CYBER SECURITY IN FIREWALL

RV.SANJAY KUMAR

The kavery engineering college

Outline:

1 Firewall-meaning and definition
2 Types of firewall
3 Firewall working
4 Function of firewall
5 How to use firewall protection
6.Advantages of using firewall
Conclusion

CYBER SECURITY

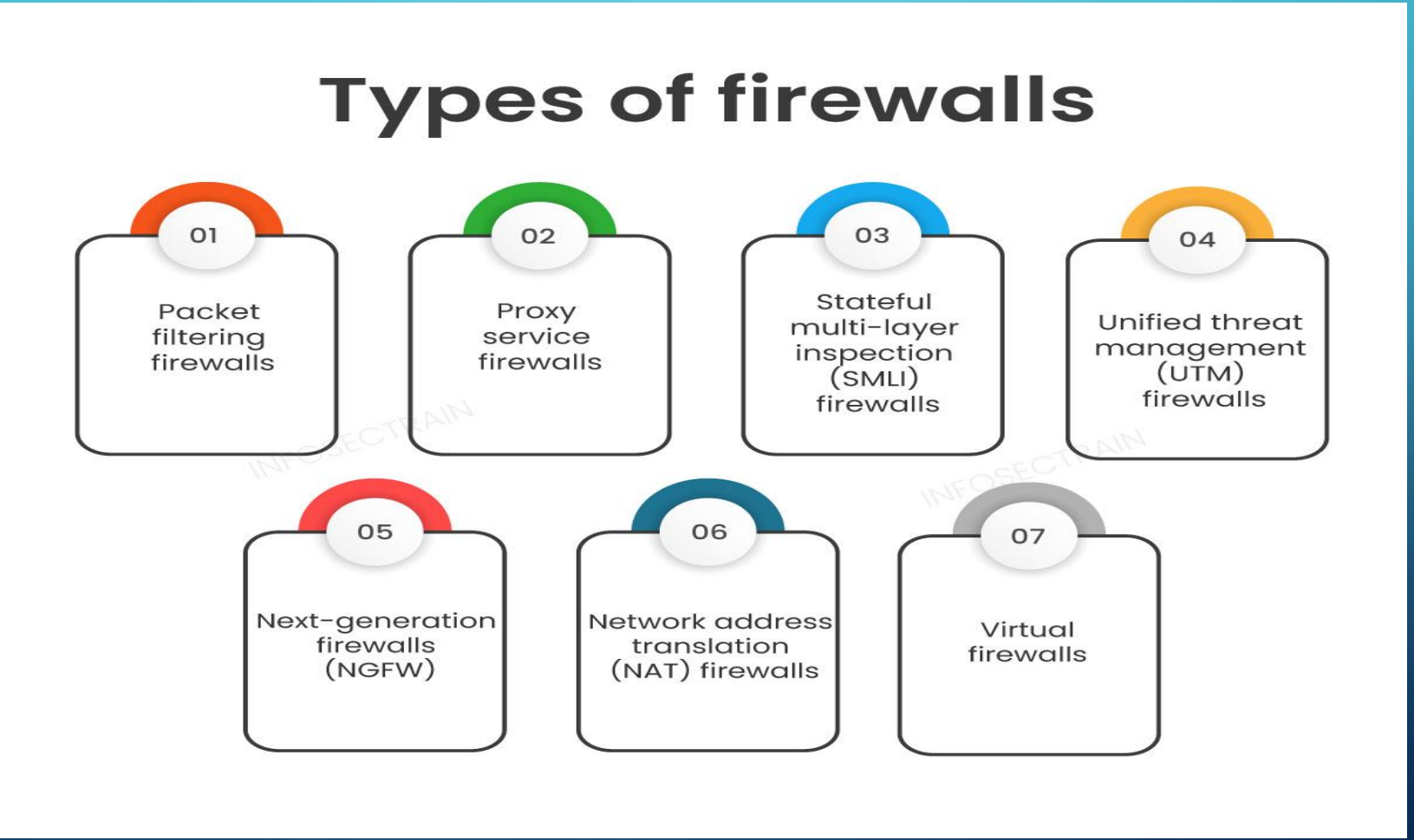
FIREWALL

FIREWALL – MEANING AND DEFINITION

- A firewall is a computer network security system that restricts internet traffic in to, out of, or within a private network.

- This software or dedicated hardware-software unit functions by selectively blocking or allowing data packets. It is typically intended to help prevent malicious activity and to prevent anyone—inside or outside a private network—from engaging in unauthorized web activities.

