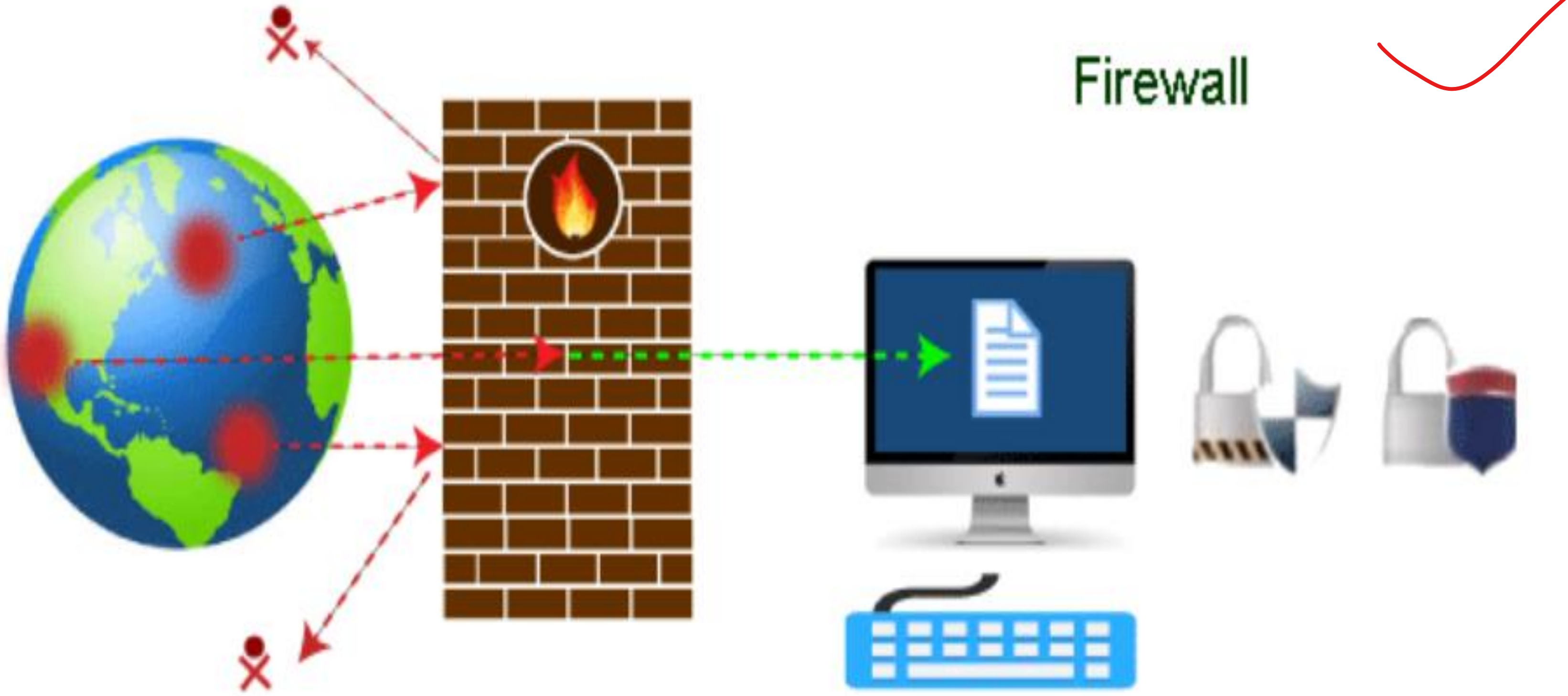
- What is a Firewall?
- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules.
- It acts as a barrier between internal private networks and external sources (such as the public Internet).
- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.
- A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



Firewall

- Firewall: Hardware or Software
- This is one of the most problematic questions whether a firewall is a hardware or software.
- As stated above, a firewall can be a network security device or a software program on a computer.
- This means that the firewall comes at both levels, i.e., hardware and software, though it's best to have both.
- Each format (a firewall implemented as hardware or software) has different functionality but the same purpose.
- A hardware firewall is a physical device that attaches between a computer network and a gateway.
- On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

