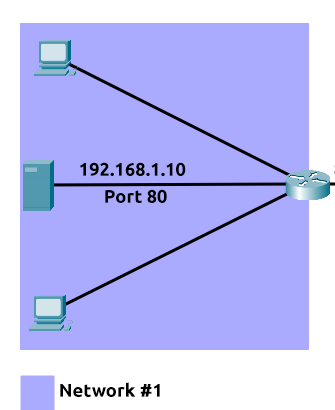
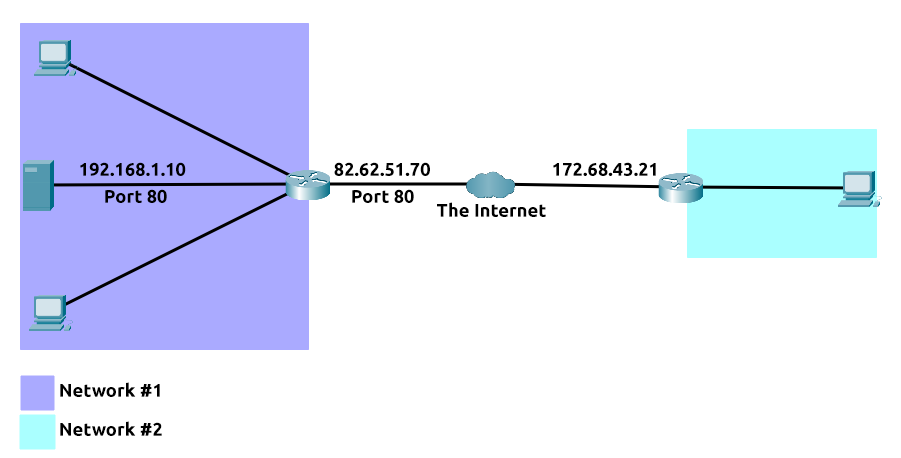
**Giới thiệu về chuyển tiếp cổng:**

Chuyển tiếp cổng là 1 thành phần cần thiết trong việc kết nối những ứng dụng và dịch vụ với Internet. Không có chuyển tiếp cổng, những ứng dụng và dịch vụ như máy chủ web chỉ có thể chạy trong cùng 1 mạng.

Lấy mạng bên dưới làm ví dụ. Trong mạng này, máy chủ với địa chỉ IP là 192.168.1.10 chạy máy chủ web ở cổng 80. Chỉ có hai máy tính khác trên mạng này có thể truy cập nó (mạng nội bộ)



Nếu nhà quản trị muốn trang web có thể truy cập công cộng (bằng việc sử dụng Internet), bọn họ phải thực thi chuyển tiếp cổng như hình bên dưới:



Với thiết kế này, mạng 2 sẽ truy cập được máy chủ web chạy trên mạng 1 bằng cách sử dụng địa chỉ IP công cộng là 82.62.51.70

Rất dễ nhầm lẫn giữa việc chuyển tiếp cổng với những hành vi của tường lửa. Tuy vậy, ở giai đoạn này, chỉ nên hiểu chuyển tiếp cổng là mở những cổng chỉ định. Còn tường lửa xác định xem lưu lượng có thể đi qua những cổng đó được không.

Chuyển tiếp cổng được cấu hình ở router của 1 mạng.

**Tường lửa 101**

Tường lửa là 1 thiết bị trong mạng chịu trách nhiệm xác định lưu lượng được phép vào hoặc ra. Hãy xem tường lửa như 1 ranh giới bảo mật cho mạng

Quản trị có thể cấu hình tường lửa dựa trên 1 số yếu tố sau:

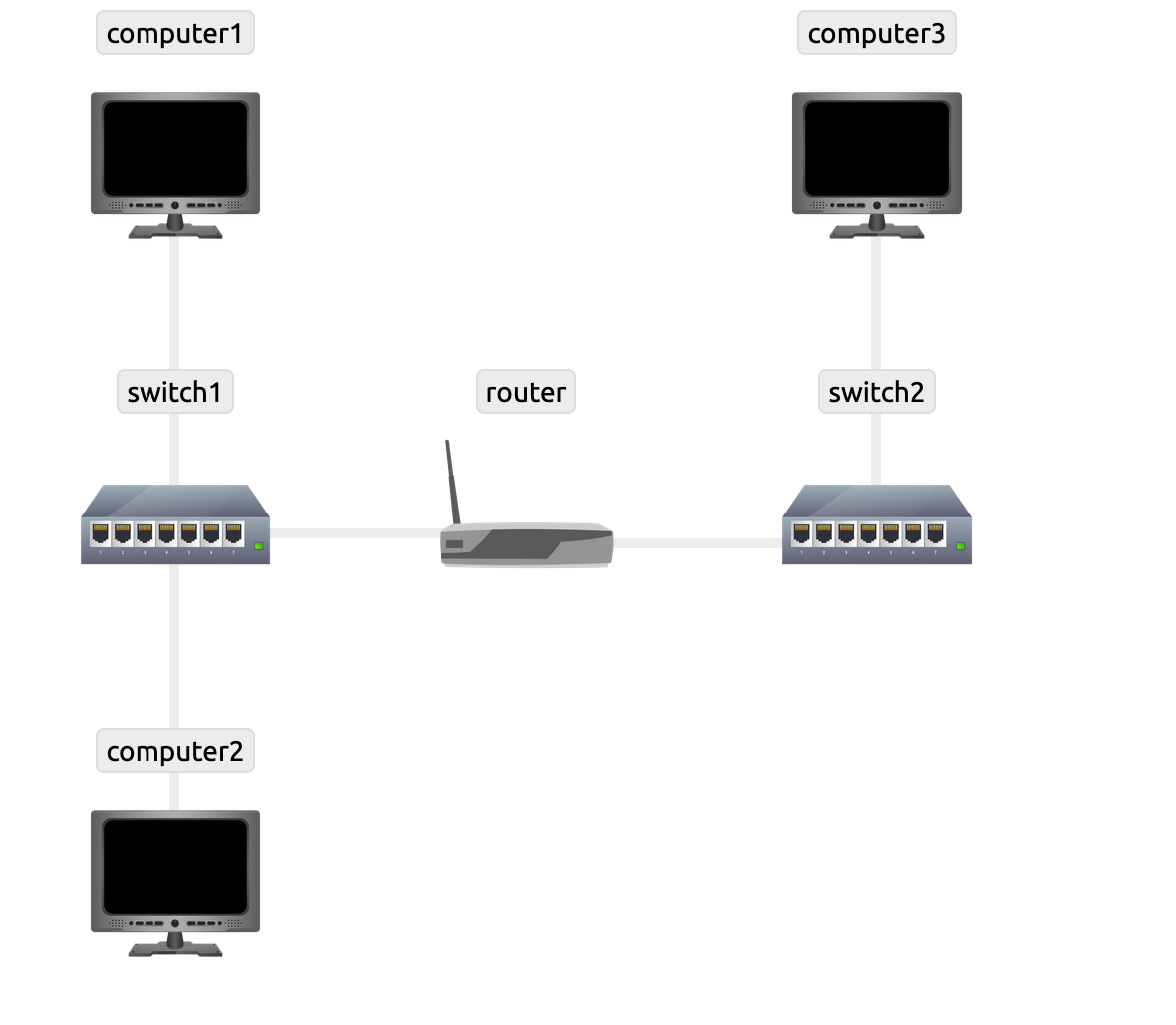
* Lưu lượng đến từ đâu?
* Lưu lượng sẽ đi đâu?
* Lưu lượng truy cập cho cổng nào?
* Giao thức lưu lượng sử dụng?

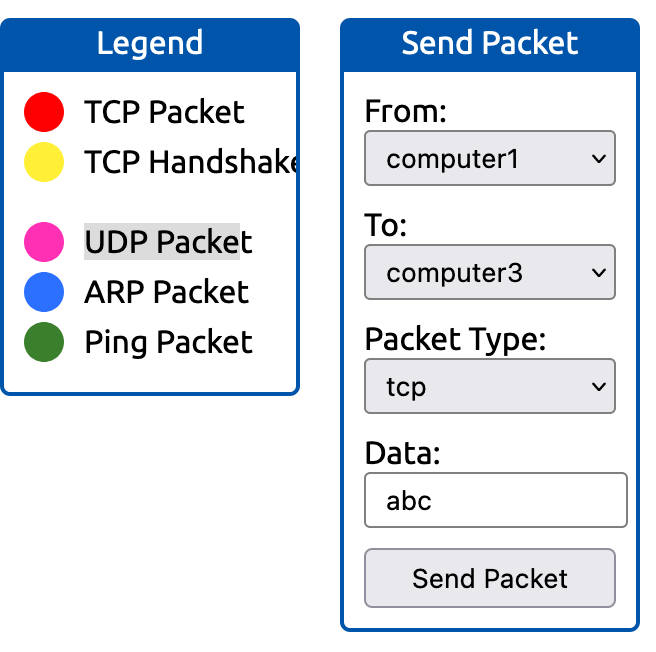
Tường lửa phân tích những gói tin để trả lời cho những câu hỏi trên.