TYPES OF FIREWALLS



- **Packet Filtering**

  A packet filtering firewall controls data flow to and from a network. It allows or blocks the data transfer based on the packet's source address, the destination address of the packet, the application protocols to transfer the data, and so on.

- **Proxy Service Firewall**

  This type of firewall protects the network by filtering messages at the application layer. For a specific application, a proxy firewall serves as the gateway from one network to another.

- **Stateful Inspection**

  Such a firewall permits or blocks network traffic based on state, port, and protocol. Here, it decides filtering based on administrator-defined rules and context.

- **Next-Generation Firewall**

  According to Gartner, Inc.’s definition, the next-generation firewall is a deep-packet inspection firewall that adds application-level inspection, intrusion prevention, and information from outside the firewall to go beyond port/protocol inspection and blocking.

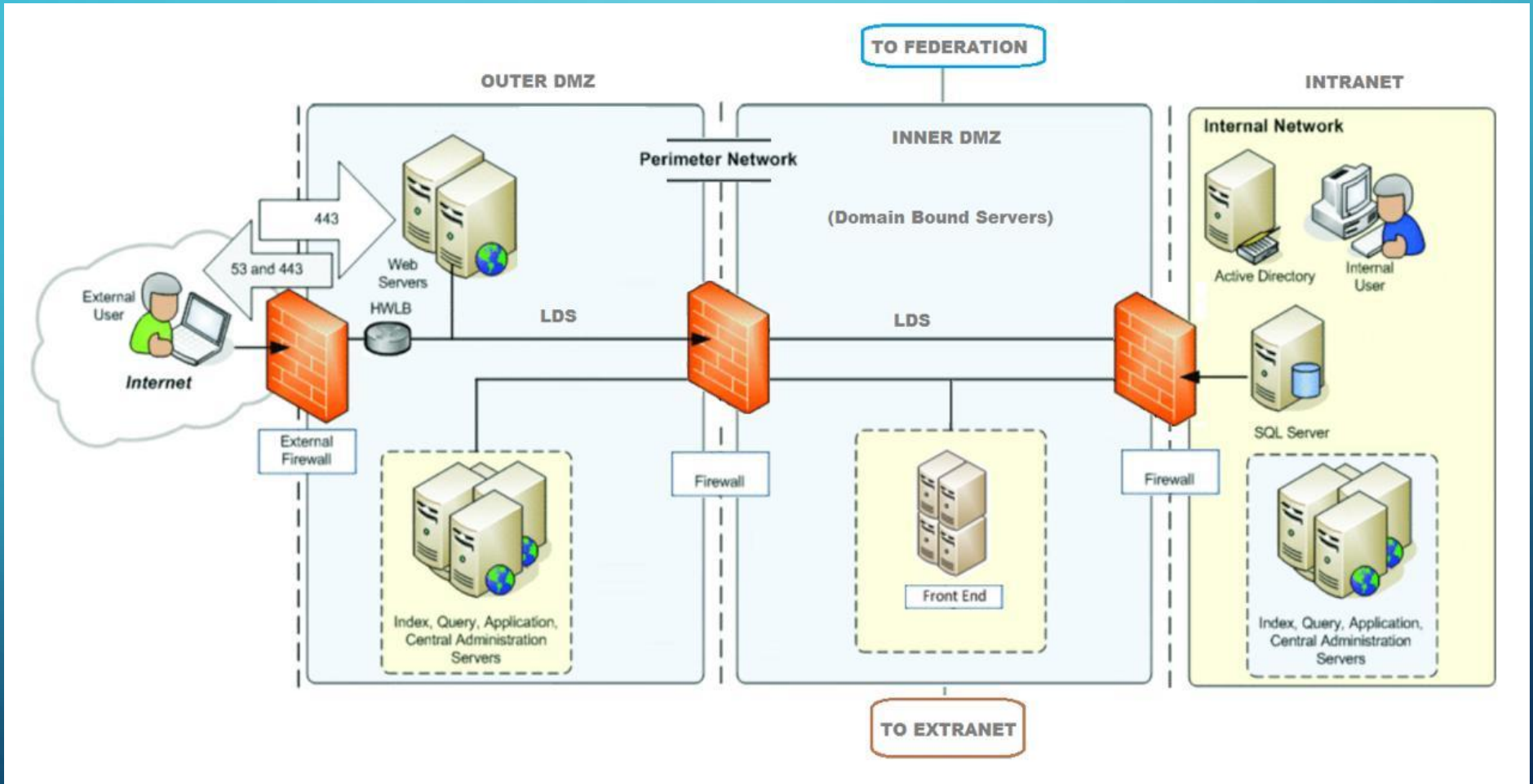
- Unified Threat Management (UTM) Firewall

A UTM device generally integrates the capabilities of a stateful inspection firewall, intrusion prevention, and antivirus in a loosely linked manner. It may include additional services and, in many cases, cloud management. UTMs are designed to be simple and easy to use

- Threat-Focused NGFW

These firewalls provide advanced threat detection and mitigation. With network and endpoint event correlation, they may detect evasive or suspicious behavior.