- Apart from that, there are cloud-based firewalls.
- They are commonly referred to as FaaS (firewall as a service).
- A primary advantage of using cloud-based firewalls is that they can be managed centrally.
- Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

- Why Firewall
- Firewalls are primarily used to prevent malware and network-based attacks.
- Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier.
- They monitor every attempt between our computer and another network.
- They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.
- Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network.
- They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

- Some of the important risks of not having a firewall are:
- Open Access
- If a computer is running without a firewall, it is giving open access to other networks.
- This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks coming through our network.
- Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.
- Lost or Comprised Data
- Without a firewall, we are leaving our devices accessible to everyone.
- This means that anyone can access our device and have complete control over it, including the network.
- In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

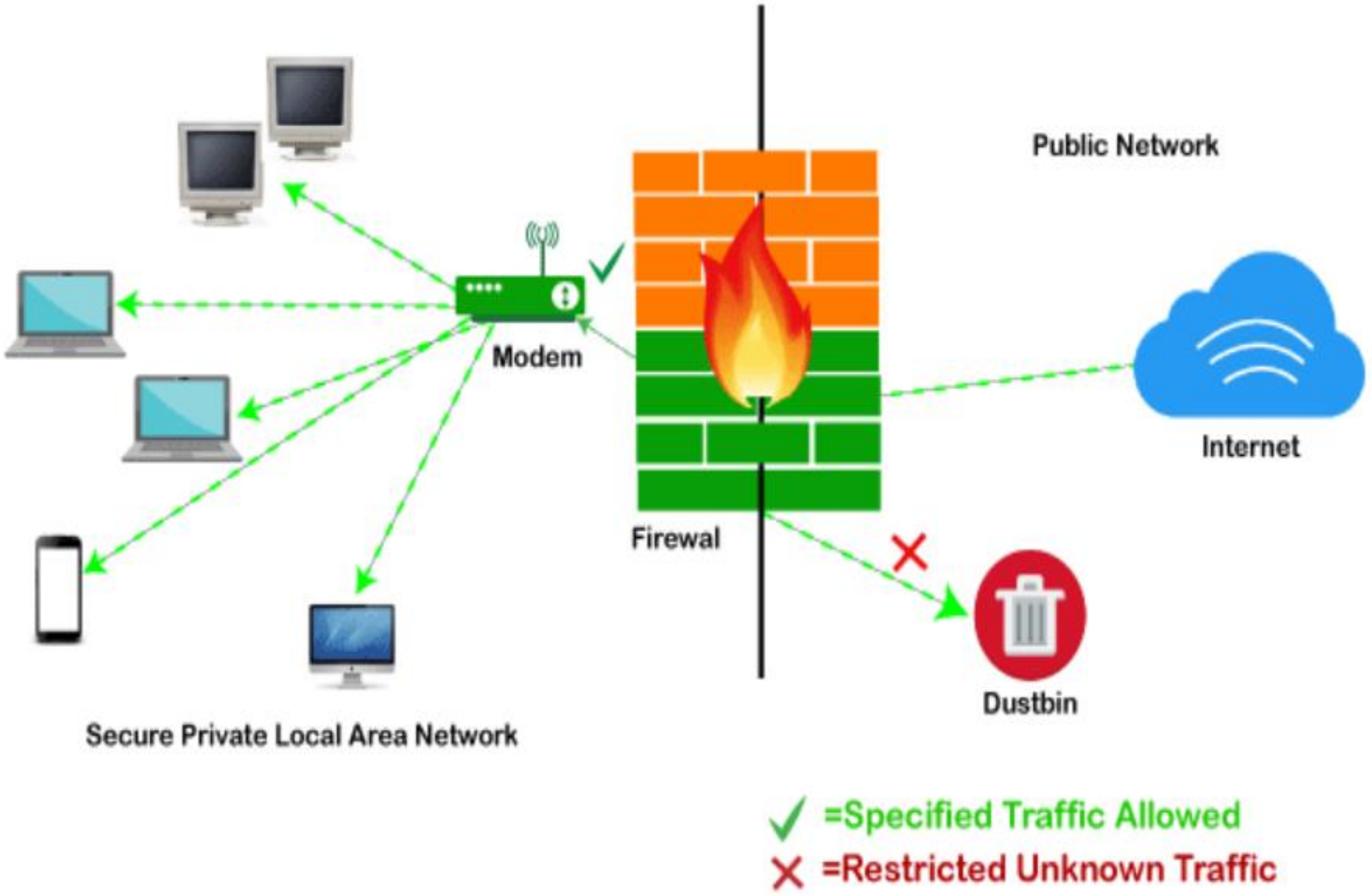
- Network Crashes
- In the absence of a firewall, anyone could access our network and shut it down. It may lead us to invest our valuable time and money to get our network working again.
- Therefore, it is essential to use firewalls and keep our network, computer, and data safe and secure from unwanted sources.

