**BAN CƠ YẾU CHÍNH PHỦ**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**



***Môn học: Phòng chống và điều tra tội phạm máy tính***

**Chương 7: Proxy, tường lửa và bộ định tuyến**

|  |  |
| --- | --- |
| Giảng viên hướng dẫn : | Lại Minh Tuấn |
| Nhóm thực hiện : | Tạ Phúc Trực  Vũ Văn Thận  Nguyễn Văn Lâm |

Hà Nội, ngày 05 tháng 12 năm 2019

**BAN CƠ YẾU CHÍNH PHỦ**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**

***Môn học: Phòng chống và điều tra tội phạm máy tính***

**Chương 7: Proxy, tường lửa và bộ định tuyến**

|  |  |
| --- | --- |
| Giảng viên hướng dẫn : | Lại Minh Tuấn |
| Nhóm thực hiện : | Tạ Phúc Trực  Vũ Văn Thận  Nguyễn Văn Lâm |

Hà Nội, ngày 05 tháng 12 năm 2019

**Nhận xét của giảng viên**

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

**MỤC LỤC**

[Chương VII. Proxy, tường lửa và bộ định tuyến 1](#_Toc26462770)

[**7.1. Khái niệm Proxy** 1](#_Toc26462771)

[**7.1.1. Vai trò proxy** 1](#_Toc26462772)

[**7.1.2. Các loại proxy** 2](#_Toc26462773)

[**7.1.3 Hiểu biết về proxy** 5](#_Toc26462774)

[**7.1.4. Khai quật bằng chứng** 11](#_Toc26462775)

[**7.2. Giao tiếp trong tường lửa** 15](#_Toc26462776)

[**7.2.1. Vai trò tường lửa** 15](#_Toc26462777)

[**7.2.2. Các loại tường lửa** 17](#_Toc26462778)

[**7.2.3.** **Phân tích nhật kí tường lửa** 20](#_Toc26462779)

[**7.3.** **Router Bộ định tuyến** 25](#_Toc26462780)

[Kết luận 29](#_Toc26462781)

**Chương VII. Proxy, tường lửa và bộ định tuyến**

Giống như mọi liên kết trong chuỗi có vai trò riêng, mọi thành phần trong mạng đều có một vai trò và bằng chứng để đóng góp cho cuộc điều tra của chúng tôi. Trong chương này, ta sẽ tập trung hoàn toàn vào việc hiểu các proxy web, tường lửa và bộ định tuyến; lý do để điều tra chúng và làm thế nào điều này sẽ giúp trong việc đưa cuộc điều tra về phía trước.

Trong chương này, chúng tôi sẽ đề cập đến các chủ đề sau:

* Bắt proxy để thú nhận
* Giao tiếp trong tường lửa
* Câu chuyện bộ định tuyến kể

**7.1. Khái niệm Proxy**

Proxy là một thành phần rất quan trọng của bất kỳ mạng nào. Một proxy hoạt động như một trung gian giữa các máy tính khác của mạng và Internet. Nói một cách đơn giản, điều này có nghĩa là tất cả lưu lượng truy cập vào hoặc ra khỏi mạng phải đi qua máy chủ proxy.

Nhìn lại chương trước, ta nhớ ghi nhớ lại nhật ký có thể là một điều tra viên pháp lý bạn tốt nhất. Máy chủ proxy có thể tạo ra các bản ghi như vậy mà chúng ta có thể sử dụng cho các cuộc điều tra của mình.

**7.1.1. Vai trò proxy**

Máy chủ proxy thường được triển khai với một số mục tiêu cuối cùng trong tâm trí. Họ có thể được sử dụng cho các mục sau:

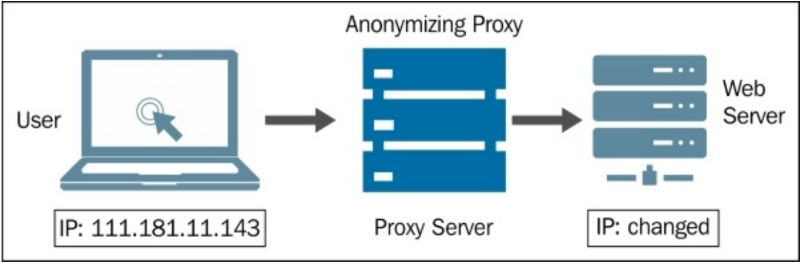
* Chia sẻ kết nối mạng trên mạng cục bộ: Tại đây, nhiều người dùng có thể chia sẻ một kết nối Internet.
* Tăng tốc truy cập web: Kết nối Internet được chia sẻ này được truy cập thông qua một proxy cho phép proxy lưu trữ các trang yêu cầu thường xuyên như Google. Điều này cho phép máy chủ phân phối ngay một trang trong bộ đệm, tăng tốc đăng nhập trang web. Giảm mức sử dụng độ rộng băng tần: Bộ nhớ đệm cục bộ này cho phép máy chủ giảm yêu cầu dự phòng hoặc trùng lặp được gửi đi, giảm sử dụng băng thông và yêu cầu.
* Tính ẩn danh: Máy chủ proxy cho phép người dùng ẩn địa chỉ IP của họ đằng sau địa chỉ của Ủy quyền. Điều này cũng hỗ trợ trong việc ngăn chặn truy cập bất ngờ / trực tiếp vào máy người dùng bằng cách máy bên ngoài mạng.
* Thực hiện kiểm soát truy cập Internet: Proxy cũng có thể được sử dụng để xác thực người dùng truy cập Internet hoặc ngăn người dùng truy cập một số trang web nhất định để kiểm soát sử dụng trong thời gian cụ thể và dưới dạng bộ lọc web hoặc nội dung.
* Bỏ qua an ninh và hạn chế: Một số quốc gia có Internet kiểm duyệt tại chỗ ảnh hưởng đến quyền truy cập vào các trang web nhất định. Một máy chủ proxy có thể giúp bỏ qua những hạn chế này bằng cách làm cho dường như kết nối bắt nguồn từ hoàn toàn địa chỉ IP hoặc địa điểm khác nhau.

**7.1.2. Các loại proxy**

Máy chủ proxy có đủ hình dạng và kích cỡ. Trong khi một số chuyên ẩn danh truy cập Internet, một số khác tập trung vào lưu lượng bộ đệm để tối ưu hóa việc sử dụng tài nguyên Internet. Để hiểu rõ hơn về vũ trụ proxy, chúng ta hãy xem nhanh các loại khác nhau của proxy, như sau:

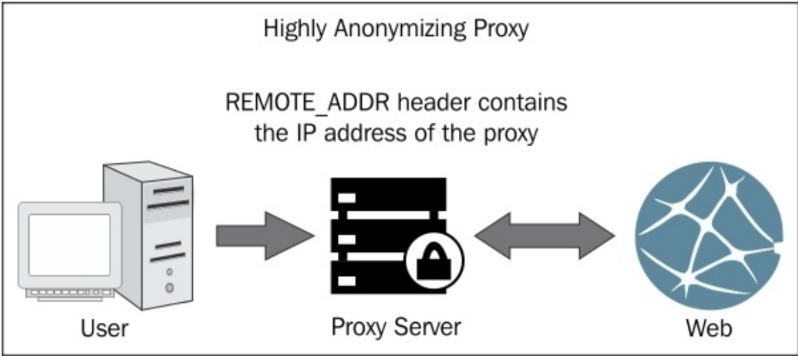
- Proxy ẩn danh:

Proxy ẩn danh thường là proxy web thường nằm giữa người dùng và Internet và hoạt động theo hướng ẩn hoặc ẩn danh địa chỉ IP và vị trí của người dùng Internet. Điều này cực kỳ hữu ích cho người dùng chính phủ hoặc doanh nghiệp không muốn tiết lộ thông tin của họ cho các bên độc hại. Điều này cũng khá hữu ích cho việc liên lạc an toàn và ẩn danh:



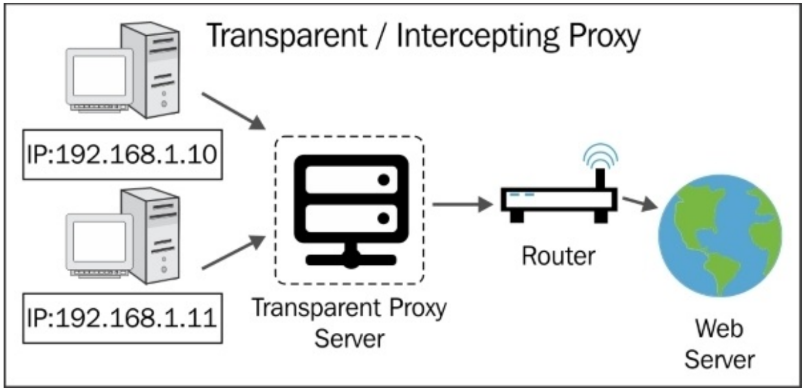
* Proxy ẩn danh cao:

Như tên cho thấy, proxy này sẽ ẩn danh ở cấp độ tiếp theo. Nó không chỉ ẩn IP của người dùng, mà còn che giấu sự thật rằng có một proxy giữa người dùng cuối và Internet. Không giống như proxy thông thường, đích trong trường hợp này không biết rằng nó đang được truy cập thông qua proxy. Đến đích, có vẻ như nó đang được khách hàng truy cập trực tiếp. Tiêu đề REMOTE\_ADDR chứa địa chỉ IP của chính proxy, dẫn đến đích tin rằng proxy là máy khách thực sự truy cập vào nó, như được hiển thị trong hình ảnh sau:



