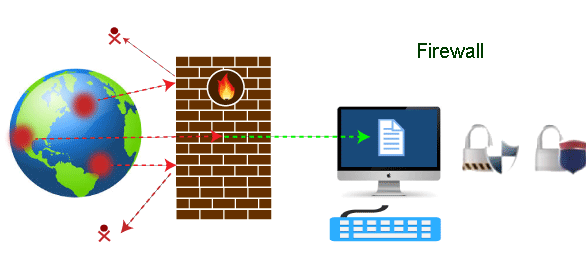
What is a Firewall?

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](https://www.javatpoint.com/internet) in infected computers.



## Firewall: Hardware or Software

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](https://www.javatpoint.com/hardware) and [software](https://www.javatpoint.com/software), though it's best to have both.

a software firewall is a simple program installed on a computer that works through port numbers and other installed software. A hardware firewall is a physical device that attaches between a [computer network](https://www.javatpoint.com/computer-network-tutorial) and a gateway. For example, a broadband router.

## 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**

### **Lost or Comprised Data**

### **Network Crashes**

Types Of Firewalls

1. Packet Filtering FW
2. Proxy FW
3. Stateful FW
4. NGFW
5. NAT FW
6. Cloud FW(FAAS)

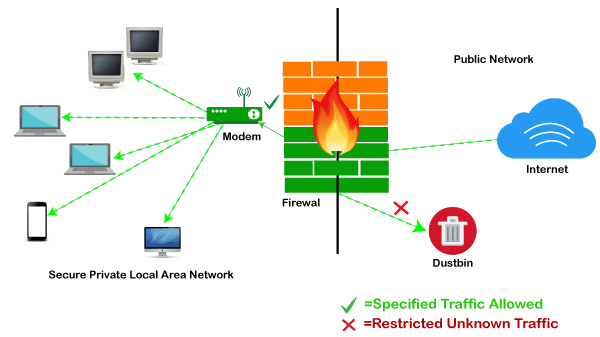
## Brief History of Firewall

Firewalls first came into existence in the late 1980s. As the technology emerged, **Gil Shwed** from **Check Point Technologies** introduced the first stateful inspection firewall in 1993. 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.

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](https://www.javatpoint.com/ip) addresses, or sources.



Firewalls have become so powerful, and include a variety of functions and capabilities with built-in features:

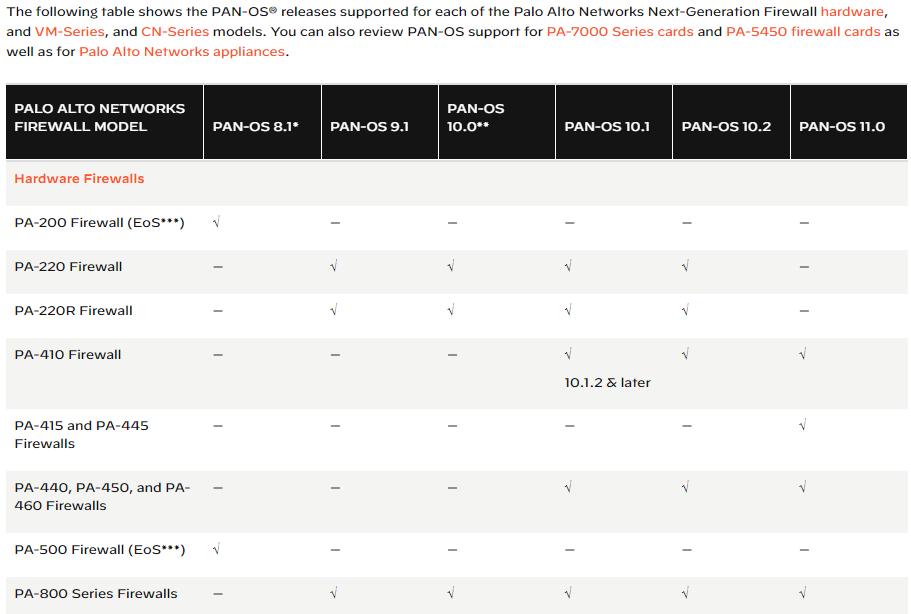
* Network Threat Prevention
* Application and Identity-Based Control
* Hybrid Cloud Support
* Scalable Performance
* Network Traffic Management and Control
* Access Validation
* Record and Report on Events

