MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

THÔNG TIN KẾT QUẢ NGHIÊN CỨU

1. Thông tin chung

Tên đề tài: Nghiên cứu triển khai hệ thống firewall ASA

Sinh viên thực hiện: Trần Văn Hiếu
Lớp: Mạng máy tính K57
Hệ đào tạo: Chính quy
Điện thoại: 0979156622
Email: mr.tranhieu2905@gmail.com

Thời gian thực hiện: 2017

2. Mục tiêu

Để bảo vệ hệ thống chống lại các nguy cơ từ mạng Internet bên ngoài, các giải pháp bảo mật luôn được chú trọng và có đóng góp to lớn đối với bảo mật mạng. Trong số các giải pháp đó, hệ thống sử dụng firewall là một phương pháp bảo mật có khả năng chống lại các kiểu tấn công mới, xử lý các vấn đề lỗ hổng từ bên trong và hỗ trợ tốt cho các phương pháp bảo mật truyền thống.

Đồ án hướng tới việc nghiên cứu và triển khai hệ thống firewall ASA. Đồ án tổng hợp được lý thuyết về bảo mật nói chung và hệ thống firewall ASA nói riêng. Đồ án cũng đưa ra phương pháp thiết kế xây dựng phương án bảo mật hệ thống bằng firewall và phương thức cài đặt cấu hình cho hệ thống mô phỏng sử dụng firewall ASA.

3. Nội dung chính

Đồ án gồm 3 chương:

Chương 1: Tổng quan về tường lửa

Chương 2: Hệ thống firewall ASA

Chương 3: Thiết kế xây dựng mô phỏng hệ thống firewall ASA

4. Kết quả chính đạt được

- Báo cáo đồ án tốt nghiệp gồm: Đồ án tốt nghiệp và video quay lại các bước triển khai cấu hình
- Lý thuyết về các vấn đề an ninh mạng, các phương thức tấn công, bức tường lửa; giới thiệu về firewall ASA, cơ chế hoạt động và chức năng của firewall ASA

- Thiết kế và xây dựng phương án bảo mật hệ thống bằng firewall ASA
- Minh họa phương thức giả lập firewall ASA và các bước triển khai cấu hình ASA.

MỞ ĐẦU

1. Tổng quan tình hình nghiên cứu thuộc lĩnh vực của đề tài

An ninh thông tin nói chung và an ninh mạng nói riêng đang là vấn đề được quan tâm không chỉ ở Việt Nam mà trên toàn thế giới. Cùng với sự phát triển nhanh chóng của mạng Internet, việc đảm bảo an ninh cho các hệ thống thông tin càng trở nên cấp thiết hơn bao giờ hết.

Trong lĩnh vực an ninh mạng, firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép, nhằm bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống. Firewall được coi như là một hệ thống phòng thủ mà tại đó nó kiểm soát tất cả các luồng lưu thong nhập xuất.

Xây dựng hệ thống an ninh mạng sử dụng firewall là một giải pháp nhằm nâng cao tính bảo mật của hệ thống.

Hiện tại firewall ASA vẫn đang được nghiên cứu, phát triển và sử dụng rộng rãi.

2. Tính cấp thiết, ý nghĩa khoa học và thực tiễn của đề tài

Với sự bùng nổ ngày càng mạnh mẽ của mạng máy tính và Internet, các quốc gia, các tổ chức, các công ty và tất cả mọi người đều có thể kết nối vào Internet để khai thác và truyền bá thông tin.

Chính vì thông tin có tầm quan trọng lớn như vậy nên việc bảo vệ, làm trong sạch nguồn tài nguyên thông tin trên mạng đã, đang và sẽ luôn là vấn đề rất cần thiết không chỉ đối với những chuyên gia an ninh mạng mà còn với tất cả những người tham gia vào mạng máy tính và Internet. Vì vậy việc sử dụng tường lửa cho các mạng máy tính là một vấn đề cần thiết.

Đề tài nghiên cứu tổng quan tường lửa, các cách thức tấn công hệ thống, các chính sách an ninh mạng; giới thiệu về firewall ASA, các chức năng cơ bản và cách cấu hình firewall ASA cho một hệ thống.

Ứng dụng firewall ASA nhằm kiểm soát luồng thông tin đi qua nó, cho phép người dùng hợp lệ đi qua và chặn các người dùng không hợp lệ, bảo vệ mạng nội bộ, chống virus. Ứng dụng hỗ trợ tốt cho các phương pháp bảo mật truyền thống khác.

Đề tài triển khai firewall ASA phù hợp với thực tiễn, nên được ứng dụng rộng rãi và rất phù hợp với các doanh nghiệp vừa và nhỏ.

LỜI CẢM ƠN

Em xin bày tỏ sự cảm ơn sâu sắc của mình tới tất cả mọi người: gia đình, thầy cô, bạn bè. Trong quá trình học tập và đặc biệt thời gian thực hiện đồ án tốt nghiệp, em đã nhận được sự động viên và giúp đỡ to lớn để hoàn thành đồ án này.

Em xin chân thành cảm ơn ThS. Đào Anh Thư, người đã định hướng cho em trong việc lựa chọn đề tài, đưa ra những nhận xét quý giá và trực tiếp hướng dẫn, hỗ trợ em trong quá trình nghiên cứu và hoàn thành luận văn tốt nghiệp.

Em xin cảm ơn các thầy cô bộ môn Mạng Máy Tính, Khoa Công nghệ thông tin, Trường Đại học Mỏ- Địa chất đã tận tình giảng dạy em trong suốt thời gian học tập tại trường.

Cuối cùng, em xin gửi lời cảm ơn đặc biệt tới gia đình của mình, nơi đã động viên em rất lớn, cổ vũ nhiệt tình và là động lực để em nỗ lực học tập, nghiên cứu và hoàn thiện bản thân.

Hà Nội, ngày 1 tháng 6 năm 2017

Trần Văn Hiếu

CHƯƠNG 1
TỔNG QUAN VỀ TƯỜNG LỬA

1.1. Các vấn đề an ninh mạng

Các cuộc tấn công mạng hiện nay đều có chủ đích và gây ra những thiệt hại vô cùng to lớn. Chính vì vậy, an ninh mạng đang là vấn đề nóng bỏng và cấp thiết.

Năm 2016, mức thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam lên tới 10.400 tỷ, vượt qua mức 8.700 tỷ đồng năm 2015. Đây là kết quả từ chương trình đánh giá an ninh mạng được Tập đoàn công nghệ Bkav thực hiện vào tháng 12/2016. Mã độc mã hóa dữ liệu Ransomware, virus lây qua USB, vấn nạn tin nhắn rác và nguy cơ từ các cuộc tấn công có chủ đích APT là những chủ điểm nóng nhất của năm 2016.

- **Bùng nổ mã độc mã hóa dữ liệu Ransomware**

Đúng như dự báo trong tổng kết cuối năm 2015 của các chuyên gia Bkav, năm 2016 đã ghi nhận sự bùng nổ của mã độc mã hóa dữ liệu tống tiền ransomware. Thống kê từ hệ thống giám sát virus của Bkav cho thấy, có tới 16% lượng email lưu chuyển trong năm 2016 là email phát tán ransomware, nhiều gấp 20 lần năm 2015. Như vậy cứ trung bình 10 email nhận được trong năm 2016 thì người sử dụng sẽ gặp 1,6 email chứa ransomware, một con số rất đáng báo động.

Ransomware chuyên mã hóa các file dữ liệu trên máy, khiến người sử dụng không thể mở file nếu không trả tiền chuộc cho hacker. Số tiền chuộc khổng lồ hacker kiếm được chính là nguyên nhân dẫn tới sự bùng nổ của loại mã độc nguy hiểm này. Để phòng tránh, tốt nhất người dùng nên trang bị cho mình phần mềm diệt virus để được bảo vệ tự động, luôn mở file tải về từ email trong môi trường cách ly an toàn Safe Run.

- **Virus USB chưa hết thời**

Việc cắt bỏ tính năng Auto Run trong các hệ điều hành của Microsoft không làm cho virus USB trở nên hết thời. Theo chương trình đánh giá an ninh mạng 2016 của Bkav, tỷ lệ USB bị nhiễm virus trong năm 2016 vẫn ở mức rất cao 83%, không giảm so với 2015.

Lý giải điều này, các chuyên gia của Bkav phân tích, nỗ lực của Microsoft chỉ hạn chế được các dòng virus lây trực tiếp qua Auto Run như W32.AutoRunUSB. Tuy nhiên, sự tăng trưởng mạnh của dòng W32.UsbFakeDrive, dòng virus không cần AutoRun vẫn có thể lây nhiễm chỉ với một cú "click" khiến cho USB tiếp tục là nguồn

lây nhiễm virus phổ biến nhất. Theo thống kê từ hệ thống giám sát virus của Bkav, có tới 16,7 triệu lượt máy tính được phát hiện là nhiễm virus lây qua USB trong năm 2016. Trong đó chỉ 11% là đến từ dòng virus lây trực tiếp bằng Auto Run, còn tới 89% là dòng W32.UsbFakeDrive.

Đã đến lúc phải kiểm soát chặt chẽ việc sử dụng USB để hạn chế sự lây lan của virus. Người dùng cá nhân cần trang bị phần mềm diệt virus thường trực để quét USB trước khi sử dụng, hạn chế sử dụng USB trên các máy lạ. Với các cơ quan doanh nghiệp, cần trang bị giải pháp kiểm soát chính sách an ninh đồng bộ, trong đó có kiểm soát, phân quyền sử dụng USB theo nhu cầu và độ quan trọng của từng máy.

- **Tấn công có chủ đích APT - quả bom hẹn giờ**

Tấn công có chủ đích, hay tấn công APT gần đây được nhắc tới liên tục, đặc biệt trong an toàn thông tin năm 2016.

Thuật ngữ APT (Advanced Persistent Threat) được dùng để chỉ kiểu tấn công dai dẳng và có chủ đích vào một thực thể. Kẻ tấn công có thể được hỗ trợ bởi chính phủ của một nước nào đó nhằm tìm kiếm thông tin tình báo từ một chính phủ nước khác. Tuy nhiên không loại trừ mục tiêu tấn công có thể chỉ là một tổ chức tư nhân.

Điều đặc biệt nguy hiểm của tấn công APT là hacker có thể tạo ra malware riêng cho từng mục tiêu cụ thể, ủ bệnh rất lâu, thậm chí theo chia sẻ của các chuyên gia bảo mật thì có những loại malware có hành vi thể hiện rất ít nên cực kỳ khó phát hiện, kể cả khi chạy kiểm thử trong môi trường giả lập Sandbox. Với những loại malware này, giải pháp truyền thống dựa trên phân tích chữ ký (signature) trở nên bất lực trong việc phát hiện và ngăn chặn.

Chiêu thức đánh lừa kiểu phi kỹ thuật (social engineering) thông qua những email hay website có chứa mã độc vẫn được hacker dùng nhiều và rất hiệu quả. Xu hướng BYOD (mang máy tính cá nhân đi làm) và người dùng truy cập làm việc từ xa cũng tạo điệu kiện hơn cho hacker xâm nhập mạng TC/DN (dữ liệu nội bộ). Việc truy tìm hacker không hề dễ, chưa kể là tội phạm tấn công mạng và nạn nhân thường không cùng một quốc gia nên càng gây khó cho các cơ quan thực thi pháp luật.

Hacker có quá nhiều lợi thế so với bên bị tấn công. Chúng dễ dàng kết nối với các hacker lão luyện trên mạng, có nhiều điểm yếu trên hệ thống phòng thủ để khai thác tấn công và có mục tiêu rõ ràng. Trong khi đó đối tượng bị tấn công có quá nhiều công việc thường ngày, không dễ gì tập trung toàn bộ sức lực cho hệ thống phòng thủ vốn luôn có nhiều sơ hở, họ cũng không có điều kiện giao tiếp thường xuyên với các chuyên gia và chỉ một sai lầm là phải trả giá.

"Không tổ chức nào có thể an toàn" khi tội phạm mạng đang gia tăng xu hướng tấn công có mục đích, có tổ chức và có trình độ cao.

- **Xu hướng tấn công 2017**

Với thực trạng nhiều cơ quan, doanh nghiệp đã bị nhiễm mã độc gián điệp nằm vùng, năm 2017 sẽ còn tiếp tục chứng kiến nhiều cuộc tấn công có chủ đích APT với quy mô từ nhỏ tới lớn. Mã độc mã hóa tống tiền tiếp tục bùng nổ, xuất hiện nhiều hình thức phát tán tinh vi và biến thể mới. Mã độc trên di động tiếp tục tăng với nhiều dòng mã độc khai thác lỗ hổng nhằm chiếm quyền root, kiểm soát toàn bộ điện thoại.

Bên cạnh đó, nhiều lỗ hổng nguy hiểm trên nền tảng Linux được phát hiện sẽ đặt các thiết bị chạy trên nền tảng này trước nguy cơ bị tấn công. Sự bùng nổ thiết bị kết nối Internet như Router Wifi, Camera IP… khiến an ninh trên các thiết bị này thành vấn đề nóng. Thiết bịn kết nối Internet có thể sẽ là đích nhắm của hacker trong năm tới.

1.2. Các phương thức tấn công

1.2.1. Mã độc

- **Virus**

Về cơ bản, đó là một chương trình mà có thể lây lan (lặp lại) từ một máy tính khác. Một virus thường phải được đưa thẳng vào một tập tin thực thi để chạy. Khi tập tin thực thi bị nhiễm được khởi chạy, nó có thể sẽ lây lan sang các file thực thi khác với nhiều tốc độ khác nhau nhưng thường là rất nhanh. Hiểu chính xác để cho một virus lây lan, nó thường đòi hỏi một số can thiệp của người dùng. Ví dụ nếu bạn đã tải về một tập tin đính kèm từ email của bạn và hậu quả sau khi mở tập tin nó đã lây nhiễm đến hệ thống của bạn, đó chính là virus vì nó đòi hỏi người sử dụng phải mở tập tin. Virus có nhiều cách rất khéo léo để chèn mình vào các file thực thi. Có một loại virus được gọi là cavity virus, có thể chèn chính nó vào phần sử dụng của một tập tin thực thi, do đó nó lại không làm tổn tại đến tập tin cũng như làm tăng kích thước của file.

- **Computer Worm**

Một computer worm giống như virus ngoài trừ việc nó có thể tự tái tạo. Nó không chỉ có thể nhân rộng mà không cần đến việc phải "đột kích" vào "bộ não" của

file và nó cũng rất ưa thích sử dụng mạng để lây lan đến mọi ngóc ngách của hệ thống. Điều này có nghĩa là một computer worm có đủ khả năng để làm thiệt hại nghiêm trọng cho toàn thể mạng lưới, trong khi một "em" virus chỉ thường nhắm đến các tập tin trên máy bị nhiễm.

Tất cả worm đều có hoặc không có tải trọng. Nếu không có tải trọng, nó sẽ chỉ sao chép chính nó qua mạng và cuối cùng làm chậm mạng xuống vì chúng làm tăng lưu lượng của mạng. Nếu một worm có tải trọng nhân bản, nó sẽ cố gắng thực hiện một số nhiệm vụ khác như xóa tập tin, gởi email, hay cài đặt backdoor. Thông qua backdoor, hệ thống của bạn được xem như là một "vùng trời tự do" vì mọi sự xác thực sẽ được bỏ qua và sự truy cập từ xa vào máy tính không phải là điều không thể.

Worms lây lan chủ yếu là do lỗ hổng bảo mật trong hệ điều hành. Đó là lý do tại sao điều quan trọng nhất đối với bảo mật là người dùng phải luôn cài đặt, update các bản cập nhật bảo mật mới nhất cho hệ điều hành của mình.

- **Trojan horse**

Một Trojan Horse là một chương trình phần mềm độc hại mà không cố gắng để tự tái tạo, thay vào đó nó sẽ được cài đặt vào hệ thống của người dùng bằng cách giả vờ là một chương trình phần mềm hợp pháp. Tên của nó xuất phát từ thần thoại Hy Lạp cũng đã khiến nhiều người dùng tưởng chừng như nó vô hại và đó lại chính là thủ đoạn của nó để khiến người dùng cài đặt nó trên máy tính của mình.

Khi một Trojan Horse được cài đặt trên máy tính của người dùng, nó sẽ không cố gắng để gài chính nó vào một tập tin như virus, nhưng thay vào đó nó sẽ cho phép các hacker hoạt động để điều khiển máy tính của người dùng từ xa. Một trong những ứng dụng phổ biến nhất của một máy tính bị nhiễm Trojan Horse là làm cho nó trở thành một phần của botnet. Một botnet cơ bản là một loạt các máy được kết nối qua Internet và sau đó có thể được sử dụng để gửi thư rác hoặc thực hiện một số nhiệm vụ như các cuộc tấn công Denial of service (từ chối dịch vụ) thường có trên các Website.

Trước đây, vào thời điểm năm 1998, có một loại Trojan Horse rất phổ biến là Netbus. Chính Trojan này lại được các sinh viên đại học nước ngoài rất ưa dùng để cài đặt nó trên máy tính lẫn nhau với mục đích chỉ là "chơi khăm" đối thủ. Nhưng hậu quả không chỉ dừng ở đó vì Netbus đã làm sụp đổ nhiều máy tính, ăn cắp dữ liệu tài chính, điều khiển bàn phím để đăng nhập hệ thống và gây nên những hậu quả khôn lường khiến những người tham gia cuộc chơi cũng phải ân hận.

- **Rootkit**

Rootkit là loại phần mềm độc hại rất khó để phát hiện vì nó vốn tích cực cố gắng để tự ẩn mình trốn thoát người sử dụng, hệ điều hành và các chương trình Antivirus/Anti malware. Chúng có thể được cài đặt trong nhiều cách, trong đó có phương án khai thác một lỗ hổng trong hệ điều hành hoặc bằng cách tiếp cận quản trị viên máy tính hoặc cài đặt vào hạt nhân của hệ điều hành, do đó đa phần khi bị Rootkit tấn công sự lựa chọn duy nhất của bạn đôi khi là phải cài đặt lại toàn bộ hệ điều hành đang sử dụng.

Theo các nhà chuyên môn, để thoát khỏi một rootkit mà không phải cài đặt lại hệ điều hành, bạn nên khởi động vào một hệ điều hành thay thế và sau đó cố gắng để làm sạch các rootkit hoặc ít nhất nếu không muốn dùng lại hệ điều hành đó bạn cũng có thể tạo ra bản sao các dữ liệu quan trọng để sử dụng trở lại. Cần chú ý rằng, rootkit cũng có thể đi kèm với trọng tải, theo đó chúng ẩn các chương trình khác như virus và key logger, do đó sự tàn phá của nó đến hệ thống của bạn có thể xem là tối nghiêm trọng nếu không may bạn là nạn nhân!

- **Spyware**

Spyware là một lớp các ứng dụng phần mềm có thể tham gia vào một cuộc tấn công mạng. Spyware là một ứng dụng cài đặt và vẫn còn để ẩn trên máy tính tay mục tiêu. Một khi các ứng dụng phần mềm gián điệp đã được bí mật cài đặt, phần mềm gián điệp bắt thông tin về những gì người dùng đang làm với máy tính của họ. Một số thông tin bị bắt bao gồm các trang web truy cập, e-mail gửi đi, và mật khẩu sử dụng. Những kẻ tấn công có thể sử dụng các mật khẩu và thông tin bắt được để đi vào được mạng để khởi động một cuộc tấn công mạng.

Ngoài việc được sử dụng để trực tiếp tham gia vào một cuộc tấn công mạng, phần mềm gián điệp cũng có thể được sử dụng để thu thập thông tin có thể được bán một cách bí mật. Thông tin này, một lần mua, có thể được sử dụng bởi một kẻ tấn công khác đó là "khai thác dữ liệu" để sử dụng trong việc lập kế hoạch cho một cuộc tấn công mạng khác.

1.2.2. Tấn công từ chối dịch vụ

- **Denial of Service**

Một cuộc tấn công từ chối dịch vụ (DoS) là một cuộc tấn công mạng có kết quả trong việc từ chối dịch vụ bằng một ứng dụng yêu cầu như là một máy chủ web. Có một vài cơ chế để tạo ra một cuộc tấn công DoS.

Các phương pháp đơn giản nhất là tạo ra một lượng lớn những gì xuất hiện để được lưu lượng mạng hợp lệ. Đây là loại tấn công DoS mạng cố gắng để làm nghẽn các ống dẫn lưu lượng truy cập mạng để sử dụng hợp lệ không thể có được thông qua kết nối mạng. Tuy nhiên, loại DoS thông thường cần phải được phân phối bởi vì nó thường đòi hỏi nhiều nguồn để tạo ra các cuộc tấn công.

Một cuộc tấn công DoS lợi dụng thực tế là hệ thống mục tiêu như các máy chủ phải duy trì thông tin trạng thái và có thể có kích thước bộ đệm và dự kiến nội dung gói tin mạng cho các ứng dụng cụ thể. Một cuộc tấn công DoS có thể khai thác lỗ hổng này bằng cách gửi các gói có giá trị kích cỡ và dữ liệu mà không như mong đợi của các ứng dụng nhận được.

Một số loại tấn công DoS tồn tại, bao gồm các cuộc tấn công Teardrop và Ping of Death, mà gửi các gói thủ công mạng khác nhau từ những ứng dụng dự kiến và có thể gây ra sụp đổ các ứng dụng và máy chủ. Những cuộc tấn công DoS trên một máy chủ không được bảo vệ, chẳng hạn như một máy chủ thương mại điện tử, có thể gây ra các máy chủ bị lỗi và ngăn chặn người dùng bổ sung thêm hàng vào giỏ mua sắm của họ.

- **Distributed Denial-of-Service**

DDoS tương tự như trong ý định của cuộc tấn công DoS, ngoại trừ cuộc tấn công DDoS tạo ra nhiều nguồn tấn công. Ngoài ra để tăng lượng truy cập mạng từ nhiều kẻ tấn công phân tán, một cuộc tấn công DDoS cũng đưa ra những thách thức của yêu cầu bảo vệ mạng để xác định và ngăn chặn mỗi kẻ tấn công phân tán.

1.2.3. Tấn công lỗ hổng bảo mật web

Thứ nhất là các tấn công như SQL injection được sử dụng ngày càng nhiều. Đặc biệt, các website sử dụng chung server hoặc chung hệ thống máy chủ của nhà cung cấp dịch vụ ISP dễ bị trở thành cầu nối tấn công sang các đích khác.

Thứ hai là tấn công vào mạng nội bộ LAN thông qua VPN. Thứ ba là hình thức tấn công vào cơ sở dữ liệu của trang web với mục đích lấy cắp dữ liệu, phá hoại, thay đổi nội dung. Hacker xâm nhập vào cơ sở dữ liệu của trang web, từng bước thay đổi quyền điều khiển website và tiến tới chiếm toàn quyền điều khiển trang web và cơ sở dữ liệu. Trong nhiều vụ, hacker lấy được quyền truy cập cao nhất của web server, mail server, backup và đã kiểm soát hoàn toàn hệ thống mạng một cách bí mật, để cùng lúc tấn công, phá hoại cơ sở dữ liệu của cả website và hệ thống backup.

1.2.4. Sử dụng Proxy tấn công mạng

Proxy server là một Internet server làm nhiệm vụ chuyển tiếp, kiểm soát thông tin và bảo đảm an toàn cho việc truy cập Internet của máy khách hàng sử dụng dịch vụ Internet. Proxy có địa chỉ IP và một cổng truy cập cố định, làm server trung gian giữa máy trạm yêu cầu dịch vụ và máy chủ cung cấp tài nguyên.

Khi có một yêu cầu từ máy trạm, trước tiên yêu cầu này được chuyển tới proxy server để kiểm tra. Nếu dịch vụ này đã được ghi nhớ (cache) sẵn trong bộ nhớ, proxy sẽ trả kết quả trực tiếp cho máy trạm mà không cần truy cập tới máy chủ chứa tài nguyên. Nếu không có cache, proxy sẽ kiểm tra tính hợp lệ của các yêu cầu. Nếu yêu cầu hợp lệ, proxy thay mặt máy trạm chuyển tiếp tới máy chủ chứa tài nguyên. Kết quả sẽ được máy chủ cung cấp tài nguyên trả về qua proxy và proxy sẽ trả kết quả về cho máy trạm.

Hacker luôn ẩn danh khi thực hiện các cuộc tấn công website, upload hoặc download dữ liệu, bằng cách sử dụng Proxy server - loại công cụ mạnh nhất để giả mạo hoặc che giấu thông tin cá nhân và IP truy cập, tránh bị cơ quan chức năng phát hiện. Nhu cầu sử dụng Proxy ẩn danh chủ yếu xuất phát từ những hoạt động trái pháp luật của hacker. Bên cạnh đó, người dùng cũng có nhu cầu sử dụng Proxy để bảo vệ thông tin cá nhân hợp pháp.

Theo log file hệ thống để lại, với cùng một User Agent nhưng cứ khoảng 10 phút, IP tấn công lại thay đổi sang địa chỉ tên miền của các quốc gia khác nhau, làm cho không thể xác định được địa chỉ đối tượng tấn công. Hacker cũng thường sử dụng các công cụ Proxy trong các vụ gian lận thẻ tín dụng, như SOCKS, Tor, Hide My Ass!, I2P..., tạo địa chỉ IP hợp lệ, nhằm vượt qua các công cụ kỹ thuật nhận biết IP của các website thương mại điện tử. Trên các diễn đàn UG (Under Ground Forum), các chủ đề trao đổi, mua bán live SOCKS (những SOCKS Proxy Server đang hoạt động và sử dụng được) là một trong những chủ đề phổ biến, có lượng truy cập và trao đổi sôi động nhất.