- Brief History of Firewall
- Firewalls have been the first and most reliable component of defense in network security for over 30 years. Firewalls first came into existence in the late 1980s.
- They were initially designed as packet filters. These packet filters were nothing but a setup of networks between computers. The primary function of these packet filtering firewalls was to check for packets or bytes transferred between different computers.
- Firewalls have become more advanced due to continuous development, although such packet filtering firewalls are still in use in legacy systems.

- As the technology emerged, **Gil Shwed** from **Check Point Technologies** introduced the first stateful inspection firewall in 1993.
- It was named as FireWall-1.
- Back in 2000, **Netscreen** came up with its purpose-built firewall **'Appliance’**.
- It gained popularity and fast adoption within enterprises because of increased internet speed, less latency, and high throughput at a lower cost.

- The turn of the century saw a new approach to firewall implementation during the mid-2010.
- The **'Next-Generation Firewalls'** were introduced by the **Palo Alto Networks**.
- These firewalls came up with a variety of built-in functions and capabilities, such as Hybrid Cloud Support, Network Threat Prevention, Application and Identity-Based Control, and Scalable Performance, etc.
- Firewalls are still getting new features as part of continuous development. They are considered the first line of defense when it comes to network security.

- How does a firewall work?
- A firewall system analyzes network traffic based on pre-defined rules. It then filters the traffic and prevents any such traffic coming from unreliable or suspicious sources. It only allows incoming traffic that is configured to accept.
- Typically, firewalls intercept network traffic at a computer's entry point, known as a port.
- Firewalls perform this task by allowing or blocking specific data packets (units of communication transferred over a digital network) based on pre-defined security rules.
- Incoming traffic is allowed only through trusted IP addresses, or sources

