Post by: Jonathan Callaghan

Thank you, Michael for the great insight into firewalls. As suggested, the benefit of the Proxy firewall on the A\application level is that the server cannot be accessed easily by any internal network nodes. If poor configured, the firewall would discard the connection without the appropriate proxy code (Firkhan Ali Bin Hamid, 2011). Subsequently, this is beneficial as there is reasonable control on connections with the IP address and managing services such as allowing HTTP requests but not FTP connections meaning that this platform cannot launch an attack.

The proxy firewall can log information of connections but will have limitations utilising speed. Applications can be limited in support of the network, but the added level of security can slow the process. A further issue is that it can be proxied but not filtered when considering HTTPS, which raises concern of whether usability or security is the trade-off. For example, it would need consideration to allow all protocols by default or only those that can be proxied and block others (Arnott, 2002). If we default to deny all this, it becomes more restrictive but more secure, easier to maintain, and allows administrators more control over what the internal users can access.

Arnott, R. 2002. A Review of Current Firewall Technologies. Master of Science, University of Otago.

Firkhan Ali Bin Hamid, A. A study of technology in firewall system. 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA), 25-28 Sept. 2011 2011. 232-236.