Việc sử dụng firewall để chặn các truy cập vào các website phản động, cờ bạc, cá độ, website vi phạm thuần phong mỹ tục... có rất ít tác dụng đối với truy cập sử dụng Proxy. Như vậy, việc sử dụng Proxy như Tor, I2P, SOCKS... làm cho tình hình vi phạm, tội phạm trong lĩnh vực CNTT trở nên phức tạp hơn và cũng là thách thức lớn đối với lực lượng thực thi pháp luật trong lĩnh vực an ninh mạng.

Với chức năng ẩn danh, Proxy cũng được sử dụng để truy cập vào các tài nguyên bị firewall cấm: Khi muốn vào một trang web bị chặn, để che giấu địa chỉ IP thật của

trang web đó, có thể truy cập vào một proxy server, thay máy chủ của trang web giao tiếp với máy tính của người sử dụng. Khi đó, firewall chỉ biết Proxy Server và không biết địa chỉ trang web thực đang truy cập. Proxy Server không nằm trong danh sách cấm truy cập (Access Control List – ACL) của firewall nên firewall không thể chặn truy cập này.

Phần lớn HTTP Proxy chỉ có tác dụng cho dịch vụ HTTP (web browsing), còn SOCKS Proxy có thể được sử dụng cho nhiều dịch vụ khác nhau (HTTP, FTP, SMTP, POP3...). Một loại phần mềm như vậy là Tor hiện đang được sử dụng miễn phí, rất phổ biến để vượt tường lửa, truy cập Internet ẩn danh. Ban đầu, Tor được Phòng thí nghiệm và nghiên cứu Hải quân Hoa Kỳ thiết kế, triển khai và thực hiện dự án định tuyến "mạng củ hành" thế hệ thứ 3, với mục đích bảo vệ các kết nối của Chính phủ Mỹ. Chức năng của Tor gồm:

- Xóa dấu vết, giấu địa chỉ IP của máy truy cập khi gửi và nhận thông tin qua Internet, để vượt qua tường lửa: Thông tin được Tor mã hóa và truyền qua nhiều máy chủ trung gian và tự động thay đổi proxy để bảo mật dữ liệu. Nếu một máy trung gian Tor bị truy cập, cũng không thể đọc được thông tin vì đã được mã hóa.

- Chống bị Traffic analysis giám sát truy tìm địa chỉ nguồn và đích của lưu lượng dữ liệu Internet. Dữ liệu Internet gồm 2 phần: phần data payload (phần dữ liệu bị mã hóa) và phần header không được mã hóa (chứa thông tin địa chỉ nguồn, địa chỉ đích, kích thước gói tin, thời gian...), được sử dụng để định tuyến mạng. Do vậy, traffic analysis vẫn có thể tìm được thông tin ở phần header.

- Phần mềm Tor trên máy người dùng thu thập các nút Tor thông qua một directory server, chọn ngẫu nhiên các nút khác nhau, không để lại dấu vết và không nút Tor nào nhận biết được đích hay nguồn giao tiếp. Hiện đã có hàng triệu nút Tor luôn sẵn sàng cho người dùng sử dụng. Việc tìm ra nguồn gốc gói tin là gần như không thể thực hiện. Tor làm việc với trình duyệt Firefox và các trình duyệt khác như Internet Explorer. Trình duyệt Opera và Firefox đã được tích hợp sẵn với Tor thành trình duyệt Opera Tor và Tor Firefox. Do mạng Tor hoạt động qua nhiều máy chủ trung gian và liên tục thay đổi các máy chủ nên tốc độ truy cập internet bị chậm hơn. Ngoài ra còn có những Proxy Tools mạnh khác như: Hide the Ip, GhostSurf Proxy Platinum, Anonymizer Anonymous Surfing, Proxy Finder Pro, Hide My Ass.

1.2.5. Tấn công dựa vào yếu tố con người

Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ

thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác. Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi. Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.

1.3. Chính sách an ninh mạng

1.3.1. Chính sách an toàn thông tin

- **Chính sách quản lý truy cập**

Chính sách quản lý truy cập tồn tại để xác định các phương pháp cho phép và cách truy cập quản lý tường lửa. Chính sách này có xu hướng giải quyết sự toàn vẹn vật lý tường lửa và lớp bảo mật cấu hình tường lửa tĩnh. Các chính sách quản lý truy cập cần phải định nghĩa cho cả hai giao thức quản lý từ xa và cục bộ sẽ được cho phép, cũng từ đó người dùng có thể kết nối với tường lửa và có quyền truy cập để thực hiện tác vụ.

Ngoài ra, các chính sách quản lý truy cập cần xác định các yêu cầu đối với các giao thức quản lý như Network Time Protocol (NTP), syslog, TFTP, FTP, Simple Network Management Protocol (SNMP), và bất kỳ giao thức khác có thể được sử dụng để quản lý và duy trì thiết bị.

- **Chính sách lọc**

Các chính sách lọc cần phải chỉ và xác định chính xác các loại lọc mà phải được sử dụng và nơi lọc được áp dụng. Chính sách này có xu hướng để giải quyết cấu hình tường lửa tĩnh và chi tiết trong lớp lưu lượng mạng qua tường lửa. Ví dụ, một chính sách lọc tốt cần phải yêu cầu cả hai lối vào và đi ra bộ lọc được thực hiện với các bức tường lửa. Các chính sách lọc cũng cần xác định các yêu cầu chung trong việc kết nối mạng cấp độ bảo mật và nguồn khác nhau. Ví dụ, với một DMZ, tùy thuộc vào hướng của lưu lượng, các yêu cầu lọc khác nhau có thể cần thiết và nó là vai trò của các chính sách lọc để xác định những yêu cầu.

- **Chính sách định tuyến**

Các chính sách định tuyến thường không phải là một tài liệu tường lửa trung tâm. Tuy nhiên, với thiết kế phức tạp hơn cũng như việc sử dụng ngày càng tăng của các bức tường lửa trong mạng nội bộ, tường lửa có thể dễ dàng trở thành một phần của

cơ sở hạ tầng định tuyến. Các chính sách định tuyến cần phải có một phần có quy định cụ thể bao gồm một tường lửa trong các cơ sở hạ tầng định tuyến và định nghĩa các phương thức sẽ xảy ra định tuyến. Chính sách này có xu hướng để giải quyết các lớp cấu hình tường lửa tĩnh và cấu hình tường lửa động. Trong hầu hết trường hợp, các chính sách định tuyến nên ngăn cấm firewall một cách rõ ràng từ việc chia sẻ bảng định tuyến mạng nội bộ với bất kỳ nguồn bên ngoài. Tương tự như vậy, các chính sách định tuyến cần xác định các trường hợp trong đó các giao thức định tuyến động và định tuyến tĩnh là phù hợp. Các chính sách cũng nên xác định bất kỳ cơ chế bảo mật giao thức cụ thể cần phải được cấu hình, (ví dụ, việc sử dụng thuật toán băm để đảm bảo chỉ các nút được chứng thực có thể vượt qua dữ liệu định tuyến).

- **Chính sách Remote access/VPN**

Trong lĩnh vực hội tụ hiện nay, sự khác biệt giữa tường lửa và bộ tập trung VPN đã ngày càng trở nên mờ nhạt. Hầu hết các thị trường tường lửa lớn có thể phục vụ như là điểm kết thúc cho VPN, và do đó chính sách remote-access/VPN cần thiết xác định các yêu cầu về mức độ mã hóa và xác thực mà một kết nối VPN sẽ yêu cầu. Trong nhiều trường hợp, các chính sách VPN kết hợp với chính sách mã hóa của tổ chức xác định phương pháp VPN tổng thể sẽ được sử dụng. Chính sách này có xu hướng để giải quyết các lớp cấu hình tường lửa tĩnh và lưu lượng mạng qua tường lửa.

Các chính sách remote-access/VPN cũng cần xác định các giao thức sẽ được sử dụng: IP Security (IPsec), Layer 2 Tunneling Protocol (L2TP), hoặc Point-to-Point Tunneling Protocol (PPTP). Trong hầu hết các trường hợp, IPsec được sử dụng riêng biệt. Giả sử IPsec, chính sách remote-access/VPN cần phải yêu cầu sử dụng của các preshared keys, chứng thực mở rộng, với việc sử dụng giấy chứng nhận, mật khẩu một lần, và Public Key Infrastructure (PKI) cho môi trường an toàn nhất. Tương tự như vậy, các chính sách remote-access/VPN nên xác định những khách hàng sẽ được sử dụng (có nghĩa là, trong xây dựng- Microsoft VPN Client, Cisco Secure VPN Client, vv).

Cuối cùng, các chính sách remote-access/VPN cần xác định các loại truy cập và các nguồn lực sẽ được cung cấp để kết nối từ xa và các loại kết nối từ xa sẽ được cho phép.

- **Chính sách giám sát / ghi nhận**

Một trong những yếu tố quan trọng nhất đảm bảo rằng một tường lửa cung cấp mức bảo mật được mong đợi là thực hiện một hệ thống giám sát tường lửa. Chính

sách giám sát / ghi nhận xác định các phương pháp và mức độ giám sát sẽ được thực hiện. Tối thiểu, các chính sách giám sát / ghi nhận cần cung cấp một cơ chế để theo dõi hiệu suất của tường lửa cũng như sự xuất hiện của tất cả các sự kiện liên quan đến an ninh và các mục đăng nhập. Chính sách này có xu hướng giải quyết các lớp cấu hình tường lửa tĩnh.

Chính sách giám sát / ghi nhận cũng nên xác định cách các thông tin phải được thu thập, duy trì, và báo cáo. Trong nhiều trường hợp, thông tin này có thể được sử dụng để xác định các yêu cầu quản lý của bên thứ ba và các ứng dụng theo dõi như CiscoWorks, NetIQ Security Manager, hoặc Kiwi Syslog Daemon.

- **Chính sách vùng DMZ**

Các chính sách DMZ là một văn bản diện rộng để xác định tất cả các yếu tố của không chỉ chính DMZ mà còn các thiết bị trong DMZ. Mục tiêu của chính sách DMZ là xác định các tiêu chuẩn và yêu cầu của tất cả các thiết bị được kết nối và lưu lượng của nó vì nó liên quan đến DMZ. Chính sách này có xu hướng để giải quyết các lớp cấu hình tường lửa tĩnh và lưu lượng mạng qua tường lửa.

Do sự phức tạp của môi trường DMZ điển hình, các chính sách DMZ là có khả năng sẽ là một tài liệu lớn nhiều trang. Để giúp đảm bảo rằng các chính sách DMZ thiết thực và hiệu quả, ba tiêu chuẩn cần được xác định rộng rãi cho tất cả các thiết bị liên quan đến DMZ:

- Trách nhiệm quyền sở hữu
- Yêu cầu cấu hình an toàn
- Yêu cầu hoạt động và kiểm soát thay đổi

1.3.2. Chính sách áp dụng phổ biến

Ngoài các chính sách tường lửa cụ thể, có nhiều chính sách có thể áp dụng thông thường mặc dù không phải là tường lửa cụ thể (đã ứng dụng trên nhiều thiết bị, không chỉ là tường lửa) dù sao cũng nên được áp dụng đối với tường lửa. Chúng bao gồm những chính sách sau:

- Chính sách mật khẩu: chính sách mật khẩu nên được để cập đến để xác định truy cập quản trị tường lửa.
- Chính sách mã hóa: chính sách mã hóa nên được đề cập đến để xác định tất cả các hình thức truy cập mã hóa, bao gồm Hypertext Transfer Protocol, Secure (HTTPS), Secure Sockets Layer (SSL), Secure Shell (SSH), và truy cập IPsec / VPN.

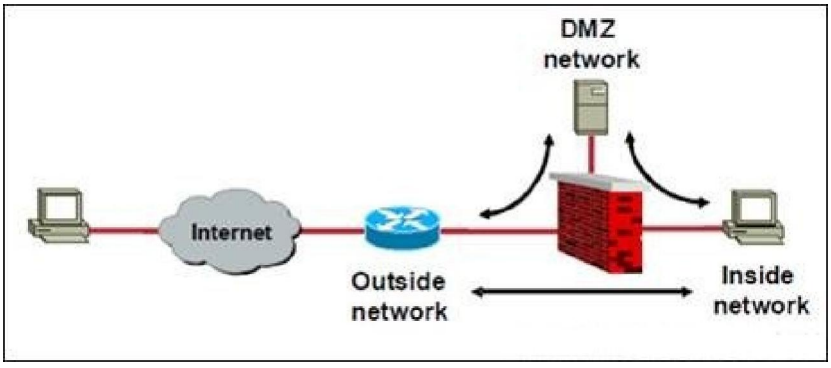
- Chính sách kiểm định: chính sách kiểm định phải được đề cập để xác định các yêu cầu kiểm định của tường lửa.
- Chính sách đánh giá rủi ro: chính sách đánh giá rủi ro cần được đề cập để xác định phương pháp sẽ được sử dụng để xác định các rủi ro liên quan với tất cả hệ thống, di chuyển và thay đổi vì nó liên quan đến tường lửa và bố cục mạng.

1.4. Bức tường lửa

1.4.1. Khái niệm

Thuật ngữ firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hỏa hoạn.

Trong công nghệ thông tin, firewall là một kỹ thuật được tích hợp vào hệ thống mạng để chống sự truy cập trái phép nhằm bảo vệ các nguồn thông tin nội bộ cũng như hạn chế sự xâm nhập vào hệ thống nhằm mục đích phá hoại, gây tổn thất cho tổ chức, doanh nghiệp. Cũng có thể hiểu firewall là một cơ chế để bảo vệ mạng tin tưởng (trusted network) khỏi các mạng không tin tưởng (untrusted network).



Hình 1-1: Mô hình firewall cơ bản

1.4.2. Chức năng tường lửa

Về cơ bản firewall có khả năng thực hiện các nhiệm vụ sau đây:

- Quản lý và điều khiển luồng dữ liệu trên mạng.
- Xác thực quyền truy cập
- Hoạt động như một thiết bị trung gian
- Bảo vệ tài nguyên
- Ghi nhận và báo cáo các sự kiện

1.4.2.1 Quản lý và điều khiển luồng dữ liệu trên mạng

Việc đầu tiên và cơ bản nhất mà tất cả các firewall đều có là quản lý và kiểm soát luồng dữ liệu trên mạng, firewall kiểm tra các gói tin và giám sát các kết nối đang thực hiện và sau đó lọc các kết nối dựa trên kết quả kiểm tra gói tin và các kết nối được giám sát.

- **Packet inspection (kiểm tra gói tin)**

Là quá trình chặn và xử lý dữ liệu trong một gói tin để xác định xem nó được phép hay không được phép đi qua firewall. Kiểm tra gói tin có thể dựa vào các thông tin sau:

- Địa chỉ IP nguồn
- Port nguồn.
- Địa chỉ IP đích
- Port đích
- Giao thức IP
- Thông tin trong header (sequence number, checksum, data flag, payload information…)

- **Connections và state (kết nối và trạng thái)**

Khi hai TCP/IP host muốn giao tiếp với nhau, chúng cần thiết lập một số kết nối với nhau. Các kết nối phục vụ hai mục đích. Thứ nhất, nó dùng để xác thực bản thân các host với nhau. Firewall dùng các thông tin kết nối này để xác định kết nối nào được phép và các kết nối nào không được phép. Thứ hai, các kết nối dùng để xác định cách thức mà hai host sẽ liên lạc với nhau (dùng TCP hay dùng UDP…).

- **Stateful Packet Inspection (giám sát gói tin theo trạng thái)**

Statefull packet inspection không những kiểm tra gói tin bao gồm cấu trúc, dữ liệu gói tin … mà kiểm tra cả trạng thái gói tin.

1.4.2.2 Xác thực quyền truy cập

Firewall có thể xác thực quyền truy cập bằng nhiều cơ chế xác thực khác nhau. Thứ nhất, firewall có thể yêu cầu username và password của người dùng khi người dùng truy cập (thường được biết đến như là extended authentication hoặc xauth). Sau khi firewall xác thực xong người dùng, firewall cho phép người dùng thiết lập kết nối và sau đó không hỏi username và password lại cho các lần truy cập sau (thời gian firewall hỏi lại username và password phụ thuộc vào cách cấu hình của người quản

trị). Thứ hai, firewall có thể xác thực người dùng bằng certificates và public key. Thứ ba, firewall có thể dùng pre-shared keys (PSKs) để xác thực người dùng.

1.4.2.3 Hoạt động như một thiết bị trung gian

Khi user thực hiện kết nối trực tiếp ra bên ngoài sẽ đối mặt với vô số nguy cơ về bảo mật như bị virus tấn công, nhiễm mã độc hại… do đó việc có một thiết bị trung gian đứng ra thay mặt user bên trong để thực hiện kết nối ra bên ngoài là cần thiết để đảm bảo an toàn. Firewall được cấu hình để thực hiện chức năng này và firewall được ví như một proxy trung gian.

1.4.2.4 Bảo vệ tài nguyên

Nhiệm vụ quan trọng nhất của một firewall là bảo vệ tài nguyên khỏi các mối đe dọa bảo mật. Việc bảo vệ này được thực hiện bằng cách sử dụng các quy tắc kiểm soát truy cập, kiểm tra trạng thái gói tin, dùng application proxy hoặc kết hợp tất cả để bảo vệ tài nguyên khỏi bị truy cập bất hợp pháp hay bị lạm dụng. Tuy nhiên, firewall không phải là một giải pháp toàn diện để bảo vệ tài nguyên của chúng ta.

1.4.2.5 Ghi nhận và báo cáo các sự kiện

Ta có thể ghi nhận các sự kiện của firewall bằng nhiều cách nhưng hầu hết các firewall sử dụng hai phương pháp chính là syslog và proprietaty logging format. Bằng cách sử dụng một trong hai phương pháp này, chúng ta có thể dễ dàng báo cáo các sự kiện xẩy ra trong hệ thống mạng.

1.4.3. Phân loại

1.4.3.1 Phân loại theo tầng giao thức

- **Packet-filtering router**

Packet-filtering router áp dụng một bộ quy tắc để mỗi gói tin IP vào và ra và sau đó là chuyển tiếp hay loại bỏ gói tin. Router thường được cấu hình để lọc các gói tin theo cả hai hướng (từ trong và ngoài vào mạng nội bộ). Quy tắc lọc dựa trên các thông tin chứa trong một gói tin mạng (packet):

- Địa chỉ IP nguồn (Source IP address): Địa chỉ IP của hệ thống là nguồn gốc của các gói tin (sender). Ví dụ: 192.178.1.1
- Địa chỉ IP đích (Destination IP address): Địa chỉ IP của hệ thống mà gói tin IP đang cần được chuyển tới. Ví dụ 192.168.1.2
- Địa chỉ nguồn và đích của tầng giao vận: gói tin là TCP hay UDP, port number, xác định các ứng dụng như SNMP hay TELNET.

- IP protocol field: Xác định giao thức vận chuyển.
- Interface: Đối với một router có nhiều port, các gói tin sẽ đến từ interface nào và đi đến interface nào.

Packet-filtering thường được thiết lập là một danh sách các quy tắc dựa trên phù hợp cho các trường trong IP header hoặc TCP header. Nếu có tương ứng với một trong các quy tắc, quy tắc này sẽ được gọi để xác định xem sẽ chuyển tiếp hay loại bỏ các gói tin. Nếu không phù hợp với bất kỳ một quy tắc nào thì hành động mặc định sẽ được thực hiện. Hai hành động được mặc định đó là:

- Default = discard: gói tin sẽ bị cấm và bị loại bỏ.
- Default = forward: gói tin được cho phép đi qua.

Tuy nhiên, default là discard thường được dùng hơn. Vì như vậy, ban đầu, mọi thứ đều bị chặn và các dịch vụ phải được thêm vào trong từng trường hợp cụ thể. Chính sách này rõ ràng hơn cho người dùng, những người mà ko am hiểu nhiều lắm về firewall. Còn cách thứ hai thì liên quan đến vấn đề bảo mật nhiều hơn, đòi hỏi người quản trị phải thường xuyên kiểm tra để có phản ứng với những kiểu đe dọa mới ..

Ưu điểm của loại này là sự đơn giản của nó và packet-filtering thường là trong suốt cho người sử dụng và rất nhanh.

Hạn chế :

- Tường lửa loại này không thể kiểm tra dữ liệu lớp trên, không thể ngăn chặn các cuộc tấn công có sử dụng các lỗ hổng ứng dụng cụ thể. Ví dụ, một bức tường lửa loại này không thể ngăn chặn các lệnh ứng dụng cụ thể, nếu nó cho phép một ứng dụng nhất định, tất cả các chức năng có sẵn trong ứng dụng đó sẽ được cho phép.
- Do các thông tin có sẵn hạn chế cho tường lửa, hiện tại thì chức năng đăng nhập vào tường lửa bị hạn chế. Packet-filtering lọc các bản log thông thường chứa các thông tin tương tự được sử dụng để đưa ra quyết định kiểm soát truy cập (địa chỉ nguồn, địa chỉ đích, và loại hình lưu lượng).
- Hầu hết các tường lửa loại này không hỗ trợ các chương trình xác thực người dùng cao cấp. Một lần nữa hạn chế này chủ yếu là do thiếu chức năng lớp trên của tường lửa.
- Chúng thường bị tấn công và khai thác bằng cách tận dụng các problem của các đặc điểm kỹ thuật TCP/IP và chồng giao thức, chẳng hạn như giả mạo địa chỉ lớp network. Nhiều tường lửa packet-filtering không thể phát hiện một gói

tin mà trong đó các thông tin của lớp 3 đã bị thay đổi. Các cuộc tấn công giả mạo thường được sử dụng bởi những kẻ xâm nhập để vượt qua kiểm soát an ninh được thực hiện bên trong tường lửa.

- Cuối cùng, do số lượng nhỏ của các biến được sử dụng trong quyết định kiểm soát truy cập, packet-filtering dễ bị vi phạm an ninh gây ra bởi các cấu hình không phù hợp. Nói cách khác, rất dễ cấu hình tường lửa cho phép các loại lưu lượng, nguồn và đích đáng lẽ nên bị từ loại bỏ dựa trên chính sách đặt ra của tổ chức.

Từ đó, có một số cách tấn công có thể được thực hiện trên các tường lửa packet-filtering và một số biện pháp đối phó với chúng:

- IP address spoofing (Giả mạo địa chỉ IP): Kẻ xâm nhập truyền các gói dữ liệu từ bên ngoài với địa chỉ nguồn là địa chỉ IP của một máy nội bộ. Kẻ tấn công hy vọng rằng việc sử dụng một địa chỉ giả mạo sẽ cho phép xâm nhập vào các hệ thống chỉ sử dụng bảo mật địa chỉ nguồn đơn giản, trong đó, các gói tin từ máy nội bộ sẽ được chấp nhận. Biện pháp đối phó là loại bỏ các gói tin với địa chỉ nguồn ở nội bộ nếu như gói tin này đến từ interface bên ngoài.
- Source routing attack: Các trạm nguồn quy định các đường đi mà một gói tin sẽ được đưa vào khi đi trên mạng Internet, với mong muốn rằng điều này sẽ bỏ qua các biện pháp an ninh mà không phân tích các thông tin định tuyến nguồn. Biện pháp đối phó là lựa chọn loại bỏ tất cả các gói dữ liệu sử dụng tùy chọn này.
- Tiny fragment attack: Kẻ xâm nhập loại này sử dụng tùy chọn cho phép phân mảnh của gói tin IP để tạo ra các mảnh cực kỳ nhỏ và ép các TCP header vào một đoạn gói tin riêng biệt. Tấn công loại này được thiết kế để phá vỡ các quy tắc lọc phụ thuộc vào thông tin tiêu đề TCP. Thông thường, một packet-filtering sẽ đưa ra quyết định lọc trên đoạn đầu tiên của một gói. Tất cả các đoạn tiếp theo của gói tin được lọc ra chỉ duy nhất trên cơ sở đó là một phần của gói có đoạn đầu tiên bị loại bỏ. Kẻ tấn công hy vọng rằng các router chỉ lọc xem xét đoạn đầu tiên và các đoạn còn lại được thông qua. Cách chống lại tấn công loại này là nguyên tắc thực thi đoạn đầu tiên của một gói tin phải có một số xác định trước tối thiểu của TCP header. Nếu đoạn đầu tiên bị loại bỏ, packet-filtering có thể ghi nhớ các gói tin và loại bỏ tất cả các đoạn tiếp theo.

➢ **Application-Level Gateway**

Application-Level Gateway, còn được gọi là một proxy server, hoạt động như một trạm chuyển tiếp của các lưu lượng lớp ứng dụng. Người sử dụng sẽ liên lạc với

gateway sử dụng các ứng dụng TCP/IP như TELNET hay FTP và gateway sẽ hỏi user name của máy chủ từ xa sẽ được truy cập. Khi user đáp lại và cung cấp một ID người dùng hợp lệ và xác thực thông tin, gateway sẽ liên lạc đến cổng ứng dụng tương ứng trên máy chủ từ xa và chuyển tiếp các đoạn TCP chứa các dữ liệu giữa hai thiết bị đầu cuối này. Nếu các cổng không thực hiện các proxy code cho một ứng dụng cụ thể, dịch vụ không được hỗ trợ và không thể được chuyển tiếp qua tường lửa. Hơn nữa, gateway có thể được cấu hình để chỉ hỗ trợ tính năng cụ thể của một ứng dụng mà người quản trị xem xét chấp nhận được trong khi từ chối tất cả các tính năng khác.

Application-Level gateway có xu hướng an toàn hơn packet-filtering router. Thay vì cố gắng để đối phó với hàng loạt kết hợp có thể có từ việc cấm và cho phép ở tầng TCP/IP, application-level gateway chỉ cần rà soát lại một vài ứng dụng cho phép. Ngoài ra, nó rất dễ dàng cho ghi lại và theo dõi tất cả các lưu lượng đến ở tầng ứng dụng.

Một nhược điểm chính của loại này là chi phí xử lý bổ sung trên mỗi kết nối. Trong thực tế, có hai kết nối ghép giữa các người dùng đầu cuối, với các cổng ở điểm kết nối và gateway phải kiểm tra lưu lượng trên cả hai chiều.

