Introduction to Port Forwarding

Port forwarding is an essential component in connecting applications and services to the Internet. Without port forwarding, applications and services such as web servers are only available to devices within the same direct network.

Take the network below as an example. Within this network, the server with an IP address of "192.168.1.10" runs a webserver on port 80. Only the two other computers on this network will be able to access it (this is known as an intranet).

If the administrator wanted the website to be accessible to the public (using the Internet), they would have to implement port forwarding, like in the diagram below:

With this design, Network #2 will now be able to access the webserver running on Network #1 using the public IP address of Network #1 (82.62.51.70).

It is easy to confuse port forwarding with the behaviours of a firewall (a technology we'll come on to discuss in a later task). However, at this stage, just understand that port forwarding opens specific ports (recall how packets work). In comparison, firewalls determine if traffic can travel across these ports (even if these ports are open by port forwarding).

Port forwarding is configured at the router of a network.

Answer the questions below

What is the name of the device that is used to configure port forwarding?

Firewalls 101

A firewall is a device within a network responsible for determining what traffic is allowed to enter and exit. Think of a firewall as border security for a network. An administrator can configure a firewall to **permit** or **deny** traffic from entering or exiting a network based on numerous factors such as:

* Where the traffic is coming from? (has the firewall been told to accept/deny traffic from a specific network?)
* Where is the traffic going to? (has the firewall been told to accept/deny traffic destined for a specific network?)
* What port is the traffic for? (has the firewall been told to accept/deny traffic destined for port 80 only?)
* What protocol is the traffic using? (has the firewall been told to accept/deny traffic that is UDP, TCP or both?)

Firewalls perform packet inspection to determine the answers to these questions.

Firewalls come in all shapes and sizes. From dedicated pieces of hardware (often found in large networks like businesses) that can handle a magnitude of data to residential routers (like at your home!) or software such as [Snort](https://www.snort.org/), firewalls can be categorised into 2 to 5 categories.

We'll cover the two primary categories of firewalls in the table below:

|  |  |
| --- | --- |
| **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) |

Answer the questions below

What layers of the OSI model do firewalls operate at?

For this answer, just provide the numbers in ascending order, separated by an ampersand (&) **I.e:** 4 & 5

Principio del formulario

SubmitHint

Final del formulario

What category of firewall inspects the **entire connection**?

Principio del formulario

Submit

Final del formulario

What category of firewall inspects individual packets?

VPN Basics

A **V**irtual **P**rivate **N**etwork (or **VPN** for short) is a technology that allows devices on separate networks to communicate securely by creating a dedicated path between each other over the Internet (known as a tunnel). Devices connected within this tunnel form their own private network.

For example, only devices within the same network (such as within a business) can directly communicate. However, a VPN allows two offices to be connected. Let's take the diagram below, where there are three networks:

1. Network #1 (Office #1)
2. Network #2 (Office #2)
3. Network #3 (Two devices connected via a VPN)

The devices connected on Network #3 are still a part of Network #1 and Network #2 but also form together to create a private network (Network #3) that only devices that are connected via this VPN can communicate over.

Let's cover some of the other benefits offered by a VPN in the table below:

|  |  |
| --- | --- |
| **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 is provided by the network. You can use a VPN to protect your traffic from being viewed by other people. |
| Offers anonymity. | 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 uses a VPN to connect you to our vulnerable machines without making them directly accessible on the Internet! This means that:

* You can securely interact with our machines
* Service providers such as ISPs don't think you are attacking another machine on the Internet (which could be against the terms of service)
* The VPN provides security to TryHackMe as vulnerable machines are not accessible using the Internet.

VPN technology has improved over the years. Let's explore some existing VPN technologies below:

|  |  |
| --- | --- |
| **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. |

Answer the questions below

What VPN technology **only**encrypts & provides the authentication of data?

Principio del formulario

SubmitHint

Final del formulario

What VPN technology uses the IP framework?

Principio del formulario

**What is a Router?**

It's a router's job to connect networks and pass data between them. It does this by using routing (hence the name router!).

Routing is the label given to the process of data travelling across networks. Routing involves creating a path between networks so that this data can be successfully delivered. Routers operate at Layer 3 of the OSI model. They often feature an interactive interface (such as a website or a console) that allows an administrator to configure various rules such as port forwarding or firewalling.

Routing is useful when devices are connected by many paths, such as in the example diagram below, where the most optimal path is taken:

Routers are dedicated devices and do not perform the same functions as switches.

We can see that Computer A's network is connected to the network of Computer B by two routers in the middle. The question is: what path will be taken? Different protocols will decide what path should be taken, but factors include:

- What path is the shortest?

- What path is the most reliable?

- Which path has the faster medium (e.g. copper or fibre)?

What is a Switch?

A switch is a dedicated networking device responsible for providing a means of connecting to multiple devices. Switches can facilitate many devices (from 3 to 63) using Ethernet cables.

Switches can operate at both layer 2 and layer 3 of the OSI model. However, these are exclusive in the sense that Layer 2 switches cannot operate at layer 3.

Take, for example, a layer 2 switch in the diagram below. These switches will forward frames (remember that the original IP packets are encapsulated within the frames) onto the connected devices using their MAC address.

These switches are solely responsible for sending frames to the correct device.

Now, let's move onto layer 3 switches. These switches are more sophisticated than layer 2, as they can perform *some*of the responsibilities of a router. Namely, these switches will send frames to devices (as layer 2 does) and route packets to other devices using the IP protocol.

Let's take a look at the diagram below of a layer 3 switch in action. We can see that there are two IP addresses:

* 192.168.1.1
* 192.168.2.1

A technology called **VLAN** (**V**irtual **L**ocal **A**rea **N**etwork) allows specific devices within a network to be virtually split up. This split means they can all benefit from things such as an Internet connection but are treated separately. This network separation provides security because it means that rules in place determine how specific devices communicate with each other. This segregation is illustrated in the diagram below:

In the context of the diagram above, the "Sales Department" and "Accounting Department" will be able to access the Internet, but not able to communicate with each other (although they are connected to the same switch).

Answer the questions below

What is the verb for the action that a router does?

Principio del formulario

SubmitHint

Final del formulario

What are the two different layers of switches? Separate these by a comma I.e.: Layer X,Layer Y

Principio del formulario

Final del formulario