Firewalls

Are designed to control and filter which communications are allowed in and out They can install on one computer and in this case called Host-Based Firewall or be standalone Protect Network and in this case called Network-based Firewall

Types

(1) *Network Layer Firewall:* It Filter Communication based on The Source and destination IP address.
(2) *Transport Layer Firewall:* It Filter Communication based on The Source and destination Data Port and The Connection status
(3) *Application Layer Firewall:* It Filter Communication based on The Application, Program and Service
(4) *Context Aware Layer Firewall:* It Filter Communication based on The User, Device, Role, Application Type and Threat Profile
(5) *Proxy Server :* It Filter Web Content Requests, URL, Domain Names and Media Types
(6) *Reverse Proxy Server:* it is in front of the web server Protect, hide, offload and Distributed Access to Web Server
(7) *Network Address Translation NAT Firewall:* hide and masquerades private address of network hosts
(8) *Host-Based Firewall:* Filters Ports and System Service calls on single computer operating system

Port Scanning

Each Application Runs on device is assigned to a port number used in source and destination so that data passed to the correct application. Open Port can used maliciously to identify the operating system of the device and services OR it may be used by the system admin to verify security policy .
program for Port Scanning NMAP , ZENMCP

Intrusion Detection System IDS	Intrusion Prevention System IPS
Doesn't Take Action It only Detects ,logs it and alert the network administrator and reports and won't prevent the attack from happening As IDS Slow down the network It is Preferred to work offline to over come latency so data passed to the switch then it copies it to the IDS	It Blocks and Deny Malicious Traffic based on positive Rule or Signature match one of IDS/IPS System is Snort. The commercial version of Snort is Cisco's Sourcefire. Sourcefire can perform real-time traffic and port analysis, logging, content searching and matching, as well as detect probes, attacks and execute port scans.