- **Circuit-Level Gateway**

Dạng thứ 3 của firewall đó là Circuit-level gateway. Nó có thể là một hệ thống độc lập hoặc có thể là một hoạt động chuyên biệt được thực hiện bởi một application-level gateway cho các ứng dụng nhất định. Circuit-level gateway không cho phép một kết nối TCP end-to-end mà thay vào đó, gateway sẽ thiết lập hai kết nối TCP, một là giữa nó và TCP user bên trong và một giữa nó và TCP user bên ngoài. Khi hai kết nối này được thiết lập, gateway sẽ chuyển tiếp các TCP segment từ đầu cuối này đến đầu cuối khác mà không kiểm tra nội dung các segment này. Các chức năng bảo mật bao gồm việc xác định cho phép kết nối.

Một điển hình của Circuit-level gateway là một tình huống mà trong đó người quản trị hệ thống tin tưởng các user nội bộ. Gateway có thể được cấu hình để hỗ trợ application-level hay dịch vụ proxy cho các kết nối bên trong và chức năng circuit-level cho các kết nối bên ngoài. Trong trường hợp này, gateway có thể phải chịu các chi phí kiểm tra các incoming data cho các chức năng bị cấm nhưng không chịu chi phí của outgoing data.

1.4.3.2 Phân loại theo đối tượng sử dụng

Firewall có thể được phân loại theo hai loại sau:

- Personal firewall
- Network firewall

Sự khác biệt chính giữa hai loại trên chính là số lượng host được firewall bảo vệ. Trong khi Personal firewall chỉ bảo vệ cho một máy duy nhất thì Network firewall lại bảo vệ cho một hệ thống mạng.

➢ **Personal Firewall**

Personal firewall được thiết kế để bảo vệ một máy trước những truy cập trái phép. Trong quá trình phát triển, personal firewall đã được tích hợp thêm nhiều chức năng bổ sung như theo dõi phần mềm chống virus, phần mềm phát hiện xâm nhập để bảo vệ thiết bị. Một số personal firewall phổ biến như Cisco Security Agent, Microsoft Internet connection firewall, Symantec personal firewall…

Personal firewall rất hữu ích đối với người dùng gia đình và cá nhân bởi vì họ đơn giản chỉ cần bảo vệ từng máy tính riêng rẻ của họ nhưng đối với doanh nghiệp điều này lại gây bất tiện, khi số lượng host quá lớn thì chi phí cho việc thiết lập, cấu hình và vận hành personal firewall là một điều cần phải xem xét.

➢ **Network firewall**

Network firewall được thiết kế để bảo vệ các host trong mạng trước sự tấn công. Một số ví dụ về appliance-based network firewall như Cisco PIX, Cisco ASA, Juniper NetScreen firewall, Nokia firewalls, Symantec's Enterprise Firewall. Và một số ví dụ về software-based firewall bao gồm Check Point's Firewall, Microsoft ISA Server, Linux-based IPTables.

Cùng với sự phát triển của công nghệ, firewall dần được tích hợp nhiều tính năng mới như phát hiện xâm nhập, thiết lập kết nối VPN cũng như nhiều sản phẩm firewall mới ra đời.

1.4.3.3 Phân loại theo công nghệ tường lửa

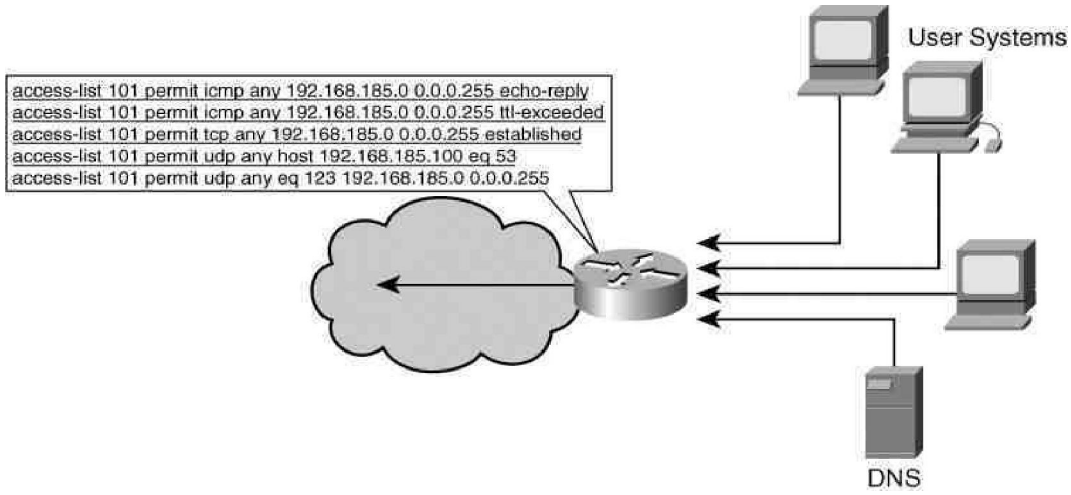
Dựa vào công nghệ sử dụng trong firewall người ta chia firewall thành các loại như sau:

- Personal firewall
- Packet filter
- Network Address Translations (NAT) firewall
- Circuit-level firewall
- Proxy firewall

- Stateful firewall
- Transparent firewall
- Virtual firewall

➢ **Personal firewall:** Được thiết kế để bảo vệ một host duy nhất, thường được tích hợp sẵn trong các laptop, desktop…

➢ **Packet filter:** Là thiết bị được thiết kế để lọc gói tin dựa trên những đặc điểm đơn giản của gói tin. Packet filter tiêu biểu cho dạng staless vì nó không giữ bảng trạng thái các kết nối và không kiểm tra trạng thái các kết nối.



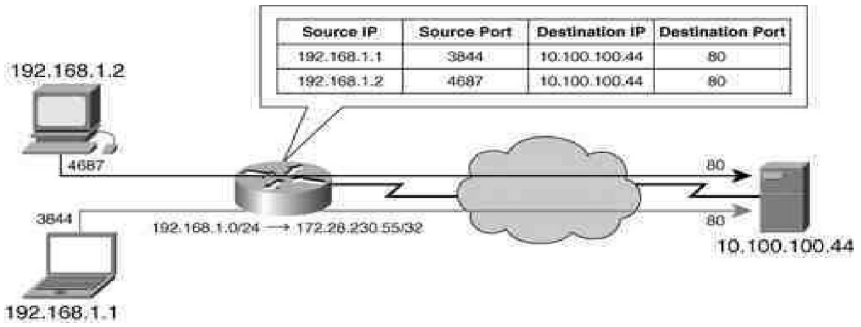
Hình 1-2 : Simple Access List Sample Network

```
access-list 101 permit icmp any 192.168.185.0 0.0.0.255 echo-reply
access-list 101 permit icmp any 192.168.185.0 0.0.0.255 ttl-exceeded
access-list 101 permit tcp any 192.168.185.0 0.0.0.255 established
access-list 101 permit udp any host 192.168.185.100 eq 53
access-list 101 permit udp any eq 123 192.168.185.0 0.0.0.255
```

Hình 1-3: Simple Access List

➢ **Network Address Translations (NAT) firewall**

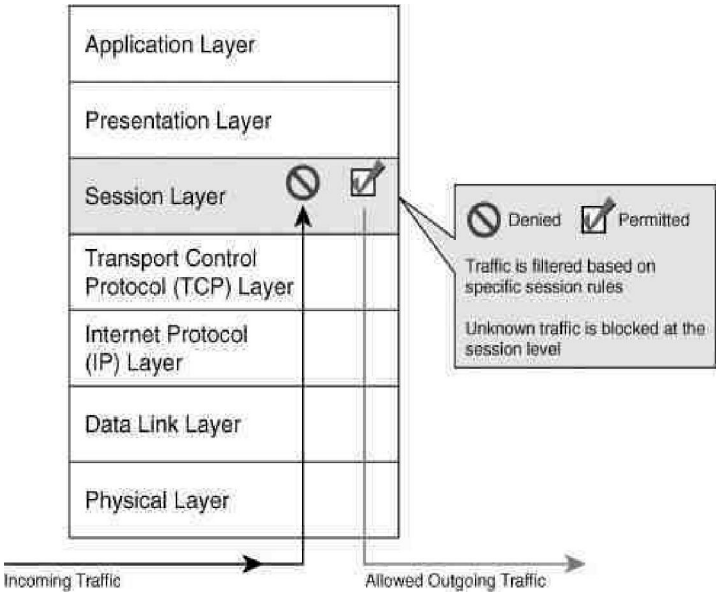
Thực hiện chức năng chuyển đổi địa chỉ IP public thành địa chỉ IP private và ngược lại, nó cung cấp cơ chế che dấu IP của các host bên trong.



Hình 1-4: NAT firewall

- **Circuit-level firewall**

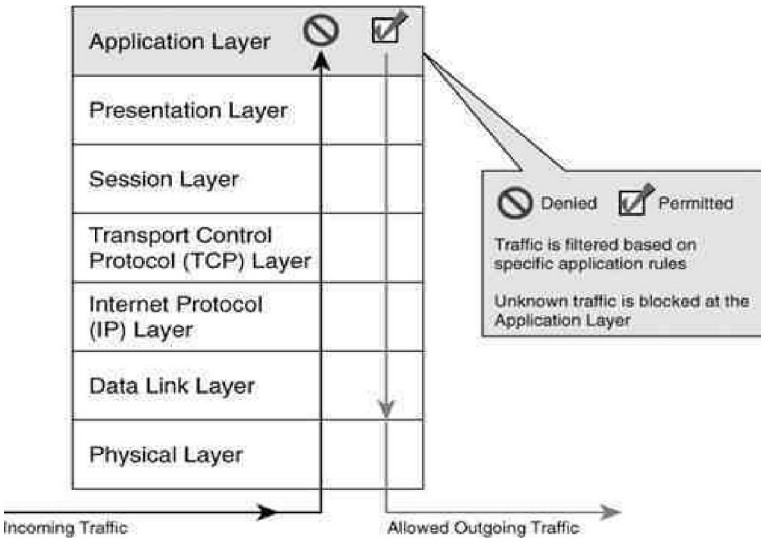
Hoạt động tại lớp session của mô hình OSI, nó giám sát các gói tin "handshaking" đi qua firewall, gói tin được chỉnh sửa sao cho nó xuất phát từ circuit-level firewall, điều này giúp che dấu thông tin của mạng được bảo vệ.



Hình 1-5: Circuit-level firewall

- **Proxy firewall**

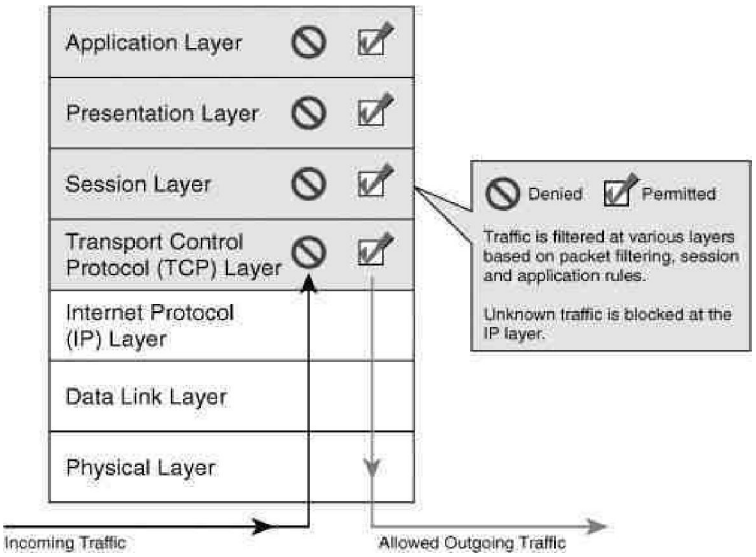
Hoạt động tại lớp ứng dụng của mô hình OSI, nó đóng vai trò như người trung gian giữa hai thiết bị đầu cuối. Khi người dùng truy cập dịch vụ ngoài Internet, proxy đảm nhận việc yêu cầu thay cho client và nhận trả lời từ server trên Internet và trả lời lại cho người dùng bên trong.



Hình 1-6: Proxy firewall

- **Stateful firewall**

Được kết hợp với các firewall khác như NAT firewall, circuit-level firewall, proxy firewall thành một hệ thống firewall, nó không những kiểm tra các đặc điểm của gói tin mà lưu giữ và kiểm tra trạng thái của các gói tin đi qua firewall, một ví dụ cho stateful firewall là sản phẩm PIX firewall của Cisco.



Hình 1-7: Stateful firewall

- **Transparent firewall**

Hoạt động ở layer 2 của mô hình OSI, nó hỗ trợ khả năng lọc các gói tin IP (bao gồm IP, TCP, UDP và ICMP). Transparent firewall thực chất chỉ là tính năng layer 2 brigde kết hợp với tính năng filter trên nền IP bằng cách sử dụng tính năng Context Based Access Control. Vì nó hoạt động ở layer 2 nên ta không cần cấu hình IP cũng như thay đổi IP của các thiết bị được nó bảo vệ.

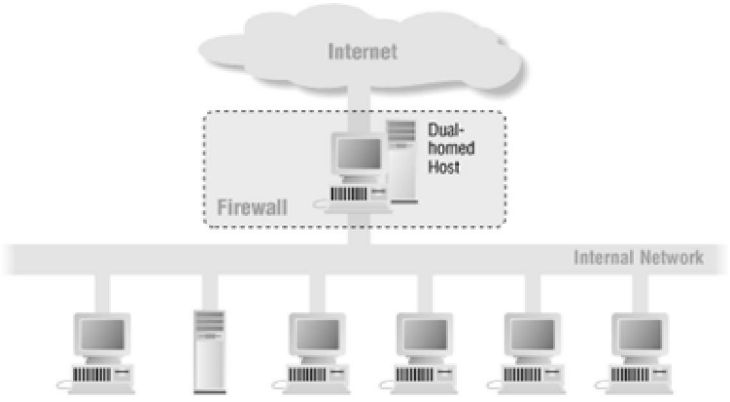
- **Virtual firewall**

Bao gồm nhiều logical firewall hoạt động trên một thiết bị thật. Một trong những ứng dụng của nó hiện nay là dùng trong việc quản lý các máy ảo trong VMWare hay Hyper-V.

1.4.3.4 Phân loại theo kiến trúc

- **Dual homed host**

Firewall kiến trúc kiểu Dual-homed host được xây dựng dựa trên máy tính dual-homed host. Một máy tính được gọi là dual-homed host nếu nó có ít nhất hai network interface, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau và như thế máy tính này đóng vai trò là Router mềm. Kiến trúc dual-homed host rất đơn giản. Dual-homed host ở giữa, một bên được kết nối với Internet và bên còn lại nối với mạng nội bộ (LAN).



Hình 1-8: Mô hình Dual-homed host

Dual-homed host chỉ có thể cung cấp các dịch vụ bằng cách ủy quyền (proxy) chúng hoặc cho phép user đăng nhập trực tiếp vào dual-homed host. Mọi giao tiếp từ một host trong mạng nội bộ và host bên ngoài đều bị cấm, dual-homed host là nơi giao tiếp duy nhất.

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 đó trên các hệ điều hành Linux chỉ cần cấu hình lại nhân của hệ điều hành là đủ.

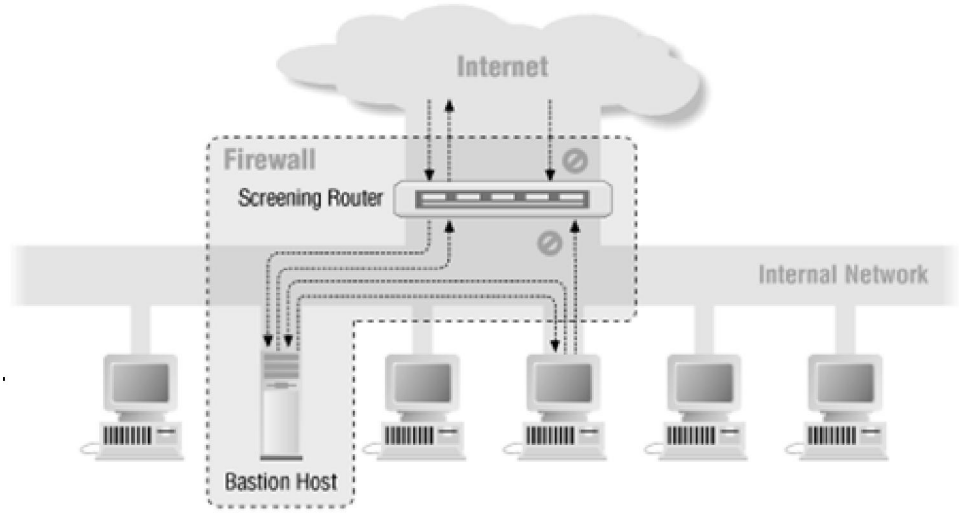
Nhược điểm của Dual-homed host:

- Không đáp ứng được những yêu cầu bảo mật ngày càng phức tạp, cũng như những phần mềm mới được tung ra trên thị trường.
- Không có khả năng chống đỡ những cuộc tấn công nhằm vào chính bản thân của dual-homed host, và khi dual-homed host bị đột nhập nó sẽ trở thành nơi lý tưởng để tấn công vào mạng nội bộ, người tấn công (attacker) sẽ thấy được toàn bộ lưu lượng trên mạng.

➢ **Screened host**

Screened Host có cấu trúc ngược lại với cấu trúc Dual-homed host. Kiến trúc này cung cấp các dịch vụ từ một host bên trong mạng nội bộ, dùng một Router tách rời với mạng bên ngoài. Trong kiểu kiến trúc này, bảo mật chính là phương pháp Packet Filtering. Bastion host được đặt bên trong mạng nội bộ. Packet Filtering được cài trên Router. Theo cách này, Bastion host là hệ thống duy nhất trong mạng nội bộ mà những host trên Internet có thể kết nối tới.

Mặc dù vậy, chỉ những kiểu kết nối phù hợp (được thiết lập trong Bastion host) mới được cho phép kết nối. Bất kỳ một hệ thống bên ngoài nào cố gắng truy cập vào hệ thống hoặc các dịch vụ bên trong đều phải kết nối tới host này. Vì thế Bastion host là host cần phải được duy trì ở chế độ bảo mật cao.



Hình 1-9: Mô hình Screened Host

Packet filtering cũng cho phép bastion host có thể mở kết nối ra bên ngoài. Cấu hình của packet filtering trên screening router như sau:

- Cho phép tất cả các host bên trong mở kết nối tới host bên ngoài thông qua một số dịch vụ cố định.
- Không cho phép tất cả các kết nối từ các host bên trong (cấm những host này sử dụng dịch proxy thông qua bastion host).

Bạn có thể kết hợp nhiều lối vào cho những dịch vụ khác nhau:

- Một số dịch vụ được phép đi vào trực tiếp qua packet filtering.
- Một số dịch vụ khác thì chỉ được phép đi vào gián tiếp qua proxy.

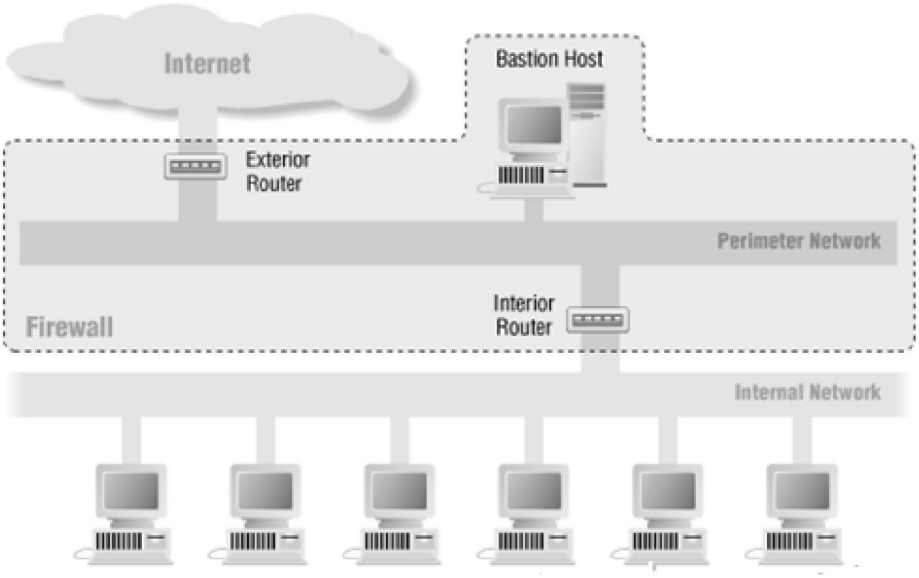
Bởi vì kiến trúc này cho phép các packet đi từ bên ngoài vào mạng bên trong, nó dường như là nguy hiểm hơn kiến trúc Dual-homed host, vì thế nó được thiết kế để không một packet nào có thể tới được mạng bên trong. Tuy nhiên trên thực tế thì kiến trúc dual-homed host đôi khi cũng có lỗi mà cho phép các packet thật sự đi từ bên ngoài vào bên trong (bởi vì những lỗi này hoàn toàn không biết trước, nó hầu như không được bảo vệ để chống lại những kiểu tấn công này. Hơn nữa, kiến trúc dual-homed host thì dễ dàng bảo vệ Router (là máy cung cấp rất ít các dịch vụ) hơn là bảo vệ các host bên trong mạng.

Xét về toàn diện thì kiến trúc Screened host cung cấp độ tin cậy cao hơn và an toàn hơn kiến trúc Dual-homed host.

So sánh với một số kiến trúc khác, chẳng hạn như kiến trúc Screened subnet thì kiến trúc Screened host có một số bất lợi. Bất lợi chính là nếu kẻ tấn công tìm cách xâm nhập Bastion Host thì không có cách nào để ngăn tách giữa Bastion Host và các host còn lại bên trong mạng nội bộ. Router cũng có một số điểm yếu là nếu Router bị tổn thương, toàn bộ mạng sẽ bị tấn công. Vì lý do này mà Screened subnet trở thành kiến trúc phổ biến nhất.

- **Screened Subnet**

Nhằm tăng cường khả năng bảo vệ mạng nội bộ, thực hiện chiến lược phòng thủ theo chiều sâu, tăng cường sự an toàn cho bastion host, tách bastion host khỏi các host khác, phần nào tránh lây lan một khi bastion host bị tổn thương, người ta đưa ra kiến trúc firewall có tên là Screened Subnet.



Hình 1-10: Mô hình Screened subnet

Kiến trúc Screened subnet dẫn xuất từ kiến trúc screened host bằng cách thêm vào phần an toàn: mạng vành đai (perimeter network) nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách bastion host ra khỏi các host thông thường khác. Kiểu screened subnet đơn giản bao gồm hai screened router:

- Router ngoài (External router còn gọi là access router): nằm giữa mạng ngoại vi và mạng ngoài có chức năng bảo vệ cho mạng ngoại vi (bastion host, interior router). Nó cho phép hầu hết những gì outbound từ mạng ngoại vi. Một số qui tắc packet filtering đặc biệt được cài đặt ở mức cần thiết đủ để bảo vệ bastion

host và interior router vì bastion host còn là host được cài đặt an toàn ở mức cao. Ngoài các qui tắc đó, các qui tắc khác cần giống nhau giữa hai Router.

- Router trong (Interior Router): nằm giữa mạng ngoại vi và mạng nội bộ, nhằm bảo vệ mạng nội bộ trước khi ra ngoài và mạng ngoại vi. Nó không thực hiện hết các qui tắc packet filtering của toàn bộ firewall. Các dịch vụ mà interior router cho phép giữa bastion host và mạng nội bộ, giữa bên ngoài và mạng nội bộ không nhất thiết phải giống nhau.

Giới hạn dịch vụ giữa bastion host và mạng nội bộ nhằm giảm số lượng máy (số lượng dịch vụ trên các máy này) có thể bị tấn công khi bastion host bị tổn thương và thoả hiệp với bên ngoài. Chẳng hạn nên giới hạn các dịch vụ được phép giữa bastion host và mạng nội bộ như SMTP khi có Email từ bên ngoài vào, có lẽ chỉ giới hạn kết nối SMTP giữa bastion host và Email server bên trong.

Ưu điểm của Screened Subnet Host:

- Kẻ tấn công cần phá vỡ ba tầng bảo vệ: Router ngoài, Bastion Host và Router trong.
- Bởi vì router ngoài chỉ quảng bá Bastion host ra Internet nên cí thể nhìn thấy hệ thống mạng nội bộ (invisible). Chỉ có một số hệ thống đã được chọn ra trên DMZ là Internet được biết đến qua routing table và trao đổi thông tin DNS (Domain Name Server).
- Bởi vì router trong chỉ quảng bá Bastion host tới mạng nội bộ nên các hệ thống bên trong mạng nội bộ không thể truy cập trực tiếp tới Internet. Điều này đảm bảo rằng những user bên trong bắt buộc phải truy cập qua Internet qua dịch vụ Proxy.
- Đối với những hệ thống yêu cầu cung cấp dịch vụ nhanh và an toàn cho nhiều người sử dụng đồng thời nâng cao khả năng theo dõi lưu lượng của mỗi người sử dụng trong hệ thống và dữ liệu trao đổi giữa các người dùng trong hệ thống cần được bảo vệ thì kiến trúc cơ bản trên là phù hợp.
- Để tăng độ an toàn trong internal network, kiến trúc Screened Subnet Host ở trên sử dụng thêm một dạng vành đai (perimeter network) để che một phần lưu lượng bên trong internal network, tách biệt internal network với Internet.