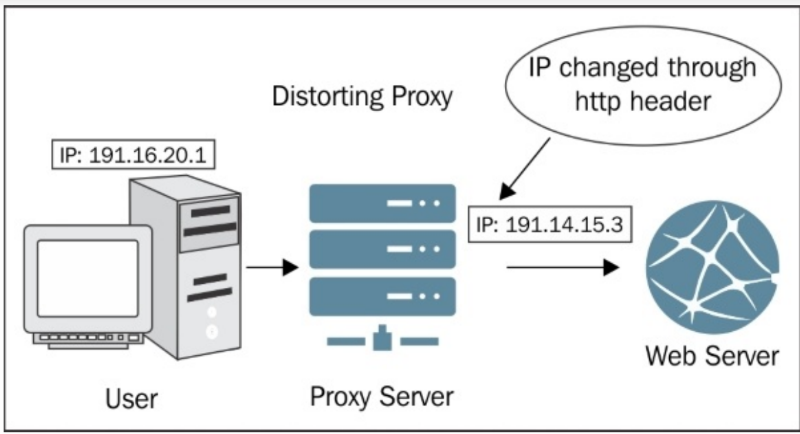
* Proxy trong suốt:

Proxy trong suốt là máy chủ proxy và cổng được cuộn vào một thiết bị. Điều này cũng được gọi là một proxy chặn. Tất cả các kết nối được thực hiện bởi người dùng cuối thông qua cổng được chuyển hướng liền mạch qua proxy. Điều này không yêu cầu bất kỳ cấu hình nào ở phía máy khách. Như tên cho thấy, điều này chuyển tiếp yêu cầu đến đích một cách minh bạch, mà không ẩn IP khách hàng địa chỉ nhà. Proxy trong suốt có thể dễ dàng được phát hiện bằng cách kiểm tra các tiêu đề HTTP phía máy chủ, như trong hình sau:



* Proxy bóp méo:

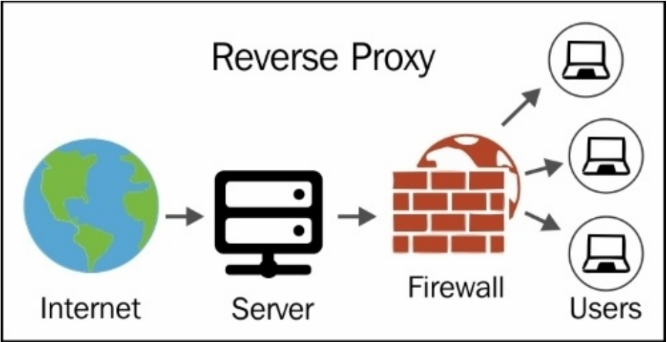
Một proxy loại này xác định chính xác nó là một máy chủ proxy; tuy nhiên, nó cố ý định hướng sai bằng cách đăng một địa chỉ IP không chính xác thông qua các tiêu đề HTTP, như trong hình sau:



- Proxy Ngược:

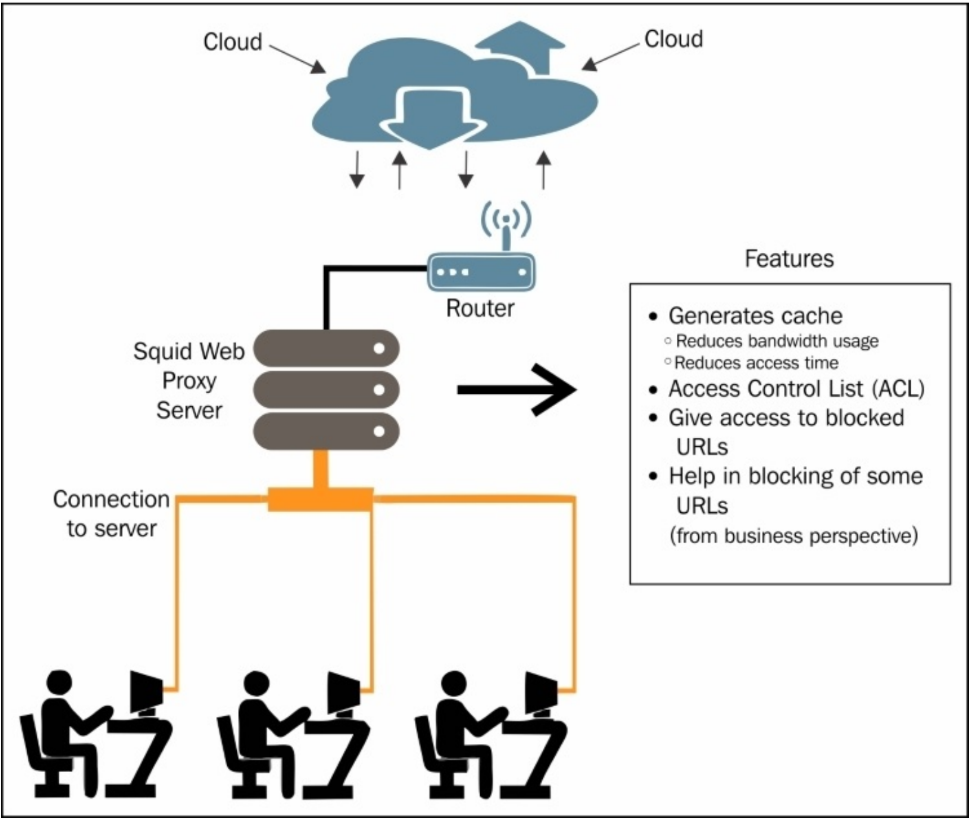
Proxy ngược là các máy chủ proxy khá phổ biến được định vị giữa Internet và tường lửa được kết nối với các mạng riêng.

Các yêu cầu có nguồn gốc từ Internet được nhận bởi proxy ngược và được chuyển đến tường lửa mạng. Điều này ngăn các máy khách Internet có được quyền truy cập không được giám sát và truy cập trực tiếp vào thông tin hạn chế được lưu trữ trên các máy chủ mạng. Khi bộ nhớ đệm được bật trong proxy ngược, lưu lượng mạng có thể giảm đáng kể bằng cách cung cấp thông tin được lưu trong bộ nhớ cache trước đó cho người dùng mạng mà không hướng mọi yêu cầu tới Internet, như trong hình sau:



**7.1.3 Hiểu biết về proxy**

Bằng chứng từ proxy thường nằm trong bộ đệm và nhật ký. Nếu bạn nhớ lại, trong chương trước, chúng tôi đã dành một lượng thời gian đáng kể để hiểu các khái niệm nhật ký, ghi nhật ký và quản lý nhật ký. Trong phần này, chúng ta sẽ xem xét bằng chứng rằng chúng ta có thể khai thác chúng. Một vài trong số các proxy phổ biến bao gồm Squid, NetCache, ISA, BlueCoat, v.v. Proxy có sẵn trong cả hai loại nguồn mở và trả phí. Sách toàn diện và đồ sộ đã được viết về proxy web; tuy nhiên, vì kế hoạch của chúng tôi là tập trung vào việc tìm hiểu vai trò của họ và cách sử dụng chúng với chiếc mũ 007 của chúng tôi, chúng tôi sẽ chọn một và làm việc để hiểu sâu hơn về cách thức hoạt động và loại bằng chứng mà chúng tôi có thể thoát khỏi nó. Với mục đích của bài học này, chúng tôi sẽ làm việc với Squid. Squid là một proxy nguồn mở rất phổ biến và linh hoạt, thích sử dụng rộng rãi trên toàn thế giới. Mực được cung cấp theo các điều khoản của Giấy phép Công cộng GNU. Nó cực kỳ linh hoạt và có thể tùy chỉnh và hoạt động trong cả hai kịch bản proxy thuận và ngược. Mực hoạt động bằng cách lưu trữ các đối tượng web của nhiều loại khác nhau. Điều này có thể bao gồm các trang web, tệp phương tiện được truy cập thường xuyên, v.v., bao gồm cả những trang được truy cập qua HTTP cũng như FTP. Điều này làm giảm thời gian đáp ứng và tắc nghẽn băng thông. Máy chủ proxy Squid là một máy chủ riêng biệt và hoạt động bằng cách theo dõi việc sử dụng một đối tượng qua mạng. Tại thời điểm yêu cầu đầu tiên, Squid sẽ đóng vai trò trung gian và sẽ chuyển yêu cầu máy khách đến máy chủ và ngược lại, trên phản hồi của máy chủ đối với máy khách, đồng thời lưu một bản sao cục bộ của đối tượng được yêu cầu. Tuy nhiên, đối với mọi yêu cầu tiếp theo của cùng một đối tượng, nó sẽ phục vụ đối tượng từ bộ đệm cục bộ của nó. Trong các tổ chức lớn, đây là lý do mà việc cập nhật và vá lỗi hệ thống tốn ít thời gian và băng thông hơn rất nhiều ngay cả khi cập nhật hàng trăm máy cùng lúc. Đồ họa sau đây thể hiện bằng hình ảnh của máy chủ proxy web Squid đang hoạt động. Như chúng ta có thể thấy, nó nằm giữa người dùng và bộ định tuyến và đóng một số vai trò:



Một tác dụng phụ đáng kinh ngạc của hành vi bộ đệm này là sự sẵn có của các mục (chưa hết hạn) quan tâm đến bộ đệm mà Squid (hoặc bất kỳ máy chủ proxy nào) đã tiết lộ để cải thiện hiệu suất mạng. Đối với chúng tôi, những vật phẩm như thế này thực sự có thể giúp chúng tôi trình bày khẩu súng hút thuốc.

