau:

* + Khi thông tin lưu trên máy tính.
  + Khi thông tin đang chuyển tới một hệ thống khác.
  + Khi thông tin lưu trên các băng từ sao lưu.

**CHƯƠNG 4: TỔNG QUAN VỀ FIREWALL**

* 1. **Firewall:**
     1. **Khái niệm:**

Firewall hiểu một cách chung nhất là cơ cấu để bảo vệ một mạng máy tính chống lại sự truy nhập bất hợp pháp từ các (mạng) máy tính khác. Firewall bao gồm các cơ cấu nhằm:

• Ngăn chặn truy nhập bất hợp pháp.

• Cho phép truy nhập sau khi đã kiểm tra tính xác thực của thực thể yêu cầu truy nhập.

Trên thực tế, Firewall được thể hiện rất khác nhau: bằng phần mềm hoặc phần cứng chuyên dùng, sử dụng một máy tính hoặc một mạng các máy tính. Theo William Cheswick và Steven Beilovin thì bức tường lửa có thể được xác định như là một tập hợp các cấu kiện đặt giữa hai mạng.

Nhìn chung bức tường lửa có những thuộc tính sau :

* Thông tin giao lưu được theo hai chiều.
* Chỉ những thông tin thoả mãn nhu cầu bảo vệ cục bộ mới được đi qua.
* Bản thân bức tường lửa không đòi hỏi quá trình thâm nhập.
  + 1. **Chức năng:**

**Ưu điểm:**

- Firewall có thể bảo vệ hệ thống máy tính chống lại những kẻ đột nhập qua khả năng ngăn chặn những phiên làm việc từ xa (remote login).

- Ngăn chặn thông tin từ bên ngoài (Internet) vào trong mạng được bảo vệ, trong khi cho phép người sử dụng hợp pháp được truy nhập tự do mạng bên ngoài.

- Firewall ngăn chặn các dịch vụ ít tin cậy.

- Truy nhập có điều khiển đến từng host.

- Tập trung hóa chính sách bảo mật

- Xác nhận người dùng và lưu trữ thông tin.

**Hạn chế:**

• Firewall không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó. Firewall chỉ có thể ngăn chặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phải xác định rõ các thông số địa chỉ.

• Firewall không thể ngăn chặn một cuộc tấn công nếu cuộc tấn công này không “đi qua” nó. Một cách cụ thể, Firewall không thể chống lại một cuộc tấn công từ một đường dial–up, hoặc sự mất mát thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm.

• Firewall cũng không thể chống lại các cuộc tấn công bằng dữ liệu (data–drivent attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua Firewall vào trong mạng được bảo vệ và bắt đầu hoạt động ở đây.

• Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi khả năng kiểm soát của Firewall (một ví dụ là các virus máy tính).

* 1. **Phân loại:**

Các công ty như CISCO và các nhà cung cấp khác đã đưa ra vô số sản phẩm Firewall, chúng có khả năng hiển thị các đường truyền với các kỹ thuật khác nhau. Một số loại Firewall ngày nay có khả năng ngăn chặn các gói dữ liệu đẩy lên lớp 4(TCP layer). Một số khác cũng có khả năng ngăn chặn tất cả các lớp và được xem như là *deep packet firewalls.* Có 3 kiểu phương thức ngăn chặn là:

* Packet filtering and stateless filtering
* Stateful filtering
* Deep packet layer inspection

Packet filters (basic access-list filters on routers) là block ngay lập tức.Sau đây giới thiệu về proxy Server no có khả năng kiểm soát các sự tấn công từ thiết bị độc lập. Prixy server là một Server được đặt ở giữa các client ứng dụng như Web browser và real server.

Nó chặn tất cả các request tới realserver với cái nhìn nếu nó có thể đáp ứng các request của bản thân nó. Nếu không, nó chuyển các request tới real server. Proxy yêu cầu kết nối tới internet căn cứ vào các yêu cầu từ nội bộ hoặc các nguồi ẩn. Proxy server là các ứng dụng cơ bản, chậm và khó quản lý đối với một mạng IP lớn. Thế hệ tiếp theo của Packet filter là stateless Firewalls. Vấn đề cơ bản là stateless firewall cho phép chỉ nhận một gói thông tin nó là căn cứ trong địa chỉ và cổng nguồn từ mạng có thật.

Stateless firewall được đưa ra việc cộng thêm sự linh hoạt và cơ động tới khả năng cấu hình mạng. Stateless firewall ngăn chặn các thông tin cơ bản về địa chỉ nguồn và địa chỉ đích. Hìn 4.2 giới thiệu khả năng ngăn chặn chiều sâu của lọc gói tin và stateless Firewall. Các gói tin được ngăn chặn ở lớp 3 trong mô hình OSI mô hình phân lớp mạng. Bởi vậy stateless Firewall có khả năng ngăn chặn các địa chỉ IP nguồn và đích và các giao thức cổng nguồn và đích.

Diagram

Description automatically generated

*Hình 4.2.a: Stateless Firewall*

Statefull firewall giới hạn thông tin mạng từ địa chỉ cơ bản nguồn và đíchtrong địa chỉ IP nguồn, đích, cổng nguồn TCP/UDP, cổng đích TCP/UDP.Statefull firewall cũng có thể ngăn chặn nội dung dữ liệu và kiểm tra các giao thức bất thường về giao thức.Ví dụ như statefull firewall có thể trang bị tốt hơn proxy server hoặc packet filter trong việc phát hiện và dừng các tấn công từ chối dịch vụ. Bởi vì địa chỉ nguồn và đích biến đổi, dữ liệu được cho phép thông qua nơi xát thực hoặc được cố gắng chắn lại trong mạng. Statefull firewall có thể ngăn chặn từ lớp 4 trong mô hình OSI :

Diagram

Description automatically generated

##### Hình 4.2.b: Stateful Firewall

Cùng với sự ngăn chặn lớp gói tin chiều sâu, firewall còn ngăn chặn các thông tin từ nguồn tới đích căn cứ vào địa chỉ IP nguồn đích, cổng TCP/UDP nguồn và đích. Nó cũng có thể ngăn chặn các thích ứng về giao thức, kiểm tra các tấn công vào các ứng dụng cơ bản, sự chắc chắn về bảo toàn luông dữ liệu giữa các thiết bị TCP/IP. Các sản phẩm IDS (Intrusion detection system) và NetScrem firewall hỗ trợ sự ngăn chặn lớp gói tin chiều sâu. Cisco PIX Firewall hỗ trợ hoạt động stateless và statefull:

Diagram

Description automatically generated

##### Hình4.2.c: Deep Packet Layer Firewall

Đặc biệt, các chức năng này được thực hiện trong phần cứng. Dữ liệu được tính toán theo tiêu chuẩn như là từ chối đối với DoS là loại bỏ ngay lập tức và có thể đưa vào bộ đệm …

* + 1. **Hardware Firewalls: PIX and NetScreen**

1. **PIX (Ciscosecure private internet exchange).**

Pix là thiết bị phần cứng mạng chuyên dụng được thiết kế nhằm đảm bảo chỉ một đường truyền được tính toán thiết lập theo chuẩn là cho phép truy nhập vào nguồn từ mạng với tốc độ bảo vệ.Việc thiết lập các tính năng của Cisco PIX và Cisco IOS được thiết kế nhằm nâng cao mức độ bảo mật trong mạng. Firewall PIX có thể ngăn chặn các kết nối không xác thực giữa nhiều mạng, cho phép xác thực (authentication, authorization), dịch vụ quản lý(AAA), access-list, cấu hình VPN (IPSec), FTP logging.