1.4.4. Các sản phẩm firewall

1.4.4.1 Software firewall

Software firewall: firewall mềm là những firewall được cài đặt trên một hệ điều hành. Firewall mềm bao gồm các sản phẩm như SunScreen firewall, IPF,

Microsoft ISA server, Check Point NG, Linux's IPTables …Firewall mềm thường đảm nhận nhiều vai trò hơn firewall cứng, nó có thể đóng vai trò như một DNS server hay một DHCP server.

Một nhược điểm của firewall mềm là nó được cài đặt trên một hệ điều hành và do đó khả năng có lỗ hổng trên hệ điều hành này là có thể xẩy ra. Khi lỗ hổng được phát hiện và được cập nhật bản vá lỗi, rất có thể sau khi cập nhật bản vá lỗi cho hệ điều hành thì firewall không hoạt động bình thường như trước, do đó cần tiến hành cập nhật bản vá cho firewall từ nhà cung cấp sản phẩm firewall.

Một ưu điểm nổi trội của firewall mềm là việc thay đổi và nâng cấp thiết bị phần cứng là tương đối dễ dàng và nhanh chóng.

Do hệ điều hành mà firewall mềm chạy trên nó không được thiết kế tối ưu cho firewall nên firewall mềm có hiệu suất thấp hơn firewall cứng

1.4.4.2 Appliance firewall

Appliance firewall – firewall cứng – là những firewall được tích hợp sẵn trên các phần cứng chuyên dụng, thiết kế dành riêng cho firewall. Các sản phẩm firewall cứng đáng chú ý như Cisco PIX, NetScreen firewall, SonicWall Appliaces, WatchGuard Fireboxes, Nokia firewall…

Trong nhiều trường hợp firewall cứng cung cấp hiệu suất tốt hơn so firewall mềm vì hệ điều hành của firewall cứng được thiết kế để tối ưu cho firewall. Lợi ích điển hình khi sử dụng firewall cứng là hiệu suất tổng thể tốt hơn firewall mềm, tính bảo mật được nâng cao, tổng chi phí thấp hơn so với firewall mềm.

Firewall cứng không được linh hoạt như firewall mềm (không thể thêm chức năng, thêm các quy tắc như trên firewall mềm). Hạn chế của firewall cứng là khả năng tích hợp thêm các chức năng bổ sung khó khăn hơn firewall mềm, chẳng hạn như chức năng kiểm soát thư rác đối với firewall mềm chỉ cần cài đặt chức năng này như một ứng dụng còn đối với firewall cứng phải có thiết bị phần cứng hỗ trợ cho chức năng này.

1.4.4.3 Integrated firewall

Integrated firewall – firewall tích hợp – ngoài chức năng cơ bản của firewall thì nó còn đảm nhận các chức năng khác như VPN, phát hiện phòng chống xâm nhập, lọc thư rác, chống virus. Lợi ích của việc dùng firewall tích hợp là đơn giản hóa thiết kế mạng bằng cách giảm lượng thiết bị mạng cũng như giảm chi phí quản lý, giảm gánh nặng cho các chuyên viên quản trị, ngoài ra nó còn tiết kiệm chi phí hơn so với việc dùng nhiều thiết bị cho nhiều mục đích khác nhau.

Tuy nhiên việc tích hợp nhiều chức năng trên cùng một thiết bị dẫn đến khó khăn trong khắc phục sự cố vì tính phức tạp của hệ thống khi tích hợp.

1.5. Kết luận chương 1

Chương 1 đã trình bày các thông tin nổi cộm về an ninh mạng năm 2016, gồm thông tin về: bùng nổ mã độc mã hóa dữ liệu ransomware, virus USB, tấn công APT và xu hướng tấn công năm 2017. Các phương thức tấn công có tác động xấu tới hoạt động của hệ thống mạng từ mức độ thấp đến cao, xâm nhập hệ thống từ bên trong như là mã độc, xâm nhập hệ thống từ bên ngoài như là: tấn công lỗ hổng bảo mật web, sử dụng proxy tấn công mạng… Từ đó các chính sách an ninh mạng được triển để đảm bảo an toàn thông tin như chính sách lọc, quản lý truy cập, chính sách định tuyến.. Chương này cũng đưa ra khái niệm của bức tường lửa, các chức năng tường lửa ví dụ như chức năng quản lý và điều khiển luồng dữ liệu trên mạng, bảo vệ tài nguyên, xác thực quyền truy cập… Thông tin về phân loại tường lửa: phân loại theo tầng giao thức, theo đối tượng sử dụng, theo công nghệ tường lửa, theo kiến trúc và các sản phẩm tường lửa như: software firewall, appliance firewall, integrated firewall.

CHƯƠNG 2
HỆ THỐNG FIREWALL ASA

2.1. Giới thiệu

Thiết bị phần cứng đảm nhận vai trò bảo vệ hạ tầng mạng bên trong, trước đây thương hiệu PIX Firewall của hãng Cisco Systems đã giành được một trong những vị trí hàng đầu của lĩnh vực này. Tuy nhiên theo đà phát triển của công nghệ và xu hướng tích hợp đa chức năng trên các kiến trúc phần cứng hiện nay (gọi là Appliance), hãng Cisco Systems cũng đã nhanh chóng tung ra dòng sản phẩm bảo mật đa năng Cisco ASA (Adaptive Security Appliance). Dòng thiết bị này ngoài việc thừa hưởng các tính năng ưu điểm của công nghệ dùng trên Cisco PIX Firewall, Cisco IPS 4200 và Cisco VPN 3000 Concentrator, còn được tích hợp đồng thời 3 nhóm chức năng chính cho một hạ tầng bảo vệ là Firewall, IPS và VPN. Thông qua việc tích hợp những tính năng như trên, Cisco ASA sẽ chuyển giao một giải pháp hiệu quả trong việc bảo mật hoá các giao tiếp kết nối mạng nhằm có thể chủ động đối phó trên diện rộng đối với các hình thức tấn công qua mạng hoặc các hiểm họa mà tổ chức, doanh nghiệp thường phải đương đầu.

Cisco ASA viết tắt của từ Cisco Adaptive Security Appliance. ASA là một giải pháp bảo mật đầu cuối chính của Cisco. Hiện tại ASA là sản phẩm bảo mật dẫn đầu trên thị trường về hiệu năng và cung cấp các mô hình phù hợp doanh nghiệp, tích hợp giải pháp bảo mật mạng. Dòng sản phẩm ASA giúp tiết kiệm chi phí, dễ dàng triển khai.

Nó bao gồm các thuộc tính sau:

+ Bảo mật thời gian thực, hệ điều hành độc quyền của Cisco

+ Công nghệ Stateful firewall sử dụng thuật toán SA của Cisco

+ Sử dụng SNR để bảo mật kết nối TCP

+ Sử dụng Cut through proxy để chứng thực Telnet, HTTP, FTP

+ Chính sách bảo mật mặc định gia tăng bảo vệ mức tối đa và cũng có khả năng tùy chỉnh những chính sách này và xây dựng lên chính sách của riêng bạn

+ VPN: IPSec, SSL và L2TP

+ Tích hợp hệ thống ngăn ngừa và phát hiện xâm nhập IDS/IPS

+ NAT động, NAT tĩnh, NAT port

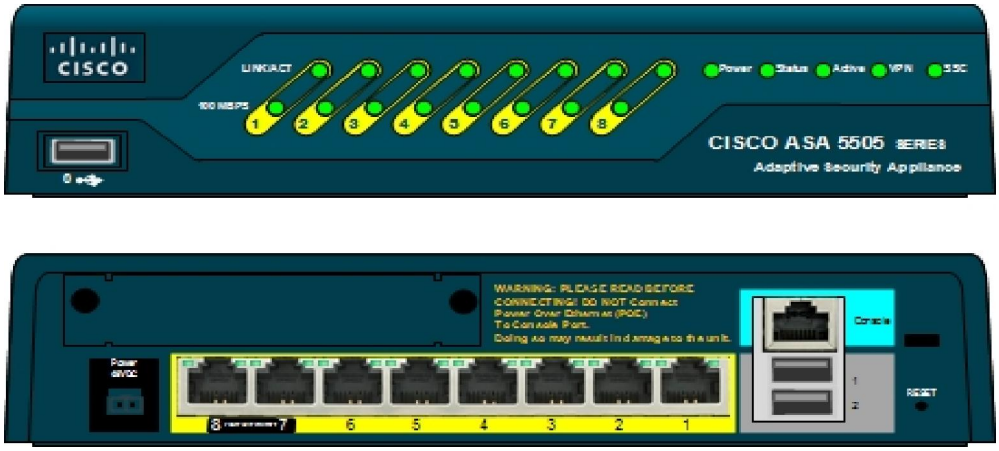
+ Ảo hóa các chính sách sử dụng Context

2.2. Dòng sản phẩm firewall ASA của Cisco

Có tất cả 6 model ASA khác nhau. Dòng sản phẩm này phân loại khác nhau từ tổ chức đến mô hình doanh nghiệp vừa hay cho nhà cung cấp dịch vụ ISP.

Mô hình càng cao thì thông lượng, số port, chi phí càng cao. Sản phẩm bao gồm: ASA 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40.

2.2.1. ASA 5505



Hình 2-1: ASA 5505

ASA 5505 là model nhỏ nhất trong các dòng sản phẩm của ASA, cả về kích thước vật lý cũng như hiệu suất. Nó được thiết kết dành cho các văn phòng nhỏ và văn phòng gia đình Đối với các doanh nghiệp lớn hơn, ASA 5505 thường được sử dụng để hỗ trợ cho các nhân viên làm việc từ xa.

Có 8 cổng FastEthernet trên ASA 5505, tất cả kết nối đến một switch nội bộ. 2 trong số các cổng có khả năng cung cấp Power over Ethernet (PoE) với các thiết bị kèm theo (ASA chính nó không thể hỗ trợ bởi PoE). Theo mặc định, tất cả 8 cổng được kết nối đến các VLAN giống nhau trong switch, cho phép kết nối các thiết bị để giao tiếp ở lớp 2.

Các cổng của switch có thể chia thành nhiều VLAN để hỗ trợ các khu vực hoặc chức năng khác nhau trong một văn phòng nhỏ. ASA kết nối với mỗi VLAN qua các interface các nhân vật lý. Bất kỳ luồng dữ liệu nào qua giữa các VLAN đều qua ASA và các chính sách bảo mật của nó.

ASA 5505 có một khe Security Services Card (SSC) có thể chấp nhận một tùy chọn AIPSSC-5 IPS module. Với module được cài đặt, ASA có thể tăng cường các đặc tính bảo mật của nó với các chức năng mạng IPS.

2.2.2. ASA 5510, 5520 và 5540

Hình 2-2: ASA 5510

Các model ASA 5510, 5520 và 5540 sử dụng một khuôn chung như hình trên và có các chỉ số ở mặt trước và các phần cứng kết nối giống nhau. Các model khác nhau trong xếp hạng hiệu suất an ninh của chúng. Tuy nhiên, ASA 5510 được thiết kết cho các doanh nghiệp nhỏ và vừa (SMB) và các văn phòng từ xa của doanh nghiệp lớn. ASA 5520 thích hợp cho các doanh nghiệp vừa trong khi ASA 5540 dành cho các doanh nghiệp vừa và lớn và các nhà cung cấp dịch vụ mạng.

ASA 5520 và 5540 có 4 cổng 10/100/100 có thể sử dụng để kết nối vào cơ sở hạ tầng mạng. 4 cổng là các interface firewall chuyên dụng và không kết nối với nhau. ASA 5510 có thể sử dụng 4 cổng 10/100 là mặc định. Nếu mua thêm một giấy phép bảo mật thì kích hoạt 2 port làm việc ở 10/100/1000 và 2 port FastEthernet. Một interface thứ 5 dùng để quản lý cũng có sẵn.

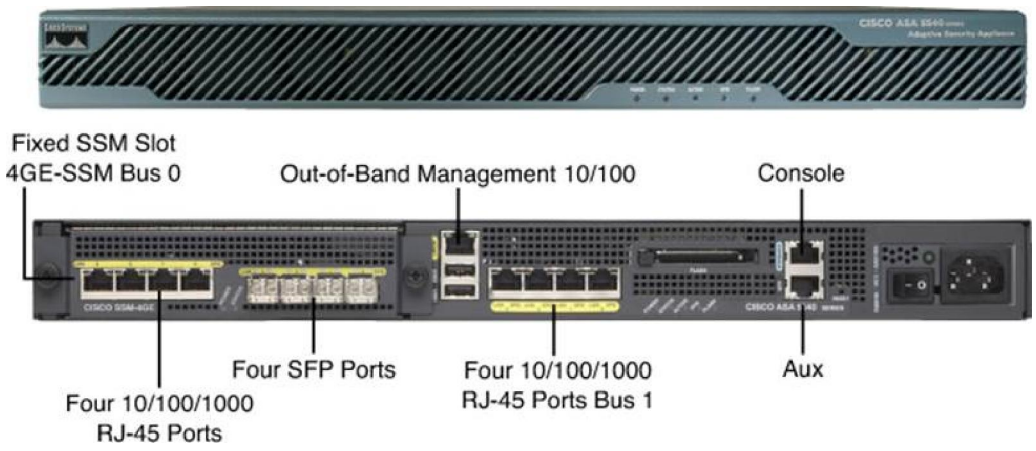
Các ASA 5510, 5520 và 5540 có một khe cắm SSM có thể gắn card vào :

+ Four-port Gigabit Ethernet SSM: module này thêm vào 4 interface firewall vật lý, hoặc 10/100/100 RJ45 hoặc small form-factor pluggable (SFP)- cổng cơ bản

+ Advanced Inspection and Prevention (AIP) SSM: module này thêm các khả năng của mạng nội tuyến IPS để phù hợp với bảo mật của ASA

+ Content Security and Control (CSC) SSM: module này các dịch vụ kiểm soát nội dung và chống virus toàn diện cho phù hợp với bảo mật của ASA.

2.2.3. ASA 5550



Hình 2-3: ASA 5550

ASA 5550 được thiết kế để hỗ trợ doanh nghiệp lớn và các nhà cung cấp dịch vụ mạng. Hình trên cho thấy mặt trước và sau. Chú ý rằng ASA 5550 trông giống ASA 5510, 5520 và 5540. Sự khác biệt đáng chú ý nhất là ASA 5550 có 4 cổng Gigabit Ethernet (4GE-SSM) cố định trong khe cắm SSM, không thể tháo bỏ và thay đổi.

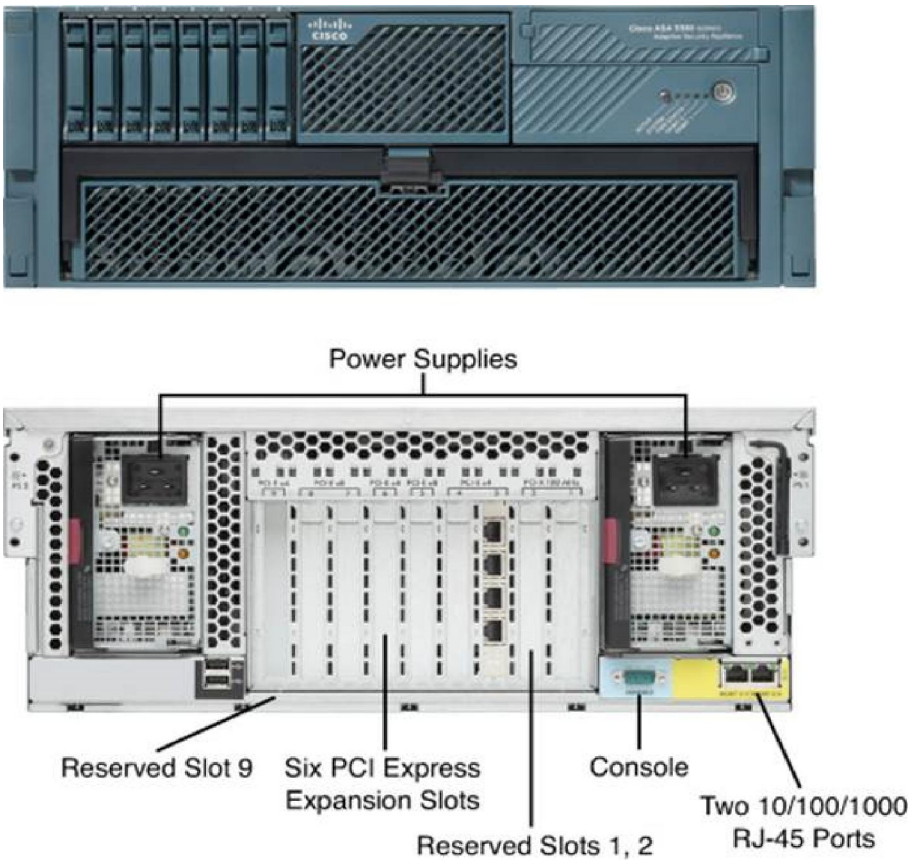
Đặc điểm kiến trúc ASA 5550 có 2 nhóm interface vật lý kết nối đến 2 bus nội được chia ra. Các nhóm interface được gọi là khe cắm 0 và 1 tương ứng với bus 0 và 1. Khe cắm 0 gồm 4 cổng Gigabit Ethernet cáp đồng. Khe cắm 1 gồm 4 cổng SFP Gigablit Ethernet cáp đồng, mặc dù chỉ có 4 trong 8 cổng có thể được sử dụng bất cứ lúc nào.

ASA 5550 cung cấp hiệu suất cao cho các môi trường được đòi hỏi. Để tối đa hóa thông lượng firewall, phần lớn lưu lượng nên đi từ các switch port trên bus 0 đến switch port trên bus 1. ASA có thể chuyển tiếp lưu lượng hiệu quả hơn rất nhiều từ bus này đến bus kia nếu lưu lượng nằm trong một bus đơn.

2.2.4. ASA 5580

ASA 5580 là một model có hiệu suất cao trong họ và được thiết kế cho các doanh nghiệp lớn, trung tâm dữ liệu, các nhà cung cấp dịch vụ lớn. Nó có thể hỗ trợ lên đến 24 Gigabit Ethernet interfaces hoặc 12 10 Gigabit Ethernet interfaces. Đây là một trong hai model khung lớn hơn một đơn vị rack tiêu chuẩn (RU).

ASA 5580 thể hiện trong hình 2-4, có 2 model: ASA 5580-20 (5Gbps) và ASA 5580-40 (10Gbps). Bộ khung bao gồm 2 port 10/100/1000 được sử dụng cho quản lý lưu lượng out-of-band. Hệ thống cũng sử dụng nguồn cung cấp điện dự phòng kép.



Hình 2-4: ASA 5580

ASA 5580 khung tổng cộng có 9 khe cắm PCI Express mở rộng. Khe cắm 1 được dành riêng cho module mã hóa gia tốc để hỗ trợ cho các phiên làm việc VPN hiệu suất cao. Khe 2-9 dành cho việc sử dụng trong tương lai, để lại 6 khe cắm có sẵn cho các card interface mạng sau đây:

+ 4-port 10/100/1000BASE-T cáp đồng Gigabit Ethernet interfaces

+ 4-port 1000BASE-SX cáp quang Gigabit Ethernet interfaces

+ 2-port 10GBASE-SR 10Gigabit Ethernet cáp quang interfaces

2.3. Cơ chế hoạt động

Cisco ASA hoạt động theo cơ chế giám sát gói tin theo trạng thái (Stateful Packet Inspection), thực hiện điều khiển trạng thái kết nối khi qua thiết bị bảo mật (ghi nhận trạng thái của từng gói tin thuộc kết nối xác định theo loại giao thức hay ứng dụng). Cho phép kết nối một chiều (outbound-đi ra) với rất ít việc cấu hình. Một

kết nối đi ra là một kết nối từ thiết bị trên cổng có mức bảo mật cao đến thiết bị trên mạng có mức bảo mật thấp hơn.

Trạng thái được ghi nhận sẽ dùng để giám sát và kiểm tra gói trở về. Thay đổi ngẫu nhiên giá trị tuần tự (sequence number) trong gói TCP để giảm rủi ro của sự tấn công.

Hoạt động theo kiến trúc phân vùng bảo mật dựa theo cổng, cổng tin cậy (trusted) hay mức bảo mật cao và cổng không tin cậy (untrusted) hay mức bảo mật thấp. Quy tắc chính cho mức bảo mật đó là thiết bị từ vùng tin cậy có thể truy cập được thiết bị trong vùng không tin cậy. Ngược lại thiết bị từ vùng không tin cậy không thể truy cập tới thiết bị vùng tin cậy trừ khi được cho phép bởi ACL.

2.4. Các chức năng cơ bản của firewall ASA

2.4.1. Quản lý file

Có hai loại file cấu hình trong các thiết bị an ninh Cisco: *running-configuration* và *startup-configuration*.

Loại file đầu tiên running-configuration là một trong những file hiện đang chạy trên thiết bị, và được lưu trữ trong bộ nhớ RAM của firewall. Bạn có thể xem cấu hình này bằng cách gõ *show running-config* từ các chế độ Privileged. Bất kỳ lệnh mà bạn nhập vào firewall được lưu trực tiếp bằng trong running-config và có hiệu lực thi hành ngay lập tức. Kể từ khi cấu hình chạy được lưu trong bộ nhớ RAM, nếu thiết bị bị mất nguồn, nó sẽ mất bất kỳ thay đổi cấu hình mà không được lưu trước đó. Để lưu lại cấu hình đang chạy, sử dụng *copy run start* hoặc *write memory*. Hai lệnh này sẽ copy running-config vào startup-config cái mà được lưu trữ trong bộ nhớ flash.

Loại thứ hai startup-configuration là cấu hình sao lưu của running-configuration. Nó được lưu trữ trong bộ nhớ flash, vì vậy nó không bị mất khi các thiết bị khởi động lại. Ngoài ra, startup-configuration được tải khi thiết bị khởi động. Để xem startup-configuration được lưu trữ, gõ lệnh *show startup-config*.

2.4.2. Mức độ bảo mật

Security Level được gán cho interface (hoặc vật lý hay logical sub-interfaces) và cơ bản nó là một số từ 0-100 được chỉ định với interface liên quan đến một interface khác trên thiết bị. Mức độ bảo mật cao hơn thì interface càng đáng tin cậy hơn. Vì mỗi interface firewall đại diện cho một mạng cụ thể (hoặc khu vực an ninh) bằng cách sử dụng mức độ bảo mật. Các quy tắc chính cho mức độ bảo mật là một interface với một mức độ bảo mật cao hơn có thể truy cập vào một interface với một

mức độ bảo mật thấp hơn. Mặt khác, một interface với một mức độ bảo mật thấp hơn không thể truy cập vào một interface với một mức độ bảo mật cao hơn, mà không có sự cho phép rõ ràng của một quy tắc bảo mật (Access Control List - ACL).

Một số mức độ bảo mật điển hình:

- Security Level **0**: Đây là mức độ bảo mật thấp nhất và nó được gán mặc định interface bên ngoài của firewall. Đó là mức độ bảo mật ít tin cậy nhất và phải được chỉ định phù hợp với mạng (interface) mà chúng ta không muốn nó có bất kỳ truy cập vào mạng nội bộ của chúng ta. Mức độ bảo mật này thường được gán cho interface kết nối với Internet. Điều này có nghĩa rằng tất cả các thiết bị kết nối Internet không thể có quyền truy cập vào bất kỳ mạng phía sau firewall, trừ khi một quy tắc ACL rõ ràng cho phép.
- Security Level **1 đến 99**: Những mức độ bảo mật có thể được khu vực bảo mật vòng ngoài (ví dụ như khu vực DMZ, khu vực quản lý,...).
- **Security Level 100**: Đây là mức độ bảo mật cao nhất và nó được gán mặc định interface bên trong của tường lửa. Đây là mức độ bảo mật đáng tin cậy nhất và phải được gán cho mạng (interface) mà chúng ta muốn áp dụng bảo vệ nhiều nhất từ các thiết bị an ninh.Mức độ bảo mật này thường được gán cho interface kết nối mạng nội bộ công ty đằng sau nó.

Việc truy cập giữa Security Level tuân theo các quy định sau:

- Truy cập từ Security Level cao hơn tới Security Level thấp hơn: Cho phép tất cả lưu lượng truy cập có nguồn gốc từ Security Level cao hơn trừ khi quy định cụ thể bị hạn chế bởi một Access Control List (ACL). Nếu NAT-Control được kích hoạt trên thiết bị, sau đó phải có một cặp chuyển đổi *nat/global* giữa các interface có Security Level từ cao tới thấp.
- Truy cập từ Security Level thấp hơn Security Level cao hơn: Chặn tất cả lưu lượng truy cập trừ khi được cho phép bởi một ACL. Nếu NAT-Control được kích hoạt trên thiết bị này, sau đó phải là một NAT tĩnh giữa các interface có Security Level từ cao tới thấp.
- Truy cập giữa các interface có cùng một Security Level: theo mặc định là không được phép, trừ khi bạn cấu hình lệnh *same-security-traffic permit***.**

2.4.3. Điều khiển truy cập mạng

Cisco Adaptive Security Appliances (ASA) có thể giúp bảo vệ một hoặc nhiều mạng từ những kẻ xâm nhập và tấn công. Kết nối giữa các mạng này có thể được kiểm soát và theo dõi bằng cách sử dụng các tính năng mạnh mẽ mà Cisco ASA cung cấp. Có thể đảm bảo rằng tất cả lưu lượng truy cập từ các mạng tin cậy cho đến mạng không tin cậy (và ngược lại) đi qua các tường lửa dựa trên chính sách đảm bảo an toàn của hệ thống tường lửa ASA.

