Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch:C3 **Roll No.:110**
Experiment No.

Title: Understanding the role of firewall in network security.

Objective: Understand various firewalls in network security.

Expected Outcome of Experiment:

CO	Outcome
3	Network security

Books/ Journals/ Websites referred:

https://www.javatpoint.com/types-of-firewall

https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls

https://www.youtube.com/watch?v=3NvN93lq7MM&list=PLY-M-dfKubpe35s_P6kYJ1-xrCqb5i7Qs

Abstract:-

Firewalls can be viewed as gated borders or gateways that manage the travel of permitted and prohibited web activity in a private network. The term comes from the concept of physical walls being barriers to slow the spread of fire until emergency services can extinguish it. By comparison, network security firewalls are for web traffic management — typically intended to slow the spread of web threats.

Firewalls create 'choke points' to funnel web traffic, at which they are then reviewed on a set of programmed parameters and acted upon accordingly. Some firewalls also track the traffic and connections in audit logs to reference what has been allowed or blocked.

Firewalls are typically used to gate the borders of a private network or its host devices. As such, firewalls are one security tool in the broader category of user access control. These barriers are typically set up in two locations — on dedicated computers on the network or the user computers and other endpoints themselves (hosts).

Related Theory: -

There are mainly three types of firewalls, such as software firewalls, hardware firewalls, or both, depending on their structure. Each type of firewall has different functionality but the same purpose. However, it is best practice to have both to achieve maximum possible protection.

A hardware firewall is a physical device that attaches between a computer network and a gateway. For example- a broadband router. A hardware firewall is sometimes referred to as an Appliance Firewall. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software. This type of firewall is also called a Host Firewall.

Implementation Details:

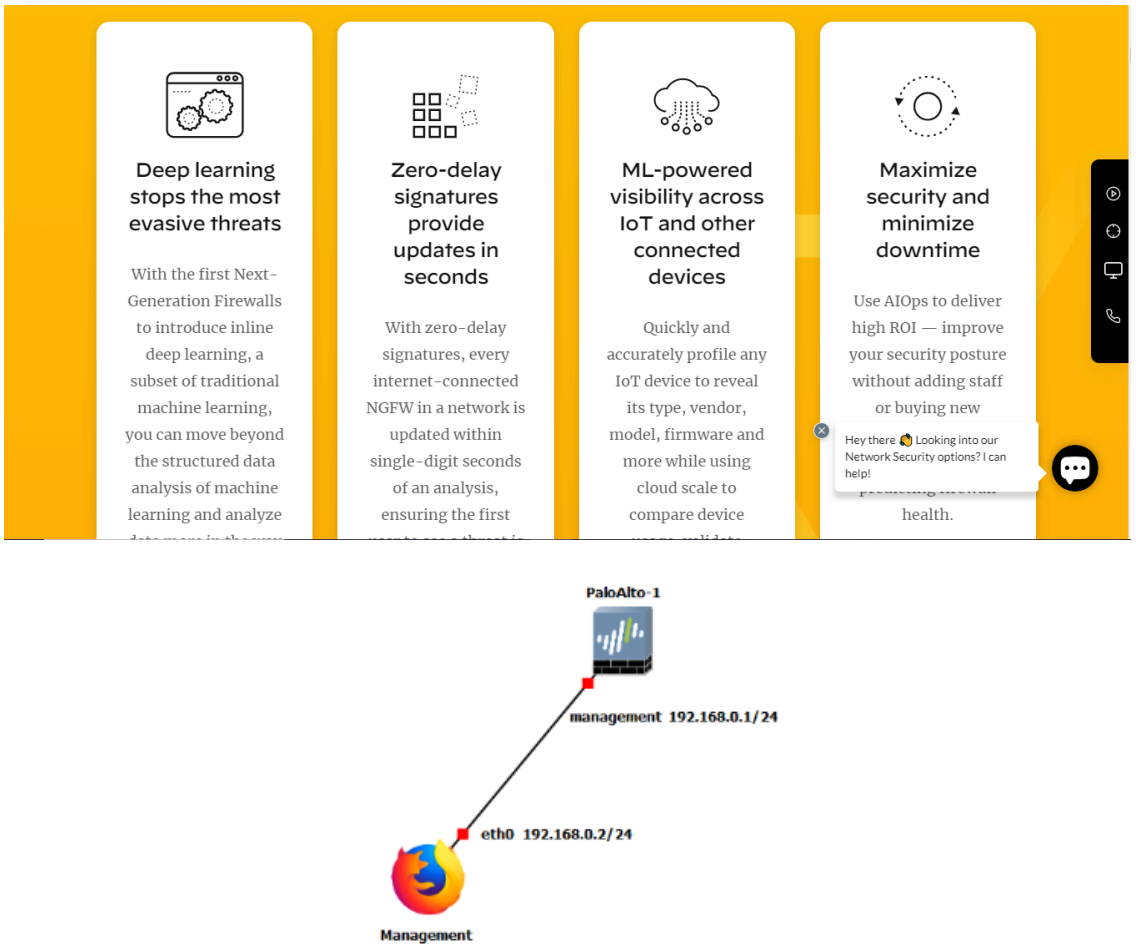
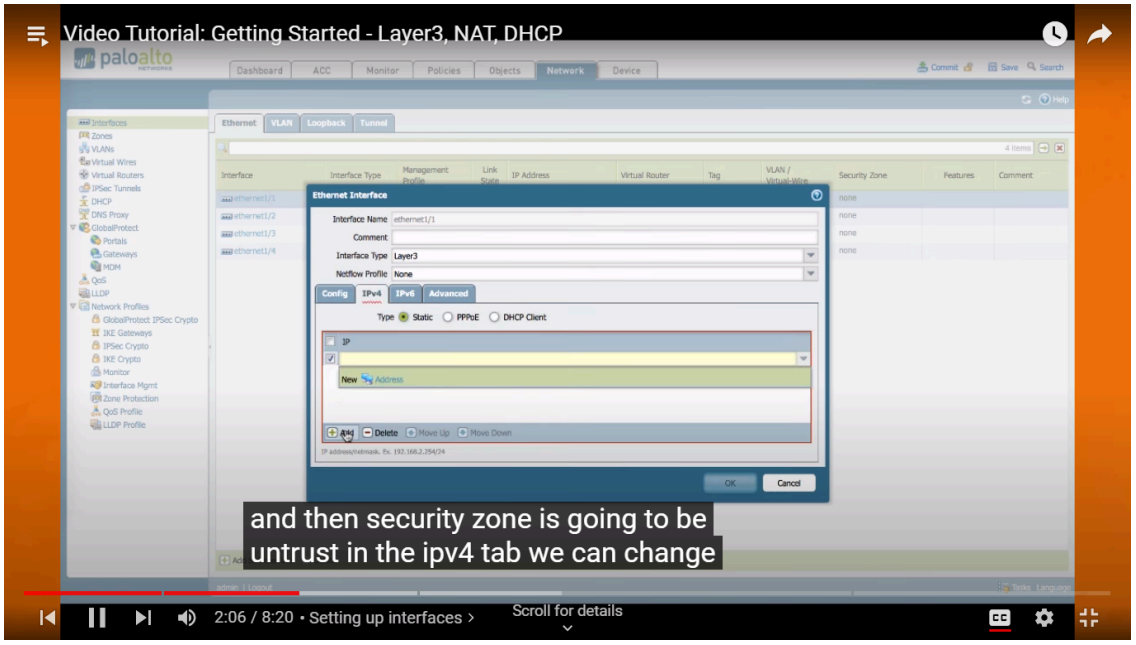
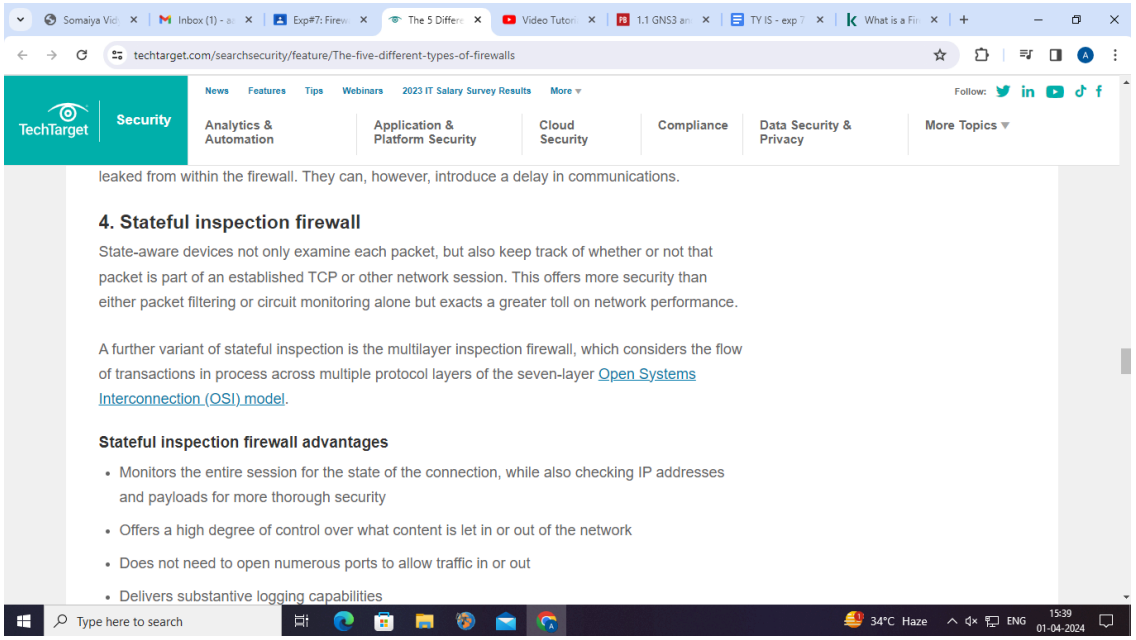