*Diagram

Description automatically generated*

*Hình 4.2.1a: Giao diện PIX*

1. **NetScreen.**

NetScreen firewall là các firewall ngăn chặn chiều sâu cho phép bảo vệ lớp ứng dụng. Trong khi PIX firewall có thể cấu hình stateless và statefull firewall hỗ trợ bảo mật lớp mạng và lớp giao vận

NetScreen firewall là thiết bị bảo vệ trạng thái và lớp chiều sâu gói tin nó căn cứ vào tất cả các kiểm tra của nó và quyết định được tạo ra bằng đường song song khác,bao gồm địa chỉ nguồn, địa chỉ đích , cổng nguồn, cổng đích, dữ liệu được kiểu tra sự phù hợp giao thức.

Thiết bị NetScreen bảo trì bảng phiên mà đường ngoài giữa mọi thứ khác như địa chỉ nguồn, địa chỉ đích, cổng nguồn, cổng đích, và các tác động phiên.

Diagram

Description automatically generated

##### Hình 4.2.1b: Bố trí NetScreen Firewall.

#### Phần mềm Check Point Firewalls

Hầu hết, các hardware firewalls cing cấp hiệu quả điều khiển truy nhập mạng, nhiều không được thiết kế để phát hiện và cản trở tấn công đặc biệt với đích tại các mức độ ứng dụng. Các kiểu ngăn chặn của kẻ tấn công là hiệu quả nhất với phần mềm firewall.

Check Point là nhà bán hàng phần mềm firewall trong thị trường ngày nay. Các phần mềm firewall cho phép các mạng và nhiều đặc biệt các ứng dụng mạng được bảo vệ từ không xác thực địa chỉ nguồn như internet. Mối liên quan với sự mở của web tạo ra khả năng nhiều người có khả năng truy nhập vào mạng cá nhân.Việc bảo vệ mạng vành đai là thiết lập cốt lõi của giải pháp Check Point.

Các hoạt động của Check Point phù hợp các sản phẩm tích hợp các đường nối mạng bảo mật, chất lượng dịch vụ và quản lý mạng đối với mạng IP rộng lớn.

* 1. **Các kiểu cấu trúc:**
     1. **Kiến trúc Dual-homed host firewall:**



*Hình 4.3.1: Sơ đồ kiến trúc Dual–homed Host*

Dual–homed Host là hình thức xuất hiện đầu tiên trong cuộc đấu để bảo vệ mạng nội bộ. Dual–homed Host là một máy tính có hai giao tiếp mạng: một nối với mạng cục bộ và một nối với mạng ngoài (Internet).

Hệ điều hành của Dual–homed Host được sửa đổi để chức năng chuyển các gói tin (packet forwarding) giữa hai giao tiếp mạng này không hoạt động. Để làm việc được với một máy trên Internet, người dùng ở mạng cục bộ trước hết phải login vào Dual–homed Host, và từ đó bắt đầu phiên làm việc.

**Ưu điểm của Dual–homed Host**:

• Cài đặt dễ dàng, không yêu cầu phần cứng hoặc phần mềm đặc biệt.

• Dual–homed Host chỉ yêu cầu cấm khả năng chuyển các gói tin, do vậy, thông thường trên các hệ Unix, chỉ cần cấu hình và dịch lại nhân (kernel) của hệ điều hành là đủ.

**Nhược điểm của Dual–homed Host:**

• Không đáp ứng được những yêu cầu bảo mật ngày càng phức tạp, cũng như những hệ phần mềm mới được tung ra thị trường.

• Không có khả năng chống đỡ những cuộc tấn công nhằm vào chính bản thân nó, và khi Dual–homed Host đó bị đột nhập, nó sẽ trở thành đầu cầu lý tưởng để tấn công vào mạng nội bộ.

**Đánh giá về kiến trúc Dual–homed Host:**

Để cung cấp dịch vụ cho những người sử dụng (user) bên trong (internal network) có một số giải pháp như sau:

* Kết hợp với các proxy server cung cấp những proxy service
* Cấp các account cho user trên máy dual–homed host này và khi mà người sử dụng muốn sử dụng dịch vụ từ Internet hay dịch vụ từ mạng bên ngoài (external network) thì họ phải truy nhập (login) vào máy này trước.

Nếu dùng phương pháp cấp account cho user trên máy dual–homed host thì user không thích sử dụng dịch vụ phiền phức như vậy, vì mỗi lần họ muốn sử dụng dịch vụ thì phải logi in vào máy khác (dual–homed host) khác với máy của họ đây là vấn đề rất là không trong suốt với người sử dụng.

Nếu dùng proxy server : Khó có thể cung cấp được nhiều dịch vụ cho người sử dụng vì phần mềm proxy server và proxy client không phải loại dịch vụ nào cũng có sẵn. Khi số dịch vụ cung cấp nhiều thì khả năng đáp ứng của hệ thống có thể giảm xuống vì tất cả các proxy server đều đặt trên cùng một máy.

Một khuyết điểm cơ bản của hai mô hình trên nữa là: khi mà máy dual–homed host nói chung cũng như các proxy server bị đột nhập vào. Người tấn công (attacker) đột nhập vào được qua nó thì lưu thông bên trong internal network bị attacker này thấy hết điều này thì hết sức nguy hiểm. Trong các hệ thống mạng dùng ethernet hoặc token ring thì dữ liệu lưu thông trong hệ thống có thể bị bất kỳ máy nào nối vào mạng đánh cắp dữ liệu cho nên kiến trúc trên chỉ thích hợp với một số mạng nhỏ.

* + 1. **Kiến trúc Screened host firewall:**

Kiến trúc này kết hợp 2 kỹ thuật đó là Packet Filtering và Proxy Services.

Packet Filtering: Lọc một số loại dịch vụ mà hệ thống muốn cung cấp sử dụng proxy server, bắt người sử dụng nếu muốn dùng dịch vụ thì phải kết nối đến proxy server mà không được bỏ qua proxy server để nối trực tiếp với mạng bên trong/bên ngoài (internal/external network), đồng thời có thể cho phép “pháo đài” (bastion host) mở một số kết nối với internal/external host.

Proxy Service: bastion host sẽ chứa các proxy server để phục vụ một số dịch vụ hệ thống cung cấp cho người sử dụng qua proxy server.



*Hình 4.3.2: Sơ đồ kiến trúc Screened Host*

**Đánh giá một số ưu, khuyết điểm chính của kiến trúc Screened Host:**

Screened Host: Đã tách chức năng lọc các gói IP và các proxy server ở hai máy riêng biệt. Packet Filtering chỉ giữ chức năng lọc gói nên có thể kiểm soát, cũng như khó xảy ra lỗi (tuân thủ qui tắc ít chức năng). Proxy Servers được đặt ở máy khác nên khả năng phục vụ (tốc độ đáp ứng) cũng cao.

Cũng tương tự như kiến trúc dual–homed host khi mà packet filtering system cũng như bastion host chứa các proxy server bị đột nhập vào (người tấn công đột nhập được qua các hàng rào này) thì lưu thông của internal network sẽ bị người tấn công thấy và điều này là rất nguy hiểm.

Từ khuyết điểm chính của 2 kiến trúc trên ta có kiến trúc thứ 3 sau đây khắc phục được phần nào khuyết điểm đó.

* + 1. **Kiến trúc Screened-subnet host firewall:**



*Hình4.3.3: Sơ đồ kiến trúc Screened Subnet Host*

Với kiến trúc này, hệ thống này bao gồm hai packet–filtering router và một bastion host (hình 4.3.3). Kiến trúc này có độ an toàn cao nhất vì nó cung cấp cả mức bảo mật network và application trong khi định nghĩa một mạng perimeter network.

Để tăng độ an toàn trong internal network, kiến trúc screen subnet ở trên sử dụng thêm một mạng DMZ (DMZ hay perimeter network) để che phần nào lưu thông bên trong internal network. Tách biệt internal network với Internet.