## Limitations of Firewall

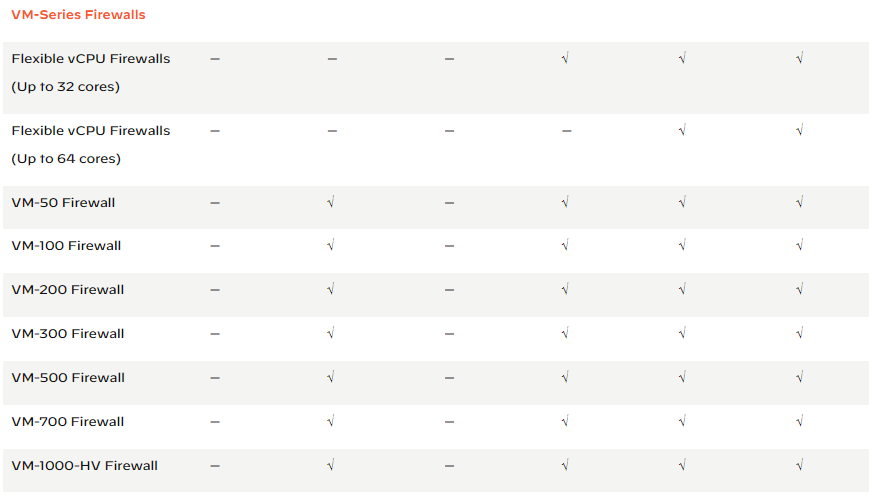
firewalls have some limitations:

* 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.

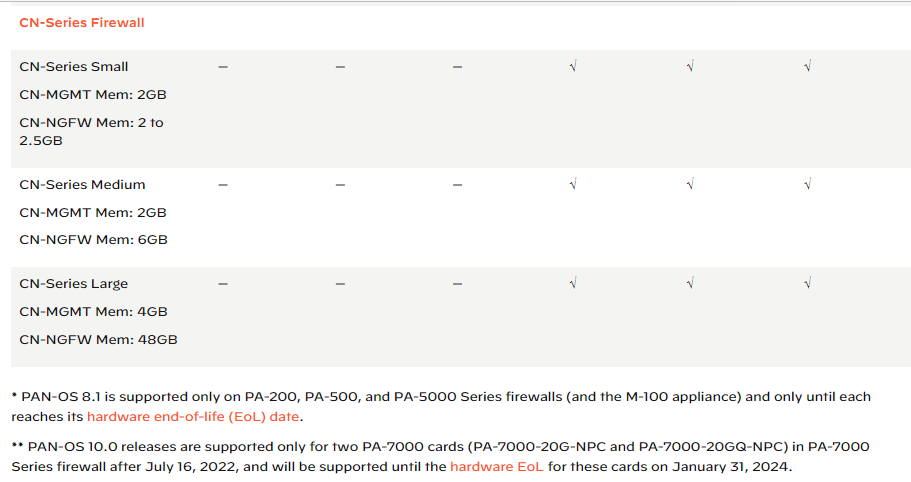
Palo Alto Firewall Models with supported OS Versions







Containerized next-generation firewall (CN-series FW)



**Throughput**

In the context of a firewall, throughput refers to the measure of data or traffic handling capacity of the firewall device. It represents the maximum amount of data that can pass through the firewall within a given time frame, typically measured in bits per second (bps) or megabits per second (Mbps).





