Limit Remote Desktop Access from Specified Sources via Windows Firewall

These instructions pertain to Windows 7 using the built-in Windows Firewall. You should always connect to the VPN before accessing your computer from off-campus. VPN Instructions are here.

The following instructions walk you through limiting Remote Desktop connections to the VPN IP address ranges. A similar configuration should be setup for any other Operating System or third-party firewall prior to using Remote Desktop.

1) Open Windows Advanced Firewall Settings via Start Button → Control Panel → System and Security → Windows Firewall. Confirm that Windows Firewall is enabled and then click Advanced Settings.
2) Click on Inbound Rules:

3) Find the rule named “Remote Desktop (TCP-In):”
4) Double click the rule and confirm that the rule is Enabled and the Action is set to Allow:

5) Click on Scope to limit where you are going to permit Remote Desktop connections from. Under the Remote IP address section, choose the radio button next to “These IP addresses:” Type the IP addresses of machines you will be connecting from.

Note: If you are connecting from home using the VPN, you should limit it to the VPN DHCP range, which is currently 129.49.6.0/24 and 129.49.203.0/26. If you are connecting from a specific computer on-campus, you would have to request that IP address to be reserved so that it does not change over time.
6) Click Add and then type in the desired IP address or IP address range. In this case, we are limiting access to the VPN so we will add 129.49.30.0/24 first. Click OK.

7) Repeat the process for 129.49.203.0/26. When you are finished it will look similar to the below screenshot. Click OK.