

Table of Contents

Barrier Methods of Protection (Personal Firewalls) 1

Barrier Methods of Protection (Personal Firewalls)

Fester approves of barrier methods of protection and so has always installed a personal software firewall on his computer (not the server, just the client computer).

Don't get confused, I am not referring to the firewall built into your router but an additional software firewall that you install on a personal computer.

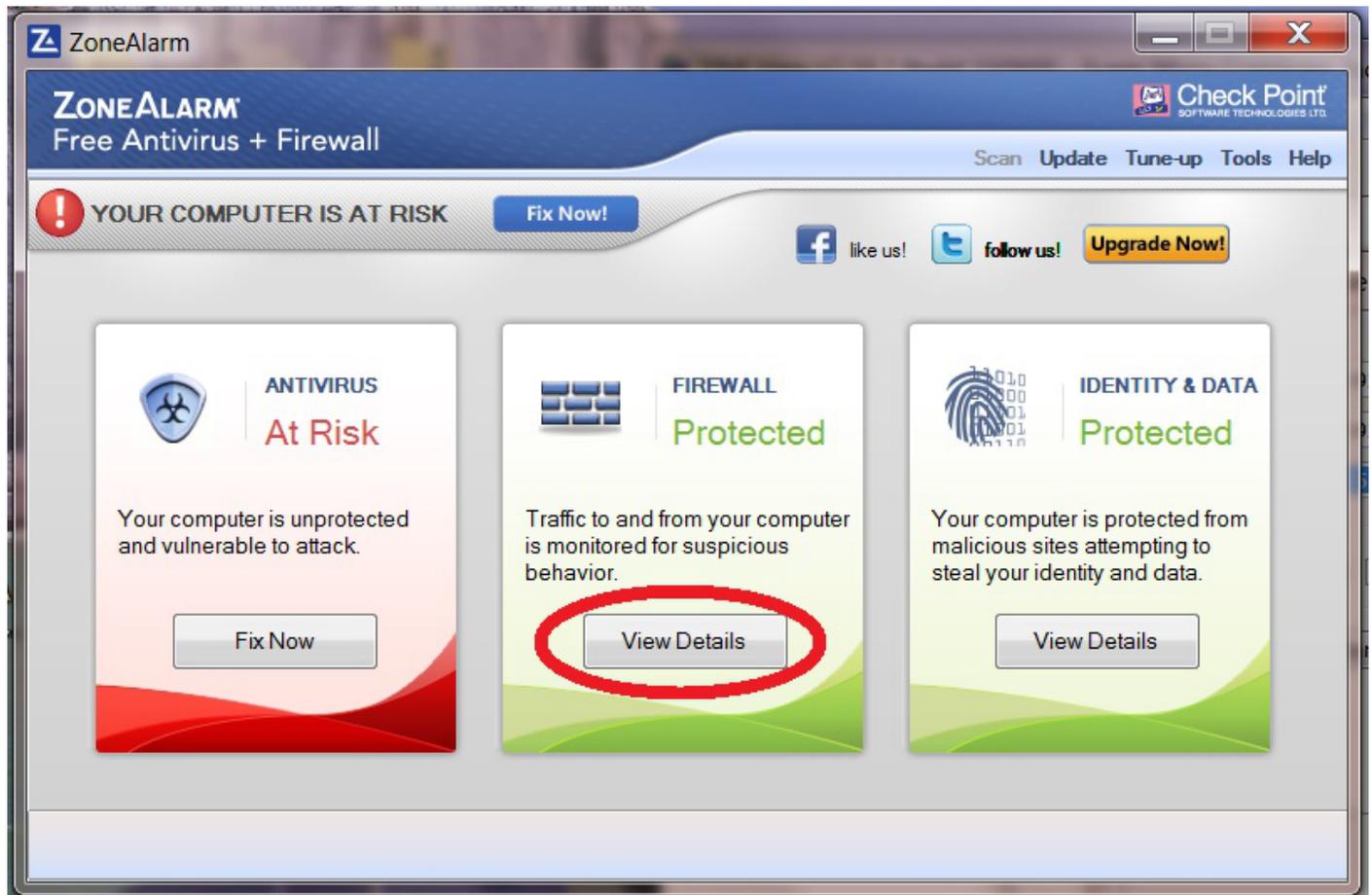
This software firewall will stop any shares created on your server from working on the client. Therefore, we must configure the software firewall to allow the server and client to share nicely.

