DMZ Architecture

Coleman Kane
Coleman.Kane@ge.com

August 24, 2014

DeMilitarized Zone (DMZ)

Korea: Example of a real-life DMZ. The 150-mile wide Korean DMZ was established between north and south Korea in an agreement to halt the fighting in the Korean War, in 1953. Access by either country to the DMZ is tightly controlled, while the DMZ itself is closely monitored for unauthorized intrusion.

Figure 1: Korean Peninsula DMZ[1]

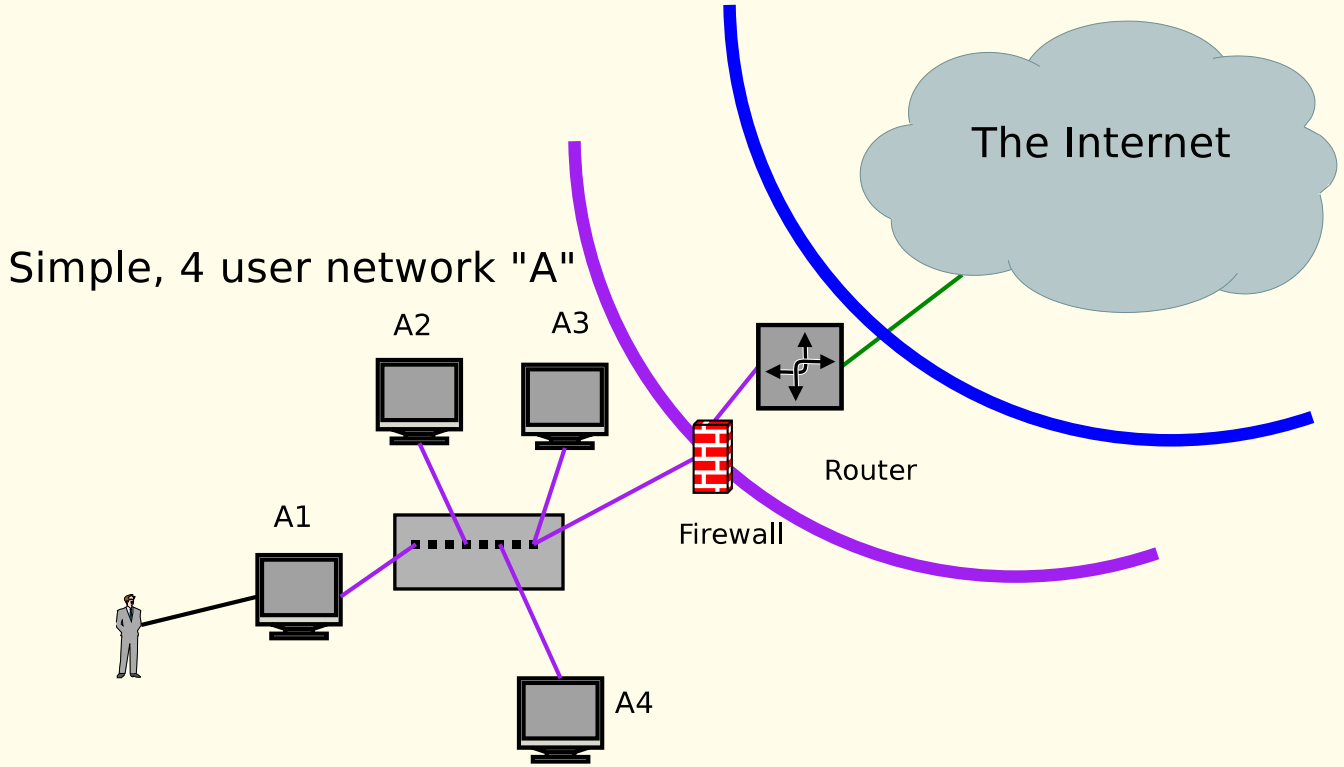
Both North & South Korean geo-political interests are served by establishing this DMZ. The purpose of this "land barrier" is to maintain a buffer zone between both countries so as to make it nearly impossible to pass from one country to another.

- Access to North Korea is limited primarily to residents, as well as its geo-political allies to the north, namely: China & Russia
- Access to South Korea is restricted primarily to residents, as well as its geo-political allies, who mostly are transported by sea, such as from Japan and the USA.