Trong một trường hợp liên quan đến quấy rối tình dục tại nơi làm việc, một nhân viên được xác định đang tải xuống tài liệu khiêu dâm và gửi cho nhân viên nữ bằng ID e-mail của đồng nghiệp. Ý tưởng đằng sau điều này là ngụ ý rằng đồng nghiệp và quấy rối nhân viên khác. Trong khi các bản ghi nghi ngờ, cho thấy các tệp có tên lạ (mặc dù có vẻ vô tội) được lưu trữ trên các máy chủ được truy cập thông qua địa chỉ IP (DNS chưa được giải quyết), bộ đệm có nội dung tương ứng thực sự chứng minh rằng nghi phạm là thủ phạm thực sự đằng sau cả hai tội ác.

Với vai trò là một proxy chuyển tiếp thông thường, Squid cung cấp các chức năng sau:

- Bộ nhớ đệm

- Xác thực ủy quyền

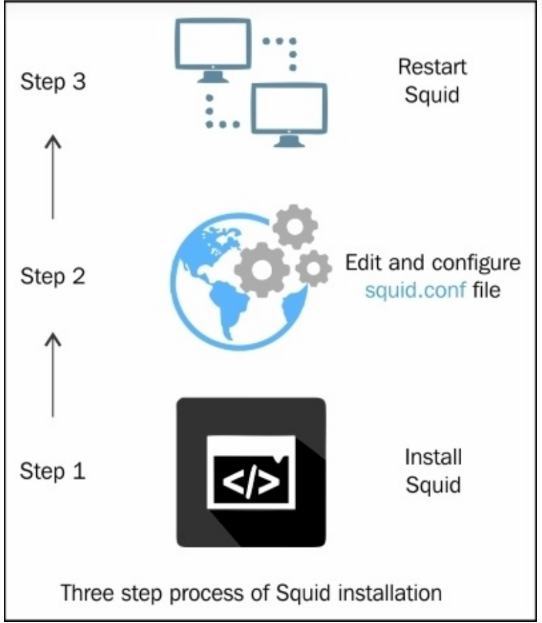
- Lọc nội dung hoặc thực thi chính sách Internet

- Quản lý sử dụng tài nguyên mạng

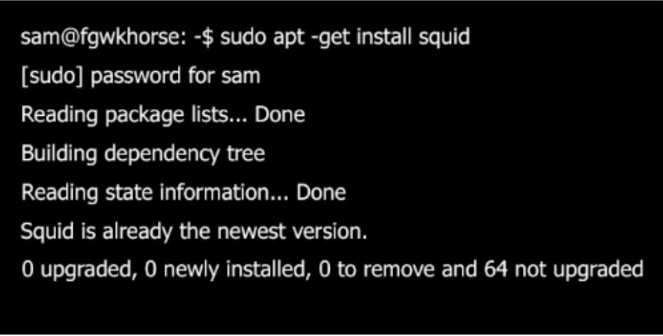
Trong vai trò của proxy ngược, Squid có thể thực hiện các chức năng sau:

* Ngồi trước bộ đệm trang trại máy chủ và phục vụ nội dung tĩnh
* Tối ưu hóa việc sử dụng máy chủ web trong khi phục vụ dữ liệu cho khách hàng
* Tăng cường bảo mật bằng cách lọc nội dung web
* Hoạt động như một cổng IPv4 - IPv6

Cài đặt Squid khá đơn giản. Quá trình cài đặt bao gồm ba bước và mặc dù chỉ có ba bước, chúng có thể thay đổi đôi chút với các hương vị khác nhau của Linux:



Ảnh chụp màn hình sau đây cho thấy cài đặt của nó trong Ubuntu:



Chúng tôi bắt đầu bằng cách chạy lệnh cài đặt như siêu người dùng. Tại thời điểm này, hộp Ubuntu của chúng tôi yêu cầu mật khẩu. Một khi điều này được cung cấp, nó sẽ tiếp tục và kiểm tra xem Squid đã được cài đặt chưa. Nếu có, sau đó nó kiểm tra xem nó có phải là phiên bản mới nhất không, nếu không, nó sẽ nâng cấp nó trong trường hợp của tôi, như được hiển thị trước đó, nó đã làm mọi thứ và thấy rằng tôi đã cài đặt phiên bản mới nhất. Điều này cho thấy chúng tôi rất tốt để đi đến giai đoạn thứ hai.

Giai đoạn tiếp theo là sửa đổi tệp cấu hình squid.conf của chúng tôi.

Tập tin này cho Ubuntu được tìm thấy theo đường dẫn sau:

**etc/squid3/squid.conf**

Trong Linux, nó có thể được tìm thấy ở phần sau:

**etc/squid/squid.conf**

Trong chương trước, bạn có thể nhớ lại rằng chúng tôi đã dành thời gian sửa đổi tệp splunk.conf để có thể chạy Splunk hiệu quả. Chúng ta cần phải làm tương tự ở đây cho Mực. Để chỉnh sửa tệp squid.conf, chúng tôi mở nó trong trình soạn thảo văn bản yêu thích của chúng tôi và thực hiện các thay đổi cần thiết, như sau:

**sam@fgwkhorse: -$ sudo vim /etc/squid3/squid.conf**

Mặc dù có một số lượng lớn các thay đổi có thể được thực hiện đối với tệp squid.conf để điều chỉnh Squid để chạy chính xác theo nhu cầu của chúng tôi, rất nhiều tùy chọn này nằm ngoài phạm vi của chương này. Đủ để nói, ý tưởng của chúng tôi là cảm nhận chủ đề và sau đó đi đến các khía cạnh điều tra.

Theo mặc định, hầu hết các cài đặt trong tệp cấu hình không cần phải thay đổi. Về mặt lý thuyết, Squid có thể được chạy với một tệp cấu hình hoàn toàn trống. Trong hầu hết các trường hợp, nếu chúng ta bắt đầu với tệp squid.conf mặc định (mà chúng ta thường làm), ít nhất một phần sẽ phải được thay đổi cho chắc chắn. Theo mặc định, squid.conf chặn truy cập vào tất cả các trình duyệt. Chúng ta cần thay đổi điều này nếu không Squid sẽ cắt chúng ta khỏi Internet.

Điều đầu tiên cần làm trong tệp cấu hình là đặt (các) cổng HTTP mà Squid sẽ lắng nghe các yêu cầu đến. Theo mặc định, điều này được đặt thành 3128.  
Như chúng tôi biết, các dịch vụ mạng lắng nghe tại các cổng cụ thể cho các yêu cầu hướng đến chúng. Chỉ quản trị viên hệ thống mới có quyền sử dụng các cổng dưới 1024. Chúng được sử dụng bởi các chương trình cung cấp dịch vụ như POP, SMTP, HTTP, DNS, v.v. Số cổng lớn hơn 1024 được coi là thuộc về các dịch vụ không đáng tin cậy của quản trị viên cũng như các yêu cầu kết nối nhất thời, chẳng hạn như các yêu cầu liên quan đến dữ liệu gửi đi.

Giao thức truyền siêu văn bản (HTTP) thường sử dụng cổng 80 để nghe các yêu cầu web đến. Rất nhiều ISP sử dụng cổng 8080 như một loại tiêu chuẩn giả cho lưu lượng HTTP.

Như bạn đã học trước đó một chút, cổng bộ nhớ cache HTTP mặc định của Squid là 3128. Nếu chúng ta muốn thêm cổng 8080 vào cấu hình của mình, một trong những cách để làm điều đó là thêm nó vào tệp cấu hình, như sau:

**http\_port 3128 8080**

Một khía cạnh khác để xem xét là lưu trữ dữ liệu được lưu trữ. Như chúng tôi đã nghiên cứu, một trong những vai trò chính của proxy web là lưu trữ dữ liệu để tăng tốc truy cập và giảm mức sử dụng băng thông. Tất cả dữ liệu này phải được lưu trữ phải được lưu trữ, do đó, cần phải có bộ lưu trữ tốc độ cao thích hợp cho máy chủ proxy. Tùy thuộc vào yêu cầu thông lượng, phần cứng có sẵn cho Squid (hoặc bất kỳ máy chủ proxy nào khác cho vấn đề đó) có thể thực hiện hoặc cài đặt.

Là một phần của quy trình cấu hình, chúng tôi cần hướng dẫn Squid bằng cách cung cấp cho nó thông tin liên quan đến các thư mục cần lưu trữ dữ liệu được lưu trong bộ nhớ cache. Điều này được thực hiện với toán tử cache\_dir. Vì yêu cầu lưu trữ có thể thay đổi và chúng tôi có thể cần chỉ định thêm hơn một thư mục cho dữ liệu được lưu trong bộ nhớ cache, Squid cho phép chúng ta sử dụng nhiều toán tử cache\_dir.

Hãy để xem xét các giá trị mặc định cho toán tử cache\_dir trong tệp cấu hình squid.conf tiêu chuẩn, như sau:

**cache\_dir ufs /usr/local/squid/var/cache/ 100 16 256**

Hãy để có một cái nhìn nhanh về điều này có nghĩa là gì.