Firewall working



Firewall Work

As mentioned previously, firewalls filter the network traffic within a private network. It analyses which traffic should be allowed or restricted based on a set of rules. Think of the firewall like a gatekeeper at your computer's entry point which only allows trusted sources, or IP addresses, to enter your network.

These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block traffic coming from suspicious sources to prevent cyberattacks.

For example, the image depicted below shows how a firewall allows good traffic to pass to the user's private network.

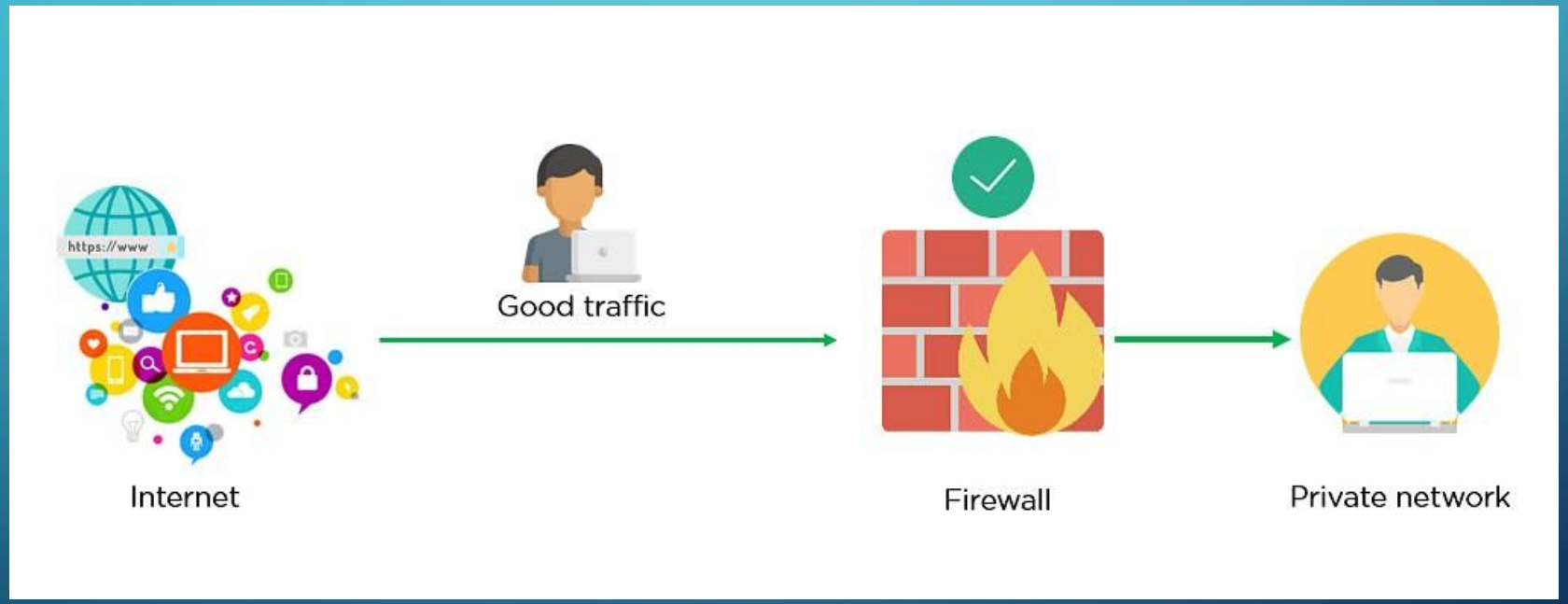


Fig: Firewall allowing Good Traffic

However, in the example below, the firewall blocks malicious traffic from entering the private network, thereby protecting the user's network from being susceptible to a cyberattack.