After much experimentation (netbios names, etc) I got more consistent results by specifying an IP address range within the firewall software that corresponded to the IP address range used by the server.

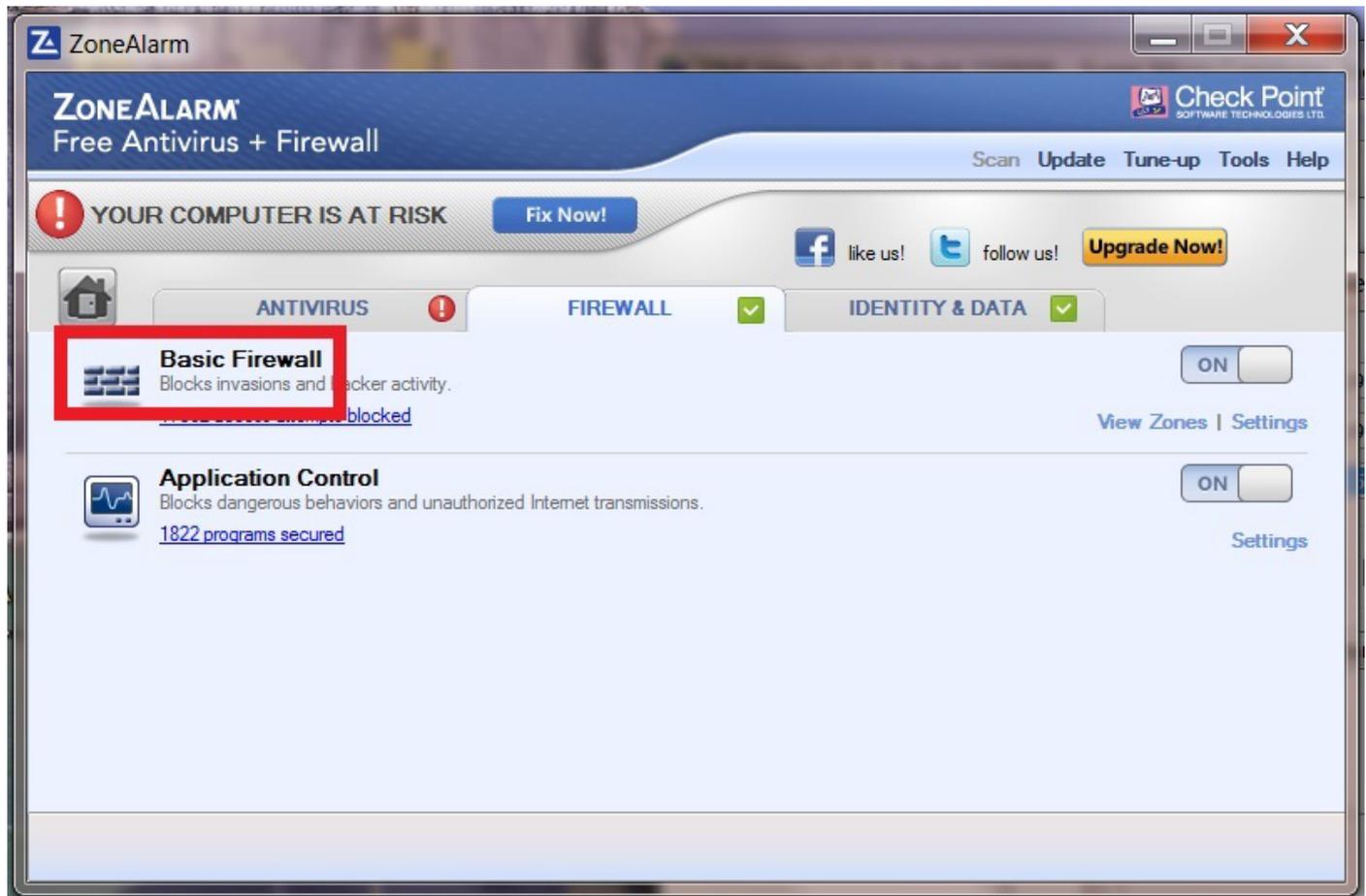
Fester's server IP address range goes from 192.168.0.2 - 192.168.0.49. If we tell the firewall to trust this range of IP addresses then all will be well.