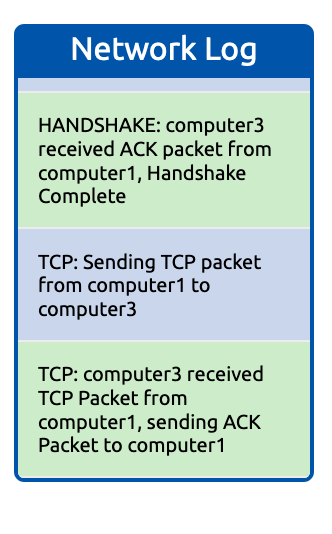
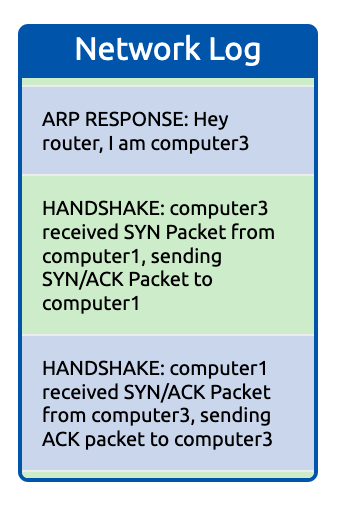
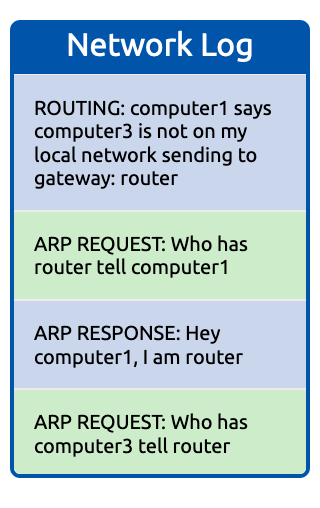
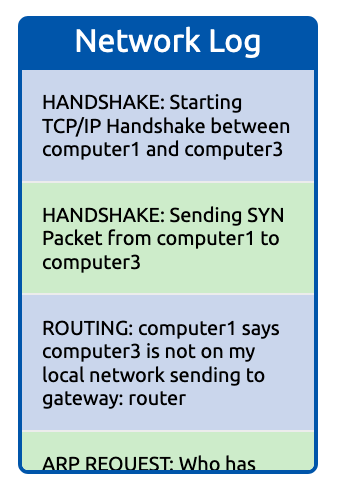
Tường lửa có rất nhiều hình dạng và kích thước. Từ những phần cứng chuyên dụng (thường tìm thấy ở những mạng lớn như doanh nghiệp) có thể xử lí 1 lượng lớn dữ liệu đến bộ định tuyến nhỏ hoặc phần mềm như Snort, tường lửa có thể được phân thành 2 đến 5 loại:

|  |  |
| --- | --- |
| **Firewall Category** | **Description** |
| Stateful | This type of firewall uses the entire information from a connection; rather than inspecting an individual packet, this firewall determines the behaviour of a device **based upon the entire connection**.  This firewall type consumes many resources in comparison to stateless firewalls as the decision making is dynamic. For example, a firewall could allow the first parts of a TCP handshake that would later fail.  If a connection from a host is bad, it will block the entire device. |
| Stateless | This firewall type uses a static set of rules to determine whether or not **individual packets** are acceptable or not. For example, a device sending a bad packet will not necessarily mean that the entire device is then blocked.  Whilst these firewalls use much fewer resources than alternatives, they are much dumber. For example, these firewalls are only effective as the rules that are defined within them. If a rule is not exactly matched, it is effectively useless.  However, these firewalls are great when receiving large amounts of traffic from a set of hosts (such as a Distributed Denial-of-Service attack) |