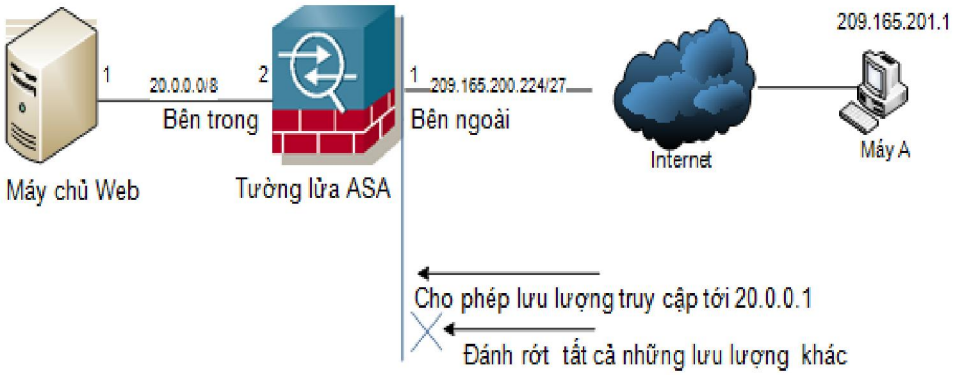
2.4.3.1 Lọc gói

Cisco ASA có thể bảo vệ mạng bên trong (inside), các khu phi quân sự (DMZ) và mạng bên ngoài (outside) bằng cách kiểm tra tất cả lưu lượng đi qua nó. Có thể xác định chính sách và quy tắc cho những lưu lượng được cho phép hoặc không cho phép đi qua interface. Các thiết bị bảo mật sử dụng access control list (ACL) để giảm lưu lượng truy cập không mong muốn hoặc không biết khi nó cố gắng để vào mạng đáng tin cậy. Một ACL là danh sách các quy tắc an ninh, chính sách nhóm lại với nhau cho phép hoặc từ chối các gói tin sau khi nhìn vào các tiêu đề gói (packet header) và các thuộc tính khác. Mỗi phát biểu cho phép hoặc từ chối trong ACL được gọi là một access control entry (ACE). Các ACE có thể phân loại các gói dữ liệu bằng cách kiểm tra ở layer 2, layer 3 và layer 4 trong mô hình OSI bao gồm:

- Kiểm tra thông tin giao thức layer 2: ethertypes.
- Kiểm tra thông tin giao thức layer 3: ICMP, TCP or UDP, kiểm tra địa chỉ IP nguồn và đích .
- Kiểm tra thông tin giao thức layer 4: port TCP/UDP nguồn và đích.

Khi một ACL đã được cấu hình đúng, có thể áp dụng vào interface để lọc lưu lượng. Các thiết bị an ninh có thể lọc các gói tin theo hướng đi vào (inbound) và đi ra (outbound) từ interface. Khi một ACL được áp dụng đi vào interface, các thiết bị an ninh kiểm tra các gói chống lại các ACE sau khi nhận được hoặc trước khi truyền đi. Nếu một gói được cho phép đi vào, các thiết bị an ninh tiếp tục quá trình này bằng cách gửi nó qua các cấu hình khác. Nếu một gói tin bị từ chối bởi các ACL, các thiết bị an ninh loại bỏ các gói dữ liệu và tạo ra một thông điệp syslog chỉ ra một sự kiện đã xảy ra.

Trong hình 2.5, người quản trị thiết bị an ninh áp dụng cho outside interface một inbound ACL chỉ cho phép lưu lượng HTTP tới 20.0.0.1. Tất cả các lưu lượng khác sẽ bị loại bỏ tại interface của các thiết bị an ninh.



Hình 2-5: Mô tả quá trình lọc gói của tường lửa

Nếu một ACL được áp dụng trên một interface, các thiết bị an ninh xử lý các gói dữ liệu bằng cách gửi các packet thông qua các quá trình khác nhau (NAT, QoS, và VPN) và sau đó áp dụng các cấu hình ACE trước khi truyền các gói dữ liệu này. Các thiết bị an ninh truyền các gói dữ liệu chỉ khi chúng được phép đi ra ngoài.

Các loại Access Control List:

Có năm loại ACL khác nhau đã cung cấp một cách linh hoạt và khả năng mở rộng để lọc các gói trái phép bao gồm:

- Standard ACL
- Extended ACL
- IPV6 ACL
- Ethertype ACL
- WebVPN ACL

Standard ACL: Chuẩn Standard ACL được sử dụng để xác định các gói dữ liệu dựa trên địa chỉ IP đích.Các ACL ở đây có thể được sử dụng để phân chia các luồng lưu thông trong truy cập từ xa VPN và phân phối lại các luồng này bằng sơ đồ định tuyến.Chuẩn Standard ACL chỉ có thể được sử dụng để lọc các gói khi và chỉ khi các thiết bị bảo mạng hoạt động ở chế độ định tuyến,ngăn truy cập từ mạng con này đến mạng con khác.

Extended ACL: Chuẩn Extended là một chuẩn phổ biết nhất, có thể phân loại các gói dữ liệu dựa trên các đặc tính sau:

- Địa chỉ nguồn và địa chỉ đích.

- Giao thức lớp 3.
- Địa chỉ nguồn hoặc địa chỉ của cổng TCP và UDP.
- Điểm đến ICMP dành cho các gói ICMP.
- Một chuẩn ACL mở rộng có thể được sử dụng cho quá trình lọc gói, phân loại các gói QoS, nhận dạng các gói cho cơ chế NAT và mã hóa VPN.
- IPV6 ACL: Một IPV6 ACL có chức năng tương tự như chuẩn Extended ACL. Tuy nhiên chỉ nhận biết các lưu lượng là địa chỉ IPV6 lưu thông qua thiết bị bảo mật ở chế độ định tuyến.

Ethertype ACL: Chuẩn Ethertype có thể được sử dụng để lọc IP hoặc lọc gói tin bằng cách kiểm tra đoạn mã trong trường Ethernet ở phần đầu lớp 2. Một Ethertype ACL chỉ có thể được cấu hình chỉ khi các thiết bị bảo mật đang chạy ở chế độ trong suốt (transparent). Lưu ý rằng ở chuẩn này các thiết bị bảo mật không cho phép dạng IPV6 lưu thông qua, ngay cả khi được phép đi qua IPV6 Ethertype ACL.

WebVPN ACL: Một WebVPN ACL cho phép người quản trị hệ thống hạn chế lưu lượng truy cập đến từ luồng WebVPN. Trong trường hợp có một ACL WebVPN được xác định nhưng không phù hợp một gói tin nào đó,mặc định gói tin đó sẽ bị loại bỏ. Mặc khác, nếu không có ACL xác định,các thiết bị bảo mật sẽ cho phép lưu thông qua nó. ACL xác định lưu lượng truy cập bằng cách cho phép hoặc loại bỏ gói tin khi nó cố gắng đi qua thiết bị bảo mật. Một ACE đơn giản là cho phép tất cả các địa chỉ IP truy cập từ một mạng này đến mạng khác, phức tạp hơn là nó cho phép lưu thông từ một địa chỉ IP cụ thể ở một cổng riêng biệt đến một cổng khác ở địa chỉ đích. Một ACE được thiết kế bằng cách sử dụng các lệnh điều khiển truy cập để thiết lập cho thiết bị bảo mật.

2.4.3.2 Lọc nội dung và URL

Theo truyền thống firewall chặn các gói dữ liệu bằng cách kiểm tra thông tin gói ở layer 3 hoặc Layer 4. Cisco ASA có thể nâng cao chức năng này bằng cách kiểm tra nội dung thông tin một vài giao thức ở layer 7 như HTTP, HTTPS, và FTP. Căn cứ vào chính sách bảo mật của một tổ chức, các thiết bị an ninh có thể cho phép hoặc chặn các packet chứa nội dụng không cho phép. Cisco ASA hỗ trợ hai loại lớp ứng dụng lọc: Content Filtering và URL Filtering

- **Content Filtering**

Việc kích hoạt Java hoặc ActiveX trong môi trường làm việc có thể khiến người dùng dễ dàng tải về tập tin thực thi độc hại có thể gây ra mất mát các tập tin hoặc hư hại các tập tin trong môi trường sử dụng.

Một chuyên gia an ninh mạng có thể vô hiệu hoá Java và xử lý ActiveX trong trình duyệt, nhưng điều này không phải là một giải pháp tốt nhất.

Có thể chọn một cách khác là sử dụng một thiết bị mạng như Cisco ASA để loại bỏ các nội dung độc hại từ các gói tin. Sử dụng tính năng lọc nội dung cục bộ, các thiết bị an ninh có thể kiểm tra các tiêu đề HTTP và lọc ra các ActiveX và Java applet khi các gói dữ liệu cố gắng đi qua từ máy không tin cậy. Cisco ASA có thể phân biệt giữa các applet tin cậy và applet không tin cậy. Nếu một trang web đáng tin cậy gửi Java hoặc ActiveX applet các thiết bị bảo mật có thể chuyển đến các máy chủ yêu cầu kết nối. Nếu các applet được gửi từ các máy chủ web không tin cậy, thiết bị bảo mật có thể sửa đổi nội dung và loại bỏ các đính kèm từ các gói tin. Bằng cách này, người dùng cuối không phải quyết định đến các applet được chấp nhận hoặc từ chối. Họ có thể tải về bất kỳ applet mà không phải lo lắng.

- **URL Filtering**

ActiveX có thể gây ra vấn đề tiềm năng nguy hại trên các thiết bị mạng nếu mã độc ActiveX được tải về trên máy. Các mã ActiveX được đưa vào các trang web bằng cách sử dụng thẻ HTML <OBJECT> và </ OBJECT>. Các thiết bị an ninh tìm kiếm các thẻ cho lưu lượng có nguồn gốc trên một cổng cấu hình sẵn. Nếu các thiết bị an ninh phát hiện các thẻ này, nó thay thế chúng bằng các thẻ chú thích <!-- and -->. Khi trình duyệt nhận được các gói dữ liệu HTTP với <!-- and -->, nó bỏ qua các nội dung thực tế bằng cách giả sử rằng nội dung là ý kiến của tác giả.

Lưu ý: các thiết bị an ninh không thể nhận ra các thẻ HTML nếu chúng được phân chia giữa nhiều gói mạng.

2.4.3.3 Chuyển đổi địa chỉ

- **Network Address Translation**

NAT hay còn gọi là Network Address Translation là một kĩ thuật được phát minh lúc khởi đầu dùng để giải quyết vấn đề IP shortage, nhưng dần dần nó chứng tỏ nhiều ưu điểm mà lúc phát minh ra nó người ta không nghĩ tới, một trong những lợi điểm của NAT ngày nay được ứng dụng nhiều nhất là NAT cho phép:

- Chia sẻ kết nối Internet với nhiều máy bên trong LAN với một địa chỉ IP của WAN

- Firewall, nó giúp dấu tất cả IP bên trong LAN với thế giới bên ngoài, tránh sự dòm ngó của hackers.
- Tính linh hoạt và sự dễ dàng trong việc quản lý
- NAT giúp cho các home user và các doanh nghiệp nhỏ có thể tạo kết nối với internet một cách dễ dàng và hiệu quả cũng như giúp tiết kiệm vốn đầu tư.

NAT giống như một router, nó chuyển tiếp các gói tin giữa những lớp mạng khác nhau trên một mạng lớn. NAT dịch hay thay đổi một hoặc cả hai địa chỉ bên trong một gói tin khi gói tin đó đi qua một router, hay một số thiết bị khác. Thông thường, NAT thường thay đổi địa chỉ (thường là địa chỉ riêng) được dùng bên trong một mạng sang địa chỉ công cộng.

NAT cũng có thể coi như một firewall cơ bản. Để thực hiện được công việc đó, NAT duy trì một bảng thông tin về mỗi gói tin được gửi qua. Khi một PC trên mạng kết nối đến một website trên Internet, header của địa chỉ IP nguồn được thay đổi và thay thế bằng địa chỉ IP Public mà đã được cấu hình sẵn trên NAT server, sau khi có gói tin trở về NAT dựa vào bảng record mà nó đã lưu về các gói tin, thay đổi địa chỉ IP đích thành địa chỉ của PC trong mạng và chuyển tiếp đi. Thông qua cơ chế đó quản trị mạng có khả năng lọc các gói tin được gửi đến hay gửi từ một địa chỉ IP và cho phép hay cấm truy cập đến một port cụ thể.

- **NAT tĩnh**

Với NAT tĩnh, địa chỉ IP thường được ánh xạ tĩnh với nhau thông qua các lệnh cấu hình. Trong NAT tĩnh, một địa chỉ Inside Local luôn luôn được ánh xạ vào địa chỉ Inside Global. Nếu được sử dụng, mỗi địa chỉ Outside Local luôn luôn ánh xạ vào cùng địa chỉ Outside Global. NAT tĩnh không tiết kiệm địa chỉ thực.

Mặc dù NAT tĩnh không giúp tiết kiệm địa chỉ IP, cơ chế NAT tĩnh cho phép một máy chủ bên trong hiện diện ra ngoài Internet, bởi vì máy chủ sẽ luôn dùng cùng một địa chỉ IP thực.

Cách thức thực hiện NAT tĩnh thì dễ dàng vì toàn bộ cơ chế dịch địa chỉ được thực hiện bởi một công thức đơn giản:

Địa chỉ đích = Địa chỉ mạng mới OR (địa chỉ nguồn AND (NOT netmask))

- **NAT động**

NAT động phức tạp hơn NAT tĩnh, vì thế chúng phải lưu giữ lại thông tin kết nối và thậm chí tìm thông tin của TCP trong packet, dùng nó thay cho NAT tĩnh vì mục đích bảo mật. Từ bên ngoài không thể tìm được IP nào kết nối với host chỉ định vì tại thời điểm tiếp theo host này có thể nhận một IP hoàn toàn khác.

Những kết nối từ bên ngoài thì chỉ có thể tìm được địa chỉ IP khi những host này vẫn còn nắm giữ một IP trong bảng NAT động. Nơi mà NAT router lưu giữ những thông tin về IP bên trong (IP nguồn) được liên kết với NAT-IP (IP đích).

Cấu hình dynamic NAT trên thiết bị Cisco ASA: Lệnh *NAT* xác định máy chủ nội bộ sẽ được dịch, và lệnh *global* xác định các pool địa chỉ trên outgoing interface.

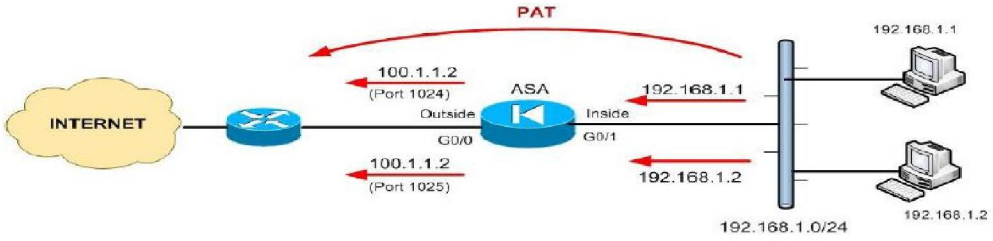
ciscoasa(config)# nat (internal_interface_name) "nat-id" "internal network IP subnet"

ciscoasa(config)# global (external_interface_name) "nat-id" "external IP pool range"

- **Port Address Translation (PAT)**

PAT dùng để ánh xạ nhiều địa chỉ IP riêng sang một địa chỉ công cộng vì mỗi địa chỉ riêng được phân biệt bằng số port. Có tới 65, 356 địa chỉ nội bộ có thể chuyển đổi sang một địa chỉ công cộng, nhưng thực tế thì chỉ có khoảng 4000 port có thể chuyển đổi sang một địa chỉ công cộng. PAT hoạt động bằng cách đánh dấu một số dòng lưu lượng TCP hoặc UDP từ nhiều máy cục bộ bên trong xuất hiện như cùng từ một hoặc một vài địa chỉ Inside Global. Và bởi vì các trường của cổng có chiều dài 16 bit, mỗi địa chỉ Inside Global có thể hỗ trợ lên đến 65,000 kết nối TCP và UDP đồng thời.

Ví dụ:



Hình 2-6: Mô tả cơ chế PAT (NAT overload)

asa(config)# nat (inside) 1 192.168.1.0 255.255.255.0 ←Inside Subnet to use PAT

asa(config)# global (outside) 1 100.1.1.2 netmask 255.255.255.255 ←Use a single global IP address for PAT

- ***Mối quan hệ giữa NAT và PAT:***

- PAT có mối quan hệ gần gũi với NAT nên vẫn thường được gọi là NAT. Trong NAT, nhìn chung chỉ địa chỉ IP được đổi có sự tương ứng 1:1 giữa địa chỉ riêng và địa chỉ công cộng.
- Trong PAT cả địa chỉ riêng của người gửi và cổng đều được thay đổi. Thiết bị PAT sẽ chọn số cổng mà các hosts trên mạng công cộng sẽ nhìn thấy.
- Trong NAT những gói tin từ ngoài mạng vào được định tuyến tới địa chỉ IP đích của nó trên mạng riêng bằng cách tham chiếu địa chỉ nguồn đi vào.
- Trong PAT chỉ có một địa chỉ IP công cộng được nhìn thấy từ bên ngoài và gói tin đi vào từ mạng công cộng được định tuyến tới đích của chúng trên mạng riêng bằng cách tham chiếu tới bảng quản lý từng cặp cổng private và public lưu trong thiết bị PAT. Cái này thường được gọi là connection tracking (truy vất kết nối).
- Một số thiết bị cung cấp NAT như broadband routers, thực tế cung cấp PAT nên có sự nhầm lẫn đáng kể giữa các thuật ngữ. Nhìn chung người ta sử dụng NAT để bao gồm những thiết bị PAT.

2.4.4. Giao thức định tuyến

Một số thực hành giao thức định tuyến tốt nhất cho các ASA:

Đối với các mạng nhỏ, chỉ sử dụng định tuyến tĩnh. Sử dụng định tuyến tĩnh mặc định chỉ là địa chỉ gateway kết nối với outside interface (thường là Internet), và cũng sử dụng các định tuyến tĩnh cho các mạng nội bộ có nhiều hơn 1 hop (tức là không kết nối trực tiếp).

Bất kỳ mạng được kết nối trực tiếp vào một ASA interface không cần bất kỳ cấu hình định tuyến tĩnh nào, firewall ASA sẽ làm những việc này.

Nếu ASA là kết nối trên vành đai của mạng (tức là biên giới giữa các mạng đáng tin cậy và không tin cậy), thì xác định một kết nối mặc định đối với các mạng bên ngoài không đáng tin cậy, và sau đó cấu hình định tuyến tĩnh cụ thể đối với các mạng nội bộ.

Nếu ASA là nằm bên trong một mạng rộng lớn với các tuyến đường mạng nội bộ nhiều, thì sử dụng cấu hình một giao thức định tuyến động.

Các kỹ thuật định tuyến:

- **Định tuyến tĩnh**

Có 3 loại định tuyến tĩnh:

- Directly Connected Route: các đường kết nối trực tiếp được tự động tạo ra trong bảng định tuyến ASA khi bạn cấu hình một địa chỉ IP trên một giao diện thiết bị
- Normal Static Route: cung cấp đường đi cố định về một mạng cụ thể nào đó.
- Default Route: Default route là tuyến đường mặc định được cấu hình tĩnh của router là nơi mà khi router nhận được một gói tin cần chuyển đến mạng nào đó mà mạng đó không có trong bảng định tuyến của router đó thì nó sẽ đẩy ra default route.

- **Định tuyến động**

- Giao thức định tuyến RIP

RIP là một trong các giao thức định tuyến động cũ nhất. Mặc dù nó không được sử dụng rộng rãi trong các mạnghiện nay, bạn vẫn tìm thấy nó trong một số trường hợp. CiscoASA phiên bản7.x hỗ trợ RIP một cách hạn chế. Các thiết bị ASA (v7.x) chỉ có thể chấp nhận các tuyến RIP và tùy chọn quảng cáo cho static route. Tuy nhiên, nó không có thể nhận được RIP quảng bá từ một mạng hàng xóm và sau đó quảng bá route cho mạng hàng xóm khác. Tuy nhiên từ ASA phiên bản 8.x, các thiết bị bảo mật hỗ trợ đầy đủ chức năng RIP. Cả hai RIPv1 và RIPv2 được hỗ trợ. Tuy nhiên, bằng cách sử dụng RIPv1 là không được khuyến khích bởi vì nó không hỗ trợ định tuyến cập nhật xác thực.

- Giao thức định tuyến OSPF

OSPF (Open Shortest Path First) là một giao thức định tuyến động dựa trên Link States chứ không phải là Distance Vectors (chẳng hạn như RIP) để lựa chọn đường đi tối ưu. Nó là một giao thức định tuyến tốt hơn và khả năng mở rộng hơn so với RIP, đó là lý do tại sao được sử dụng rộng rãi trong các mạng doanh nghiệp lớn. OSPF có thể rất phức tạp và người ta có thể viết cả một cuốn sách cho nó.

- Giao thức định tuyến EIGRP

EIGRP là phiên bản nâng cao của IGRP cũ.Nó là một giao thức độc quyền của Cisco mà chỉ chạy giữa các thiết bị Cisco. Hỗ trợ cho EIGRP trên Cisco ASA đã có từ phiên bản 8.0 trở đi.Mặc dù EIGRP rất dễ sử dụng và linh hoạt, thiết kế mạng và quản trị viên ngần ngại sử dụng nó rộng rãi kể từ khi nó chỉ làm việc với thiết bị Cisco, vì vậy chỉ phụ thuộc vào một nhà cung cấp duy nhất. (Lưu ý: IPv6 được hỗ trợ trên Cisco ASA chạy EIGRP).

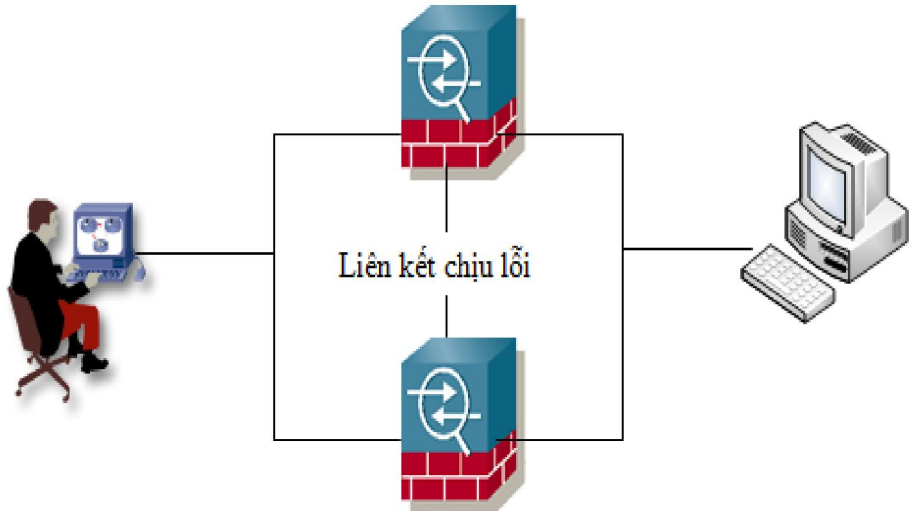
2.4.5. Khả năng chịu lỗi và dự phòng

2.4.5.1 Kiến trúc chịu lỗi

Khi hai ASA được thiết lập trong chế độ failover, một Cisco ASA ở chế độ active có trách nhiệm tạo ra trạng thái, chuyển đổi địa chỉ, chuyển giao các gói dữ liệu và giám sát các hoạt động khác, một ASA khác ở chế độ chờ(standby) có trách nhiệm theo dõi tình trạng chế độ active. Chế độ chủ động và chế độ chờ trao đổi thông tin chịu lỗi với nhau thông qua một đường link kết nối được biết như là một liên kết chịu lỗi (link failover). Khi có sự cố xảy ra trên chế độ chủ động thì chế độ chờ sẽ thực hiện vai trò của chế độ chủ động cho đến khi chế độ chủ động khôi phục lại trạng thái.

Đường chịu lỗi giữa hai ASA trao đổi các thông tin:

- Trạng thái chủ động hoặc trạng thái chờ
- Trạng thái liên kết mạng
- Thông điệp hello
- Trao đổi địa chỉ MAC
- Cấu hình đồng bộ hóa



Hình 2-7: Minh họa liên kết chịu lỗi

2.4.5.2 Điều kiện kích hoạt khả năng chịu lỗi

Khả năng chịu lỗi xảy ra khi

- Người quản trị thiết lập chuyển đổi từ chế độ chủ động sang chế độ chờ
- Khi ASA đang đảm nhiệm ở chế độ chờ không nhận được gói tin keepalive từ chế độ chủ động, sau hai lần không thấy liên lạc từ chế độ chủ động thì chế độ chờ coi chế độ chủ động đã bị lỗi và chuyển sang đóng vai trò như chế độ chủ động cho đến khi chế độ chủ động hoạt động trở lại.
- Khi một liên kết trên một cổng nhận được lệnh down .
- Kiểm tra trạng thái của cổng chịu lỗi

Để biết được trạng thái chịu lỗi thông qua liên kết chế độ chủ động và chế độ chờ trao đổi thông điệp hello 15 giây một lần.Thông diệp hello bao gồm các trạng thái hoạt động của các liên kết được cấu hình.Trước khi chuyển sang từ chế độ chờ sang chủ động ASA kiểm tra bốn trạng thái sau :

- Kiểm tra trạng thái up/down trên từng cổng nếu không hoạt động sẽ xử lý quá trình chịu lỗi.
- Kiểm tra sự hoạt động của hệ thống nếu sau năm giây mà không nhận được bất kỳ gói tin nào sẽ chuyển sang chế độ chịu lỗi bắt đầu.

- Kiểm tra sự hoạt động của hệ thống bằng cách gửi gói ARP, sau năm giây không nhận được tín hiệu trả lời xem như cổng đó bị lỗi và xủ lý quá trình chịu lỗi.
- Kiểm tra sự hoạt động của hệ thống bằng cách ping broadcast thử nghiệm nếu sau năm giây không nhận được tín hiệu trả lời xem như cổng đó bị lỗi và xử lý quá trình chịu lỗi.