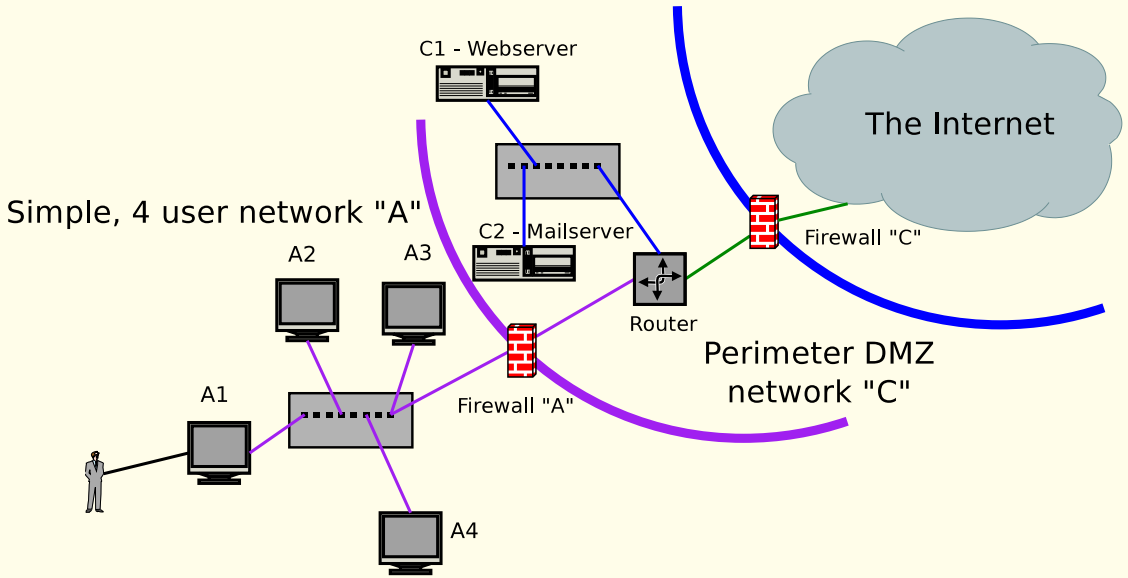
Similar methodology can be applied to network design, especially using the router + firewall example from earlier, with the exception that we can also utilize a network "DMZ" as a parition in which to host systems.

- Within the DMZ, systems have tightly-controlled access to the rest of the corporate network.
- Access to the Internet may or may not be as tightly controlled as it is for the corporate network.
- If an attacker intrudes upon the DMZ, they only have access to other DMZ-based servers, but not necessarily private corporate systems
- Targeted monitoring & instrumentation around the perimeter of the DMZ may assist in detecting and responding to adversary activity within the DMZ as they attempt to scan this environment, with minimal exposure to the actual sensitive resources.

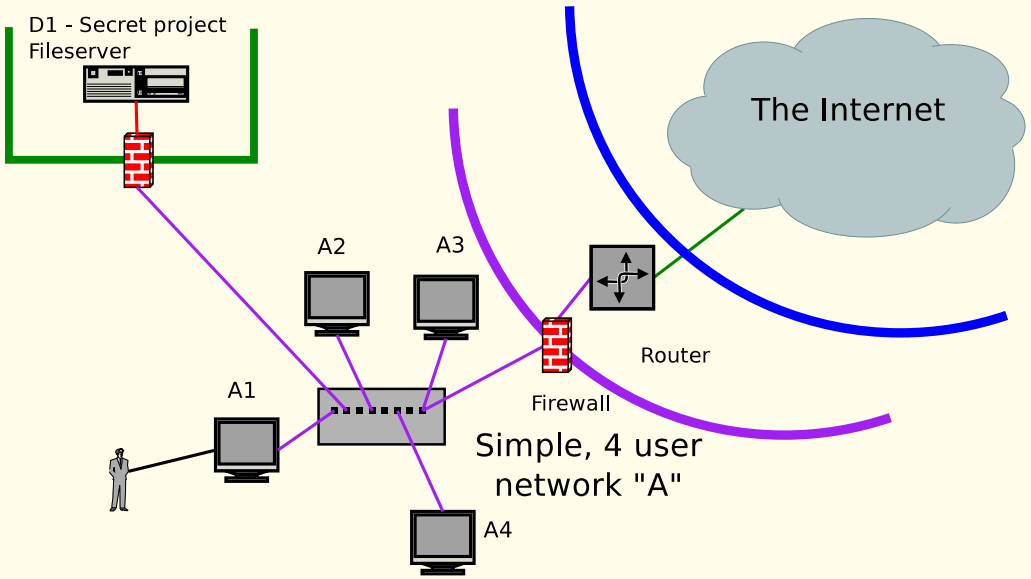
The Internet is conceptually just a big network containing "everyone else", and therefore can fit into one side of our earlier diagram



Using the same logic as presented in the network architecture section, you may create a controlled partition in which you can deploy servers that provide services to the public Internet, but which still cannot directly access your internal private network.



Sometimes you might want to protect an internal project, team, or storage network from exposure.



The firewall protecting D1 could be configured to only allow communication with A1.

Through selective partitioning of the network, it is possible to:

- Divide your systems into isolated enclaves, which may ease maintenance
- Provide extra layers of protection to reduce risks due to compromises of specific systems
- Force network traffic to follow a specific and defined path, by policy, when it involves communication between two networks and/or devices
- Temporarily contain intrusions, providing ample time to respond

[1] Unattributed BBC author. War remains sought in korea's dmz. http://news.bbc.co.uk/2/hi/asia-pacific/7679697.stm, October 2008.