**Practical – Network Simulator:**



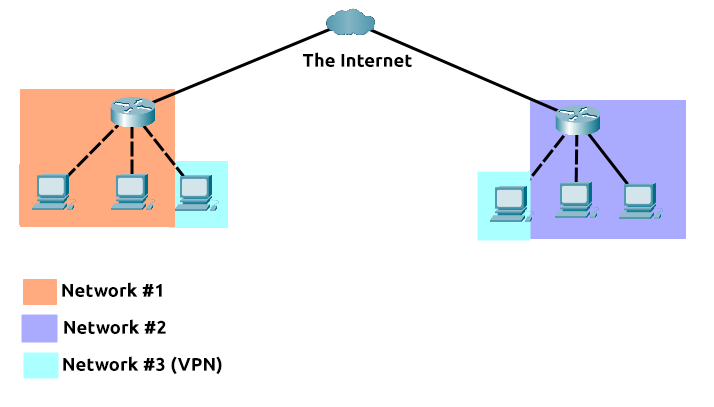




**VPN cơ bản:**

Mạng riêng ảo là 1 công nghệ cho phép những thiết bị ở các mạng riêng giao tiếp bảo mật bằng cách tạo 1 đường dẫn chuyên dụng giữa chúng qua internet (hay còn gọi là tunnel). Những thiết bị được kết nối trong tunnel này tạo thành mạng riêng.

Ví dụ, chỉ những thiết bị trong cùng 1 mạng (trong doanh nghiệp) có thể giao tiếp. Tuy nhiên VPN cho phép hai trụ sở được kết nối.



1. Mạng 1 (trụ sở 1)

2. Mạng 2 (trụ sở 2)

3. Mạng 3 (hai thiết bị kết nối qua VPN)

Những thiết bị kết nối trên mạng 3 vẫn là 1 phần của mạng 1 và mạng 2 nhưng cùng nhau hình thành 1 mạng riêng (mạng 3) mà chỉ những thiết bị kết nối qua VPN mới có thể giao tiếp.

Cùng xem xét 1 số lợi ích của VPN:

|  |  |
| --- | --- |
| **Benefit** | **Description** |
| Allows networks in different geographical locations to be connected. | For example, a business with multiple offices will find VPNs beneficial, as it means that resources like servers/infrastructure can be accessed from another office. |
| Offers privacy. | VPN technology uses encryption to protect data. This means that it can only be understood between the devices it was being sent from and is destined for, meaning the data isn't vulnerable to sniffing.  This encryption is useful in places with public WiFi, where no encryption provided by the network. You can use a VPN to protect your traffic from being viewed by other people. |
| Offers anonyminity. | Journalists and activists depend upon VPNs to safely report on global issues in countries where freedom of speech is controlled.  Usually, your traffic can be viewed by your ISP and other intermediaries and therefore tracked.  The level of anonymity a VPN provides is only as much as how other devices on the network respect privacy.. For example, a VPN that logs all of your data/history is essentially the same as not using a VPN in this regard. |

TryHackMe sử dụng VPN để kết nối bạn đến máy ảo có lỗ hổng mà không đưa nó trực tiếp ra internet. Điều đó có nghĩa là:

Bạn có thể tương tác 1 cách bảo mật với những máy ảo

Những nhà cung cấp dịch vụ như ISPs không nghĩ bạn đang tấn công máy ảo khác trên Internet (trái với những điều khoản của dịch vụ)

VPN cung cấp bảo mật cho TryHackMe và những máy ảo có lỗ hổng không thể truy cập qua Internet.

Công nghệ VPN đã cải thiện qua nhiều năm. Cùng khám phá một vài công nghệ dưới đây:

|  |  |
| --- | --- |
| **VPN Technology** | **Description** |
| PPP | This technology is used by PPTP (explained below) to allow for authentication and provide encryption of data. VPNs work by using a private key and public certificate (similar to **SSH**). A private key & certificate must match for you to connect.  This technology is not capable of leaving a network by itself (non-routable). |
| PPTP | The **P**oint-to-**P**oint **T**unneling **P**rotocol (**PPTP**) is the technology that allows the data from PPP to travel and leave a network.  PPTP is very easy to set up and is supported by most devices. It is, however, weakly encrypted in comparison to alternatives. |
| IPSec | Internet Protocol Security (IPsec) encrypts data using the existing **I**nternet **P**rotocol (**IP**) framework.  IPSec is difficult to set up in comparison to alternatives; however, if successful, it boasts strong encryption and is also supported on many devices. |