Mạng trung gian (DMZ) đóng vai trò như một mạng nhỏ, cô lập đặt giữa Internet và mạng nội bộ. Cơ bản, một DMZ được cấu hình sao cho các hệ thống trên Internet và mạng nội bộ chỉ có thể truy nhập được một số giới hạn các hệ thống trên mạng DMZ và sự truyền trực tiếp qua mạng DMZ là không thể được.

Với những thông tin đến, router ngoài (exterior router) chống lại những sự tấn công chuẩn (như giả mạo địa chỉ IP) và điều khiển truy nhập tới DMZ. Nó chỉ cho phép hệ thống bên ngoài truy nhập bastion host. Router trong (interior router) cung cấp sự bảo vệ thứ hai bằng cách điều khiển DMZ truy nhập mạng nội bộ chỉ với những truyền thông bắt đầu từ bastion host.

Với những thông tin đi, router trong điều khiển mạng nội bộ truy nhập tới DMZ. Nó chỉ cho phép các hệ thống bên trong truy nhập bastion host. Quy luật filtering trên router ngoài yêu cầu sử dụng dịch vụ proxy bằng cách chỉ cho phép thông tin ra bắt nguồn từ bastion host.

**Ưu điểm:**

• Kẻ tấn công cần phá vỡ ba tầng bảo vệ: router ngoài, bastion host và router trong.

• Bởi vì router ngoài chỉ quảng bá mạng trung gian (DMZ Network) tới Internet, hệ thống mạng nội bộ là không thể nhìn thấy (invisible). Chỉ có một số hệ thống đã được chọn ra trên DMZ là được biết đến bởi Internet qua bảng định tuyến (routing table) và DNS (Domain Name Server).

• Bởi vì router trong chỉ quảng cáo DMZ network tới mạng nội bộ, các hệ thống trong mạng nội bộ không thể truy nhập trực tiếp vào Internet. Điều nay đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ proxy.

**Đánh giá về kiến trúc Screened Subnet Host**:

Đối với những hệ thống yêu cầu cung cấp dịch vụ nhanh, an toàn cho nhiều người sử dụng đồng thời cũng như khả năng theo dõi lưu thông của mỗi người sử dụng trong hệ thống và dữ liệu trao đổi giữ các người dùng trong hệ thống cần được bảo vệ thì kiến trúc cơ bản trên phù hợp.

Sử dụng 2 screening router : exterior router và interior router.

Áp dụng qui tắc dư thừa có thể bổ sung thêm nhiều mạng trung gian (DMZ hay perimeter network) càng tăng khả năng bảo vệ càng cao.

Ngoài ra, còn có những kiến trúc biến thể khác như: sử dụng nhiều bastion host, ghép chung router trong và router ngoài, ghép chung bastion host và router ngoài …

* 1. **Các thành phần của Firewall & cơ chế hoạt động:**

Một Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:

• Bộ lọc gói (Packet–Filter)

• Cổng ứng dụng (Application–level Gateway hay Proxy Server)

• Cổng mạch (Circuite level Gateway)

* + 1. **Bộ lọc gói (Packet Filter)**

**a. Nguyên lý hoạt động**



*Hình 4.4.1: Sơ đồ làm việc của Packet Filtering*

Firewall hoạt động chặt chẽ với giao thức TCI/IP và làm việc theo thuật toán chia nhỏ các dữ liệu nhận được từ các ứng dụng trên mạng, hay nói chính xác hơn là các dịch vụ chạy trên các giao thức (Telnet, SMTP, DNS, SMNP, NFS...) thành các gói dữ liệu (data paket) rồi gán cho các paket này những địa chỉ để có thể nhận dạng, tái lập lại ở đích cần gửi đến, do đó các loại Firewall cũng liên quan rất nhiều đến các Packet và những con số địa chỉ của chúng.

Bộ lọc gói cho phép hay từ chối mỗi packet mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc gói hay không. Các luật lệ lọc gói này là dựa trên các thông tin ở đầu mỗi packet (packet header ), dùng để cho phép truyền các packet đó ở trên mạng. Đó là:

• Địa chỉ IP nơi xuất phát ( IP Source address)

• Địa chỉ IP nơi nhận (IP Destination address)

• Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)

• Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)

• Cổng TCP/UDP nơi nhận (TCP/UDP destination port)

• Dạng thông báo ICMP (ICMP message type)

• Giao diện Packet đến (Incomming interface of Packet)

• Giao diện Packet đi (Outcomming interface of Packet)

Nếu luật lệ lọc gói được thoả mãn thì packet được chuyển qua Firewall. Nếu không, packet sẽ bị bỏ đi. Nhờ vậy mà Firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Hơn nữa, việc kiểm soát các cổng làm cho Firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) được phép mới chạy được trên hệ thống mạng cục bộ.

**b. Ưu điểm và hạn chế của hệ thống Firewall sử dụng bộ lọc gói**

Ưu điểm:

• Đa số các hệ thống Firewall đều sử dụng bộ lọc gói. Một trong những ưu điểm của phương pháp dùng bộ lọc gói là chi phí thấp vì cơ chế lọc gói đã được bao gồm trong mỗi phần mềm router.

• Ngoài ra, bộ lọc gói là trong suốt đối với người sử dụng và các ứng dụng, vì vậy nó không yêu cầu sự huấn luyện đặc biệt nào cả.

Hạn chế:

• Việc định nghĩa các chế độ lọc gói là một việc khá phức tạp; nó đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ Internet, các dạng packet header, và các giá trị cụ thể mà họ có thể nhận trên mỗi trường. Khi đòi hỏi vể sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phức tạp, rất khó để quản lý và điều khiển.

• Do làm việc dựa trên header của các packet, rõ ràng là bộ lọc gói không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

* + 1. **Cổng ứng dụng (Application–Level Gateway)**

**a. Nguyên lý hoạt động:**



*Hình 4.4.2: Kết nối giữa người dùng (Client) với Server qua Proxy*

Đây là một loại Firewall được thiết kế để tăng cường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là proxy service (dịch vụ đại diện). proxy service là các bộ code đặc biệt cài đặt trên cổng ra (gateway) cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy code cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua Firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị mạng cho là chấp nhận được trong khi từ chối những đặc điểm khác.

Một cổng ứng dụng thường được coi như là một pháo đài (bastion host), bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp đảm bảo an ninh của một bastion host là:

* Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ thống (operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào hệ điều hành (operating system), cũng như là đảm bảo sự tích hợp Firewall.
* Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên bastion host.
* Bastion host có thể yêu cầu nhiều mức độ xác thực khác nhau, ví dụ như user password hay smart card.

• Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một số các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

• Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của giao thông qua nó, mỗi sự kết nối, khoảng thời gian kết nối. Nhật ký này rất có ích trong việc tìm theo dấu vết hay ngăn chặn kẻ phá hoại.

• Mỗi proxy đều độc lập với các proxy khác trên bastion host. Điều này cho phép đơn giản quá trình cài đặt một proxy mới, hay tháo gỡ một proxy đang có vấn đề.

Ví dụ: Telnet Proxy

Ví dụ một người dùng bên ngoài (gọi là outside client) muốn sử dụng dịch vụ telnet để kết nối vào hệ thống mạng qua môt bastion host có telnet proxy. Quá trình xảy ra như sau:

1. Outside client đó telnets đến bastion host. Bastion host kiểm tra mật khẩu (password), nếu hợp lệ thì outside client được phép vào giao diện của telnet proxy. Telnet proxy cho phép một tập nhỏ những lệnh của telnet, và quyết định những máy chủ nội bộ nào outside client được phép truy nhập.

2. Outside client chỉ ra máy chủ đích và telnet proxy tạo một kết nối của riêng nó tới máy chủ bên trong và chuyển các lệnh tới máy chủ dưới sự uỷ quyền của outside client. Outside client thì tin rằng telnet proxy là máy chủ thật ở bên trong, trong khi máy chủ ở bên trong thì tin rằng telnet proxy là client thật.