Figure 1.1: Main Scenario

Table 1.1: Addressing Table

Device	Configuration
PaloAlto-1	Management: 192.168.0.1/24
WebTerm1-Management	eth0: 192.168.0.2/24


Video Tutorial: Getting Started - Layer3, NAT, DHCP
and then security zone is going to be
untrust in the ipv4 tab we can change
2:06 / 8:20 • Setting up interfaces
Scroll for details


techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls
TechTarget
Security
leaked from within the firewall. They can, however, introduce a delay in communications.
4. Stateful inspection firewall
State-aware devices not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.
A further variant of stateful inspection is the multilayer inspection firewall, which considers the flow of transactions in process across multiple protocol layers of the seven-layer Open Systems Interconnection (OSI) model.
Stateful inspection firewall advantages
Monitors the entire session for the state of the connection, while also checking IP addresses and payloads for more thorough security
Offers a high degree of control over what content is let in or out of the network
Does not need to open numerous ports to allow traffic in or out
Delivers substantive logging capabilities

Conclusion:- Thus we have studied what firewalls are. A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

POSTLAB

7.1 Difference between stateful and stateless firewalls:

Stateful firewalls maintain context about active sessions, including source and destination IP addresses, ports, and sequence numbers. They keep track of the state of network connections and make decisions based on the context of the traffic. Stateless firewalls, on the other hand, examine individual packets without considering the context of the traffic flow. They make decisions based solely on predetermined rules, such as filtering packets based on source and destination IP addresses, ports, and protocols. Stateful firewalls are generally more sophisticated and provide better security by understanding the state of connections.

7.2 How a firewall protects data:

A firewall protects data by acting as a barrier between a trusted internal network and untrusted external networks, such as the internet. It examines incoming and outgoing network traffic based on a set of predetermined rules and policies. The firewall can block or allow traffic based on factors such as source and destination IP addresses, ports, protocols, and the state of connections. By enforcing these rules, firewalls prevent unauthorized access to the network, mitigate various types of cyber threats, and ensure the confidentiality, integrity, and availability of data.

7.3 What a firewall can't protect against:

While firewalls are essential for network security, they have limitations and cannot protect against all types of threats. Some of the things a firewall can't protect against include:

- Insider threats: Firewalls cannot prevent malicious activities carried out by authorized users within the network.

- Social engineering attacks: Firewalls do not protect against human manipulation or deception aimed at tricking users into disclosing sensitive information.
- Malware introduced through other vectors: Firewalls cannot stop malware that is introduced through other means, such as infected USB drives or phishing emails.
- Encrypted traffic: Firewalls may have limited visibility into encrypted traffic, making it difficult to detect threats hidden within encrypted communications.
- Zero-day exploits: Firewalls may not have signatures or rules to detect and block newly discovered vulnerabilities or exploits.

7.4 Difference between a firewall, an IDS, and an IPS:

- Firewall: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary function is to establish a barrier between a trusted internal network and untrusted external networks to prevent unauthorized access and mitigate cyber threats.
- IDS (Intrusion Detection System): An IDS is a passive security system that monitors network or system activities for suspicious patterns or anomalies that may indicate a security breach or unauthorized access. It analyzes network traffic and generates alerts when it detects potentially malicious behavior but does not actively block or prevent the detected threats.
- IPS (Intrusion Prevention System): An IPS is an active security system that extends the functionality of an IDS by not only detecting but also actively blocking or preventing detected threats. It can automatically respond to security incidents by blocking malicious traffic, dropping packets, or reconfiguring firewall rules to prevent further exploitation. Unlike IDS, an IPS can take immediate action to mitigate security risks in real-time.