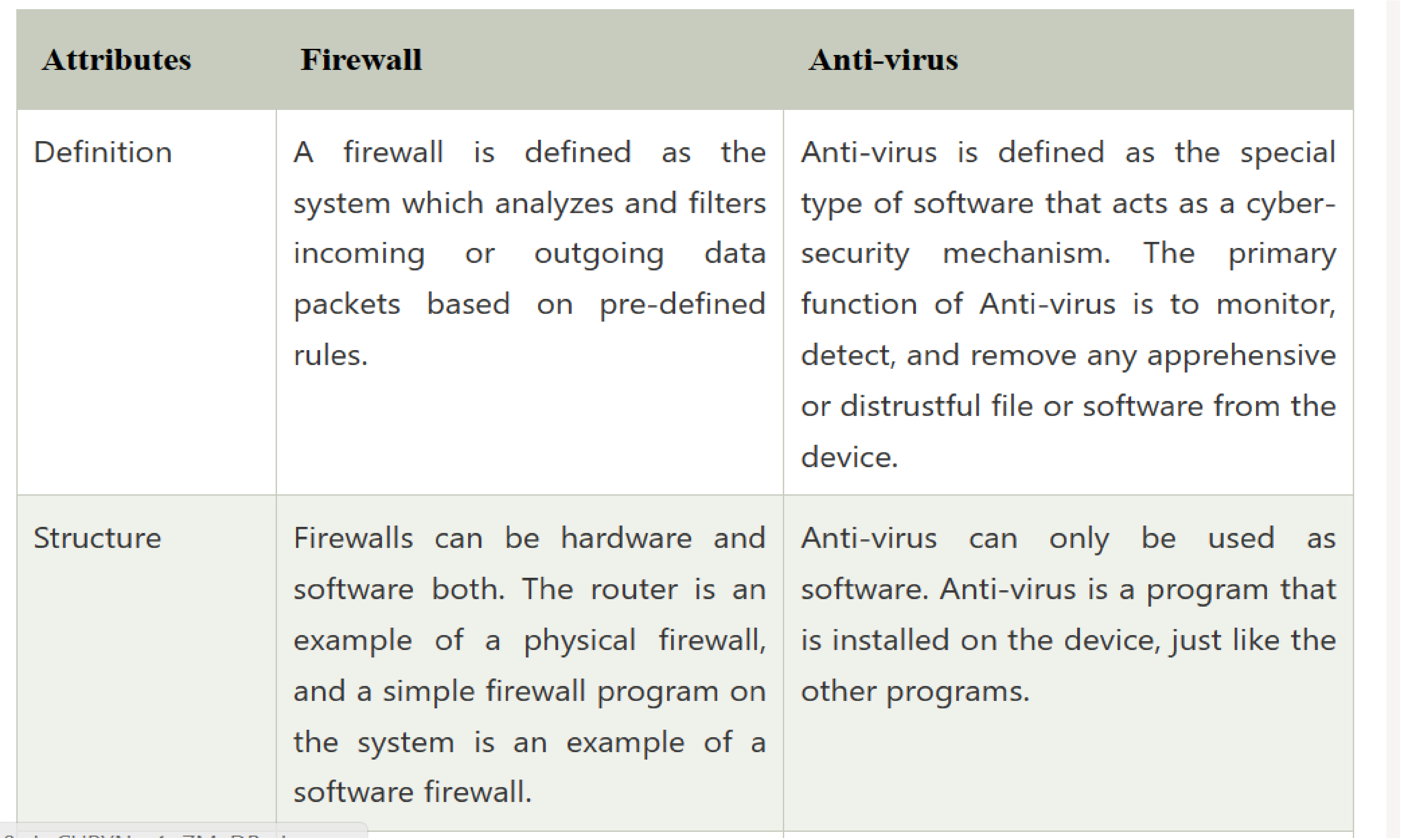

Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✗ =Restricted Unknown Traffic

- Functions of Firewall
- As stated above, the firewall works as a gatekeeper. It analyzes every attempt coming to gain access to our operating system and prevents traffic from unwanted or non-recognized sources.
- Since the firewall acts as a barrier or filter between the computer system and other networks (i.e., the public Internet), we can consider it as a traffic controller.
- Therefore, a firewall's primary function is to secure our network and information by controlling network traffic, preventing unwanted incoming network traffic, and validating access by assessing network traffic for malicious things such as hackers and malware.