**b. Ưu điểm và hạn chế**

**Ưu điểm:**

• Cho phép người quản trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.

• Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.

• Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.

• Luật lệ filltering (lọc) cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc gói.

**Hạn chế:**

• Yêu cầu các users biến đổi (modify) thao tác, hoặc modify phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy.

* + 1. **Cổng vòng (Circuit–Level Gateway)**

Diagram

Description automatically generated

*Hình 4.4.3: Kết nối qua cổng vòng (Circuit–Level Gateway.*

Cổng vòng là một chức năng đặc biệt có thể thực hiện đươc bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ chuyển tiếp (relay) các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc gói nào.

Hình 4.4.3 minh hoạ một hành động sử dụng nối telnet qua cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối telnet qua Firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục telnet nào. Cổng vòng làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên, vì sự kết nối này xuất hiện từ hệ thống Firewall, nó che dấu thông tin về mạng nội bộ.

Cổng vòng thường được sử dụng cho những kết nối ra ngoài, nơi mà các nhà quản trị mạng thật sự tin tưởng những người dùng bên trong. Ưu điểm lớn nhất là một bastion host có thể được cấu hình như là một hỗn hợp cung cấp cổng ứng dụng cho những kết nối đến, và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống bức tường lửa dễ dàng sử dụng cho những người trong mạng nội bộ muốn trực tiếp truy nhập tới các dịch vụ Internet, trong khi vẫn cung cấp chức năng bức tường lửa để bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

* 1. **Các loại Firewall trong thực tế:**

Trong thực tế các công ty cần tăng tính bảo mật băng cách sử dụng các Firewall phần cứng thường dùng các dòng của cisco như:

* Cisco PIX: các loại như PIX 5501, 5515, 5530…
* Cisco ASA: như ASA 5510, ASA 5520, ASA 5550…
* Cisco Firewall Services Module(FWSM) như Cisco catalyst router 6000, 6500 ,7000 series switchs.

**CHƯƠNG 5 : TỔNG QUAN VỀ IDS & IPS**

* 1. **Hệ thống phát hiện xâm nhập(IDS):**

Do Firewall còn có những hạn chế nhất định đó là không có khả năng phát hiện những tấn công từ bên trong mạng và một số hạn chế khác. Vì vậy người ta đã sáng chế ra hệ thống phát hiện xâm nhập (IDS) nhằm hạn chế các yếu điểm của Firewall cải thiện tính năng bảo mật hệ thống mạng nâng cao độ an toàn trong mạng.

IDS (Instrusion detection systems) là hệ thống phát hiện đột nhập và xung đột dựa vào sự thu lượm các gói tin lưu thông trên mạng (packetsniffer) và phân tích các gói tin để phát hiện những dấu hiệu khả nghi.

IDS phát hiện những xung đột và những kể tấn công từ bên ngoài cũng như bên trong đưa ra những cảnh báo để firewall hoặc các nhà quản trị mạng kịp thời ngăn chăn đảm bảo an minh mạng.

* + 1. **Các chức năng của IDS**:
* Các cuộc tấn công quen biết theo đường chữ ký (singature) và các quy tắc.
* Những biến thiên trong lưu lượng và phương hướng sử dụng các quy tắc và phương pháp thống kê phức tạp.
* Những biến đổi mẫu lưu lượng truyền thông có sử dụng phương pháp phân tích luồng.
* Phát hiện các hoạt động bất thường có sử dụng phân tích đường cơ sở (baseline deviation analysis).
* Phát hiện hoạt động đáng nghi nhờ phân tích luồng, các kỹ thuật thống kê và phát hiện sự bất bình thường.
* Quản lý và phân tích các hoạt động của người dùng và hệ thống.
* Kiểm tra cấu hình và tính toàn vẹn cảu hệ thống và các lỗ hổng.

**Các hạn chế:**

* Hệ thống IDS là hệ thống phát hiện đột nhập nhưng nó không có chức năng chống lại.
* Bù trừ cho các yếu kém trong cơ chế chứng thực và nhận dạng.
* IDS không có khả năng phân tích tất cả các dữ liệu ở mạng tốc độ cao.
  + 1. **Vai trò của IDS:**
* Kiểm tra lần nữa các điểm yếu của fire wall.
* Nhận ra các cuộc tấn công mà firewall đã cho là hợp pháp(như cuộc tấn công vào webserver).
* Nhận ra được như là việc thử nhang thất bại(bắt được việc scan port, login…).
* Nhận ra các cuộc tấn công từ bên trong.
  + 1. **Phân loại IDS:**
       1. **Network-based IDS:**

##### Network-based IDSs là phần toàn bộ của pha kiểm tra của chính sách bảo mật. Network-based IDS là sự phát triển của sự kiểm tra thời gian thực kiểm tra tại các vị trí tồn tại trong cấu trúc hạ tầng mạng. Kiểm tra này gọi là network sensors, phân tích đường truyền và phát hiện các tác động không xát thực như các tác động nguy hại. Phụ thuộc vào các chiếm lược tấn công tổ chức được lựa chọn, kiểm tra các tác động thích hợp mang lại.

##### Một trong những ưu điểm chính của việc triển khai hệ thống Network-based trên hệ thống host-based là thực tế mà quản lý mạng có khả năng tiếp tục kiểm tra mạng của nó không phải việc làm thê nào để mạng phát triển.việc cộng thêm các host không cần thiết yêu cầu thêm các network-based intrusion sensors.

##### Các cấu trúc và thành phần của Network sensors.

##### Network IDS có 2 giao diện, nó là điển hình kết nối tới các segments khác nhau của mạng của tổ chức. Một là kiểm tra các port là đáp ứng đối với việc bắt dữ liệu đối với việc phân tích. Kiểm tra cổng được kết nối tới các đoạn mạng mà có khả năng mục tiêu được kết nối như web servers, mail servers…Cổng thứ 2 là thường được tham chiếu tới các cổng lệnh và cổng điều khiển nó đáp ứng việc gây ra cảnh báo tới flatform quản lý.Giống như host-based Cisco Secure Agent Manager, flatform này được dùng để cấu hình network sensors truy nhập và hiển thị cảnh báo và các báo cáo chung của yêu cầu.

##### Diagram Description automatically generated

##### Hình 5.1.3.1Tổng quan về Network-Based IDS

##### Từ quan điểm về cấu trúc, network-based có 3 thành phần khác nhau: network sensor, director và kỹ thuật giao tiếp 2 phần trên.

##### Diagram Description automatically generated

##### Hình 5.1.3.1b. Kiến trúc Network-Based IDS

##### Network-based IDS sensor chạy trên Linux và có nhiều thành phần và mỗi kết nối bên trong và điều khiển xử lý khác nhau. Một trong những thành phần chính là cidWebServer . Web server được dùng các servlets khác nhau đẻ cung cấp các dịch vụ. cidWebServer giao tiếp cùng các trạng thái của server, sự thực hiện server và IP log server servlets được dùng Remote Data Exchange Protocol (RDEP). RDEP phục vụ như các giao thức giao tiếp của các sensor.

##### Network IDSs được phát triển bởi vì khi sự phát triển là lên kế hoạch cẩn thận tại các điểm thiết kế, các mạng quản lý, các tổ chực bảo mật có thể kiểm tra dữ liệu.Khi sự kiểm tra được thực hiện dữ liệu chỉ đang được truyền trong mạng.Bởi vậy các nhà quản lý có cơ hội để tác động vào tài khoản mà không cần biết chính xác đích tấn công là gì bởi vì các IDS kiểm tra hoàn thành từng đoạn một.

##### Một số các bước và nhiệm vụ cần là khi triển khai các network sensor trong mạng của bạn. Việc cài đặt các network sensor yêu cầu có kế hoạch trước khi có tác động kết nối các sensors tới mạng. Đó là nhiệm vụ của nhà quản lý bảo mật mạng để xác định rõ đường truyền cần gì được hiển thị tới việc bảo vệ tất cả các tài nguyên của tổ chức.

