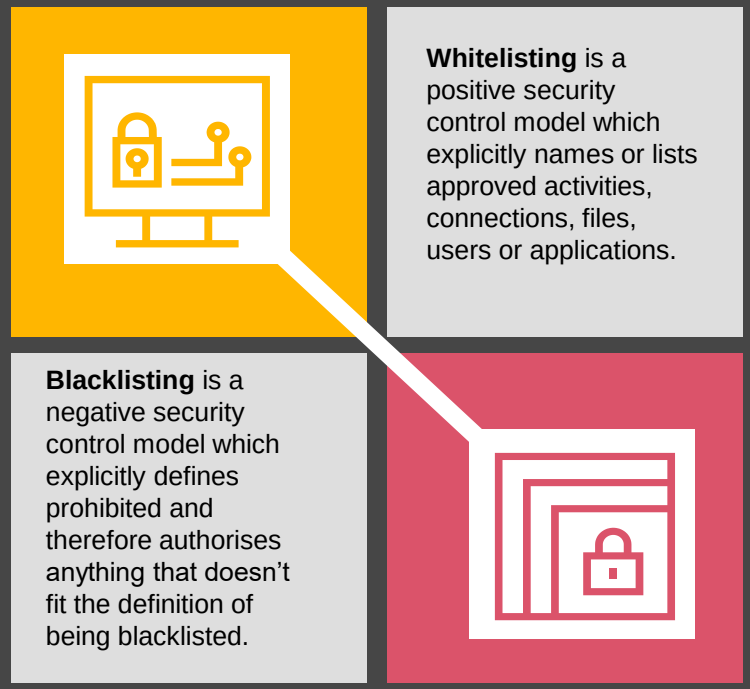
Network Segmentation

Segmentation is the process of breaking a large network into smaller ones. "The Internet" acts as if it is one gigantic network, but it's not. It's actually many millions of internet segments that come together at many different points to provide seamless service. An internet segment (sometimes called "an internet," lowercase) is a network of devices that communicate using TCP/IP and thus support the OSI 7-layer reference model. This segmentation can happen at any of the three lower layers of our protocol stacks, as we'll see in a bit. Devices within a network segment can communicate with each other, but which layer the segments connect on, and what kind of device implements that connection, can restrict the outside world to seeing the connection device (such as a router) and not the nodes on the subnet below it.

Segmentation of a large internet into multiple, smaller network segments provides a number of practical benefits, which affect the choice of how to join segments and at which layer of the protocol stack. The switch or router that runs the segment, and its connection with the next higher segment, are two single points of failure for the segment. If the device fails or the cable is damaged, no device on that segment can communicate with the other devices or the outside world. This can also help isolate other segments from failure of routers or switches, cables, or errors (or attacks) that are flooding a segment with traffic.



Source: Mike Wills, Systems Security Certified Practitioner Official Study Guide