Dòng bắt đầu với toán tử cache\_dir. Điều này cho phép Squid biết đường dẫn và tên của thư mục nơi bộ đệm sẽ được lưu trữ. Thông tin này cũng hữu ích cho chúng tôi là điều tra viên. Cách Squid cấu trúc thư mục này là tạo một lớp thư mục con khác và sau đó là một lớp khác để cho phép lưu trữ và truy xuất hiệu quả mà không làm giảm tốc độ. Thông tin này được phản ánh trong dòng theo định dạng sau:

**cache\_dir storageformat Directory-Name Mbytes L1 L2 [options]**

Hãy để so sánh hai dòng lệnh.

Chúng ta có thể thấy rằng UFS là định dạng lưu trữ, theo sau là đường dẫn và tên đầy đủ của thư mục lưu trữ và sau đó là Mbytes, đó là dung lượng ổ đĩa trong Megabyte để sử dụng trong thư mục này. Theo mặc định, đây là 100 MB. Nó thường được đề nghị thay đổi điều này cho phù hợp với yêu cầu cụ thể của chúng tôi. Không có gì lạ khi thêm một số 0 khác để làm cho bộ lưu trữ ít nhất là một Gigabyte.

L1 biểu thị số lượng thư mục con cấp một hoặc cấp một mà Squid sẽ tạo trong Thư mục được chỉ định trước đó. Theo mặc định, đây là 16.

L2 là số lượng thư mục con cấp hai hoặc cấp hai sẽ được tạo trong mỗi thư mục cấp đầu tiên được đề cập trước đó. Trong trường hợp này, mặc định là 256.

Điều tiếp theo cần đảm bảo là đăng nhập. Chúng ta cần phải ra lệnh cho Squid để ghi lại mọi yêu cầu vào bộ đệm. Điều này được thực hiện bằng cách đảm bảo sự tồn tại của dòng sau trong tệp cấu hình:

**cache\_access\_log /var/log/squid/access.log**

Tất cả các yêu cầu đến máy chủ proxy sẽ được ghi lại theo đường dẫn và tên tệp được chỉ định trước đó. Một lần nữa, những nhật ký này rất quan trọng đối với chúng tôi từ góc độ pháp y mạng.

Trước khi chúng ta chuyển từ cài đặt cấu hình trong tệp squid.conf, điều rất quan trọng là phải chạm vào điều khiển truy cập mạng. Điều này được xử lý bởi ACL.

Một trong những vấn đề mà máy chủ proxy Squid được yêu cầu xử lý là hạn chế quyền truy cập vào bất kỳ IP nào không có trên mạng. Điều này là để ngăn chặn một số khách du lịch hạnh phúc từ một mạng gần đó ghé vào để tận dụng lòng hiếu khách cởi mở của chúng tôi. Cách đơn giản nhất để làm điều này là chỉ cho phép các địa chỉ IP là một phần của mạng của bạn. Điều này được minh họa tốt nhất với ví dụ hiển thị như sau:

**acl localnet src 192.168.1.0/255.255.255.0**

**http\_access allow localnet**

Đến bây giờ, chúng ta nên có một ý tưởng khá rõ ràng về việc quản lý tệp cấu hình Squid.

Hãy để Lốc chuyển sang bước thứ ba và bước cuối cùng để khởi động máy chủ Squid để kích hoạt và kích hoạt các cấu hình mà chúng tôi đã thực hiện, như sau:

**service squid start**

Đó là tất cả những gì nó cần! Bây giờ, chúng tôi có máy chủ proxy Squid và chạy với cấu hình mà chúng tôi thiết lập cho nó.

Chúng tôi có thể xác minh trạng thái của nó bằng cách gõ lệnh sau:

**service squid status**

Đó là nó! Bây giờ chúng ta có thể chuyển sang xác định và kiểm tra bằng chứng mà các máy chủ proxy tạo ra.

**7.1.4. Khai quật bằng chứng**

Như chúng ta đã thấy trong phần trước, bằng chứng tồn tại trong thư mục bộ đệm và nhật ký của máy chủ proxy.

Một số việc sử dụng thường xuyên của proxy web như Squid bao gồm bảo mật, hiệu quả, tuân thủ, kiểm tra người dùng và giám sát. Tất cả thông tin này phần lớn được xác định bởi dữ liệu có trong nhật ký.

Nhật ký cho phép chúng ta thấy như sau:

* Hoạt động web dành riêng cho người dung
* Các hoạt động web dành riêng cho ứng dụng
* Các hoạt động phần mềm độc hại sử dụng HTTP

Chúng ta hãy nhìn vào cấu trúc điển hình của các bản ghi được tạo bởi các máy chủ proxy.

Tệp access.log về cơ bản có hai định dạng có thể tùy thuộc vào cấu hình. Đầu tiên là định dạng tệp nhật ký mặc định hoặc gốc và thứ hai là Định dạng LogFile chung. Trong chương trước, chúng tôi đã kiểm tra Định dạng tệp logfile chung ở một mức độ chi tiết nào đó, do đó, trong chương này, hãy tập trung vào định dạng tệp nhật ký gốc của Squid. Mỗi dòng đại diện cho một sự kiện hoặc yêu cầu đến máy chủ. Định dạng của nó là như sau:

**time elapsed remotehost code/status bytes method URL rfc931 hierarchy\_code type**

Trong dòng trước đó, mọi lĩnh vực đều có thông tin được quan tâm. Chúng ta hãy nhìn vào từng người một trong những điều sau đây:

|  |  |  |
| --- | --- | --- |
| **Data Field** | **Type** | **Description** |
| Time | Float | Đây là thời gian hệ thống ở định dạng Unix. Về cơ bản, nó là một danh sách của mỗi giây trôi qua kể từ năm 1970. Có một số công cụ và tập lệnh perl có sẵn để chuyển đổi nó thành thứ mà con người có thể đọc được. |
| Elapsed | integer | Đây là thời gian trôi qua / thời gian tính bằng mili giây để hoàn thành giao dịch. |
| Máy chủ từ xa | String | Đây là địa chỉ khách hàng hoặc địa chỉ IP của trình duyệt yêu cầu. |
| Mã kết quả | String | Mã kết quả được tạo bởi Squid bao gồm một số thẻ được phân tách bằng ký tự gạch dưới. Điều này thường bắt đầu với bất kỳ một trong những điều sau đây: TCP, UDP hoặc NONE để biểu thị chế độ mà kết quả được gửi. Thẻ tiếp theo là một tùy chọn và thường được phân tách khỏi thẻ này bằng dấu gạch dưới. Một ví dụ về điều này sẽ là như sau  TCP\_HIT: Điều này có nghĩa là kết quả đã được phân phối bằng TCP (cổng HTTP 3128) và HIT biểu thị rằng nó đã được gửi từ bộ đệm.  TCP\_MISS: Điều này thực sự biểu thị rằng kết quả được phân phối là phản hồi của mạng.  Trang web Squid (www.squid-cache.org) có một tài liệu phong phú về các Mã kết quả và thẻ khác nhau bao gồm nó. |
| Mã trạng thái | Integer | Mã kết quả được theo sau bởi dấu gạch chéo và sau đó là Mã trạng thái. Các mã trạng thái HTTP này hầu hết được lấy từ RFC 1945, 2518, 2616 và 4918. Một số mã này có bản chất thông tin, chẳng hạn như 101 có nghĩa là Chuyển đổi giao thức và 102 có nghĩa là Xử lý,  trong khi những người khác có liên quan đến các chi tiết giao dịch và lỗi. Ví dụ: mã trạng thái 200 sẽ biểu thị OK (giao dịch thành công), trong khi mã 401 sẽ biểu thị một  Yêu cầu trái phép. |
| Bytes | Integer | Byte rõ ràng biểu thị kích thước của dữ liệu được gửi đến máy khách bằng Byte. Báo cáo lỗi, tiêu đề và dữ liệu đối tượng đều được tính vào tổng số này. |
| Phương pháp | String | Đây là phương thức yêu cầu HTTP được sử dụng để có được đối tượng. Chúng bao gồm GET, Head, PUT, POST, v.v. Một lần nữa, tài liệu chi tiết có sẵn trên trang web Squid. |
| URL | String | Điều này chứa URL đầy đủ theo yêu cầu của khách hàng. |
| rfc931 | String | Điều này có thể chứa danh tính người dùng của người dùng cho người yêu cầu. Thông tin này thường được lấy từ xác thực HTTP / TLS, tra cứu IDENT hoặc trình trợ giúp ACL bên ngoài. Nếu không tìm thấy danh tính, thì trường này sẽ chứa phần mềm - Hồi. |
| Hierarchy\_code | String | THỜI GIAN: Đây là tiền tố được gắn thẻ nếu thời gian chờ xảy ra trong khi chờ trả lời ICP từ hàng xóm.  MÃ HIERARCHY: Mã này giải thích cách xử lý yêu cầu của máy chủ. Chẳng hạn, phản hồi của TRỰC TIẾP cho thấy dữ liệu được tìm nạp trực tiếp từ nguồn gốc chính máy chủ, trong khi phản hồi của NONE có nghĩa là không có thông tin phân cấp, lỗi TCP, v.v. Tài liệu toàn diện có sẵn trên trang web squid-cache.org.  ĐỊA CHỈ IP / HOSTNAME: Điều này có thể thuộc về máy chủ Origin, cha mẹ của máy chủ bộ đệm ngang hàng. |
| Type | String | Đây là loại đối tượng được yêu cầu, thường là loại MIME dễ nhận biết; tuy nhiên, một số đối tượng không có loại và được đại diện bởi một -. |

Một điểm khác cần lưu ý là trong trường hợp tùy chọn gỡ lỗi của log\_mime\_headers được bật, tất cả các tiêu đề yêu cầu và trả lời HTTP được ghi lại và có thể có hai cột bổ sung trong nhật ký truy cập do điều này.