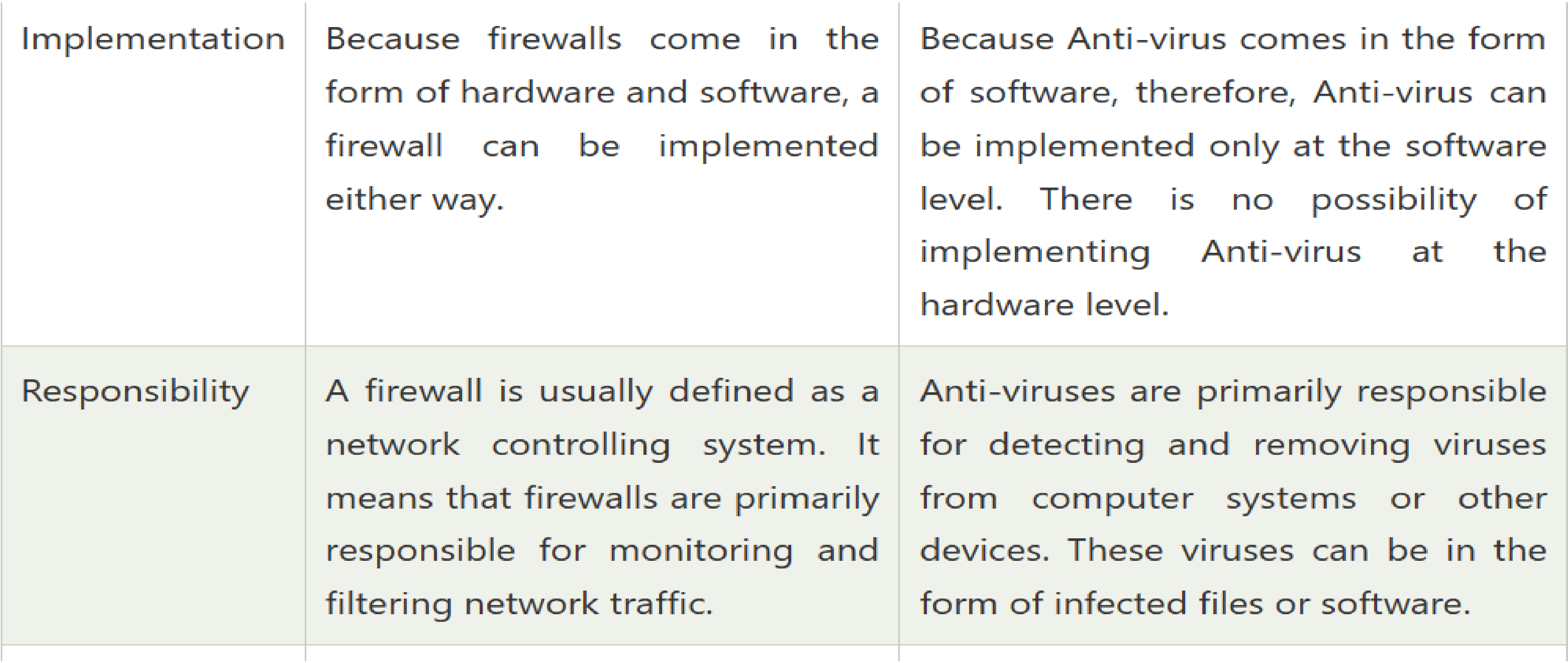
- Generally, most operating systems (for example - Windows OS) and security software come with built-in firewall support. Therefore, it is a good idea to ensure that those options are turned on. Additionally, we can configure the security settings of the system to be automatically updated whenever available.
- Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:
- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

