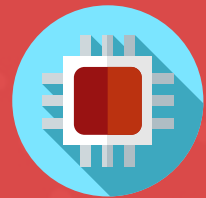


FIREWALL VS ANTIVIRUS



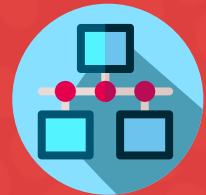
Las implementaciones de hardware y software se encuentran en el firewall.



Su capacidad de supervisión se basa en un conjunto de reglas predefinidas.



Las amenazas externas se tratan con un firewall.



Los ataques como la suplantación de IP y los ataques de enrutamiento son posibles con el contador de firewall.



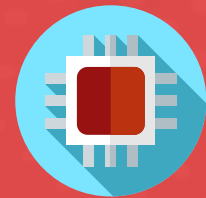
Un cortafuegos realiza filtrado y seguimiento.



Un firewall monitorea la amenaza de paquetes entrantes.



El cortafuegos inspecciona los paquetes entrantes.



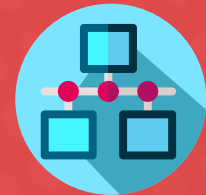
El antivirus solo se puede implementar en el software.



El fabricante impone sus técnicas de capacidad de seguimiento.



Todas las amenazas internas y externas son manejadas por antivirus.



El antivirus no requiere contraataques después de que se elimina el malware.



El antivirus se utiliza para buscar aplicaciones y computadoras comprometidas.



Antivirus monitorea la amenaza del malware.



El antivirus inspecciona el software malintencionado que reside en la computadora.

