Hardware Firewall

- A wall that prevents the spread of fire
- When data moves in and out of a server its packet information is tested against the firewall rules to see if it should be allowed or not
- In simple words, a firewall is like a watchman, a bouncer, or a shield that has a set of rules given and based on that rule they decide who can enter and leave

There are 2 type of firewalls in IT

Software	=	Runs on operating system
Hardware	=	A dedicated appliance with firewall software

- Hardware firewall is managed by security or networking team
- A Hardware Firewall is a device to which you connect your computers or network in order to protect them from unauthorized access

Key Benefits Hardware Firewalls Provide

Traffic Control

- The ability to decide which traffic should and shouldn't reach your server.

Default Rules

- A fully configurable list of default rules which can be applied to all traffic.

Port Access

- In-depth control to serve rules with options like allowing all traffic to your website or ensuring only you and your developer can access SSH ports or RDP.

Managed Equals Control On The Fly

- Access to a fully staffed networking team to configure, troubleshoot, or adjust controls on the fly

Additional Server Resources

- Access to additional server resources that would otherwise be utilized. You can even disable the software firewalls from your server and rely completely on the hardware firewall, freeing up valuable memory and processor

Ease of Management

- A single point of installation means less overall maintenance in the long run. So configuring firewall at each server level is cumbersome

Examples of Hardware Firewalls

- Cisco ASA
- Juniper
- SonicWall
- PaloAtlo
- Firewalla
- WatchGuard
- McAFEE
- F5
- Barracuda F-Series
- pfSense