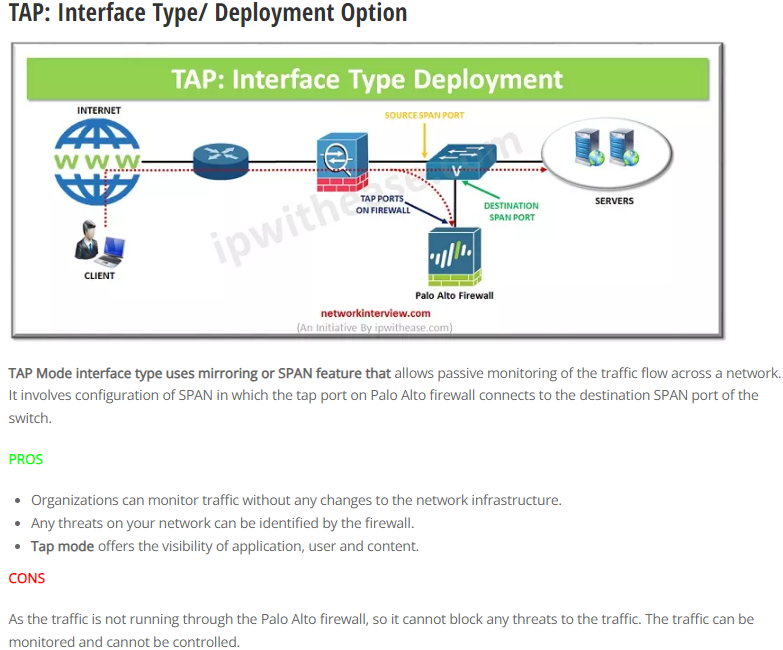


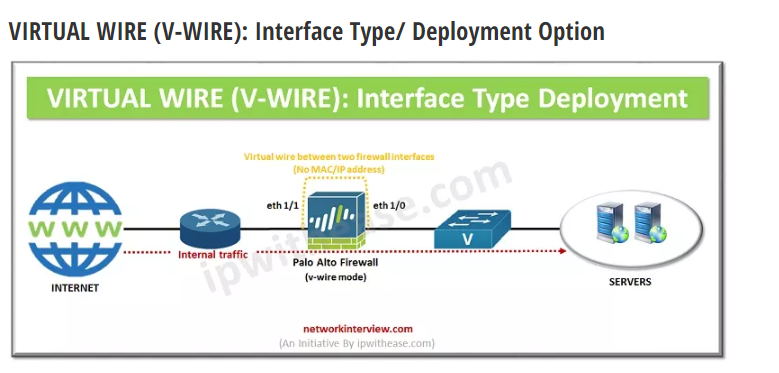


**Features**

**Next-Generation Firewall**

|  |  |
| --- | --- |
| Deep visibility and granular control for thousands of applications; ability to create custom applications; ability to manage unknown traffic based on policy |  |
| User identification and control: VPNs, WLAN controllers, captive portal, proxies, Active Directory, eDirectory, Exchange, Terminal Services, syslog parsing, XML API |  |
| Granular SSL decryption and inspection (inbound and outbound); per-policy SSH control (inbound and outbound) |  |
| Networking: dynamic routing (RIP, OSPF, BGP, multiprotocol BGP), DHCP, DNS, NAT, route redistribution, ECMP, LLDP, BFD, tunnel content inspection |  |
| QoS: policy-based traffic shaping (priority, guaranteed, maximum) per application, per user, per tunnel, based on DSCP classification |  |
| Virtual systems: logical, separately managed firewall instances within a single physical firewall, with each virtual system’s traffic kept separate |  |
| Zone-based network segmentation and zone protection; DoS protection against flooding of new sessions |  |
| **Threat Prevention (subscription required)** | |
| In-line malware prevention automatically enforced through payload-based signatures, updated daily |  |
| Vulnerability-based protections against exploits and evasive techniques on network and application layers, including port scans, buffer overflows, packet fragmentation, and obfuscation |  |
| Command-and-control (C2) activity stopped from exfiltrating data or delivering secondary malware payloads; infected hosts identified through DNS sinkholing |  |
| **URL Filtering (subscription required)** | |
| Automatic prevention of web-based attacks, including phishing links in emails, phishing sites, HTTP-based C2, and pages that carry exploit kits |  |
| Ability to stop in-process credential phishing |  |
| Custom URL categories, alerts, and notification pages |  |
| **WildFire malware prevention (subscription required)** | |
| Detection of zero-day malware and exploits with layered, complementary analysis techniques |  |
| Automated prevention in as few as five minutes across networks, endpoints, and clouds |  |
| Community-based data for protection, including more than 30,000 subscribers |  |
| **File and data filtering** | |
| Bidirectional control over the unauthorized transfer of file types and Social Security numbers, credit card numbers, and custom data patterns |  |

****

****

As the name implies, it’s a virtual interface in which a firewall is installed transparently on a network segment by binding two interfaces/ firewall ports. V-wire deployment mode simplifies the installation and configuration as the firewall can be inserted into an existing network. You need not to do any network redesigning or reconfiguration of the adjacent network devices. No [MAC or IP addresses](https://networkinterview.com/mac-address-vs-ip-address-know-the-difference/) need to be assigned to the interfaces.

