A firewall decides which network traffic is allowed to pass through and which traffic is deemed dangerous.Ports are typically assigned specific purposes, so certain protocols and IP addresses using uncommon ports or disabled ports can be a concern.These regulate inbound and outbound network traffic, separating external public networks--like the global internet--from internal networks like home Wi-Fi networks, enterprise intranets, or national intranets.The basic subnet segments are as follows: External public networks typically refer to the public/global internet or various extranets.The two most common segment models are the screened host firewall and the screened subnet firewall: Screened host firewalls use a single screening router between the external and internal networks.As a secured buffer between internal and external networks, these can also be used to house any external-facing services provided by the internal network (i.e., servers for web, mail, FTP, VoIP, etc.).Screened subnet firewalls use two screening routers-- one known as an access router between the external and perimeter network, and another known as the choke router between the perimeter and internal network.Among the networking protocols that hosts use to 'talk' with each other, TCP/IP protocols are primarily used to communicate across the internet and within intranet/sub-networks.By using these identifiers, a firewall can decide if a data packet attempting a connection is to be discarded--silently or with an error reply to the sender--or forwarded.Perimeter networks detail border networks made of bastion hosts -- computer hosts dedicated with hardened security that are ready to endure an external attack.Host firewalls can also dive deeper into web traffic, filtering based on HTTP and other networking protocols, allowing the management of what content arrives at your machine, rather than just where it comes from.Host firewalls or 'software firewalls' involve the use of firewalls on individual user devices and other private network endpoints as a barrier between devices within the network.A network firewall requires configuration against a broad scope of connections, whereas a host firewall can be tailored to fit each machine's needs.Filtering traffic via a firewall makes use of pre-set or dynamically learned rules for allowing and denying attempted connections.Screening routers are specialized gateway computers placed on a network to segment it. They are known as house firewalls on the network-level.Network firewalls may come in the form of any of the following appliance types: dedicated hardware, software, and virtual.