##### Khi lên kế hoạch cho việc đặt các IDS, nhà quản lý mạng phải tính đến số lượng và độ phức tạp của mạng kết nối với mạng khác và tổng số và kiểu đường truyền trong mạng. Sau khi lựa chọn các thông tin đó và biết được thông tin gì được bảo vệ, vị trí và kiểu sensor được xác định. Các sensor được đặt ở miền inside phải có tránh nhiệm khác với các sensor đặt ở miền outside:

Diagram

Description automatically generated

##### Hình 5.1.3.1c Bố trí Network-Based IDS Sensor

* + - 1. **Host-based IDS:**

##### Hiện nay tất cả các nhà quản lý mạng đều quan tâm đến vấn đề bảo mật mạng với cái nhìn tiếp tục xây dựng xử lý thông qua các chính sách bảo mật mạng. Xử lý này là phương thức 4 bước bao gồm: bảo mật hệ thống (secure the system), kiểm tra mạng (monitor the network), kiểm tra hiệu quả của các giải pháp và cải thiện các triển khai bảo mật.

##### Host IDS có thể mô tả bằng cách phân phối các agent tập trung trong mỗi server của mạng để hiển thị các tác động của mạng trong thời gian thực.Host IDS xác định phạm vi bảo mật và có thể cấu hình đề mà các đáp ứng tự động được ngăn chặn tấn công từ các nguyên nhân các mối nguy hiểm trước khi nó tấn công vào hệ thống.

##### Cấu trúc và các thành phần của Host sensor

##### Cisco IDS sensor có hai thành phần chính:

##### Cisco Secure Agent

##### Cisco secure Agent là phần mềm bắt gói tin được chạy trên mỗi server riêng biệt hoặc trên workstation để bảo vệ chống lại các kẻ tấn công.

##### Cisco IDS sensor cung cấp các phân tích thời gian thực và tác động trở lại các tấn công xâm nhập. Host sensor xử lý và phân tích mỗi và mọi yêu cầu tới hệ điều hành và các giao diện chương trình ứng dụng và phòng chống các host nếu cần thiết. Các agent đó có thể điều khiển tất cả các trạng thái trong các files, các bộ đệm của mạng, việc đăng ký và truy nhập COM. Cấu trúc của Cisco secure Agent là cấu trúc các phương tiện luật lệ đánh chặn của bảo mật agent INCORE (Security Agent’s Intercept Correlate rules engine architecture).

##### Các Host sensor Agent được cài đặt hệ điều hành. Các phần mềm này được chạy cùng hệ điều hành đề sự bảo vệ được đảm bảo chính hệ điều hành đó. Các agents bảo vệ các hosts chống lại các tấn công được bắt đầu thông qua mạng và cũng bảo vệ chống lại các tấn công các tác động nguy hiểm của người dùng người mà log vào hệ điều hành, web và các luật [FTP. Cơ](ftp://FTP.Cơ) sở dữ liệu chứa đựng các tham số chính sách bảo mật, các xác định người dùng ngoại lệ và danh sách các ứng dụng được bảo vệ.

##### Diagram Description automatically generated

##### Hình 5.1.3.2a: Cấu trúc của Host Sensor Agent

##### Chúng ta đều thừa nhận rằng sự tấn công làm hại đến các dịch vụ thông tin Internet (IIS) trong web server.Các agent core dự đoán luồng dữ liệu đến theo các luật FTP chúng được lưu trữ trong Rules engine, các ứng dụng cho chính sách và các thông số ngoại lệ. Nếu các hành động nguy hiểu được phát hiện, các tác động thích hợp được xác định rõ.

##### Nhà quản lý Cisco Secure Agent:

##### Cisco secure Agent manager chịu tránh nhiệm trong việc quản lý Cisco secure Agent và việc giao tiếp từ các agent. Cisco secure Agent manager cung cấp các chức năng quản lý đối với tất cả các agent trong kiểu kiểm soát. Nó cũng được cấu thành từ các thông báo của tổchuwcs bảo mật trong trường hợp tấn công và các báo cáo chung. Các phiên quản lý này được dùng các kỹ thuật mã hóa dữ liệu là thiết thực, kín đáo và an toàn. Cisco secure Agent manager có 3 thành phần chính: Giao diện đồ họa người dung (GUI), server, các cảnh báo người điều khiển. Cả hai GUI và server đều được link tới cơ sở dữ liệu nơi mà các thông tin cấu hình được lưu trữ.

##### Các agents được kết nối trực tiếp với server.Khi agent gửi cảnh báo tới server, server cung cấp các chỉ dẫn người điều khiển một cách cẩn thận tất cả các yêu cầu chú thích cấu hình như e-mail và trang chú thích.

##### Sự triển khai HIDS trong mạng:

##### Sự phát triển của các Host-based IDS thông qua các thổ chức mạng yêu cầu các thiết kế thông qua rất tốt.

##### Vấn đề cơ bản là xác định những gì trong chính sách bảo mật của các công ty, nhà thiết kế được đáp ứng nhận ra và quyết định hệ thống nào được bảo vệ. Toàn vẹn đối tượng trong phase thiết kế xác định các kiểu hệ thống khác nhau: là servers UNIX hay Windows platforms, chúng ta cần bảo vệ chỉ server hay chúng ta lo lắng về máy tính laptop tốt như desktop…

##### Diagram Description automatically generated

##### Hình 5.1.3.2b Triển khai Host IDS

##### Việc xem xét sự quan trọng trong phase thiết kế là sự giao tiếp quản lý IDS. Các agents giao tiếp với các Agent Manager trên port TCP đặc biệt. Điều này trở nên quan trọng khi các agents cư trú trong mạng khác trong mạng Agent Manager. Điều đặc biệt đó đúng với các agents chạy trong miền DMZ hay trong nhánh hay remote home office.

##### Các kế hoạch chung đối với hạ tầng công ty là sự phát triển các web server, các mail server, DNS (domain name system), FTP và các agents khác trong mạng DMZ. Đường truyền tới và từ các agents chạy trong các server đó tới các Agents Manager được cho phép thông qua firewall.

##### Đối với mote offices hay home offices, VPN và IPSec cũng được tính toán đến khi thiết kế kênh giao tiếp quản lý giữa các agent và Agent Manager.

* + 1. **Các thành phần của IDS :**

Một IDS thông thường gồm có các thành phần sau:

* Bộ cảm biến (sensor network):

Bộ cảm biến dùng để lọc thông tin và loại bỏ dữ liệu không tương thích đặt từ các sự kiện liện quan với hệ thống bảo vệ vì vậy có thể phát hiện các hành vi nghi ngờ.

* Bộ phân tích:

Bộ phân tích sử dụng cơ sở dữ liệu chính sách phát hiện cho mục này.

* Bộ phát các tín hiệu cảnh báo: dùng để phát ra các tín hiệu cảnh báo tới các thiết bị ngăn chặn hay tới nhà quản trị để kịp thời ngăn chặn các cuộc tấn công.
* Cơ sở dữ liệu: Cung cấp các như các tham số cần thiết các tham số cấu hình và các mức đánh giá xung đột cũng như là nơi lưu trữ các báo cáo phân tích.

Có 2 loại sản phẩm chính là: CSIDS(Cisco secure instrusion detection sennsor) và IDSM-2( IDS switch module) và PIX Firewall IDS .

* 1. **Hệ thống ngăn chăn xâm nhập(IPS):**
     1. **Khái niệm IPS:**

Hệ thống xâm nhập IPS(Instrusion prevention systems) là bất kỳ một thiết bị phần cứng hay phần mềm nào có khả năng phát hiện và ngăn ngừa các nguy cơ mất an ninh mạng.