Bây giờ chúng tôi có một ý tưởng tốt về cấu trúc của nhật ký proxy web, chúng tôi cần tìm ra cách sử dụng chúng trong cuộc điều tra của chúng tôi.

Một số điều tra phổ biến mà chúng được sử dụng như sau:

* Vi phạm chính sách liên quan đến truy cập Internet
* Giám sát hoạt động của người dung
* Theo dõi sự lây lan của phần mềm độc hại và phần mềm gián điệp trong mạng của chúng tôi
* Tấn công xâm nhập vào máy khách và máy chủ. Cả nội bộ và bên ngoài
* Phát hiện hành vi trộm cắp IP và rò rỉ thông tin

Điều tra nhật ký máy chủ proxy có thể rất nhiều niềm vui. Chỉ cần quét về mục đích thông qua nhiều nhật ký có thể khá khác nhau, nhưng ngoài việc nâng cao mức độ hiểu biết của bạn, nó có thể không mang lại kết quả nhanh chóng.

Vì vậy, làm thế nào để chúng ta đi tìm kiếm bằng chứng trên proxy web?

Hãy bắt đầu với một kịch bản cụ thể. Chúng tôi có một người dùng không xác định trên mạng của mình, người đang tải lên các tệp bí mật của công ty chúng tôi (được gọi một cách thích hợp là secret.pdf) bên ngoài mạng của chúng tôi.

Như chúng tôi biết rằng các phương thức HTTP được sử dụng để xác định xem các tệp đang được tải về hoặc tải lên. Bất cứ khi nào chúng tôi gửi yêu cầu cho một trang web hoặc đồ họa, phương thức HTTP được sử dụng là GET. Tương tự, mỗi khi tải lên xảy ra (ví dụ: e-mail được gửi kèm theo tệp đính kèm), phương thức HTTP được sử dụng là POST.

Chỉ cần nhìn vào tất cả các mục nhật ký, trong đó phương thức HTTP = POST, sẽ cho chúng ta cái nhìn sâu sắc về tất cả dữ liệu rời khỏi mạng. Tương tự, lọc loại nội dung = application / pdf ngoài phương thức HTTP sẽ cung cấp cho chúng tôi danh sách các mục nhật ký trong đó các tệp PDF đã được tải lên khỏi mạng của chúng tôi.

Những điều bổ sung cần tìm khi điều tra các hoạt động đó bao gồm:

* Tải lên các địa chỉ IP không thể phân giải bằng cách sử dụng tra cứu DNS
* Tải lên các trang lưu trữ trực tuyến như Dropbox, iCloud và Skydrive hoặc các máy chủ lưu trữ như với tư cách là chủ nhà
* Tải lên xảy ra qua các cổng không bằng 80 (ví dụ: tải lên 10.10.1.7:31333)
* Tải lên với tên tệp bí mật trong chính mục nhập tệp nhật ký

Tương tự, ổ đĩa do nhiễm trùng tải xuống sẽ được xác định bằng GET và khi chúng ta xem nhật ký, chúng ta sẽ thấy rằng các tệp thực thi đã được tải xuống.

Một cách khác là xác định vi phạm chính sách sử dụng được chấp nhận của công ty bằng cách tải xuống tệp video hoặc nhạc của người dùng bằng cách xem kích thước tệp và loại tệp đã tải xuống.

Như chúng ta đã thấy rằng một khi chúng ta biết những gì chúng ta đang tìm kiếm, sẽ rất dễ dàng để có được proxy để thú nhận.

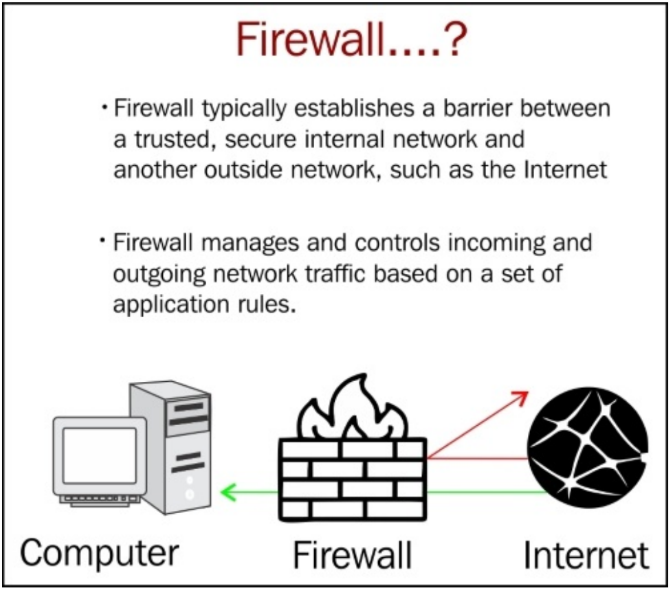
Bây giờ, hãy chuyển sang tìm hiểu và kiểm tra tường lửa và những cách mà họ có thể đóng góp cho việc kiểm tra pháp y của chúng tôi.

**7.2. Giao tiếp trong tường lửa**

**7.2.1. Vai trò tường lửa**

Đơn giản chỉ là tên, tường lửa, gợi lên hình ảnh của một bức tường lửa lớn đang đốt cháy bất cứ thứ gì trái phép và cố gắng vượt qua.

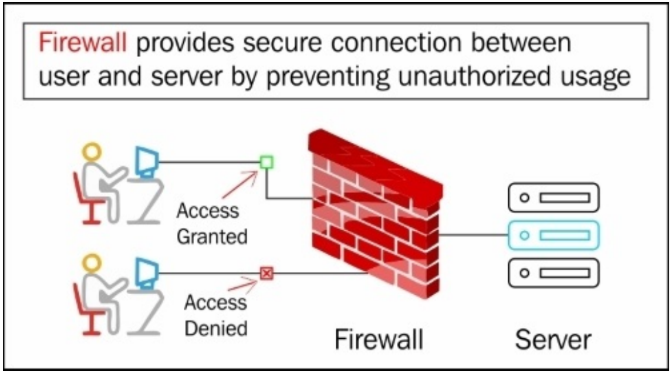
Đúng như tên gọi, trong thế giới kỹ thuật số, tường lửa ngăn chặn truy cập trái phép vào hoặc từ mạng. Một tường lửa thường ở chu vi của một mạng riêng và Internet mở, nó hoạt động như một rào cản và cho phép lưu lượng truy cập dựa trên một tập hợp được xác định trước quy tắc:



Hình ảnh trước cho thấy rõ chức năng của tường lửa. Như chúng ta có thể thấy, lưu lượng truy cập mạng có thể đi qua hoặc bị tường lửa từ chối khi phát hiện trái với quy tắc được xác định trước. Yếu tố quan tâm chính đối với chúng tôi là thực tế là mọi tương tác với tường lửa đều để lại dấu vết. Điều này được phản ánh dưới dạng một mục trong nhật ký tường lửa. Điều tra pháp y mạng yêu cầu chúng tôi hiểu tường lửa và các sự kiện tạo ra các mục trong tệp nhật ký. Với tư cách là những 007 kỹ thuật số, nó làm công việc của chúng tôi với những người khác làm cho tường lửa nói chuyện với nhau.

Một trong những điều cơ bản mà chúng ta cần hiểu là tường lửa là một hệ thống hoặc một nhóm các hệ thống hoạt động như một bouncer có nhiệm vụ là quyết định ai vào hoặc ai không vào mạng của chúng ta. Nói một cách đơn giản, tường lửa kiểm soát quyền truy cập vào mạng của chúng tôi và điều này thường dựa trên một số quy tắc được thực hiện bởi quản trị viên mạng. Ngoài ra, nó đóng một vai trò quan trọng trong việc giữ các tab trên mỗi trang truy cập mạng của chúng tôi hoặc không cố gắng truy cập nó vì bất kỳ lý do gì.

Một số tường lửa được thiết kế để cho phép chỉ một loại lưu lượng truy cập thông qua chúng, chẳng hạn như e-mail. Trong khi những người khác có thể được cấu hình để bảo vệ mạng khỏi đăng nhập trái phép từ thế giới bên ngoài. Tường lửa có thể cung cấp một điểm sặc duy nhất cho mạng. Điểm sặc này có thể được sử dụng để thực hiện các quy tắc kiểm toán và bảo mật hiệu quả nhằm bảo vệ và giám sát mạng, như được trình bày dưới đây:



**7.2.2. Các loại tường lửa**

Tường lửa có một lịch sử lâu dài. Họ bắt đầu sự nghiệp của mình khi Danh sách điều khiển truy cập (ACL) được nhúng trong các bộ định tuyến vẫn còn được sử dụng cho đến Tường lửa thế hệ mới (NGFW) mới và được quảng cáo rầm rộ.