I use Zone Alarm (you might use something different, but the principle will be the same). Here is how to set it up.

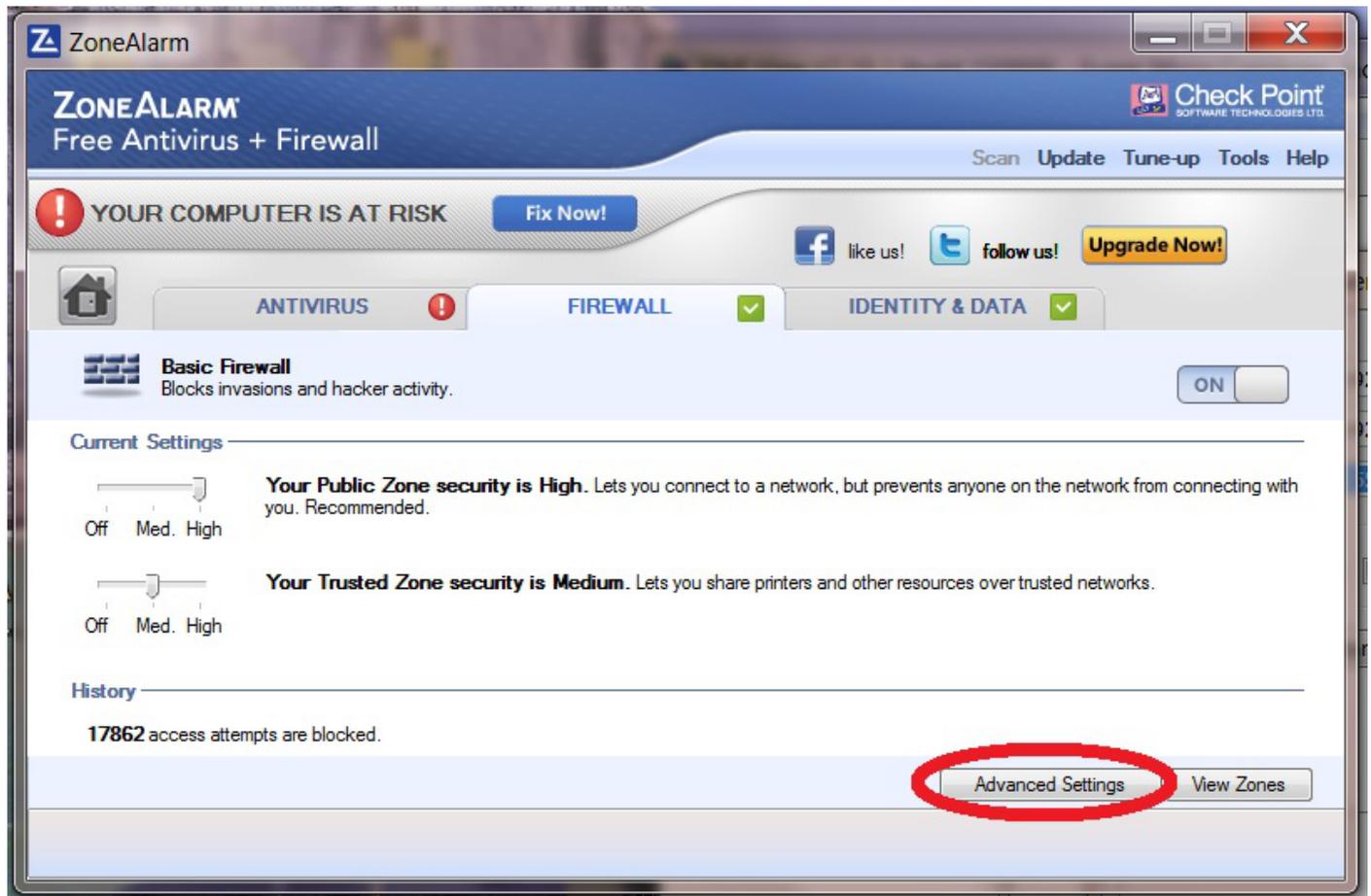
Open Zone Alarm and click "View Details" under firewall.