IPS là thiết bị tích hợp IDS và hiệ thống ngăn chặn nhằm khắc phục điểm yếu của IDS. IPS gồm hai phần chính :

* Phần phát hiện xâm nhập chính là IDS.
* Phần ngăn ngừa xâm nhập: nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe doạ tấn công bằng việc loại bỏ những lưu lượng mạng có hại hay có ác ý trong khi vẫn cho phép các hoạt động hợp pháp tiếp tục.
* Các phương thức ngăn ngừa là:  
   - Những ứng dụng không mong muốn và những cuộc tấn công “Trojan horse” nhằm vào các mạng và các ứng dụng cá nhân, qua việc sử dụng các nguyên tắc xác định và các danh sách điều khiển truy nhập (access control lists).
* Các gói tin tấn công giống như những gói tin từ LAND và WinNuke qua việc sử dụng các bộ lọc gói tốc độ cao.
* Sự lạm dụng giao thức và những hành động lảng tránh những thao tác giao thức mạng giống như Fragroute và những khảo sát lấn TCP (TCP overlap exploits)
* Thông qua sự ráp lại thông minh.
* Các tấn công từ chối dịch vụ (DOS/DDOS) như “lụt” các gói tin SYN và ICMP bởi việc sử dụng các thuật toán lọc dựa trên cơ sở ngưỡng.
* Sự lạm dụng các ứng dụng và những thao tác giao thức – các cuộc tấn công đã biết và chưa biết chống lại HTTP, FTP, DNS, SMTP .v.v. qua việc sử dụng những quy tắc giao thức ứng dụng và chữ ký.

- Những cuộc tấn công quá tải hay lạm dụng ứng dụng bằng việc sử dụng các hữu hạn tiêu thụ tài nguyên dựa trên cơ sở ngưỡng.

* + 1. **Chức năng của IPS:**

Ngăn chặn xâm nhập cung cấp nhiều khả năng ở mức độ host và cả mức độ mạng và từ các mức độ khác nhau, khả năng cung cấp bởi hệ thống ngăn chặn xâm nhập gồn các thành phần chủ yếu sau:

* **Phát hiện và ngăn ngừa:**

Nhìn bề ngoài, các giải pháp phát hiện xâm nhập và ngăn ngừa xâm nhập xuất hiện theo kiểu cạnh tranh nhau. Về bảo chất, chúng chia sẻ một danh sách các chức năng giống nhau như kiểm tra gói tin, phân tích có trạng thái, ráp lại các đoạn, ráp lại các TCP-segment, kiểm tra gói tin sâu, xác nhận tính hợp lệ giao thức và thích ứng chữ ký.

* **Phát hiện xâm nhập:**

Mục đích của “phát hiện xâm nhập” là cung cấp sự giám sát, kiểm tra, tính pháp lý và báo cáo về các hoạt động của mạng. Nó hoạt động trên các gói tin được cho phép thông qua một thiết bị kiểm soát truy nhập. Do những hạn chế về độ tin cậy và những đe dọa bên trong, “Ngăn ngừa Xâm nhập” phải cho phép một số “vùng xám” (gray area) tấn công để tránh các trường hợp báo động giả. Mặt khác, những giải pháp IDS được “nhồi” trí thông minh có sử dụng nhiều kỹ thuật khác nhau để nhận biết những cuộc xâm nhập, những khai thác, lạm dụng bất chính và các cuộc tấn công tiềm tàng. Một IDS có thể thực hiện các hoạt động mà không làm ảnh hưởng đến các kiến trúc tính toán và kết nối mạng.

Bản chất bị động của IDS nằm ở chỗ cung cấp sức mạnh để chỉ đạo phân tích thông minh các lưu lượng gói tin. Những vị trí IDS này có thể nhận ra:  
 - Các cuộc tấn công quen biết theo đường chữ ký (singature) và các quy tắc.  
 - Những biến thiên trong lưu lượng và phương hướng sử dụng những quy tắc và phân tích thống kê phức tạp.

- Những biến đổi mẫu lưu lượng truyền thông có sử dụng phân tích luồng.

- Phát hiện hoạt động bất thường có sử dung phân tích độ lệch đường cơ sở (baseline deviation analysis).

- Phát hiện các hoạt động đáng nghi nhờ phân tích luồng, các kỹ thuật thống kê và phát hiện sự bất bình thường.

* **Ngăn ngừa xâm nhập**

Các giải pháp“Ngăn ngừa Xâm nhập” nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe doạ tấn công bằng việc loại bỏ những lưu lượng mạng có hại hay có ác ý trong khi vẫn cho phép các hoạt động hợp pháp tiếp tục. Mục đích ở đây là một hệ thống hoàn hảo – không có những báo động giả nào làm giảm năng suất người dùng cuối và không có những từ chối sai nào tạo ra rủi ro quá mức bên trong môi trường. Có lẽ một vai trò cốt yếu hơn sẽ là cần thiết để tin tưởng, để thực hiện theo cách mong muốn dưới bất kỳ điều kiện nào. Điều này có nghĩa các giải pháp “Ngăn ngừa Xâm nhập” được đặt vào đúng vị trí để phục vụ với:

* Những ứng dụng không mong muốn và những cuộc tấn công “Trojan horse” nhằm vào các mạng và các ứng dụng cá nhân, qua việc sử dụng các nguyên tắc xác định và các danh sách điều khiển truy nhập (access control lists).
* Các gói tin tấn công giống như những gói tin từ LAND và WinNuke qua việc sử dụng các bộ lọc gói tốc độ cao.
* Sự lạm dụng giao thức và những hành động lảng tránh – những thao tác giao thức mạng giống như Fragroute và những khảo sát lấn TCP (TCP overlap exploits) – thông qua sự ráp lại thông minh.
* Những cuộc tấn công quá tải hay lạm dụng ứng dụng bằng việc sử dụng các hữu hạn tiêu thụ tài nguyên dựa trên cơ sở ngưỡng.

Tất cả các cuộc tấn công và trạng thái dễ bị tấn công cho phép chúng tình cờ xảy ra đều được chứng minh bằng tài liệu. Ngoài ra, những khác thường trong các giao thức truyền thông từ mạng qua lớp ứng dụng không có chỗ cho bất cứ loại lưu lượng hợp pháp nào, làm cho các lỗi trở thành tự chọn lọc trong ngữ cảnh xác định.

* + 1. **Phân loại IPS**
       1. **NIPS:**

NIPS (Network-based IPS) là loại IPS được dùng để lắp đặt vào mạng để ngăn chặn sự xâm nhập từ ngoài mạng vào nội mạng.

Network IPS cung cấp các thành phần thực hiện trước mà có hiệu quả toàn diện trong toàn bộ khung bảo mật mạng của bạn. Sự kết hợp giữa NIPS với các thành phần như HIPS, IDS và firewall vành đai cung cấp giải pháp bảo mật phòng ngừa chiều sâu mạnh mẽ.

**5.2.3.1a Các khả năng của hệ thống xâm nhập mạng cơ sở**:

Kỹ thuật ngăn chặn xâm nhập có thể dừng các đường truyền xâm nhập trước khi nó xâm nhập vào mạng bởi việc đặt sensor ở lớp 2 thiết bị forwading (Switch) trong mạng.

Diagram

Description automatically generated

*Hình 5.2.3.1a: Triển khai Intrusion Prevention Sensor*

NIPS có thể hủy đường truyền theo các cách sau :

* Hủy một gói tin: Kiểu đơn giản nhất của NIPS bao gồm việc xác định một gói tin khả nghi và hủy chúng. Các gói tin xấu sẽ không tới các hệ thống đích bởi thế mạng của bạn sẽ được bảo vệ. Tuy nhiên kẻ tấn công có thể gửi lại các gói tin xấu. Đối với mỗi gói tin IPS cần phân tích gói tin mạng và nơi mà đường truyền cho qua hay từ chối, chi phối tài nguyên trong thiết bị IPS.
* Hủy tất cả các gói tin trong kết nối: Thay vì hủy từng gói tin một, hệ thống IPS có thể hủy toàn bộ các gói tin trong kết nối đặc biệt đối với cấu hình theo chu kỳ thời gian. Sự kết nối được xác định tính toán các thành phần:
  + Địa chỉ nguồn.
  + Địa chỉ đích.
  + Cổng đích.
  + Cổng nguồn (không bắt buộc).

