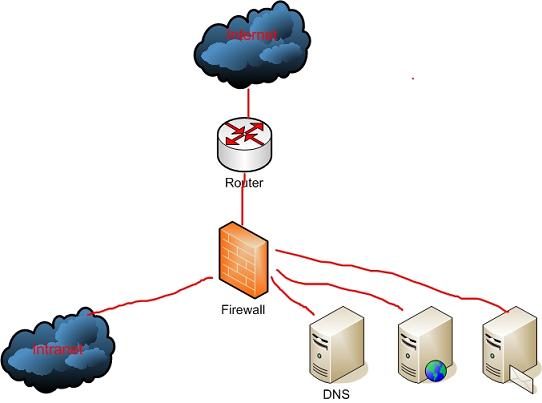
Security is a big deal for many organizations, especially if they are dealing with sensitive customer data across a wide area network (WAN) like the one we have implemented for our organization. One of the biggest threats that can get to a network is a virus. A virus is a malicious program written to either destroy or steal files typically involving data that is meant to be very secure (Dean, 2013, p.647). The company firewall should be installed in each building to help keep unwanted traffic from gaining access to the network. Employee education is also important. Usually, threats have an easier time coming in if they are invited by the user. Simple tips such as not opening unwanted or suspicious emails can save the company a lot of time and trouble. Malware and anti-virus software should be installed on each computer and should be updated on a regular basis by the administrator. This keeps everyone safe as they do their work on the network.



The way you configure the hardware can also help with security too. Make sure that administrators are the only ones who have access to key things like the routers and root privileges on the network. If someone has access that does not know what they are doing, it could be very hard to fix once the damage is done. The access should be secured by a password that is not easy to hack either. “All defenses are useless if someone has access to them” (Parker, 2006).

The administrator has a key role in monitoring the network. Once everything is kept out that should not be in the network, it is the administrator’s job to make sure that any and all activity in the network is authorized activity. A good idea is to keep a log of registered activities in a log file that has to be checked regularly. That way any irregularities can be seen and reported immediately (Dean, 2013, p. 646).

# Works Cited

Dean. (2013). *Network+ Guide to Networks, 6th Edition*.

[Bookshelf Online]. Retrieved from https://online.vitalsource.com/#/books/9781133608196/

Parker, D. (2006, August 16). *TechGenix.* Retrieved from Network design and defense: http://techgenix.com/Network-design-defense/