Limitations of Firewall

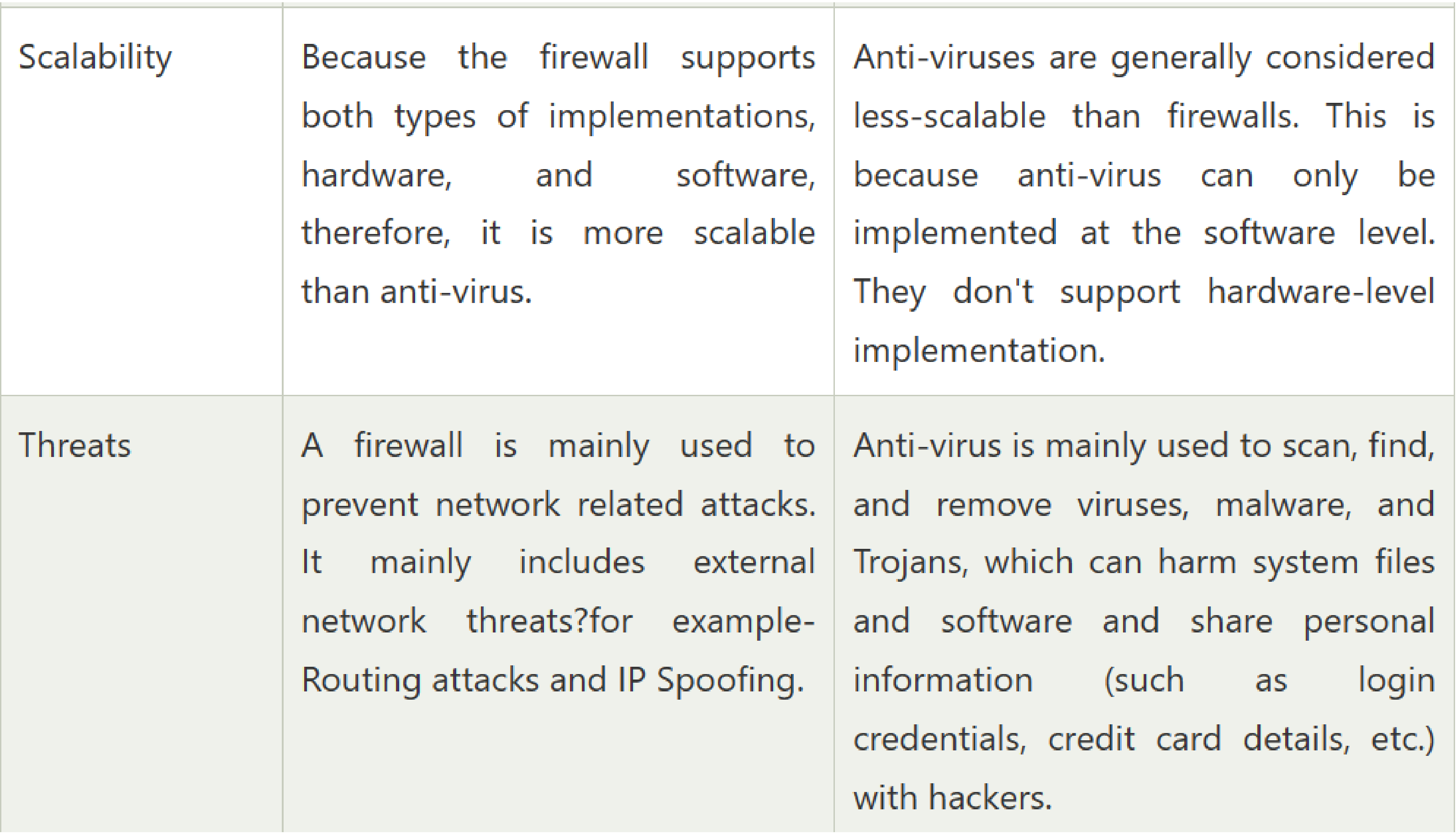
- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.



Attributes	Firewall	Anti-virus
Definition	A firewall is defined as the system which analyzes and filters incoming or outgoing data packets based on pre-defined rules.	Anti-virus is defined as the special type of software that acts as a cyber-security mechanism. The primary function of Anti-virus is to monitor, detect, and remove any apprehensive or distrustful file or software from the device.
Structure	Firewalls can be hardware and software both. The router is an example of a physical firewall, and a simple firewall program on the system is an example of a software firewall.	Anti-virus can only be used as software. Anti-virus is a program that is installed on the device, just like the other programs.



Implementation	Because firewalls come in the form of hardware and software, a firewall can be implemented either way.	Because Anti-virus comes in the form of software, therefore, Anti-virus can be implemented only at the software level. There is no possibility of implementing Anti-virus at the hardware level.
Responsibility	A firewall is usually defined as a network controlling system. It means that firewalls are primarily responsible for monitoring and filtering network traffic.	Anti-viruses are primarily responsible for detecting and removing viruses from computer systems or other devices. These viruses can be in the form of infected files or software.



Scalability	Because the firewall supports both types of implementations, hardware, and software, therefore, it is more scalable than anti-virus.	Anti-viruses are generally considered less-scalable than firewalls. This is because anti-virus can only be implemented at the software level. They don't support hardware-level implementation.
Threats	A firewall is mainly used to prevent network related attacks. It mainly includes external network threats?for example-Routing attacks and IP Spoofing.	Anti-virus is mainly used to scan, find, and remove viruses, malware, and Trojans, which can harm system files and software and share personal information (such as login credentials, credit card details, etc.) with hackers.