Ưu điểm của ngắt kết nối là các gói tin đến sau tính toán kết nối có thể ngắt tự động mà không cần phân tích. Về mặt hạn chê, tuy nhiên kẻ tấn công vẫn có khả năng gửi đường truyền mà không cần tính toán kết nối có thể ngắt.

* Hủy tất cả các đường truyền từ địa chỉ nguồn:

Cơ chế ngắt cuối cùng là ngắt tất cả các đường truyền từ địa chỉ nguồn đặc biệt. Trong một số trường hợp, khi các gói tin khả nghi được phát hiện, nó sẽ được ngắt, cùng với tất cả đường truyền tương ứng với địa chỉ nguồn đối với cấu hình trong chu kỳ thời gian. Bởi vì tất cả đường truyền từ host tấn công có thể bị ngắt trong vài phiên.Thiết bị IPS sử dụng ít tài nguyên. Hạn chế chính là nếu kẻ tấn công có thể giả mạo địa chỉ nguồn và giả vờ là hệ thống quan trọng như phần thương mại, nếu bắt đầu đăng ký là khả năng lỗi và đường truyền sẽ từ chối mạng của bạn.

Lợi ích chính của việc sử dụng NIPS là ngăn chặn tấn công đảm bảo đường truyền bình thường và thực thi các chính sách bảo mật có hiệu quả.

* + - 1. **b Các thành phần của hệ thống ngăn chặn xâm nhập mạng cơ sở NIPS:**

Sản phẩm ngăn chặn xâm nhập mạng cơ sở dùng sensor để phân tích đường truyền mạng tại một số vị trí thông qua mạng. Các sensor này phát triển từ các kiểu nhân tố như:

* Các thiết bị sensor độc lập (Standalone appliance sensors): Các thiết bị sensor độc lập cung cấp tính linh hoạt nhất khi phát tiển sensor IPS trong mạng. Các sensor này có thể triển khai tại hầu như nhiều vị trí trong mạng. Yếu điểm chính của thiết bị sensor là phải tạo khoảng trống trong việc đặt sensor. Sensor 4200 series là một minh chứng.
  + Blade-based sensors: có thể tạo ưu thế của các thiết bị hạ tầng tồn tại khi triển khai thiết bị IPS. Blade-based sensors không cần khoảng trống lớn để đặt và có nhiều ưu thế của hướng đường truyền nhận từ đường đi của thiết bị hạ tầng nơi mà nó được triển khai. Một yếu điểm của Blade-based sensors là nó có thể có giá nếu như đã tồn tại thiết bị hạ tầngtrong mạng. Prevention Security Service Module (AIP-SSM).
* Phần mềm Intrusion Prevention System (IPS) tích hợp trong hệ điều hành (OS) trong thiết bị hạ tầng: Khi mà phần mềm IPS được tích hợp trong thiết bị hệ tầng đang tồn tại.Các chức năng được cung cấp thường được so sánh với Blade-based sensors bởi vì thiết bị hạ tầng mang lại nhiều tránh nhiệm và đáp ứng. Sự phụ thuộc vào môi trường mạng nó làm giảm nhiều chức năng không phải là vấn đề.

Không quan tâm đến các tác nhân trong mạng, sensor phải nhận được đường truyền mạng mà cần được phân tích. Việc bắt đường truyền biến đổi phụ thuôc vào nơi mà bạn sử dụng mode inline hay mode ngẫu nhiên. Sau khi bắt được đường truyền, sensor sẽ phân tích đường truyền phân theo các kiểu đường chữ ký sử dụng trong đường truyền mạng.

Kết quả phân tích đường truyền thực hiện bởi các sensors IPS được dùng để kiểm tra thông qua bảng hiển thị kiểm soát. Giống như các ứng dụng kiểm soát có thể cấu hình có hiệu quả đối với số lượng lớn các sensors IPS trong mạng. Việc quản lý sensor IPS thông qua hai kiểu: Triển khai sensor nhỏ và triển khai sensor rộng lớn.

* + - 1. **HIPS:**

##### Hệ thống phát hiện xâm nhập HIPS là một loại kỹ thuật tương đối mới trong thị trường bảo mật. Ngay từ ngày đầu, nó đã có nhiều lợi ích được chấp thuận và sự sử dụng và được dự đoán là sẽ phát triển nhanh chóng trong tương lai. Mặc dù có được lợi thế đó, song loại thiết bị này không được xác định rõ ràng hơn các kỹ thuật được thiết lập như firewall và antivirus. Các tài liệu kỹ thuật còn mơ hồ, các thuật ngữ mơ hồ và sự phát triển sản phẩm nhanh chóng làm đảo lộn thị trường tới điểm mà thật là khó để xác định các sản phẩm thực sự là hệ thống phát hiện xâm nhập HIPS (Host Intrusion Prevention Systems).

##### 5.2.3.2.a Các khả năng của hệ thống ngăn chặn xâm nhập từ máy chủ(HIPS):

* Ngăn chặn các tác động có hại: Một HIPS phải có khả năng làm nhiều hơn việc cảnh báo hay tác động vào khi các đoạn mã nguy hiểm tấn công tới các host. Nó sẽ phải có hành động ngắt các tác động của các đoạn mã nguy hiểm. Nếu các hành động này được ngăn chặn các tấn công sẽ thất bại. HIPS cũng có thể giữ việc truy nhập và có khả năng cảnh báo bởi thế mà người dùng sẽ biết HIPS làm gì nhưng với các yêu cầu khác nhau làm cho HIPS cũng có khả năng mang lại các tác động.
* Không phá vỡ các hoạt động bình thường: Một cách khác bảo vệ các host là gỡ nó ra khỏi mạng. Không kết nối nó với mạng sẽ tạo ra sự bảo vệ nó tốt hơn nhưng host lại lấy đi ở nó sự đáp ứng các dịch vụ thương mại trong mạng. Ngắt kết nối không phải là cách bảo mật thường dùng bởi vì nó cũng ngắt các hoạt động bình thường.
* Phân biệt giữa trạng thái tấn công và trạng thái bình thường: Sản phẩm HIPS phải đủ xác thực để xác định đúng đắn đâu là trạng thái bị tấn công và đâu là trạng thái bình thường để từ đó mới phát hiện ra lỗi hay các cuộc tấn công kịp thời ngăn chặn.
* Dừng các tấn công mới và các tấn công không biết: Với mỗi nguy hại và tấn công mới bạn sẽ phải cần update hay xử lý cấu hình lại. Sản phẩm HIPS phải có khả năng dừng các tấn công mới và các tấn công không biết mà không cần cấu hình lại hay update đây là cách mà sản phẩm HIPS dừng các tấn công.
* Bảo vệ ngăn chặn các lỗ hổng của các ứng dụng được cho phép: Bằng một vài dấu hiệu, HIPS phải không cho phép các ứng dụng được cho phép bị làm hại bởi các kẻ tấn công. Tuy vậy sản phẩm HIPS cũng có khả năng bảo vệ ngăn chặn các lỗ hổng của các ứng dụng được cho phép.
* Ngoài ra HIPS còn có các lợi ích khác như :
* Ngăn chặn các tấn công có hại.
* Sửa chữa đường dẫn.
* Ngăn chặn sự nhân các tấn công nội bộ.
* Đưa ra các chính sách có hiệu lực.
* Điều chỉnh các yêu cầu.