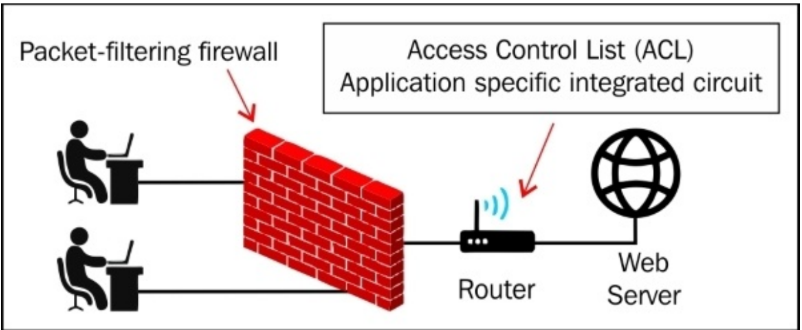
Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) 800 - 10 phân loại rộng rãi tường lửa thành ba loại khác nhau sau:

* Tường lửa lọc gói
* Tường lửa kiểm tra nhà nước
* Tường lửa ứng dụng / Proxy

Trong môi trường mạng ngày nay, có một mức độ trùng lặp khá cao với một số sản phẩm thương mại có các tính năng của cả ba loại.

1. **Tường lửa lọc gói.**

Các tường lửa này xác định quyền truy cập vào tài nguyên bên trong hoặc bên ngoài dựa trên Danh sách điều khiển truy cập. Việc lọc có thể dựa trên cơ sở địa chỉ IP nguồn hoặc đích, cổng, giao thức, phạm vi thời gian, v.v. Tất cả thông tin này có sẵn trong tiêu đề gói. Các bộ lọc gói kiểm tra tiêu đề và dựa trên một bộ quy tắc (ACL) được chỉ định, điều này quyết định xem có cho phép nó đi qua (ACCEPT) hay ngăn không cho nó đi qua (DROP), như trong hình sau:



Một điểm quan trọng cần nhớ là các tường lửa như vậy KHÔNG có cái nhìn sâu sắc về nội dung gói và đưa ra quyết định cho phép hoặc không cho phép các gói cụ thể dựa trên sự phù hợp của tiêu đề gói với thiết lập ACL vào thời điểm đó. Những tường lửa này hoạt động ở cấp độ mạng của mô hình OSI.

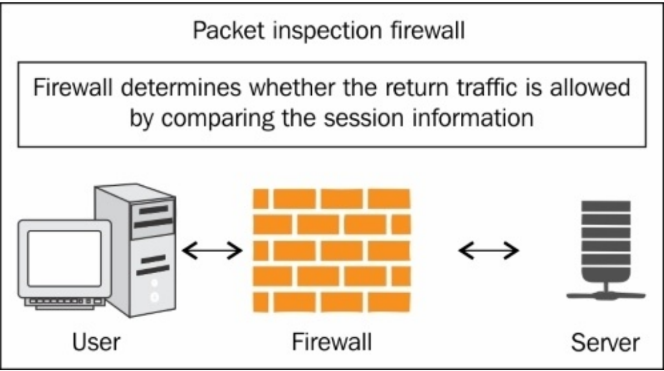
  Tuy nhiên, điểm yếu của họ nằm ở chính bản chất của họ. Hãy để một tình huống mà ACL đang sử dụng cho phép một cổng 80 mở.

Điều này khá phổ biến vì nó được sử dụng cho các yêu cầu HTTP (www). Bất kỳ người dùng độc hại nào cũng có thể thiết lập các gói của họ được chế tạo để chúng được chuyển đến cổng 80 và được chuyển qua thường xuyên.

   Mặc dù các tường lửa này đã có từ lâu, nhưng chúng không nên được giảm giá. Chúng khá phổ biến, cung cấp phản hồi rất nhanh và là một phần của tổ chức phòng thủ trong một tổ chức bảo vệ chuyên sâu.

1. **Tường lửa kiểm tra nhà nước**

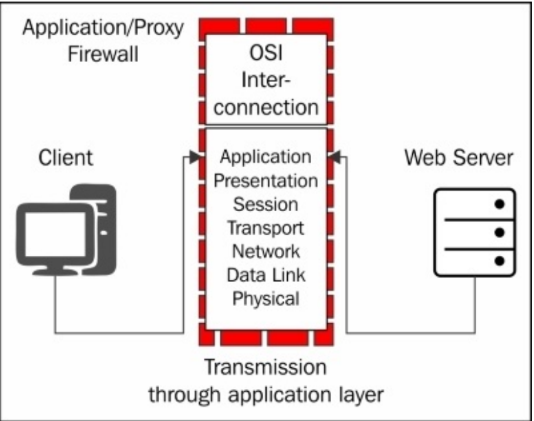
Tường lửa kiểm tra nhà nước là bước tiến hóa lớn tiếp theo. Một điểm yếu lớn trong loại bộ lọc gói tường lửa là khả năng bị đánh lừa bởi thông tin trong tiêu đề. Trong khi họ sẽ xem xét và phân tích một gói với SYN trong tiêu đề, họ sẽ cho phép một gói có ACK ngay lập tức, giả sử rằng nó đáp ứng với SYN của gói trước đó. Điều này cho phép các cá nhân độc hại tạo các gói chuyên dụng với ACK được cấu hình để tường lửa chỉ cho phép gói thông qua. Điều này là do thực tế là tường lửa bộ lọc gói không duy trì một bản ghi về trạng thái liên lạc giữa các thiết bị. Do đó, tường lửa kiểm tra gói trạng thái đã ra đời:



Họ phân loại và theo dõi trạng thái lưu lượng bằng cách giám sát tất cả các tương tác kết nối cho đến khi kết nối được đóng lại. Họ thu thập tất cả các gói liên quan đến tương tác, xác định khả năng chấp nhận của chúng và sau đó phát hành chúng ra mạng. Chúng hoạt động đến lớp bốn của mô hình OSI. Đây là lớp vận chuyển.  
 Những tường lửa này là một trợ giúp chính trong việc ngăn chặn các cuộc tấn công từ chối dịch vụ phân tán (DDOS).

1. **Tường lửa lớp ứng dụng**

Các tường lửa này hoạt động ở cấp ứng dụng của ngăn xếp TCP / IP. Các ứng dụng địa chỉ này như lưu lượng truy cập trình duyệt (HTTP), telnet hoặc lưu lượng Giao thức truyền tệp (FTP). Các tường lửa này được thiết kế để chặn, kiểm tra và thả hoặc chấp nhận các gói đi đến và đi từ một ứng dụng. Là một phần của vai trò, chúng được thiết kế để loại bỏ các gói khác mà không có bất kỳ sự thừa nhận nào đối với người gửi, như trong hình sau:



Mặc dù các tường lửa này có thể được thiết lập để kiểm tra và chặn các gói mạng có chứa Trojans và Worms, nhưng điều này lại có thêm chi phí trễ, dẫn đến sự chậm trễ trong việc chuyển tiếp gói.

  Tường lửa ứng dụng có thể hoạt động bằng cách nối vào các cuộc gọi ổ cắm và lọc các kết nối giữa các lớp thấp hơn (của mô hình OSI) và lớp ứng dụng. Tường lửa thực hiện chức năng như vậy thường được gọi là bộ lọc ổ cắm. Một vai trò khác mà tường lửa ứng dụng có liên quan là quản lý Dịch thuật Địa chỉ Mạng (NAT) và Cổng Dịch địa chỉ (PAT). Một điểm mạnh của tường lửa ứng dụng là thông tin được thu thập trong nhật ký.

  Tường lửa ứng dụng có hai loại: tường lửa ứng dụng dựa trên mạng và tường lửa ứng dụng dựa trên máy chủ. Trong khi tường lửa ứng dụng dựa trên mạng giám sát các cuộc gọi thông qua ngăn xếp OSI, tường lửa ứng dụng dựa trên máy chủ giám sát hoạt động thông qua các cuộc gọi hệ thống. Điều này có thể giám sát đầu vào và đầu ra của ứng dụng, các cuộc gọi dịch vụ hệ thống được thực hiện bởi một ứng dụng, cũng như các cuộc gọi được thực hiện từ hoặc đến nó.

**7.2.3. Phân tích nhật kí tường lửa**

Giống như chúng ta đã thấy trước đó trong trường hợp máy chủ proxy, nhật ký được thu thập bởi tường lửa là một tài sản lớn cho nhà điều tra. Hầu hết các nhà cung cấp tường lửa có định dạng nhật ký riêng mà họ cung cấp cho người dùng để sử dụng. Đôi khi, họ có một số lượng lớn các lĩnh vực, mà thực sự làm tăng độ chi tiết của cuộc điều tra. Tuy nhiên, hầu hết các bản ghi tường lửa chia sẻ một số đặc điểm chung.