2.4.5.3 Trạng thái chịu lỗi

Khi kết nối được thiết lập thông qua Cisco ASA, Cisco ASA sẽ cập nhật bảng kết nối. Trong mục kết nối bao gồm: địa chị nguồn, địa chỉ đích, giao thức, trạng thái kết nối gắn với interface nào và số byte truyền. Tùy thuộc vào cấu hình failover, Cisco ASA có một trong những trạng thái sau đây:

Stateless failover: Duy trì kết nối nhưng không đồng bộ với trạng thái chờ. Trong trường hợp này trạng thái hoạt động sẽ không gửi các bảng cập nhật trạng thái cho chế độ chờ.Khi trạng thái hoạt động bị lỗi thì trạng thái chờ sẽ được kích hoạt và phải thiết lập lại các kết nối,tất cả các lưu lượng đều bị phá vỡ.

Stateful failover: Duy trì kết nối và đồng bộ với chế độ chờ. Ở trường hợp này các trạng thái kết nối đều được đồng bộ từ trạng thái hoạt động sang trạng thái chờ và khi trạng thái chờ được kích hoạt sẽ không phải thiết lập lại các bảng kết nối vì đã tồn tại trong cơ sở dữ liệu của nó.

2.4.6. Quản lý chất lượng dịch vụ

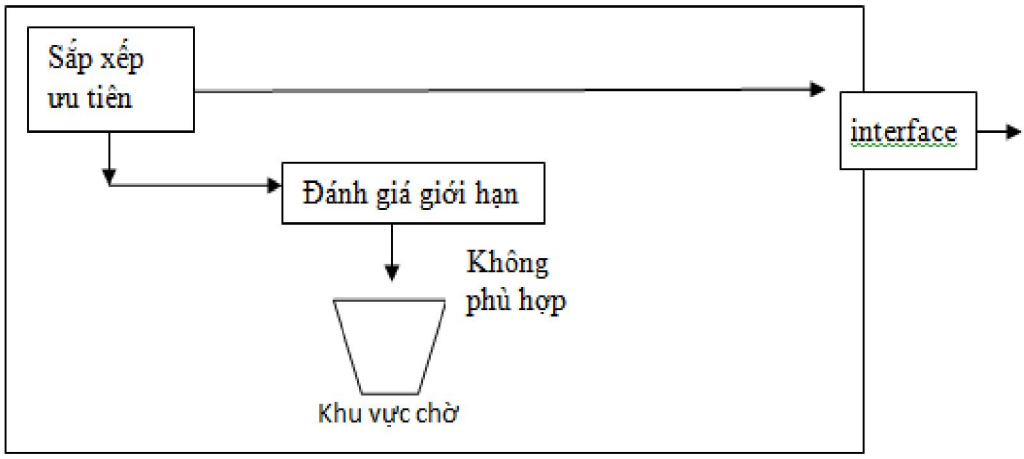
Trong một mạng IP chuẩn, tất cả các gói dữ liệu được xử lý giống nhau theo một cách tốt nhất. Các thiết bị mạng thường bỏ qua tầm quan trọng và thời gian của các dữ liệu được truyền qua mạng. Để ưu tiên cho các gói dữ liệu quan trọng hay đáp ứng được thời gian thực, gói thoại và video áp dụng chính sách quản lý chất lượng dịch vụ cho từng loại gói .Có nhiều cơ chế quản lý dịch vụ khác nhau mà có sẵn trong các thiết bị của cisco như:

- Traffic policing
- Traffic prioritization
- Traffic shaping
- Traffic marking

Tuy nhiên cisco ASA chỉ hỗ trợ hai loại là traffic policing và traffic prioritization.

2.4.6.1 Traffic policing

Chính sách lưu lượng được biết như là sự giới hạn lưu lượng cho phép kiểm soát tốc độ tối đa đủ điều kiện để đi qua interface. Các lưu lượng nào nằm trong cấu hình qui định thì được phép thông qua và các lưu lượng vượt ngưỡng giới hạn đều bị đánh rớt hết. Trong Cisco ASA khi một lưu lượng không được định nghĩa ưu tiên sẽ được xử lý thông qua đánh giá giới hạn gói tin. Nếu phù hợp với mức cấu hình QoS thì cho phép truyền; nếu không đủ mức cho phép, gói tin sẽ chờ bổ sung hoặc điều chỉnh chính sách cho phép thấp xuống; nếu phù hợp với cấu hình gói tin sẽ được đưa vào hàng đợi không ưu tiên "nonpriority".



Hình 2-8: Gói tin đi qua các công cụ QoS.

Khi rời khỏi cơ chế QoS, gói tin sẽ được chuyển đến interface cho việc chuyển đổi dữ liệu. Thiết bị an ninh thực hiện QoS cho mỗi gói mức độ khác nhau để đảm bảo cho việc truyền nhận mà gói tin không có trong danh sách ưu tiên. Quá trình xử lý gói tin dựa vào độ sâu của hàng đợi ưu tiên thấp và các điều kiện của vòng truyền. Vòng truyền sẽ có không gian bộ đệm được thiết bị sử dụng để giữ các gói tin trước khi truyền chúng cho các cấp độ điều khiển.

Nếu có tắc nghẽn xảy ra thì các gói tin trong hàng đợi được chuyển xuống hàng đợi ưu tiên thấp cho tới khi gói tin ở hàng đợi ưu tiên cao trống, nếu hàng đợi ưu tiên cao có lưu lượng truy cập thì sẽ được phục vụ trước. Thông qua việc giới hạn lưu lượng, thiết bị thực hiện một cơ chế nhỏ giọt khi gói tin không phù hợp với thông tin cấu hình QoS.Cisco ASA ghi lại sự kiện này thông qua máy chủ lưu trữ syslog hoặc trên thiết bị.

2.4.6.2 Traffic Prioritization

Trên thiết bị an ninh Cisco ASA, hai loại ưu tiên được hỗ trợ là "priority" và "nonpriority". Priority có nghĩa là gói tin được ưu tiên trong lưu lượng truy cập thường xuyên, trong khi nonpriority là các gói dữ liệu được xử lý bởi các giới hạn lưu lượng.

Khi traffic được phân loại là ưu tiên, nó sẽ được nhanh chóng chuyển tiếp mà không thông qua các giới hạn về lưu lượng. Traffic sau đó được gắn cờ và chuyển vào những hàng đợi ưu tiên truyền ra ngoài khỏi thiết bị. Để đảm bảo việc chuyển tiếp lưu lượng được ưu tiên ở các interface, thiết bị an ninh sẽ đánh dấu trên mỗi hàng đợi ưu tiên và gửi chúng ra truyền trực tiếp, nếu có tắc nghẽn các lưu lượng đưa vào trong hàng đợi ưu tiên cao và được truyền đi ngay khi vòng truyền sẵn sàng.

2.4.7. Phát hiện xâm nhập

Đối với hệ thống an ninh, hệ thống phát hiện xâm nhập (IDS) là thiết bị cố gắng phát hiện ra kẻ tấn công truy cập trái phép vào mạng hay một máy chủ để tạo ra sự cố rớt mạng hoặc để ăn cắp thông tin. IDS cũng phát hiện tấn công DDoS, worm và đợt bùng phát virus. Số lượng và sự phức tạp của các mối đe dọa an ninh đã tăng vọt trong những năm gần đây. Để đạt được hiệu quả an ninh mạng, hệ thống chống xâm nhập rất quan trọng cần phải duy trì ở mức độ cao. Thận trọng, an toàn, tránh rủi ro, giảm chi phí thiệt hại, tránh sự gián đoạn của hệ thống nên thiết bị tường lửa ASA của Cisco hỗ trợ hai loại hệ thống phát hiện xâm nhập khác nhau:

- Network-based intrusion detection systems (NIDS).
- Host-based intrusion detection systems(HIDS).

2.4.7.1 Network-based intrusion detection systems

Đối với hệ thống mạng các hệ thống phát hiện xâm nhập được thiết kế để xác định chính xác, phân loại và bảo vệ tối đa để chống lại mối đe dọa nhắm vào hệ thống. Những mối đe dọa bao gồm worm , tấn công DoS và phát hiện bất kỳ lỗ hổng … Một số phương pháp phát hiện được triển khai rộng rãi với các đặc diểm sau:

- Trạng thái và ghi lại mẫu trạng thái
- Phân tích giao thức
- Phân tích dựa trên sự bình thường
- Phân tích dựa trên sự bất thường

Hệ thống IDS dựa trên mạng sử dụng bộ dò và bộ cảm biến cài đặt trên toàn mạng. Những bộ dò này theo dõi trên mạng nhằm tìm kiếm những lưu lượng trùng với những mô tả sơ lược được định nghĩa là những dấu hiệu. Bộ cảm biến thu nhận và phân tích lưu lượng trong thời gian thực. Khi ghi nhận được một mẫu lưu lượng hay dấu hiệu, bộ cảm biến gửi tín hiệu cảnh báo đến trạm quản trị và có thể được cấu hình nhằm tìm ra biện pháp ngăn chặn những xâm nhập xa hơn. NIDS là tập nhiều sensor được đặt ở toàn mạng để theo dõi những gói tin trong mạng so sánh với với mẫu đã được định nghĩa để phát hiện đó là tấn công hay không.

NIDS được đặt giữa kết nối hệ thống mạng bên trong và mạng bên ngoài để giám sát toàn bộ lưu lượng vào ra. Có thể là một thiết bị phần cứng riêng biệt được thiết lập sẵn hay phần mềm cài đặt trên máy tính. Chủ yếu dùng để đo lưu lượng mạng được sử dụng. Tuy nhiên có thể xảy ra hiện tượng nghẽn khi lưu lượng mạng hoạt động ở mức cao.

- **Lợi thế của NIDS**
  - Quản lý cả network segment (gồm nhiều host)
  - Trong suốt với người sử dụng lẫn kẻ tấn công
  - Cài đặt và bảo trì đơn giản, không ảnh hưởng tới mạng
  - Tránh DOS ảnh hưởng tới một host nào đó.
  - Có khả năng xác định lỗi ở tầng Network (trong mô hình OSI)
  - Độc lập với hệ điều hành
- **Hạn chế của NIDS**
  - Có thể xảy ra trường hợp báo động giả (false positive), tức không có intrusion mà NIDS báo là có intrusion.
  - Không thể phân tích các traffic đã được mã hóa (vd: SSL, SSH, IPSec…)
  - NIDS đòi hỏi phải được cập nhật các signature mới nhất để thực sự an toàn. Có độ trễ giữa thời điểm bị tấn công với thời điểm phát báo động. Khi báo động được phát ra, hệ thống có thể đã bị tổn hại.
  - Không cho biết việc tấn công có thành công hay không.
  - Một trong những hạn chế là giới hạn băng thông. Bộ dò mạng phải nhận tất cả các lưu lượng mạng, sắp xếp lại những lưu lượng đó cũng như phân tích chúng. Khi tốc độ mạng tăng lên thì khả năng của đầu dò cũng vậy.

Một giải pháp là bảo đảm cho mạng được thiết kế chính xác để cho phép sự sắp đặt của nhiều đầu dò. Khi mà mạng phát triển, thì càng nhiều đầu dò được lắp thêm vào để bảo đảm truyền thông và bảo mật tốt nhất.

- Một cách mà kẻ xâm nhập cố gắng thực hiện nhằm che đậy cho hoạt động của họ khi gặp hệ thống IDS là phân mảnh những gói thông tin của họ. Mỗi giao thức có một kích cỡ gói dữ liệu giới hạn, nếu dữ liệu truyền qua mạng lớn hơn kích cỡ này thì gói dữ liệu đó sẽ được phân mảnh. Phân mảnh đơn giản chỉ là quá trình chia nhỏ dữ liệu ra những mẫu nhỏ. Thứ tự của việc sắp xếp lại không thành vấn đề miễn là không xuất hiện hiện tượng chồng chéo. Nếu có hiện tượng phân mảnh chồng chéo, bộ cảm biến phải biết quá trình tái hợp lại cho đúng. Nhiều hacker cố gắng ngăn chặn phát hiện bằng cách gửi nhiều gói dữ liệu phân mảnh chồng chéo. Một bộ cảm biến sẽ không phát hiện các hoạt động xâm nhập nếu bộ cảm biến không thể sắp xếp lại những gói thông tin một cách chính xác.

2.4.7.2 Host-based intrusion detection systems

Bằng cách cài đặt một phần mềm trên tất cả các máy tính chủ, IDS dựa trên máy chủ quan sát tất cả những hoạt động hệ thống như các file log và những lưu lượng mạng thu thập được. Hệ thống dựa trên máy chủ cũng theo dõi OS, những cuộc gọi hệ thống, lịch sử sổ kiểm tra (audit log) và những thông điệp báo lỗi trên hệ thống máy chủ. Trong khi những đầu dò của mạng có thể phát hiện một cuộc tấn công, thì chỉ có hệ thống dựa trên máy chủ mới có thể xác định xem cuộc tấn công có thành công hay không. Thêm nữa là, hệ thống dựa trên máy chủ có thể ghi nhận những việc mà người tấn công đã làm trên máy chủ bị tấn công (compromised host).

Không phải tất cả các cuộc tấn công được thực hiện qua mạng. Bằng cách giành quyền truy cập ở mức vật lý (physical access) vào một hệ thống máy tính, kẻ xâm nhập có thể tấn công một hệ thống hay dữ liệu mà không cần phải tạo ra bất cứ lưu lượng mạng (network traffic) nào cả. Hệ thống dựa trên máy chủ có thể phát hiện các cuộc tấn công mà không đi qua đường công cộng hay mạng được theo dõi, hay thực hiện từ cổng điều khiển (console), nhưng với một kẻ xâm nhập có hiểu biết, có kiến thức về hệ IDS thì hắn có thể nhanh chóng tắt tất cả các phần mềm phát hiện khi đã có quyền truy cập vật lý.

Một ưu điểm khác của IDS dựa trên máy chủ là nó có thể ngăn chặn các kiểu tấn công dùng sự phân mảnh hoặc TTL. Vì một host phải nhận và tái hợp các phân mảnh khi xử lí lưu lượng nên IDS dựa trên host có thể giám sát chuyện này.

HIDS thường được cài đặt trên một máy tính nhất đinh. Thay vì giám sát hoạt động của một network segment, HIDS chỉ giám sát các hoạt động trên một máy tính. HIDS thường được đặt trên các host xung yếu của tổ chức, và các server trong vùng DMZ - thường là mục tiêu bị tấn công đầu tiên. Nhiệm vụ chính của HIDS là giám sát các thay đổi trên hệ thống, bao gồm:

- Các tiến trình.
- Các mục của Registry.
- Mức độ sử dụng CPU.
- Kiểm tra tính toàn vẹn và truy cập trên hệ thống file.
- Một vài thông số khác.

Các thông số này khi vượt qua một ngưỡng định trước hoặc những thay đổi khả nghi trên hệ thống file sẽ gây ra báo động.

- **Lợi thế của HIDS**
  - Có khả năng xác định user liên quan tới một sự kiện (event).
  - HIDS có khả năng phát hiện các cuộc tấn công diễn ra trên một máy, NIDS không có khả năng này.
  - Có thể phân tích các dữ liệu mã hoá.
  - Cung cấp các thông tin về host trong lúc cuộc tấn công diễn ra trên host này.
- **Hạn chế của HIDS**
  - Thông tin từ HIDS là không đáng tin cậy ngay khi sự tấn công vào ASA thành công.
  - Khi tường lửa ASA bị "hạ" do tấn công, đồng thời HIDS cũng bị "hạ".
  - HIDS phải được thiết lập trên từng host cần giám sát.
  - HIDS không có khả năng phát hiện các cuộc dò quét mạng (Nmap, Netcat…).

- HIDS cần tài nguyên trên host để hoạt động.
- HIDS có thể không hiệu quả khi bị DOS.

2.4.8. Một vài chức năng khác

- SPF là cơ chế theo dõi trạng thái kết nối, thực hiện việc chuẩn hóa giao thức TCP, việc kiểm tra sự phù hợp và việc thương lượng động giữa các phiên.
- AIC cho phép phân tích các giao thức ở tầng 7 và theo dõi trạng thái kết nối và đảm bảo chúng phù hợp giao thức chuẩn.
- Session auditing: các record sẽ được tạo ra cho các phiên người dùng, và các phiên kết nối ở tầng 7.
- Security services modules: nền tảng ASA hỗ trợ nhiều module SSM gồm các thiết bị phần cứng chuyên dùng có tính năng bảo mật giúp giảm tải công việc cho bộ vi xử lý. Một ASA có thể cắm một module SSM nhằm giảm tải công việc của IPS hay cung cấp dịch vụ bảo mật.
- Reputation-based botnet traffic filtering: ASA có thể phát hiện và lọc traffic liên quan đến botnet. Cơ sở dữ liệu của botnet traffic filter được Cisco cập nhật thường xuyên.
- Cryptographic unified communications proxy: ASA phải được cấu hình với vai trò UC proxy được ủy quyền để cho phép traffic đi qua. ASA có thể ngưng hay chuyển tiếp các phiên UC được mã hóa giữa client và server.
- Denial-of-service prevention: ASA có tính năng kiểm soát traffic như chuẩn hóa các giao thức, áp đặt chính sách và kiểm soát các tần suất kết nối để hạn chế bị tấn công DoS.
- Traffic correlation: tính năng nhận diện mối đe dọa và sự tương quan giữa các traffic từ nhiều phiên kết nối khác nhau cho phép phát hiện và ngăn chặn những bất thường xuất phát từ các cuộc tấn công mạng và hành vi thăm dò.
- Remote access VPN: ASA hỗ trợ người dùng từ bên ngoài Internet kết nối VPN có mã hóa vào mạng bên trong. Clientless SSL VPN được dùng để kết nối VPN có mã hóa qua giao diện web mà không cần chương trình hỗ trợ nhưng rất hạn chế về tính năng cho nên đề nghị người dùng nên

dùng chương trình VPN client để kết nối VPN có mã hóa SSL hay IPSec với đầy đủ tính năng.

- Site-to-site VPN: ASA hỗ trợ IPSec VPN giữa các site, mô hình này thường được xây dựng trên firewall biên hay router biên.
- High availability failover clustering: hai ASA cùng dòng có thể được cấu hình lỗi dự phòng trong trường hợp lỗi phần cứng.
- Redundant interfaces: nhằm gia tăng tính luôn sẵn sàng với ASA đơn lẻ, các cổng interface có thể được cấu hình dự phòng để ASA này thay thế ASA khác trong trường hợp lỗi cổng interface vật lý.
- Etherchannel: một bó các cổng interface có thể được gom nhóm lại thành một cổng logic đơn lẻ. Bằng việc kết nối cổng etherchannel giữa ASA và switch có thể cân bằng băng thông và một số các dự phòng khác.
- Traffic and policy virtualization: ASA có thể hoạt động với đa thực thể ảo virtual instance hay còn gọi là security context, mỗi thực thể ảo là một firewall độc lập trong đó có các cổng interface logic riêng, các chính sách bảo mật riêng.
- Rich IP routing functionality: ASA có thể chuyển tiếp traffic vào mạng nội bộ qua các cổng interface mà không có bất kỳ thông tin định tuyến nào thêm. ASA hỗ trợ định tuyến tĩnh và các giao thức định tuyến động như RIPv1, RIPv2, EIGRP, OSPF.
- Transparent (bridge) operation: ASA có thể cấu hình và hoạt động như một transparent firewall, một cầu nối bảo mật giữa các cổng interface, với transparent mode, ASA có thể được thêm vào hệ thống mạng và không cần phải đặt lại địa chỉ IP.
- Integrated DHCP, DNS and PPPoE: ASA có thể cấu hình với vai trò là DHCP client hay PPPoE client để nhận địa chỉ IP động và giữ vai trò DNS client động để ghi nhận thông tin phân giải từ hostname sang địa chỉ IP. Ngoài ra, ASA còn giữ vai trò DHCP server để cấp phát địa chỉ IP động.
- IPv6 support: hỗ trợ IPv6.
- IP multicast support: ASA hỗ trợ giao thức multicast như IGMP và PIM để điều khiển IP multicast traffic.

- Management control and protocols: ASA hỗ trợ nhiều cách thức quản lý khác nhau như dùng cổng console, TELNET, SSH, HTTPS và SNMP.
- Simple software management: ASA hỗ trợ cập nhật phần mềm qua file cục bộ hay truyền tải file, việc cập nhật được thực hiện tự động hay thủ công.
- Configuration flexibility and scalabiliy: chính sách bảo mật và các quy luật được cấu hình bằng việc tái sử dụng các đối tượng object. Thông qua modular policy framework, các tính năng bảo mật có thể được cấu hình và triển khai một cách linh hoạt.
- Cisco security management suite: bộ công cụ giúp quản lý ASA một cách để dàng với giao diện đồ họa.

2.5. Kết luận chương 2

Chương 2 đã tìm hiểu kĩ hơn về một hệ thống firewall riêng biệt đó là hệ thống firewall ASA. Cisco ASA viết tắt của từ: Cisco Adaptive Security Appliance. ASA là một giải pháp bảo mật đầu cuối chính của Cisco. Cisco ASA có tất cả 6 model, phù hợp với tất hả hệ thống doanh nghiệp vừa và nhỏ hay các nhà cung cấp dịch vụ.

Cisco ASA cung cấp tất cả các giải pháp an ninh mạng trong một sản phẩm duy nhất như: Quản lý file, điều khiển truy cập mạng, cung cấp các giao thức định tuyến, phát hiện xâm nhập, khả năng chịu lỗi và dự phòng. Cisco ASA luôn cảnh giác với các cuộc tấn công và thống báo cho người quản trị trong thời gian thực. Cisco ASA tự động tránh xa các thiết bị mà nó nhận diện được là mã độc. Ngoài ra, Cisco ASA hỗ trợ gói reassembly cho phép tìm kiếm các cuộc tấn công được ẩn trên một loạt các gói dữ liệu bị phân mảnh. Cisco ASA còn cung cấp giải pháp VPN sitetosite và VPN remote access. Một trong những lợi thế lớn nhất của Cisco ASA là tiết kiệm chi phí và tăng hiệu suất hoạt động của hệ thống.

CHƯƠNG 3
THIẾT KẾ VÀ XÂY DỰNG MÔ PHỎNG HỆ THỐNG FIREWALL ASA

3.1. Đặt vấn đề

3.1.1. Nhu cầu bảo mật

Đối với hệ thống mạng hiện tại, nguy cơ bị mất mát dữ liệu là rất lớn. Nguy cơ này có thể đến từ hai hướng: bên ngoài Internet và ngay nội bộ hệ thống mạng.

- **Nguy cơ mất mát thông tin từ ngoài Internet**: hệ thống mạng hiện tại đều kết nối đến Internet, nhưng không có một thiết bị và chương trình bảo mật nào bảo vệ hệ thống khỏi các nguy cơ xâm nhập từ bên ngoài vào. Những hacker có thể sử dụng virus dưới dạng trojan để truy cập vào hệ thống ăn cắp hoặc phá hoại thông tin.
- **Nguy cơ mất mát thông tin từ bên trong hệ thống**: Với các switch hiện tại, những người trong hệ thống mạng có thể dễ dàng dùng các chương trình nghe lén (sniffer) để lấy cắp các thông tin được truyền đi trong mạng và nguy cơ mất mát thông tin từ trong hệ thống là nguy cơ ngày càng cao trong các hệ thống mạng hiện nay.
- **Nguy cơ hệ thống có kết nối Internet bị tấn công bởi các tin tặc**. Hậu quả tất yếu của các vụ tấn công như trên là server sẽ bị tê liệt, không còn khả năng xử lý các yêu cầu khác nữa. Do hệ thống mạng nội bộ có vùng quảng bá rộng nên nguy cơ tấn công cũng có thể xảy ra từ bên trong mạng, nếu một máy tính trong mạng bị nhiễm virus có khả năng tấn công mạng hoặc chạy các chương trình tấn công mạng thì có thể làm cho hệ thống mạng hoàn toàn tê liệt, không thể truy cập được Internet.
- **Virus tin học ngày càng nhiều và cũng nguy hiểm hơn**. Đã xuất hiện một số virus mà khi được kích hoạt sẽ xóa trắng các tập tin, mất quyền truy cập hệ thống, hư hại các phần mềm trong máy tính.

Vì vậy cần một giải pháp cho hệ thống mạng hiện nay.

Để giải quyết được các vấn đề trên, hệ thống cần bổ sung các thiết bị phần cứng hoặc phần mềm nhằm ngăn chặn được các nguy cơ tấn công.

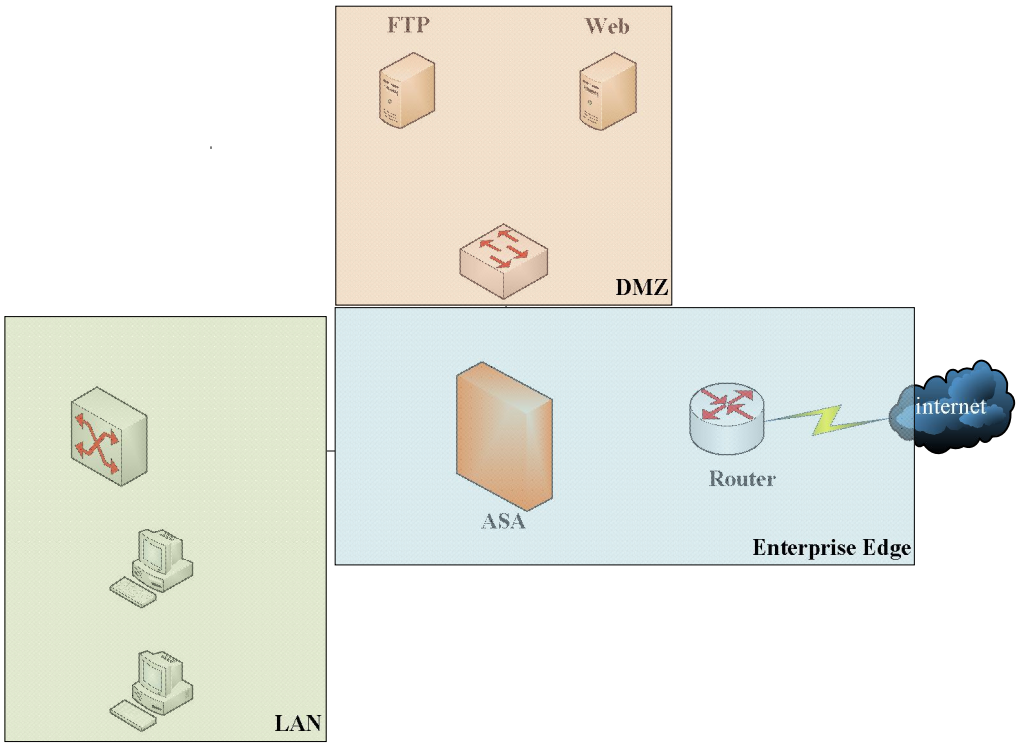
Đối với các tấn công từ ngoài Internet, hệ thống mạng nội bộ và các server cần:

- Che giấu các thông tin của hệ thống mạng nội bộ.

