**Windows firewall Lab**

Windows 7 and 8.1

1. Make sure you have internet connection.
2. Make sure the firewall is turned on if not turn it on.
3. Write down the network you are connected to currently.
4. Configure so that firewall notifies when it blocks a program.
5. On a private network configure to block all incoming connections
6. Add IE as one of the allowed program on public and private networks.
7. Allow Remote assistance program only on private network.
8. Allow Wireless portable devices on private network.
9. Allow Windows media player on private network.
10. Make sure firewall is turned on, in all the profiles
11. Make sure incoming connections are blocked and outgoing connections are not in all the profiles
12. Increase the logging size limit to MB for all profiles.
13. Save the log files in C:\Users\<your admin account name folder> for all profiles.
14. Allow connections only when secured, authenticated and integrity protected.
15. Make sure IE can be used by users 1 through 6. and user 9 and 15.
16. Make sure this is rule applies on all the network interfaces.
17. Make UAC settings to always notify
18. Make sure Windows Defender performs a quick scan everyday at 12 A.M
19. Exclude the Home folders when quick scan is performed
20. Do not scan \*.txt and \*.jgp files.
21. Use Windows Defenders to scan e-mails and removable drives too.

Windows server 2008:

1. Make sure the firewall is turned on if not turn it on.
2. Configure so that firewall notifies when it blocks a program for all profiles.
3. Increase the logging size limit to MB for all profiles.
4. Save the log files in C:\Users\<your admin account name folder> for all profiles.
5. Allow only secure connection for FTP server. (incoming rule)
6. Allow connections only from users 1 through 10 to connect to FTP server. (incoming rule)
7. Make sure the rule applies for all network interfaces for FTP server. (incoming rule)
8. Allow only secure connection for RDP. (incoming rule)
9. Allow connections only from users 1 through 10 to RDP to the server. (incoming rule)
10. Make sure the rule applies for all network interfaces for RDP. (incoming rule)
11. All outgoing TCP and UDP connections must have their connections encrypted.
12. Change UAC setting to notify always.
13. Make sure each time a problem occur the server must ask you before checking for solutions.
14. You must get recommended updates.
15. Configure to download the updates but lets you to install them.