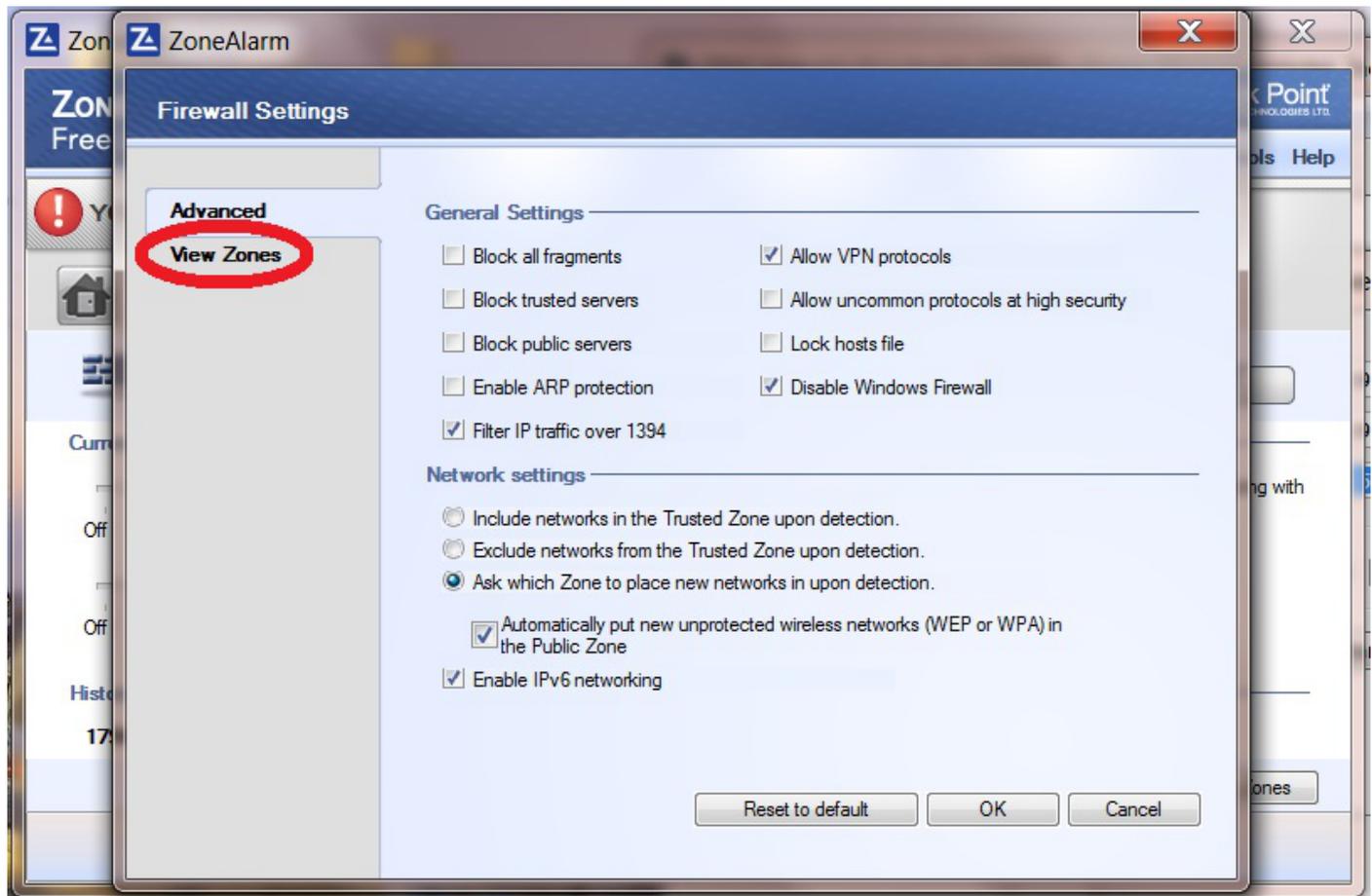
Now click on "Basic Firewall".