- Ngăn chặn các truy cập bất hợp pháp đến hệ thống mạng nội bộ và các server.
- Đối với hệ thống mạng nội bộ cần chia thành nhiều miền quảng bá để quản lý và có thể khoanh vùng khi có virut.

Tuy nhiên, để tăng tính bảo mật và ổn định của hệ thống thì giải pháp sử dụng các thiết bị phần cứng là lựa chọn thích hợp. Ngoài các trang thiết bị đã có cần trang bị thêm thiết bị firewall ASA của Cisco.

3.1.2. Mô hình hệ thống



Hình 3-1: Sơ đồ hệ thống mạng dung firewall ASA

- Vùng Enterprise Edge: bao gồm tường lửa Cisco ASA, Router

  Chức năng: cung cấp các phương pháp bảo mật

- Vùng DMZ: Vùng DMZ là một vùng mạng trung lập giữa mạng nội bộ và mạng Internet, là nơi chứa các thông tin cho phép người dùng từ Internet truy xuất vào và chấp nhận các rủi ro tấn công từ Internet. Các dịch vụ được triển khai trong vùng DMZ là: máy chủ Web, máy chủ FTP

- Vùng LAN: là nơi đặt các thiết bị mạng, máy trạm thuộc mạng nội bộ của đơn vị.

  Chức năng: cung cấp quyền truy cập cho các user/workgroup

Các chức năng chính của mô hình là cho phép truy cập an toàn, an toàn cho người dùng ở tất cả các địa điểm và cung cấp các dịch vụ mà không ảnh hưởng đến tính bí mật, tính toàn vẹn, tính sẵn sàng của tài nguyên và dữ liệu. Mô hình kết hợp các chức năng bảo mật sau:

- Enterprise router: là cổng Internet có trách nhiệm định tuyến lưu lượng truy cập giữa mạng nội bộ và Internet. Bộ định tuyến có thể được quản lý bởi nhân viên của công ty hoặc có thể được quản lý bởi nhà cung cấp dịch vụ Internet (ISP). Bộ định tuyến cung cấp mức độ bảo vệ đầu tiên chống lại các mối đe dọa bên ngoài.
- Cisco ASA cung cấp kiểm soát truy cập trạng thái và kiểm tra gói tin để bảo vệ tài nguyên và dữ liệu khỏi việc truy cập, tiết lộ trái phép. Thiết bị bảo mật được định cấu hình để ngăn chặn truy cập vào từ Internet, để bảo vệ các dịch vụ công cộng Internet của doanh nghiệp và để kiểm soát lưu lượng truy cập của người dùng bị ràng buộc với Internet. Ngoài ra, các tính năng Cisco ASA có thể được kích hoạt để bảo vệ doanh nghiệp khỏi các mối đe dọa của botnet. Khi được kích hoạt, tính năng bộ lọc lưu lượng Botnet theo dõi lưu lượng mạng trên tất cả các cổng và các giao thức cho hoạt động, để ngăn các điểm cuối nội bộ bị lây nhiễm gửi lệnh và kiểm soát lưu lượng truy cập đến các máy chủ bên ngoài trên Internet.
- Phòng chống xâm nhập - Một module kiểm tra và phòng ngừa dịch vụ trên Cisco ASA có thể được thực hiện để tăng cường phát hiện mối đe dọa và giảm nhẹ chúng. Các mô-đun có trách nhiệm xác định và ngăn chặn các truy cập bất thường và các gói tin độc hại được công nhận là đang tấn công hệ thống.
- Các Dịch vụ Công cộng DMZ - Trang web Internet, máy chủ thư tín và các dịch vụ công cộng khác của công ty có thể được đặt trên vùng phi quân sự (DMZ) vì mục đích an ninh và kiểm soát. DMZ hoạt động như một trung gian giữa Internet và tài nguyên riêng của công ty, cho phép người dùng bên ngoài trực tiếp truy cập vào.

3.2. Công cụ sử dụng

- **Phần mềm giả lập GNS3**

GNS3 là một chương trình giả lập mạng có giao diện đồ họa cho phép bạn có thể giả lập các loại router Cisco sử dụng IOS (hệ điều hành của router) thật, ngoài ra còn có thể giả lập các thiết bị mạng khác như ATM, Frame Relay, Ethernet Switch, Pix Firewall… và đặt biệt có thể kết nối vào hệ thống mạng thật và sử dụng như thiết bị thật.

GNS3 giúp xây dựng, thiết kế và kiểm tra mạng của bạn trong một môi trường ảo không có rủi ro thật và tiếp cận các cộng đồng mạng lớn nhất để trao đổi giúp đỡ cùng nhau. Cho dù bạn đang là sinh viên đang học Đại học về Quản trị mạng hoặc là kỹ sư xây dựng một mạng viễn thông toàn cơ quan thì GNS3 là một giải pháp dễ dàng để thiết kế và xây dựng mạng lưới của bất kỳ mô hình nào mà không cần lo ngại về phần cứng và chi phí. Và đặc biệt là nó hoàn toàn miễn phí.

- **Tool ASDM Cisco**

Trình quản lý thiết bị bảo mật của Cisco cung cấp quản lý và giám sát an ninh tầm cỡ thế giới thông qua giao diện quản lý dựa trên nền tảng Web dễ sử dụng và trực quan.

Trình quản lý thiết bị bảo mật của Cisco cung cấp những tính năng sau:

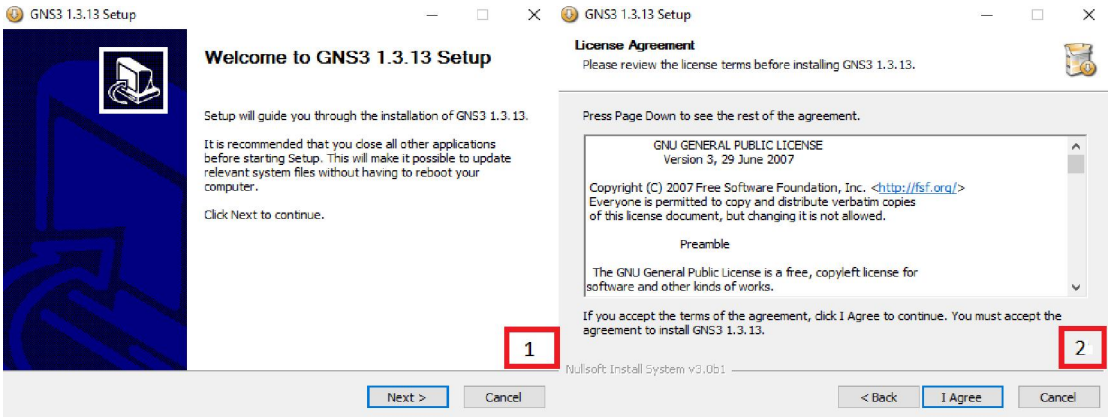
- Thiết lập các trình thủ thuật giúp bạn cấu hình và quản lý các thiết bị tường lửa của Cisco.
- Trình xem nhật ký thời gian thực mạnh mẽ và theo dõi bảng điều khiển cung cấp chế độ xem nhanh về trạng thái thiết bị và tình hình hoạt động của thiết bị tường lửa.

3.3. Giả lập firewall ASA trên GNS3

Trên GNS3 không có sẵn firewall ASA nên ta tiến hành cài đặt firewall ASA vào GNS3.

Trong bài ta sử dụng GNS3 version 1.3.13 và firewall ASA version 8.4.2

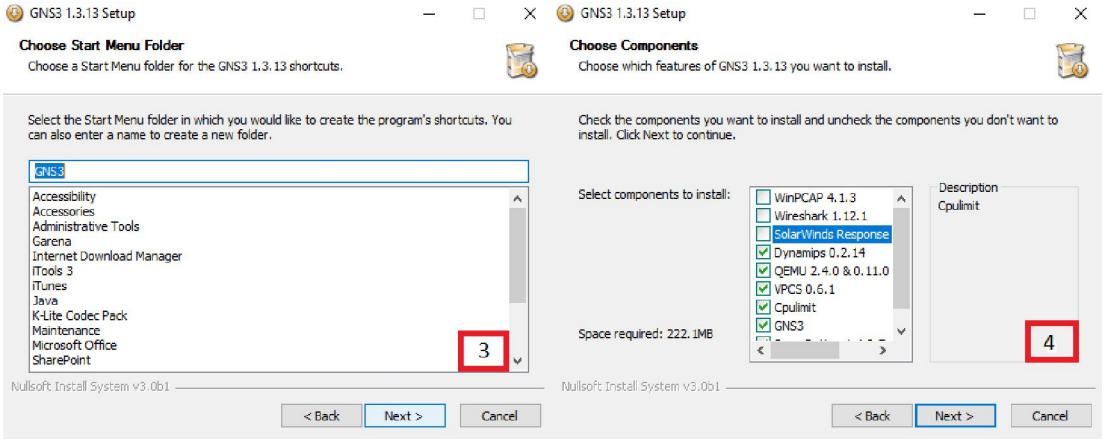
3.3.1. Cài đặt GNS3



Hình 3-2: Cài đặt GNS3

Bước 1: Chạy file cài đặt GNS3, chọn *Next*

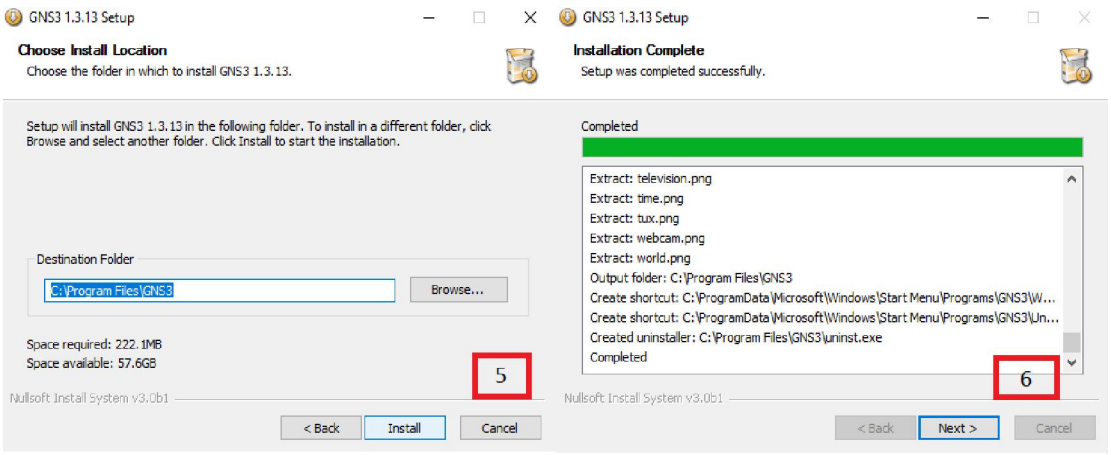
Bước 2: Trong hộp thoại *Licenes Agreement*, chọn *I Agree*



Hình 3-3: Cài đặt GNS3

Bước 3: Trong hộp thoại *Choose Start Menu Folder*, chọn *Next*

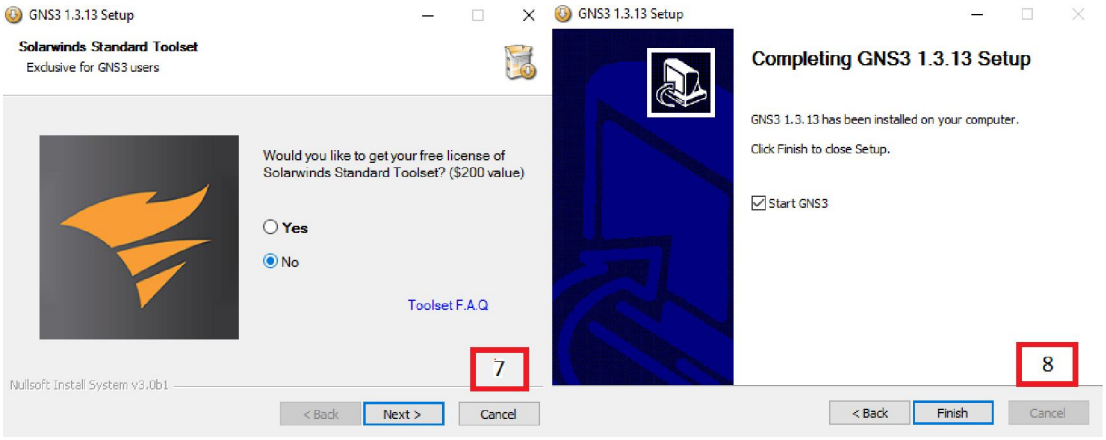
Bước 4: Trong hộp thoại *Choose Components*, chọn các ứng dụng cần thiết, chọn *Next*



Hình 3-4: Cài đặt GNS3

Bước 5: Trong hộp thoại *Choose Install Location*, chọn *Install*

Bước 6: Sau khi cài đặt xong, chọn *Next*



Hình 3-5: Hoàn tất cài đặt GNS3

Bước 7: Trong hộp thoại *Solarwinds Standard Toolset*, chọn *No*

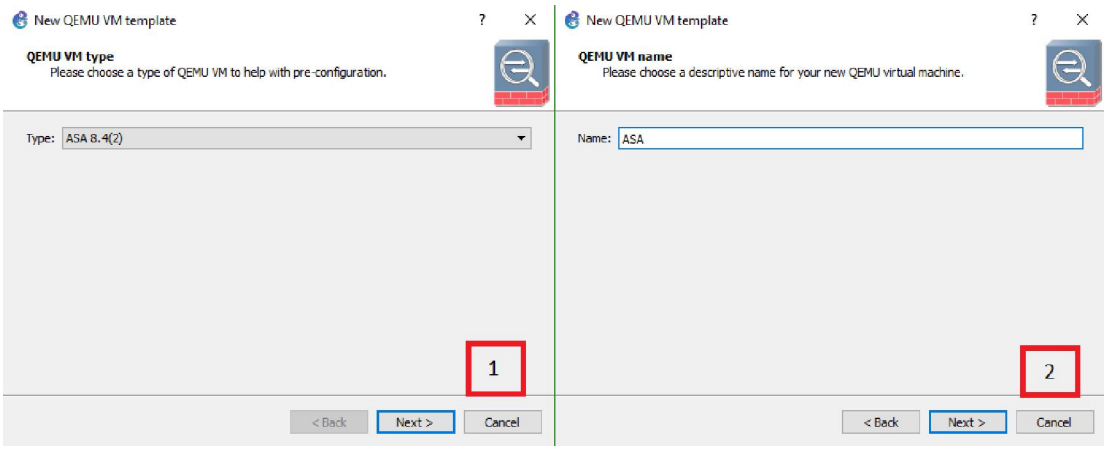
Bước 8: Chọn *Finish* để hoàn tất quá trình cài đặt

3.3.2. Giả lập firewall ASA

Download ios của ASA 8.4.2 trên web.

File cài đặt ASA bao gồm file: asa842-initrd và asa842-vmlinuz

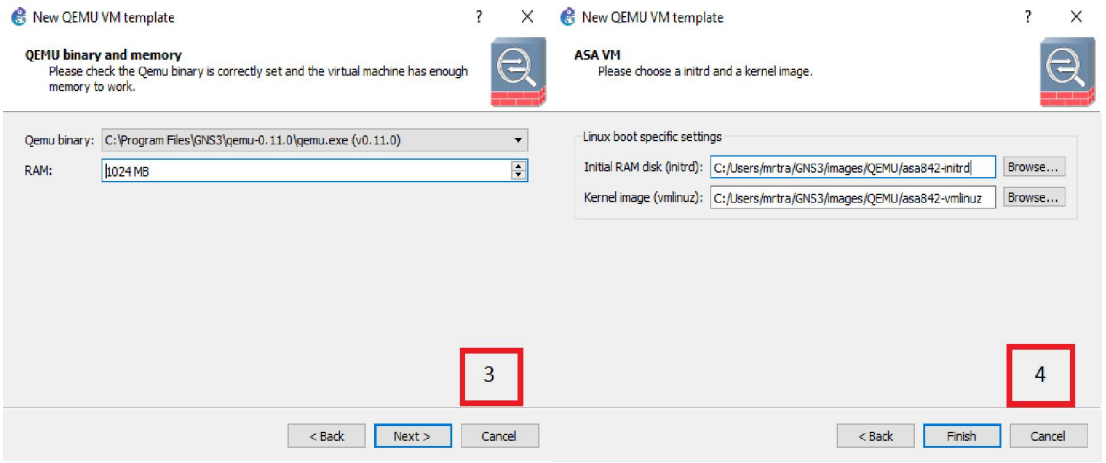
Khởi động *GNS3* => *Edit* => *Preferences* => *QEMU* => *Qemu Vms* => *New*



Hình 3-6: Giả lập firewall ASA

Bước 1: Trong hộp thoại *QEMU VM type*, chọn *type* là ASA 8.4(2), chọn *Next*

Bước 2: Trong hộp thoai *QEMU name*, chọn *Name* là ASA, chọn *Next*



Hình 3-7: Hoàn tất giả lập firewall ASA

Bước 3: Trong hộp thoai *QEMU binary and memory,* chọn dung lượng *RAM* ASA sử dụng là 1024, chọn *Next*

Bước 4: Trong hộp thoại *ASA VM, Browse* hai file initrd và vmlinuz, chọn *Finish*

Firewall ASA của Cisco phiên bản 8.4.2 trở lên có hỗ trợ tính năng Identity Firewall đây là tính năng hay mà các dòng Next-generation firewall sử dụng, đặc biệt là hãng Palo Alto đang dẫn đầu về mảng này.

Palo Alto là hãng đầu tiên đưa ra khái niệm tường lửa thế hệ mới. Không chỉ hoạt động ở Layer 4 như các loại tường lửa thế hệ trước. Palo Alto Firewall hoạt động

cả ở tầng ứng dụng, cung cấp một giải pháp toàn diện cho người quản trị cả về đảm bảo an ninh và quản lý hệ thống.

Palo Alto là thiết bị tường lửa dựa trên việc xác thực người dùng (User-ID), xác thực dựa trên ứng dụng (App-ID) và xác thực thông qua nội dung (Content-ID). Với các ứng dụng và công cụ tấn công ngày càng đa dạng, với những thiết bị tường lửa thông thường dựa trên IP, Port,… thì không thể xác định và ngăn chặn. Hơn nữa với cơ chế xác thực dựa theo User-ID, App-ID, Content-ID,…giúp cho người quản trị dễ dàng nhận dạng các ứng dụng, nội dung bên trong luồng dữ liệu với các mức độ nguy hiểm từ đó có thể ngăn chặn kịp thời, có khả năng xác định rõ các mối nguy cơ đe dọa xuất phát từ người sử dụng nào. Chính vì thế mà nó được gọi là Next-generation Firewall.

3.4. Thiết kế hệ thống mô phỏng

3.4.1. Giải pháp bảo mật

Để giải quyết được các vấn đề trên, hệ thống cần bổ sung các thiết bị phần cứng hoặc phần mềm nhằm ngăn chặn được các nguy cơ tấn công.

Đối với các tấn công từ ngoài Internet vào hệ thống mạng nội bộ và các server cần:

- Che giấu các thông tin của hệ thống mạng nội bộ: sử dụng (NAT,PAT) định tuyến cho mạng.

  NAT giúp dấu tất cả IP bên trong LAN với bên ngoài, tránh sự dòm ngó của hackers.

  NAT có tính linh hoạt và sự dễ dàng trong việc quản lý.

  NAT giúp cho các home user và các doanh nghiệp nhỏ có thể tạo kết nối với internet một cách dễ dàng và hiệu quả cũng như giúp tiết kiệm vốn đầu tư.

- Ngăn chặn các truy cập bất hợp pháp đến hệ thống mạng nội bộ và các server: chia vlan; sử dụng thiết bị phát hiện xâm nhập, phát hiện phần mềm độc hại.

Đối với hệ thống mạng nội bộ cần chia thành nhiều miền quảng bá để quản lý và có thể khoanh vùng khi có virut.

Tuy nhiên, để tăng tính bảo mật và ổn định của hệ thống thì giải pháp sử dụng các thiết bị phần cứng là lựa chọn thích hợp. Ngoài các trang thiết bị đã có cần trang

bị thêm thiết bị firewall ASA của Cisco, các switch có khả năng chia VLAN nhằm chia mạng nội bộ thành nhiều miền quảng bá.

3.4.2. Chức năng firewall ASA

Sử dụng Firewall cứng (Cisco firewall ASA) để bảo vệ hệ thống server và mạng nội bộ. Firewall sẽ chia hệ thống mạng ra làm 2 vùng có mức độ ưu tiên bảo mật khác nhau:

- Outside: đây là vùng Internet, có mức độ ưu tiên bảo mật thấp nhất.
- Inside: mạng nội bộ, đây là vùng có mức độ ưu tiên bảo vệ cao nhất, các máy trong vùng inside có khả năng truy cập ra vùng outside.

Cisco ASA có thể bảo vệ mạng bên trong (inside), các khu phi quân sự (DMZ) và mạng bên ngoài (outside) bằng cách kiểm tra tất cả lưu lượng đi qua nó. Có thể xác định chính sách và quy tắc cho những lưu lượng được cho phép hoặc không cho phép đi qua interface.

- Phát hiện các xâm nhập trái phép, giảm các nguy cơ bị tấn công, giảm chi phí thiệt hại, tránh gián đoạn hệ thống.
- Cơ chế theo dõi trạng thái kết nối, thực hiện việc chuẩn hóa giao thức TCP.

Cisco ASA được triển khai ở vùng biên mạng có trách nhiệm bảo vệ tài nguyên nội bộ của doanh nghiệp và dữ liệu khỏi các mối đe dọa từ bên ngoài bằng cách ngăn chặn truy cập vào từ Internet. Bảo về vùng LAN, DMZ khỏi các cuộc tấn công từ Internet. Kiểm soát lưu lượng truy cập Internet của người dùng.

Để triển khai, thiết bị bảo mật được cấu hình để thi hành chính sách truy cập, theo dõi trạng thái kết nối và kiểm tra các tải trọng gói theo cácyêu cầu sau:

• Từ chối bất kỳ yêu cầu kết nối nào từ Internet tới các nguồn nội bộ và mạng con.

• Cho phép truy cập Internet cho người dùng nội bộ và cho các giao thức được cho phép theo chính sách của doanh nghiệp (ví dụ HTTP và HTTPS).

• Cho phép SSL truy cập Internet để cập nhật quản trị.

• Cho phép người dùng truy cập vào các dịch vụ DMZ như trang web của công ty, E-mail (HTTP, SMTP, IMAP và DNS).

• Hạn chế truy cập Internet vào DMZ, chỉ cho các giao thức và máy chủ cần thiết như: HTTP đến máy chủ web, DNS tới máy chủ DNS.

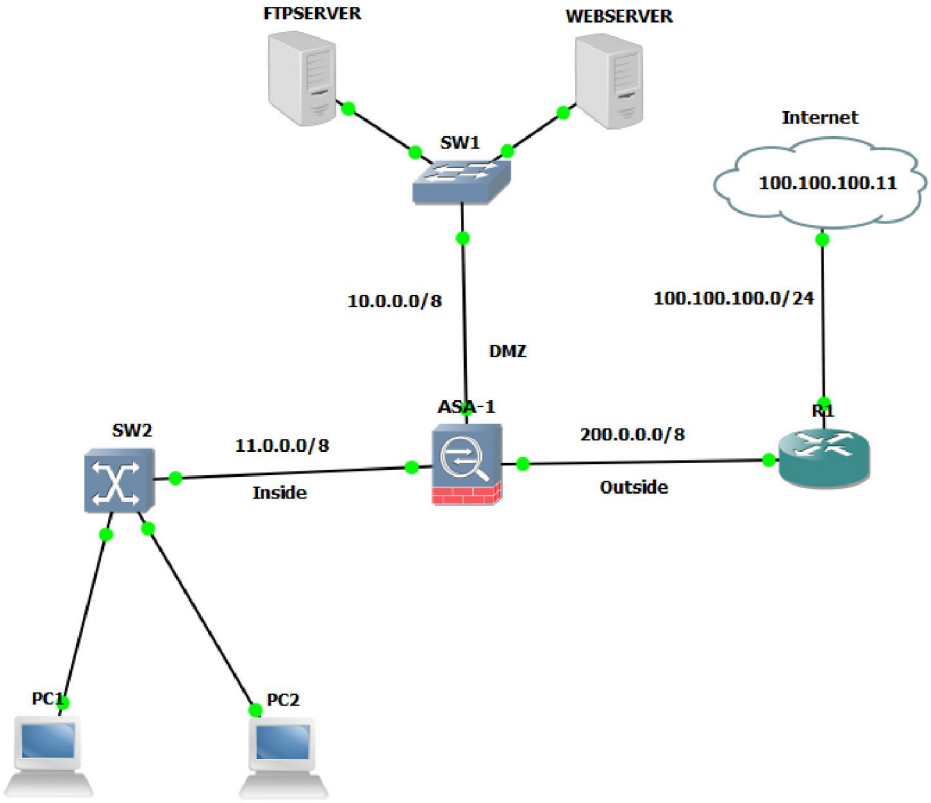
• Hạn chế các kết nối được khởi tạo từ DMZ với các giao thức: DNS từ máy chủ DNS, SMTP từ máy chủ thư, HTTP/SSL của Cisco.