Chúng bao gồm ngày và thời gian. Hãy cùng xem các bản ghi được tạo bởi thiết bị CyberRoam:

|  |  |  |
| --- | --- | --- |
| **Data Fields** | **Type** | **Description** |
| Ngày | Ngày | Ngày diễn ra sự kiện (yyyy-mm-dd). |
| Giờ | Giờ | Thời gian sự kiện (hh: mm: ss). |
| Múi giờ | Chuỗi | Múi giờ của thiết bị, ví dụ EST, PST, IST và GMT. |
| Tên thiết bị | Chuỗi | Số mô hình thiết bị. |
| Thiết bị | Chuỗi | Thiết bị định danh duy nhất. |
| Log\_id | Chuỗi | Mã 12 ký tự duy nhất bao gồm:  Loại nhật ký, ví dụ, 01 cho nhật ký tường lửa.  Đăng nhập thành phần, nghĩa là tấn công tường lửa / cục bộ ACL / DOS.  Đăng nhập loại phụ, nghĩa là cho phép / vi phạm.  Ưu tiên, ví dụ, 0 cho trường hợp khẩn cấp.  ID tin nhắn, ví dụ, 00001 cho lưu lượng được cho phép bởi tường lửa. |
| Log\_type | Chuỗi | Loại sự kiện, ví dụ, sự kiện tường lửa. |
| Log\_component | Chuỗi | Thành phần đăng nhập, ví dụ, quy tắc tường lửa. |
| Log\_subtype | Chuỗi | Loại phụ của sự kiện. |
| Trạng thái | Chuỗi | Tình trạng cuối cùng của lưu lượng truy cập cho phép hoặc bị từ chối. |
| Ưu tiên | Chuỗi | Mức độ nghiêm trọng của tuyến đường đi . |
| Thời lượng | Số nguyên | Độ bền của tuyến đường (giây). |
| Tường lửa\_rule\_id | Số nguyên | ID quy tắc tường lửa, nghĩa là ID quy tắc tường lửa được áp dụng trên lưu lượng. |
| User\_name | Chuỗi | Tên người dùng. |
| User\_group | Chuỗi | ID nhóm của người dùng. |
| Iap | Số nguyên | Chính sách truy cập Internet. |
| Ips\_policy\_id | Số nguyên | ID chính sách IPS được áp dụng trên lưu lượng. |
| Appfilter\_policy\_id | Số nguyên | ID chính sách lọc ứng dụng. |
| Ứng dụng | Chuỗi | Tên ứng dụng |
| In\_interface | Chuỗi | Giao diện cho lưu lượng đến, ví dụ, Cổng A.  Trống cho giao thông đi. |
| Out\_interface | Chuỗi | Giao diện cho lưu lượng đi, ví dụ, Cổng B.  Trống cho lưu lượng đến. |
| Src\_ip | Chuỗi | Địa chỉ IP gốc của lưu lượng. |
| Src\_mac | Chuỗi | Original source MAC address of traffic. |
| Src\_country\_code | Chuỗi | Mã của quốc gia mà IP nguồn thuộc về. |
| Dst\_ip | Chuỗi | Original destination IP address of traffic. |
| Dst\_country\_code | Chuỗi | Mã của quốc gia mà IP đích thuộc về. |
| Giao thức | Số nguyên | Giao thức số lượng đường đi . |
| Src\_port | Số nguyên | Cổng nguồn gốc của lưu lượng TCP và UDP. |
| Dst\_port | Số nguyên | Cổng đích ban đầu của TCP và UDP. |
| Icmp\_type | Số nguyên | ICMP loại lưu lượng ICMP. |
| icmp\_code | Số nguyên | Mã ICMP của lưu lượng ICMP. |
| Sent\_pkts | Số nguyên | Tổng số gói được gửi. |
| Received\_pkts | Số nguyên | Tổng số gói tin nhận được. |
| sent\_bytes | Số nguyên | Tổng số byte được gửi. |
| recv\_bytes | Số nguyên | Tổng số byte được nhận |
| trans\_src\_ip | Số nguyên | Địa chỉ IP nguồn được dịch cho lưu lượng đi. Nó chỉ được áp dụng trong chế độ tuyến đường. Các giá trị có thể là như sau:  "": Khi thiết bị được triển khai ở chế độ Cầu hoặc dịch địa chỉ IP nguồn là không được thực hiện.  Địa chỉ IP: Địa chỉ IP mà địa chỉ IP nguồn gốc được dịch. |
| trans\_src\_port | Số nguyên | Cổng nguồn được dịch cho lưu lượng đi. Nó chỉ được áp dụng trong chế độ tuyến đường.  Các giá trị có thể là như sau:  "": Khi thiết bị được triển khai ở chế độ Cầu hoặc dịch cổng cổng nguồn không được thực hiện.  Cổng: Cổng mà cổng gốc được dịch. |
| trans\_dst\_ip | Số nguyên | Địa chỉ IP đích được dịch cho lưu lượng đi. Nó chỉ được áp dụng trong chế độ tuyến đường.  Các giá trị có thể là như sau:  "": Khi thiết bị được triển khai ở chế độ Cầu hoặc dịch địa chỉ IP đích không được thực hiện.  Địa chỉ IP: Địa chỉ IP mà địa chỉ IP đích ban đầu được dịch. |
| Trans\_dst\_port | Số nguyên | Cổng đích được dịch cho lưu lượng đi. Nó chỉ được áp dụng trong chế độ tuyến đường. Các giá trị có thể là như sau:  Không áp dụng: Khi thiết bị được triển khai ở chế độ Cầu hoặc dịch cổng cổng đích không được thực hiện.  Cổng: Cổng mà cổng gốc được dịch. |
| Srczonetype | Chuỗi | Loại vùng nguồn, ví dụ, LAN. |
| Dstzonetype | Chuỗi | Loại vùng đích, ví dụ, mạng WAN. |
| Dir\_disp | Chuỗi | Hướng gói.  Các giá trị có thể là như sau:  org, trả lời và "" |
| Kết nối |  | Sự kiện mà nhật ký này được tạo ra. |
| conn\_id | Số nguyên | Định danh duy nhất của kết nối. |
| vconn\_id | Số nguyên | ID kết nối của kết nối chính. |

Bây giờ chúng ta đã thấy tất cả các biến liên quan đến một bản ghi, hãy để Lọ thấy một vài mục nhật ký để chúng ta có thể liên quan đến chúng khi chúng ta làm việc trong một trường hợp:

* Sự kiện: Lưu lượng tường lửa

Thành phần bị từ chối: Quy tắc tường lửa

Nhật ký mẫu:

**date=2015-08-07 time=16:27:27 timezone=“GMT” device\_name=“CR500ia” device\_id= C070123456-ABCDEF log\_id=010102600002 log\_type=“Firewall” log\_component=“Firewall Rule” log\_subtype=“Denied” status=“Deny” priority=Information duration=0 fw\_rule\_id=3 user\_name=”” user\_gp=”” iap=2 ips\_policy\_id=0 appfilter\_policy\_id=0 application=”” in\_interface=“PortG.16” out\_interface=“PortB” src\_mac=00:0d:48:0a:05:45 src\_ip=172.16.16.95 src\_country\_code= dst\_ip=192.168.5.2 dst\_country\_code= protocol=“UDP” src\_port=42288 dst\_port=53 sent\_pkts=0 recv\_pkts=0 sent\_bytes=0 recv\_bytes=0 tran\_src\_ip= tran\_src\_port=0 tran\_dst\_ip= tran\_dst\_port=0 srczonetype=”” dstzonetype=”” dir\_disp=”” connid=”” vconnid=””**

* Sự kiện: Lưu lượng truy cập ACL cục bộ được phép

Thành phần: ACL cục bộ

Nhật ký mẫu**:**

**date=2015-08-07 time=14:44:57 timezone=“GMT “device\_name=“CR500ia” device\_id= C070123456-ABCDEF log\_id=010301602001 log\_type=“Firewall” log\_component=“Appliance Access” log\_subtype=“Allowed” status=“Allow” priority=Information duration=30 fw\_rule\_id=0 user\_name=”” user\_gp=”” iap=0 ips\_policy\_id=0 appfilter\_policy\_id=0 application=”” in\_interface=“PortG.2” out\_interface=”” src\_mac=00: 0:00: 0:00: 0 src\_ip=172.16.16.54 src\_country\_code= dst\_ip=192.168.52.31 dst\_country\_code= protocol=“ICMP” icmp\_type=8icmp\_code=0 sent\_pkts=1 recv\_pkts=1 sent\_bytes=212 recv\_bytes=212 tran\_src\_ip= Firewall Log Format tran\_src\_port=0 tran\_dst\_ip= tran\_dst\_port=0 srczonetype=”” dstzonetype=”” dir\_disp=”” connevent=“Stop” connid=“3153155488” vconnid=””**

* Sự kiện: Lưu lượng truy cập ACL cục bộ bị từ chối

Thành phần: ACL cục bộ

Nhật ký mẫu:

**date=2013-08-07 time=13:25:27 timezone=“IST” device\_name=“CR500ia” device\_id=C070100126-VW717U log\_id=01030060234 log\_type=“Firewall” log\_component=“Appliance Access” log\_subtype=“Denied” status=“Deny” priority=Information duration=0 fw\_rule\_id=0 user\_name=”” user\_gp=”” iap=0 ips\_policy\_id=0 appfilter\_policy\_id=0 application=”” in\_interface=“PortG.4” out\_interface=”” src\_mac=d0:17:78:d6:4c:b0 src\_ip=10.104.13.140 src\_country\_code= dst\_ip=255.255.255.255 dst\_country\_code= protocol=“UDP” src\_port=47779 dst\_port=8167 sent\_pkts=0 recv\_pkts=0 sent\_bytes=0 recv\_bytes=0 tran\_src\_ip= tran\_src\_port=0 tran\_dst\_ip= tran\_dst\_port=0 srczonetype=”” dstzonetype=”” dir\_disp=”” connid=”” vconnid=””**

Các mạng của chúng tôi liên tục bị phát hiện từ Internet và từ góc độ điều tra, họ phải trả tiền để xem các bản ghi tường lửa cho các địa chỉ IP bị từ chối. Điều này cho chúng tôi thấy những gì đang được thăm dò và chúng tôi hiểu rõ hơn về những gì chúng tôi nên làm việc tại bảo vệ.

