Cybersecurity devices and technologies

Security appliances

Can be standalone devices like a router os software tools that are run on a network device  
 they have 6 categories:

ROUTERS  
 - also provide basic traffic filtering capabilities, define which computers from a   
 given network segment can communicate with which network segment

FIREWALLS  
 - look deeper into the network traffic itself and identify malicious behavior that  
 has to be blocked. It can apply sophisticated security policies that apply to the  
 network traffic

INSTRUSION PREVENTION SYSTEMS  
 - IPS systems use a set of traffic signatures that match and block malicious traffic   
 and attacks

VIRTUAL PRIVATE NETWORKS  
 - VPN let remote employees use a secure encrypted tunnel from their mobile   
 computer and security connect back to the organizations network

ANTIMALWARE OR ANTICIRUS  
 - these systems use signatures or behavioral analysis of applications to identify   
 and block malicious code from being executed

OTHER SECURITY DEVICES  
 - those can be web and email security appliances, decryption devices, client   
 access control servers and security management systems

Firewalls

Is designed to control or filter which communications are allowed in and which are allowed out   
 of a device or network

It can be installed on a single computer with the purpose of protecting that one computer   
 (host-based firewall)   
 or it can be a standalone network device that protects an entire network and all the host devices  
 (network-based firewall)  
 types:  
 network layer firewall  
 transport layer firewall  
 application layer firewall  
 context aware layer firewall  
 proxy server  
 reverse proxy server  
 network address translation (NAT) firewall  
 host-based firewall