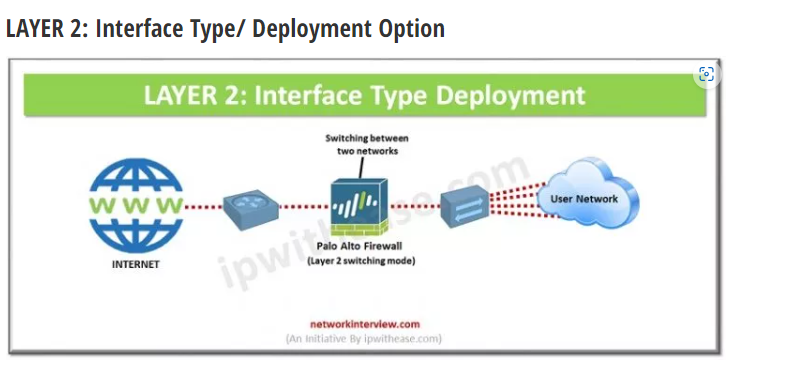
The virtual wire interfaces have no Layer 2 or Layer 3 addresses as it is directly connected to a Layer 2/Layer 3 networking device/host.

**PROS**

* The traffic can be monitored as well as controlled, this overcomes the limitation of TAP mode in which traffic can’t be controlled.
* It doesn’t require any redesigning/reconfiguring.
* It supports traffic blocking/allowing based on VLAN (Virtual LAN) tags.
* It support features like **App-ID**, **User-ID**, **Content-ID**, **NAT, QoS**and **SSL decryption.**

**CONS**

It does not support switching, VPN tunnels, or routing as no IP address is assigned to Layer 2 or Layer 3 devices.

****

In this type of interface, the firewall is configured to perform switching between two or more network segments. The traffic can be examined as per the policies which provides increased security and visibility within the internal network.

The firewall interfaces do not participate in the Spanning tree topology but they are capable of supporting the access/trunk links. Any bridge protocol data units (BPDU) received are directly transferred to the neighbouring Layer 2 switch without processing.

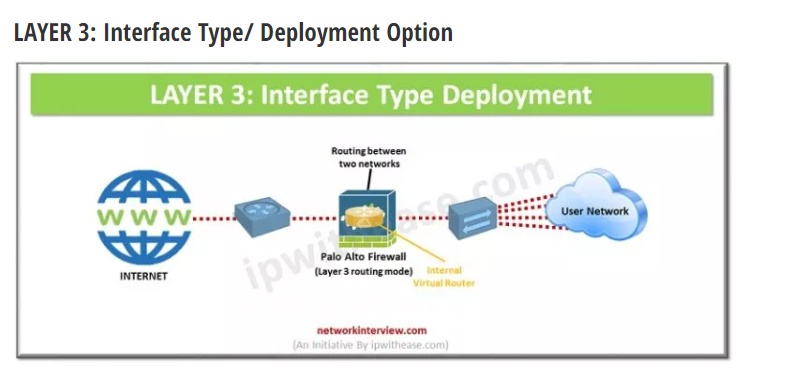
Layer 2 interface is to be configured when switching is required.

The routing of traffic between VLAN/other networks is achieved via a default gateway. This default gateway is generally a Layer 3 switch.

**PROS**

The traffic can be examined, monitored and controlled.

It supports features like **App-ID**, **User-ID**, **Content-ID**, **NAT, QoS** and SSL **decryption**.

****

**Layer 3 interface type supports IP address configuration.** The traffic routes between multiple ports. Each port is configured with an IP address and security zone. Layer 3 interface configuration requires internal virtual router. For each Layer 3 interface virtual router needs to be configured to route the traffic

**PROS**

* The traffic can be examined, monitored and controlled.
* It supports features like **App-ID**, **User-ID**, **Content-ID**, **NAT, QoS**and SSL **decryption**.
* It supports sub interfaces with VLAN tags