Tuy nhiên HIPS cũng có những yếu điểm đó là không tương thích với tất cả các công việc nó chỉ là phần triển khai các phòng ngừa chiều sâu và có những yếu điểm sau:

* Vấn đề về xáo trộn người dùng.
* Thiếu việc đưa thông tin hoàn thành.
* Các tấn công không nhằm vào các host.

**5.2.3.2.b Các thành phần của HIPS:**

Sản phẩm HIPS có hai thành phần cơ bản:

* + 1. **Gói phần mềm để cài đặt tại điểm cuối để bảo vệ nó còn gọi là client hay agent**.

Về bản chất HIPS agents cũng ứng dụng xử lý điều khiển truy nhập giống như vậy tới các máy tính. Sự xử lý này được tác động khi hoạt đỗngyar ra trong hệ thống và có thể chia theo các phase dưới đây:

* + - * Nhận dạng kiểu tài nguyên được phép truy nhập: Các angets nhận dạng nguồn tài nguyên được truy nhập. Các nhận dạng nguồn tài nguyên chung bao gồm: tài nguyên mạng, bộ nhớ, thực thi ứng dụng, cấu hình hệ thống.
      * Thu thập dữ liệu về hoạt động: Sản phẩm HIPS thu thậm dữ liệu dùng một hay nhiều cách thức: sự biến đổi nhân, sự chặn hệ thống cuộc gọi, các hệ điều hành ảo, các phân tích đường truyền mạng,
      * xác định trạng thái của hệ thống: các trạng thái hệ thống bao gồm: location, user, system.
      * Tham khảo các chính sách bảo mật: Dữ liệu sẽ tập hợp về sự tấn công tài nguyên truy nhập và trạng thái hệ thống được so sánh một hay nhiều chính sách sau:

1. Anomaly-based
2. Atomic rule-based
3. Pattern-based
4. Behavioral
5. Access control matrix

* Thực thi tác động: Đó là các trạng thái: cho phép truy nhập vào mạng hay từ chối truy nhập, trong thái nhập vào (log state), hủy gói tin, tắt máy chủ và truy vấn người dùng.

Diagram

Description automatically generated

*Hình 5.2.3.2 : Xử lý điều khiển truy nhập.*

* + 1. Hạ tầng quản lý để quản lý các agents này.

HIPS agents mà có thể có một giao diện sử dụng tốt và đôi khi hoạt động không cùng kiểu quản lý trung tâm. Tuy nhiên các lớp hoạt động HIPS yêu cầu một hạ tầng quản lý. Kiểu đặc trưng, hạ tầng bao gồm trung tâm quản lý hay điểm đầu cuối và giao diện được dùng để truy nhập vào các trạm quản lý.

* 1. **Trung tâm quản lý:**
* Trung tâm quản lý gồm 3 thành phần cơ bản. Thành phần đầu tiên đó là cơ sở dữ liệu nơi mà lưu trữ các trạng thái, chính sách, agent và các dữ liệu cấu hình khác. Thành phần thứ hai đó là khả năng trình bày trạng thái. Thành phần cuối cùng đó là chính sách quản lý. Chúng phụ thuộc vào mô hình quản lý mỗi thành phần được cài đặt trên các thành phần vật lý khác nhau.
  1. Cơ sở dữ liệu là thành phần quan trọng nhất của trung tâm quản lý. Nó là nơi lưu tất cả các thông tin chính sách. Nó phải đủ mạnh để hỗ trợ các agents sử dụng nó mà không cần xâm nhập và bảo vệ đủ để chống lại kẻ tấn công. Đó là lý do mà tất cả các công ty hoạt động cần phải có nhiều các kiểu cơ sở dữ liệu hoạt động như SQL hay ORACLE
  2. Điều khiển cảnh báo và trạng thái đó là điều khiển sự phân chia các trạng thái ở các trạm quản lý và bao gồm trạng thái mang và phát sinh cảnh báo.Nhờ hai trạnh thái này mà chúng ta biết được tình trạnh mạng hoạt động ra sao, có xâm nhập hai không.
  3. Quản lý chính sách: đó là việc chỉnh sửa các chính sách, các chính sách bảo mật thực thi thông qua thời gian trong các đáp ứng môi trường và thay đổi trong quan hệ bảo mật. Vì vậy cần chỉnh sửa chúng cho phù hợp với sự phân phối chúng tới các agents.

1. **Giao diện quản lý:**

Công cụ quản lý HIPS được dùng tương tác với trung tâm quản lý được gọi là giao diện sử dụng và có hai kiểu: được cài đặt trên giao diện người sử dụng client và giao diện web. Mặc dù giao diện người dùng thường có nhiều chức năng hơn, giao diện web thích ứng tốt hơn với nhà quản lý từ xa. Trong cả hai trường hợp sự giao tiếp giữa giao diện quản lý và trung tâm quản lý cũng được bảo vệ một các cẩn thận như sự giao tiếp giữa agents và MC.

**CHƯƠNG 6: HỆ THỐNG MÔ PHỎNG FIREWALL**

* 1. **Mục đích dựng mô phỏng:**

Mục đích của dựng mô phỏng là đưa ra một mô hình mạng thật đang được ứng dụng trong thực tế nhằm phân tích đánh giá các hoạt động của một mạng máy tính cũng như cơ chế hoạt động của FireWall trong mạng máy tính cũng như hệ thống IPS, khả năng ngăn chặn và bảo vệ của IPS cũng như FireWall trong mạng máy tính ra sao. Nhìn chung tất cả các hệ thống thật ta đều có thể mô phỏng trên máy tính nếu như máy tính của chúng ta đủ mạnh để có thể đủ khả năng xử lý cho hệ thống .

* 1. **Nguyên lý dựng mô phỏng và các yêu cầu:**

Yêu cầu cấu hình máy tính định làm mô phỏng: RAM tối thiểu 1Gb máy có cấu hình càng cao càng tốt.

Yêu cầu về phần mềm : Phải có đủ phần mềm dựng đủ các thiết bị như Router, Switch, Firewall, máy tính ảo, IPS, VMWare. Chúng ta có thể dựng Router và Switch bằng phần mềm mô phỏng Dynamic/dyogen.chúng làm việc khá tốt song yêu cầu ram cao. Firewall có thể dùng phần mềm mô phỏng Pemu hoặc chính trong Dynamic cũng hỗ trợ nhưng phải với phiên bản mới, về phần IPS có thể chạy trên Linux chúng ta có thể dùng phần mền metu.vn\_ciscoIPS.wm chạy bằng máy ảo dùng VMWare máy ảo có thể tạo bằng VMWare

* 1. **Các bước tiến hành kết nối:**

1. Bước trước tiên là đó là phải cài đặt dynagen-0.10.1\_dynamips và WinPcap để tạo có thể tạo ra được router ảo và switch ảo cũng như tạo ra tạo ra Firewall. Phiên bản mới nhất đó là GNS3 có hỗ trợ cài đặt sẵn dynamíp, pemu và winpcap.
2. Cài đặt VMWare tạo ra 2 máy PC ảo để có thể test Firewall.
3. Cài đặt ASDM 6.2 để có thể cấu hình cho firewall dạng giao diện web.
   1. **Cấu hình cho từng thiết bị:**

**Sơ đồ hệ thống cần mô phỏng:**

Cấu hình ASA

# 1. Đặt hostname và mật khẩu cho tường lửa

- Hostname: ASA

- Pass: ciscopa55

- Domain name: ccnasecurity.com

Graphical user interface, application

Description automatically generated

# 2. Cấu hình địa chỉ IP và gán tên cho các interface của ASA, đặt security-level cho các interface, cho phép interface outside nhận địa chỉ động từ internet .

Graphical user interface

Description automatically generated

Graphical user interface, chart, application

Description automatically generated

# 3. Cấu hình cho phép telnet đến ASA từ vùng inside.

Text

Description automatically generated with medium confidence