• Cho phép kiểm tra trạng thái cho các giao thức đã sử dụng để đảm bảo lưu lượng truy cập trở lại tường lửa.

• Thực hiện dịch địa chỉ mạng (NAT) và dịch địa chỉ cổng (PAT) để bảo vệ không gian địa chỉ nội bộ từ Internet.

3.4.3. Triển khai xây dựng hệ thống

3.4.3.1 Chức năng thực hiện



Hình 3-8: Mô hình ASA trên GNS3

Vùng Inside có địa chỉ: 11.0.0.0/8

Vùng Outside có địa chỉ: 200.0.0.0/8

Vùng DMZ có địa chỉ: 10.0.0.0/8

Gán địa chỉ Internet nguồn là một interface loopback có địa chỉ : 100.100.100.11/24

Triển khai xây dựng hệ thống trên phần mềm giả lập GNS3 sử dụng Cisco ASA ta thực hiện công việc sau:

- Cấu hình cơ bản các thiết bị: ASA, Router.
- Thực hiện lệnh định tuyến để cho phép các miền inside, outside có thể kết nối truyền thông được với nhau.
- Thực hiện NAT, PAT địa chỉ cổng vùng inside truy cập ra vùng outside.

3.4.3.2 Cấu hình chi tiết

a. Cấu hình cơ bản

Cấu hình cơ bản cho các interface trên ASA, chia theo từng vùng DMZ, Inside, Outside:

```
Ciscoasa > enable
Ciscoasa#  configure terminal
Ciscoasa(config)# interface GigabitEthernet0
Ciscoasa (config-if)# nameif  dmz
Ciscoasa (config-if)# security-level 50
Ciscoasa (config-if)# ip address 10.0.0.1 255.0.0.0
Ciscoasa (config-if)# no shutdown
Ciscoasa (config-if)#exit
Ciscoasa (config)# interface GigabitEthernet1
Ciscoasa (config-if)# nameif outside
Ciscoasa (config-if)# security-level 0
Ciscoasa (config-if)# ip address 200.0.0.1 255.0.0.0
Ciscoasa (config-if)# no shutdown
Ciscoasa (config)# interface GigabitEthernet2
Ciscoasa (config-if)# nameif inside
Ciscoasa (config-if)# security-level 100
```

```
Ciscoasa (config-if)# ip address 11.0.0.1 255.0.0.0
Ciscoasa (config-if)# no shutdown
Ciscoasa (config-if)# exit
```

Cấu hình cơ bản cho Router:

```
R1# configure terminal
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 200.0.0.2  255.0.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip address 100.100.100.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

b. Chuyển tiếp lưu lượng

Trong mô hình triển khai, firewall ASA có nhiệm vụ chuyển tiếp cho tất cả các mạng nội bộ đi ra ngoài Internet. Việc định tuyến có thể tùy thuộc vào nhu cầu mà ta có thể sử dụng định tuyến tĩnh (static route và default-route) hoặc định tuyến động (RIP, EIGRP, OSPF). Tuy nhiên, với các thiết bị định tuyến ở các công ty quy mô không lớn, đinh tuyến tĩnh được ưu tiên sử dụng. Trong mô hình này ta sử dụng định tuyến mặc định (default-route) để cho mạng nội bộ đi đến Enterprise router.

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 200.0.0.2
```

c. Access Control List

ASA mặc định chỉ cho phép các traffic đi từ nơi có security-level cao đến nơi có security-level thấp.

Cấu hình ACL cho phép các bản tin ICMP echo-reply gửi vào cổng outside.

```
access-list acl_DMZ  extended permit icmp any any echo-reply
```

Tương tự cũng có access list trên outside interface để cho phép các gói tin ICMP được đi qua:

```
access-list acl_outside extended permit icmp any any echo-reply
```

Với 2 access-list ở trên , ta thiết lập 2 access-group tương ứng

```
access-group acl_DMZ in interface outside
access-group acl_outside in interface outside
```

Trong sơ đồ trên (hình 3-2), công ty sẽ xây dựng hệ thống Web server và FTP server để hỗ trợ cho hoạt động của công ty. Ở đây, ta sẽ xây dựng Web server IIS và FTP server trong vùng DMZ và được NAT ra bên ngoài cho phép tất cả các máy tính ngoài Internet truy cập được Web server của công ty. Để các máy bên ngoài truy cập được, ta sẽ tạo ra access control list để cho phép HTTP và FTP truy cập vào:

```
access-list icmp-in extended permit tcp any any eq www
access-list icmp-in extended permit tcp any any
access-list icmp-in extended permit tcp any any eq ftp
```

d. Auto NAT

Như mô hình được áp dụng phổ biến hiện nay trong hệ thống mạng của các các công ty, tất cả các traffic đi từ mạng ở bên trong ra bên ngoài đều sử dụng cơ chế dịch địa chỉ (PAT). Tất cả các mạng trong mô hình gồm 11.0.0.0/8 và 10.0.0.0/8 đều được PAT. Điều này giúp tăng tính bảo mật của hệ thống mạng.

- Đối với vùng Inside:
    - Cấu hình Object Network:

```
ciscoasa(config)# object network inside
ciscoasa(config-network-object)#subnet 11.0.0.0 255.0.0.0
```

    - Cấu hình PAT (dùng địa chỉ cổng outside)

```
ciscoasa(config)# object network inside
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

- Đối với vùng DMZ:
    - Cấu hình Object Network

```
ciscoasa(config)# object network  dmz
ciscoasa(config-network-object)#subnet 10.0.0.0  255.0.0.0
```

- Cấu hình PAT (dùng địa chỉ cổng outside)

```
ciscoasa(config)# object network  dmz
ciscoasa(config-network-object)# nat (dmz,outside) dynamic interface
```

e. Cài đặt ASDM

Để dễ dàng quản lý, cấu hình firewall ASA, Cisco đã phát triển tool ASDM dựa trên nền tảng web giúp quản trị viên theo dõi trạng thái thiết bị và hoạt động của firewall.

Đầu tiên ta cần copy file cài đặt ASDM vào firewall ASA qua TFTP

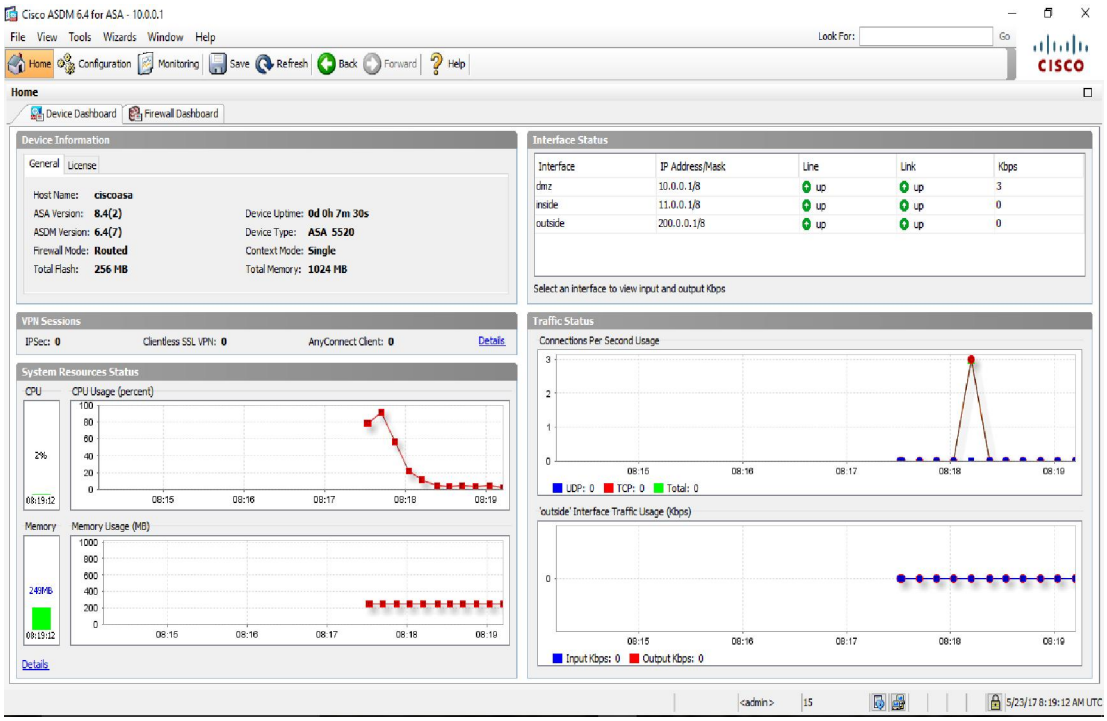
```
ciscoasa# copy tftp: flash:
Address or name of remote host []? 100.100.100.11
Source filename []? asdm-647.bin
Destination filename [asdm-647.bin]?
Accessing tftp://100.100.100.11/asdm-647.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing current ASDM file disk0:/asdm-647.bin !!!!!!!!!!!!!!!!!!!!!!!! !!!! !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Cấu hình load file ASDM trong flash

```
ciscoasa(config)# asdm image flash:asdm-647.bin
ciscoasa(config)# http server enable
ciscoasa(config)#http 10.0.0.0 255.0.0.0 dmz
```

Truy cập đến https://10.0.0.1

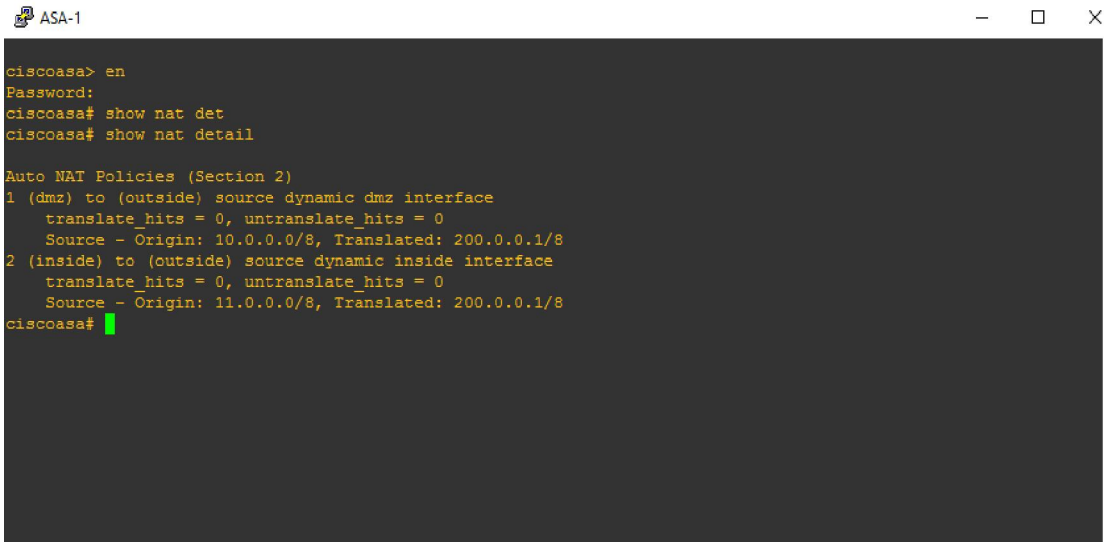
Giao diện firewall ASA



Hình 3-9: Giao diện firewall ASA

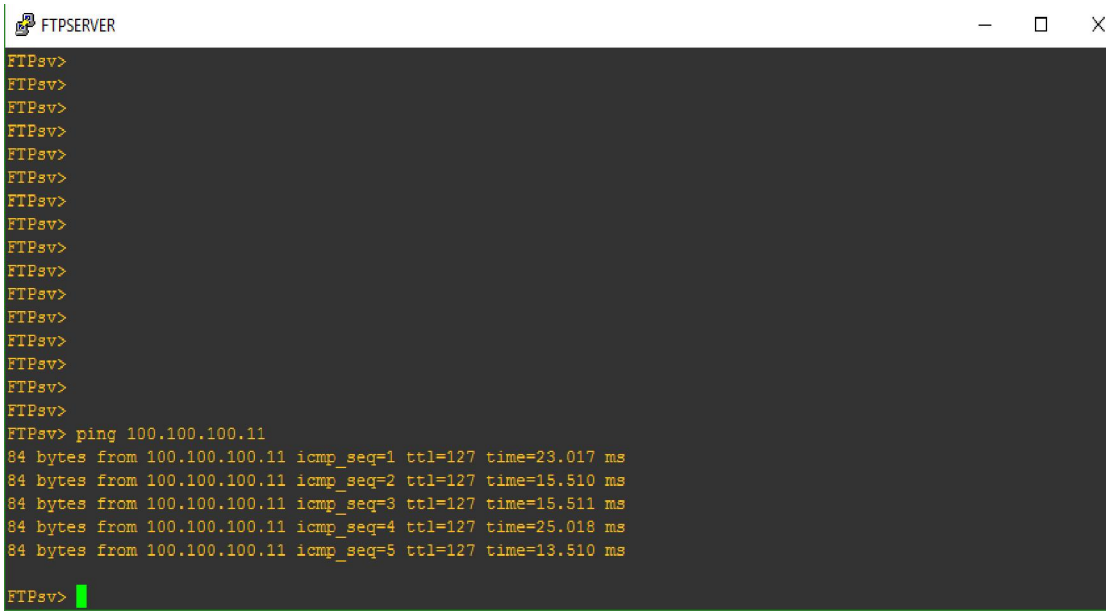
3.4.4. Kết quả kiểm tra hệ thống

Kiểm tra bảng NAT trên Cisco ASA

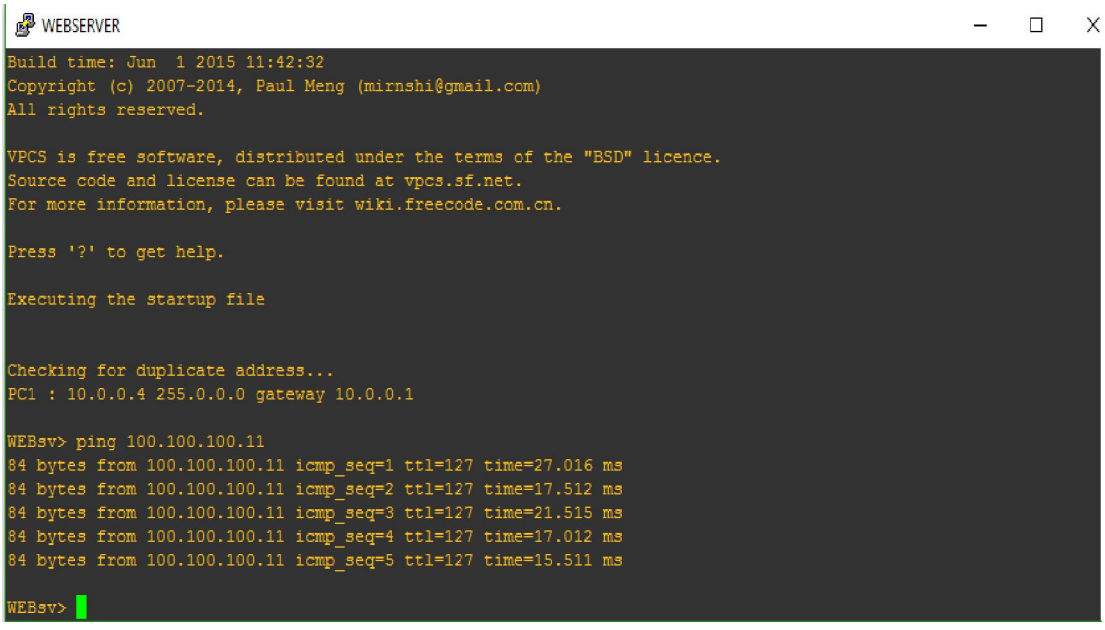


Hình 3-10: Bảng NAT trên Cisco ASA

Kiểm tra NAT từ vùng DMZ ra ngoài Internet

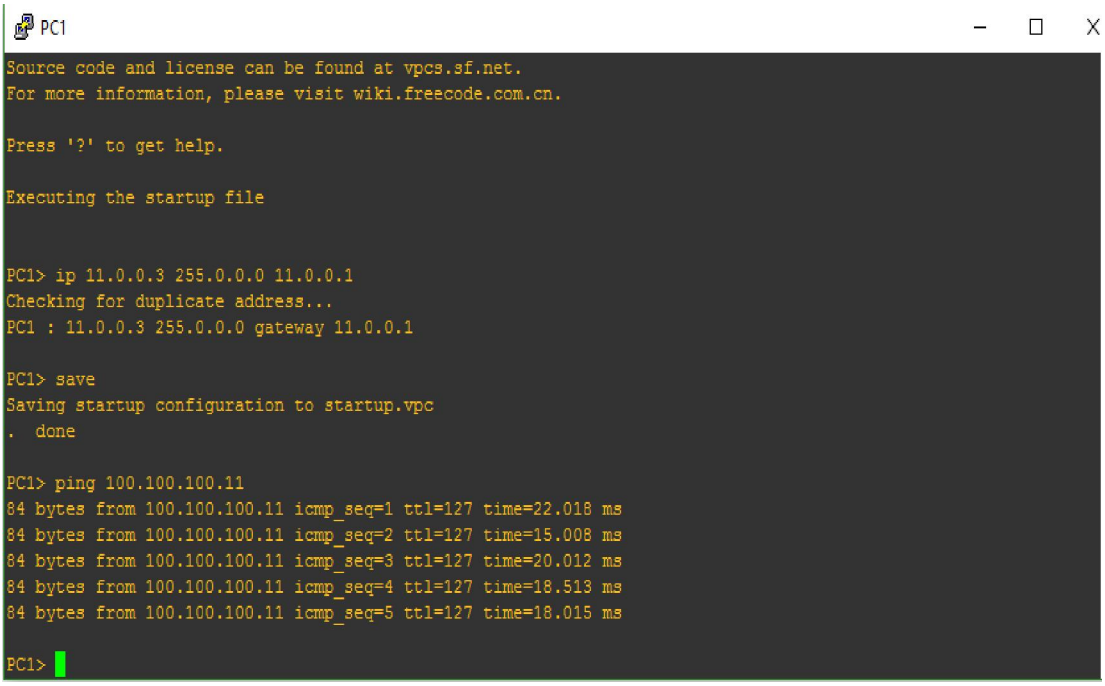


Hình 3-11: FTPserver ra Internet thành công



Hình 3-12: Webserver ra Internet thành công

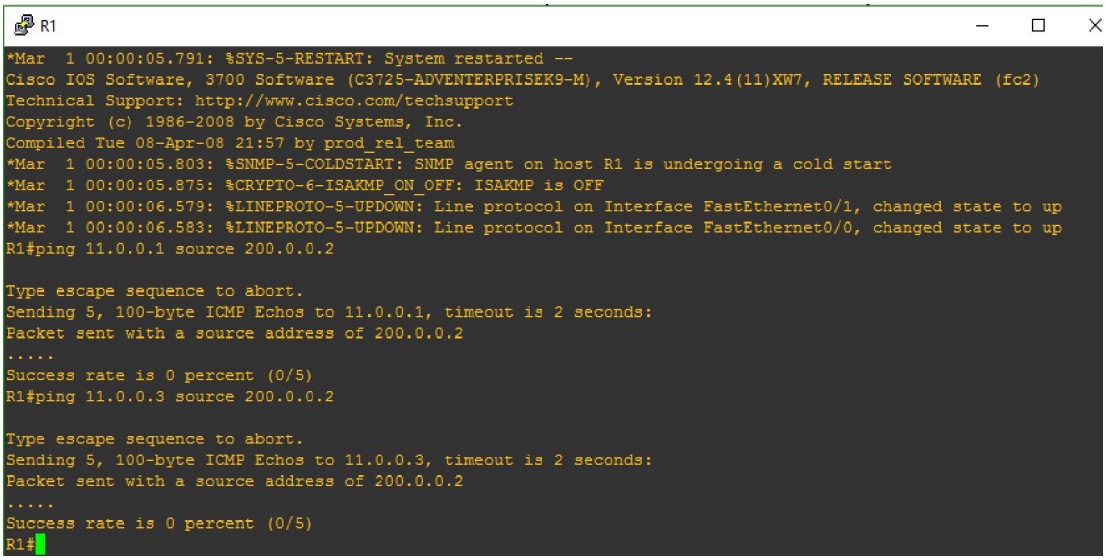
Kiểm tra kết nối từ vùng inside ra ngoài Internet



Hình 3-13: Kết nối từ mạng nội bộ ra Internet thành công

Kiểm tra kết nối từ vùng outside vào inside

Vùng outside không thể kết nối với mạng nội bộ



Hình 3-14: Kiểm tra kết nối giữa vùng outside và inside

3.5. Kết luận chương 3

Hệ thống trước khi triển khai giải pháp an ninh thì hoạt động thiếu sự bảo vệ. Các nguy cơ tấn công từ ngoài Internet của hacker thường xuyên xảy ra, bên cạnh đó vấn đề virut lây lan nhanh chóng trong hệ thống mạng nội bộ cũng như các Server luôn làm các nhân viên quản trị mạng phải tốn kém thời gian và tiền bạc để khắc phục.

Sau khi phân tích, đưa ra giải pháp và triển khai cấu hình hệ thống an ninh sử dụng firewall ASA ta có thể thấy được hiệu quả rõ nét, cụ thể:

- Hệ thống hoạt động an toàn, ổn định hơn.
- Cisco ASA được triển khai ở vùng biên mạng có trách nhiệm bảo vệ tài nguyên nội bộ của doanh nghiệp và dữ liệu khỏi các mối đe dọa từ bên ngoài bằng cách ngăn chặn truy cập vào từ Internet. Bảo về vùng LAN, DMZ khỏi các cuộc tấn công từ Internet. Kiểm soát lưu lượng truy cập Internet của người dùng
- Các Server trong vùng DMZ luôn được NAT sang IP khác khi truy cập ra ngoài Internet, vì thế nguy cơ bị tấn công là cũng rất khó. Ngoài ra khi có người dùng ngoài Internet truy cập đến hệ thống Server thì luôn bị kiểm tra và lọc rất kỹ bởi danh sách kiểm tra truy cập ACL và các dịch vụ khác của firewall ASA.

Tóm lại đối với hệ thống mạng của doanh nghiệp vừa và nhỏ sẽ được bảo vệ an toàn hơn rất nhiều sau khi triển khai hệ thống an ninh với các thiết bị bảo mật và đặc biệt là firewall ASA.

KẾT LUẬN CHUNG

Nghiên cứu về an ninh mạng và các phương thức đảm bảo an toàn cho hệ thống mạng là một đề tài có tính chất thực tế. Đồng thời đây cũng là một mảng kiến thức rộng và còn nhiều điều mới mẻ.

Đề tài **"**Nghiên cứu triển khai hệ thống firewall ASA" là một đề tài đi xây dựng hệ thống an ninh mạng dựa trên cơ sở lý thuyết và những nghiên cứu thực tế. Nhận thấy những ưu điểm mà thiết bị an ninh firewall ASA mang lại cho hệ thống mạng là rất lớn.

Đề tài giúp ta hiểu rõ hơn về an ninh mạng, tường lửa và firewall ASA. Các model của firewall ASA phù hợp với với tất cả hệ thống doanh nghiệp vừa và nhỏ hay các nhà cung cấp dịch vụ.

Đồ án đã hoàn thành được mục tiêu đặt ra đã thực hiện được một số chức năng phổ biến mà các cơ quan, doanh nghiệp đã và đang sử dụng và đạt hiệu quả nhất định trong lĩnh vực bảo mật hệ thống như: chia vùng trong một mạng cơ bản, cấu hình NAT, PAT; cấu hình Access Control List; cài đặt ASDM để theo dõi, quản lý firewall ASA.

Tường lửa Cisco ASA là một thiết bị để đảm bảo an toàn thông tin, bảo mật hệ thống và tăng năng suất hoạt động của hệ thống tuy nhiên vẫn còn mắc phải một số lỗ hổng, không có gì là an toàn tuyệt đối tuy nhiên để hạn chế rủi ro nên thường xuyên cập nhật thông tin và nhận sự hỗ trợ từ Cisco.

Trong tương lai, đồ án sẽ hướng tới việc thực hiện mô phỏng thêm các chức năng mà firewall ASA hỗ trợ cũng như có thể triển khai thực tế cho các cơ quan, doanh nghiệp.

TÀI LIỆU THAM KHẢO

Các tài liệu Tiếng Anh

[1]. **Dave Hucaby**, *Cisco ASA and PIX Firewall Handbook by*, Publisher: Cisco Press – 7/1/2005

[2]. **Harris Andrea**, "*Cisco-ASA-Firewall-Fundamentals-2nd-Edition*" step by step configuration tutorial (CCNA,CCNP,CCSP)

[3]. **Richard Deal**, "*Cisco Asa Configuration*", Network professional's library

Các tài liệu từ Internet

[4]. https://whitehat.vn/threads/huong-dan-gia-lap-firewall-asa-tren-gns3-p2.8104/

[5]. http://svuit.vn/threads/chapter-7-7-nat-0-and-static-nat-asa-8-2-vs-asa-8-4-1369/

[6]. http://www.vnpro.vn/cac-loai-firewall-cua-cisco-va-cac-tinh-nang-tiep-theo/

[7]. http://svuit.vn/threads/lab-2-5-how-to-install-asdm-on-asa-gns3-196/

[8]. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Small_Enterprise_Design_Profile/SEDP/chap5.html