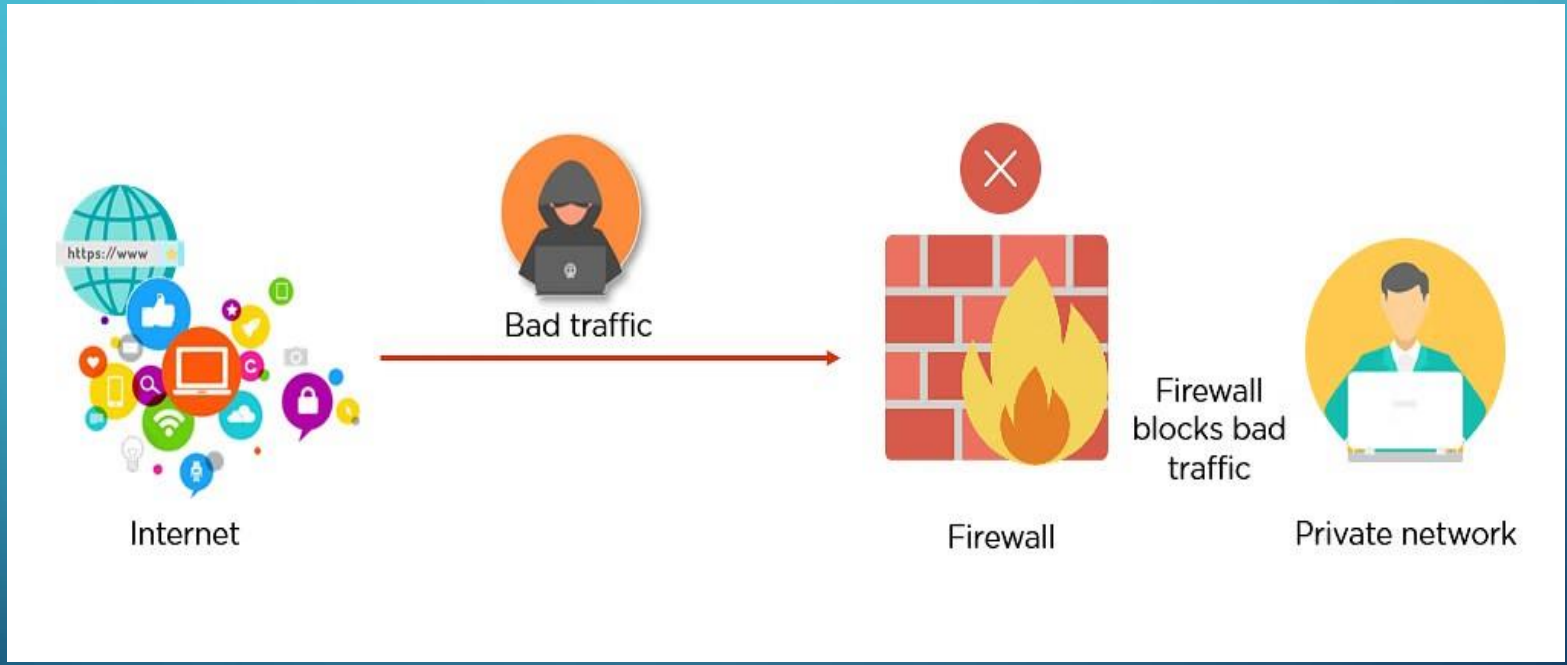


Fig: Firewall blocking Bad Traffic

Functions of Firewall

- The most important function of a firewall is that it creates a border between an external network and the guarded network where the firewall inspects all packets (pieces of data for internet transfer) entering and leaving the guarded network. Once the inspection is completed, a firewall can differentiate between benign and malicious packets with the help of a set of pre-configured rules.

- The firewall abides such packets, whether they come in a rule set or not, so that they should not enter into the guarded network.

- This packet form information includes the information source, its destination, and the content. These might differ at every level of the network, and so do the rule sets. Firewalls read these packets and reform them concerning rules to tell the protocol where to send them.

How to Use Firewall Protection:

To keep your network and devices safe, make sure your firewall is set up and maintained correctly. Here are some tips to help you improve your firewall security:

- Constantly update your firewalls as soon as possible: Firmware patches keep your firewall updated against any newly discovered vulnerabilities.

Use antivirus protection: In addition to firewalls, you need to use antivirus software to protect your system from viruses and other infections

- Limit accessible ports and host: Limit inbound and outbound connections to a strict whitelist of trusted IP addresses.

Advantages of Using Firewalls

Now that you have understood the types of firewalls, let us look at the advantages of using firewalls.

- Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.
- It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
- Firewalls provide faster response time and can handle more traffic loads.

CONCLUSION

In conclusion, cyber security is an ever-evolving field critical for protecting sensitive information, infrastructure, and individuals from digital threats. Continuous vigilance, proactive measures, and collaboration among stakeholders are essential to mitigate risks and ensure a safe digital environment for all.