Một điều khác cần chú ý trong nhật ký tường lửa của chúng tôi là các lần thử đăng nhập không thành công. Đây là một chỉ báo tuyệt vời cho thấy mạng của chúng tôi đang bị tấn công và nó cũng chỉ ra tài nguyên cụ thể đang được nhắm mục tiêu vào thời điểm đó.

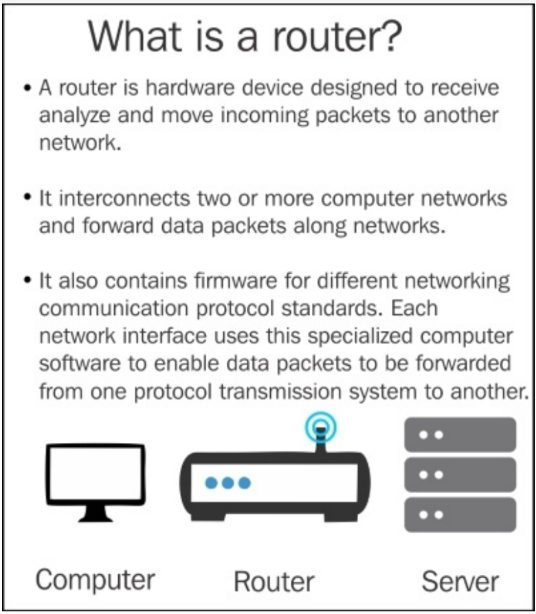
Giả sử rằng chúng tôi có một ý tưởng tốt về lưu lượng truy cập đi ra bình thường từ các hệ thống của chúng tôi, tường lửa của chúng tôi sẽ cung cấp cho chúng tôi cái nhìn sâu sắc về lưu lượng truy cập không phải là đặc trưng. Loại lưu lượng truy cập này có thể là dấu hiệu của việc nhiễm bot và làm nổi bật các máy chủ đang cố gắng báo cáo.

Như chúng ta có thể thấy, có rất nhiều thông tin trong các bản ghi tường lửa này. Do đó, chúng tôi phải theo dõi các bằng chứng từ tường lửa vì đây chắc chắn có thể là một tài sản cho cuộc điều tra pháp y mạng của chúng tôi.

**7.3. Router Bộ định tuyến**

Vào ngày 15 tháng 9 năm 2015, thế giới bảo mật thông tin đã bị chấn động bởi tin tức rằng một vụ hack có tên là SYNful gõ đã sửa đổi phần sụn của một số bộ định tuyến CISCO. Điều này cho phép những kẻ tấn công duy trì sự hiện diện liên tục trong bộ định tuyến, do đó làm lộ lưu lượng mạng và cho phép bộ định tuyến hoạt động như một bài nghe cho kẻ tấn công.

Bộ định tuyến từ lâu đã là nền tảng của Internet. Vai trò của bộ định tuyến là kết nối các mạng với Internet và chọn đường dẫn tốt nhất để thông tin đến nhanh chóng. Trên thực tế, xu hướng toàn cầu là cơ sở hạ tầng mạng quốc gia phụ thuộc vào các bộ định tuyến để xử lý lưu lượng mạng. Do đó, lý do là nếu các bộ định tuyến mang lưu lượng truy cập thế giới, họ cũng sẽ có quyền riêng tư đối với tất cả các nhật ký lưu lượng liên quan:



Nhìn thấy loại vai trò của bộ định tuyến, bộ định tuyến thường là mục tiêu của các cuộc tấn công, đặc biệt là Từ chối dịch vụ (DoS) hoặc vô hiệu hóa loại tấn công của bộ định tuyến. Thỏa hiệp bộ định tuyến cũng được biết nơi bộ định tuyến được sử dụng để vượt qua các thành phần bảo mật mạng khác như tường lửa hoặc IDS.

Bộ định tuyến lưu trữ thông tin như mật khẩu và bảng định tuyến cũng như thông tin về các khối mạng. Điều này làm cho chúng mục tiêu trung gian. Các bộ định tuyến thỏa hiệp có thể được sử dụng như bước đệm để tấn công phần còn lại của mạng.

Hãy cùng xem nhanh bộ nhớ lưu trữ trong các bộ định tuyến.

Trong khi các bộ định tuyến có hai loại bộ nhớ, bộ nhớ thực tế có sẵn là khá nhỏ. Đầu tiên là đèn flash hoặc bộ nhớ liên tục. Điều này có phần sụn, iOS và có liên quan thông tin cấu hình và là hợp lý vĩnh viễn. Thứ hai là RAM. Điều này rất dễ bay hơi và dữ liệu chứa trong đó có thể bị mất hoàn toàn nếu tắt. Từ góc độ điều tra, dữ liệu này có thể rất quan trọng vì nó chứa các thành phần sau:

* Mật khẩu tạm thời
* Cấu hình đang chạy
* Thống kê
* Nhật ký cục bộ
* Lập lịch
* Dịch vụ nghe
* Bảng ARP
* Bảng định tuyến động
* NAT
* Vi phạm ACL.

Như chúng ta có thể thấy, nếu bộ định tuyến bị tắt trước khi thu thập tất cả điều này, thông tin có giá trị sẽ bị mất. Tuy nhiên, dữ liệu liên tục (bộ nhớ flash) sẽ không bị ảnh hưởng. Để điều tra thành công, chúng tôi cần khôi phục dữ liệu dễ bay hơi trên cơ sở ưu tiên là bước đầu tiên.

Trong trường hợp như vậy, một kết nối vật lý đến bộ định tuyến là bắt buộc trước khi chúng tôi có thể có được bằng chứng cần thiết. Một máy tính xách tay có dây cáp thích hợp để kết nối với cổng console sẽ được yêu cầu. Máy tính xách tay sẽ cần phải tải phần mềm Terminal lên nó để cho phép chúng tôi kết nối trực tiếp với bộ định tuyến thay vì qua mạng.

Sau khi kết nối, chúng tôi cần xác định những điều sau đây:

* Bộ định tuyến thời gian hiện tại
* Ai đang đăng nhập
* Thời gian kể từ lần khởi động cuối cùng
* Ổ cắm nghe (như telnet)
* Cấu hình khởi động
* Chạy cấu hình
* Tuyến đường IP
* IP arp
* Ổ cắm IP
* Bản dịch IP NAT
* Nhóm và người dùng SNMP
* Ghi nhật ký.

Các khía cạnh đăng nhập cũng rất quan trọng. Sau khi kết nối với bộ định tuyến, cần kiểm tra xem liệu ghi nhật ký đệm có được bật hay không. Nếu có, lệnh ghi nhật ký chương trình sẽ hiển thị cho chúng tôi phần bên trong của bộ đệm nhật ký bộ định tuyến, mức độ được đặt thành, cũng như các máy chủ lưu trữ nhật ký được gửi đến. Ghi nhật ký đầu cuối cho phép các phiên không giao diện điều khiển để xem các mục nhật ký. Ghi nhật ký nhật ký hệ thống cho phép các tin nhắn được gửi đến một máy chủ syslog được chỉ định. Ghi nhật ký vi phạm ACL sẽ tạo ra một số lượng lớn các nhật ký thú vị trong bộ đệm ghi nhật ký ghi lại các vi phạm ACL.

Ngoài hai nguồn bằng chứng trước đó (cụ thể là bộ nhớ và nhật ký dễ bay hơi), vụ hack bộ định tuyến CISCO gần đây cho thấy bộ nhớ flash không bay hơi cũng dễ bị tấn công. Bản hack hiện tại đã chứng minh rằng mọi sửa đổi trong phần mềm vẫn nằm trong bộ nhớ liên tục và có thể gây rò rỉ dữ liệu quy mô lớn.

**Kết luận**

Chương này, mặc dù hơi dài, đã cho chúng ta thấy ba thành phần rất quan trọng của bất kỳ mạng nào. Là nhà điều tra pháp lý , bạn đã tìm hiểu về các công định tuyến. Bạn cũng đã học được vai trò của họ trong sơ đồ lớn của sự việc và hiểu cách thức và nơi các bằng chứng lưu trữ.

Chúng tôi đã xem xét máy chủ proxy Squid và các định dạng nhật ký khác nhau phổ biến cho từng thành phần này. Chúng tôi đã phát triển sự hiểu biết về các trường khác nhau trong tệp nhật ký và những gì mỗi trường này thể hiện. Chúng tôi cũng đã đạt được cái nhìn sâu sắc về vai trò chính

Bộ định tuyến phát, bộ nhớ liên tục và dễ bay hơi mà chúng có, các bản ghi, cũng như tầm quan trọng của việc thu thập thông tin từ cả những bộ nhớ và nhật ký này từ góc độ pháp y của mạng.

Chúng tôi đã đạt được tiến bộ thú vị và khi chúng tôi tiếp tục, chúng tôi sẽ nghiên cứu cách dữ liệu được nhập lậu qua các đường hầm VPN trong chương tiếp theo. Chúng tôi cũng sẽ thấy các loại đường hầm khác nhau cũng như các lỗ hổng VPN.