



“What’s the difference in a firewall and a router?”

- You likely know what an internet router is – the device you have at home that shares the internet connection among all devices in the home. A firewall is very similar to a router in that it shares internet, but has the following key differences:
- A firewall inspects all traffic coming into the building from the internet to make sure it was actually requested by a device inside the network. It discards any traffic not requested by a device inside the network for security purposes.
- A firewall allows you to block incoming and outgoing internet traffic to specific countries; for example; blocking all traffic originating from Syria or North Korea, as those countries are known for cyber attacks.
- A firewall provides perimeter antivirus and anti-spyware. This means that all incoming traffic is inspected for virus-like signatures and blocked if any are detected. A firewall does NOT take away the need for antivirus software on a computer, it supplements it.
- A firewall allows you to block certain content (such as gambling, porn, or workplace violence websites) for certain users or groups of users, or for the network as a whole.
- A firewall allows you to prioritize what kind of internet traffic is most important, for example, to allow VoIP traffic to have higher priority than e-mail traffic.
- A firewall supports multiple internet connections for load balancing (or traffic sharing) and failover, eliminating downtime to milliseconds.
- Unlike a router, a firewall typically does NOT provide wireless network coverage. Instead, wireless access points are used to provide wifi inside the building.
- Firewalls are intelligent. If an internet threat is born today, a firewall will update itself to protect against that new threat. Therefore; most firewalls include a subscription for both technical support and protection updates.
- A firewall allows secure remote access for remote users to be able to securely connect into the network.



- A firewall also allows for secure connectivity between two or more offices so that those offices can share data or network resources.
- A firewall allows you to control access to certain internet content, websites, etc. by day or time-frame.
- A firewall typically allows you to report on internet usage by username or computer/device name.
- A firewall is capable of informing the person or group whom manages IT of serious threats occurring inside the network, such as a widespread virus or malware outbreak.
- A firewall allows you to block certain types of applications or certain specific applications, such as instant messaging or peer-to-peer file sharing.
- A firewall helps protect internet facing devices on the network, for example, camera systems, web servers, etc. by monitoring incoming uses that are atypical.
- A firewall will provide spam e-mail filtering (dependent on the e-mail server that e-mail resides on).
- A firewall provides the ability to see internet usage and traffic in real time to make on the fly adjustments to resolve technical/support related issues.
- SmartPath Technologies typically recommends Sophos NexGen Firewall appliances to protect networks. Sophos is far and away the leader in cyber threat prevention; and has been consistently the leader in firewall and cyber threat prevention for the past several years. In addition to providing superior internet protection, the Sophos line of firewalls allows centralized management and logging. In non-geek terms, that means that the Sophos firewall products allow us to constantly be aware of what's going on with your private network's connection to the internet.
- As an analogy, Sophos firewalls are the equivalent to having an armed United States Marine guarding your internet connection. They keep the gremlins at the gate and provide in-depth background checks of who is coming into the network from the world.
- Firewalls are sold and priced based on their horsepower. The necessary horsepower is determined by number of internet users/devices on the private network, remote connections to branch offices, and incoming connections for road warriors and mobile employees.