Intranet Vs Extranet Vs Internet: Here are the differentiating factors

Intranet	Extranet	Internet
Intranets are designed for internal use within organizations only	Extranets extend the concept to include outside entities such as vendors and clients	The Internet is accessible to anyone in the world who has an internet connection
Intranets are private networks only accessible to authorized personnel within an organization	Extranets are also private networks. But they permit selected third parties to access only a few restricted systems, data, and applications	The Internet is a vast network of networks that connects computers and devices globally that are interconnected by routers
Intranets are mostly open to all employees. But access can also be selective for different teams if the organization decides so	Extranets are strictly based on the access granted to users by the organization	The Internet is open to anyone with an internet connection
Provide a secure means of sharing information and resources within a company	Also provide a secure means of sharing information and resources, both within a company and beyond	Anyone can share information and resources with anyone anywhere. Needs to be secured with anti-virus software.
Protect the confidentiality and privacy of the organization's information	Also, protect the confidentiality and privacy of the organization's information	The Internet is open and unprotected
Are free from the risk of unauthorized access from external sources	Extranets are not completely free from the risk of unauthorized access from external sources	The Internet is extremely risky as anyone can access any data that is unprotected at the source
Intranets often have company-specific applications and databases that are only available to its employees	Extranets can have various applications and databases that are available to authorized outsiders as well	The Internet has unlimited applications and databases accessible to anyone in the world

What is a Firewall?

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. A firewall's main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

Internet — Good traffic → Firewall ✓ → Private network

Internet — Bad traffic → Firewall ✗ — Firewall blocks bad traffic — Private network