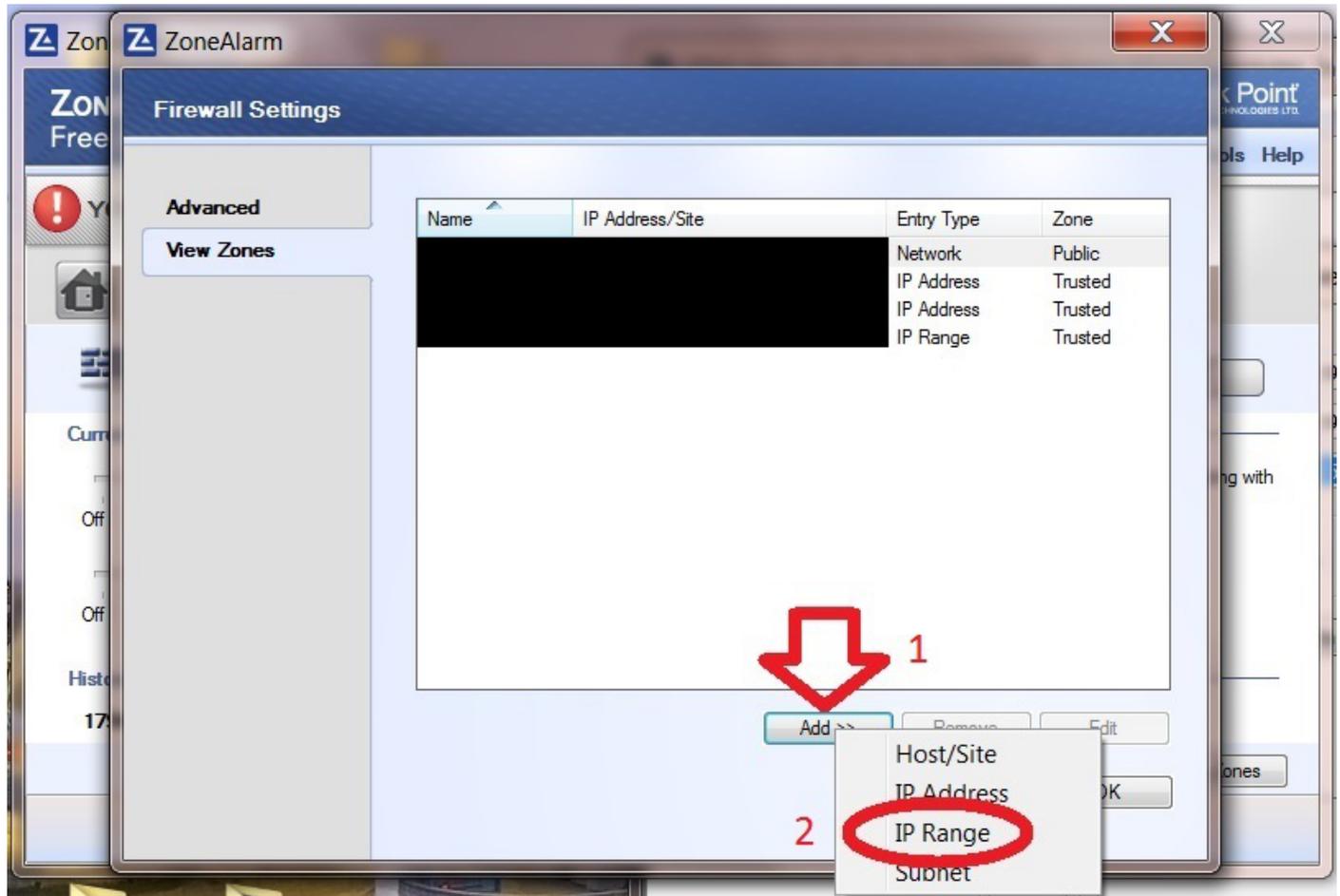
Now click on “Advanced Settings”.



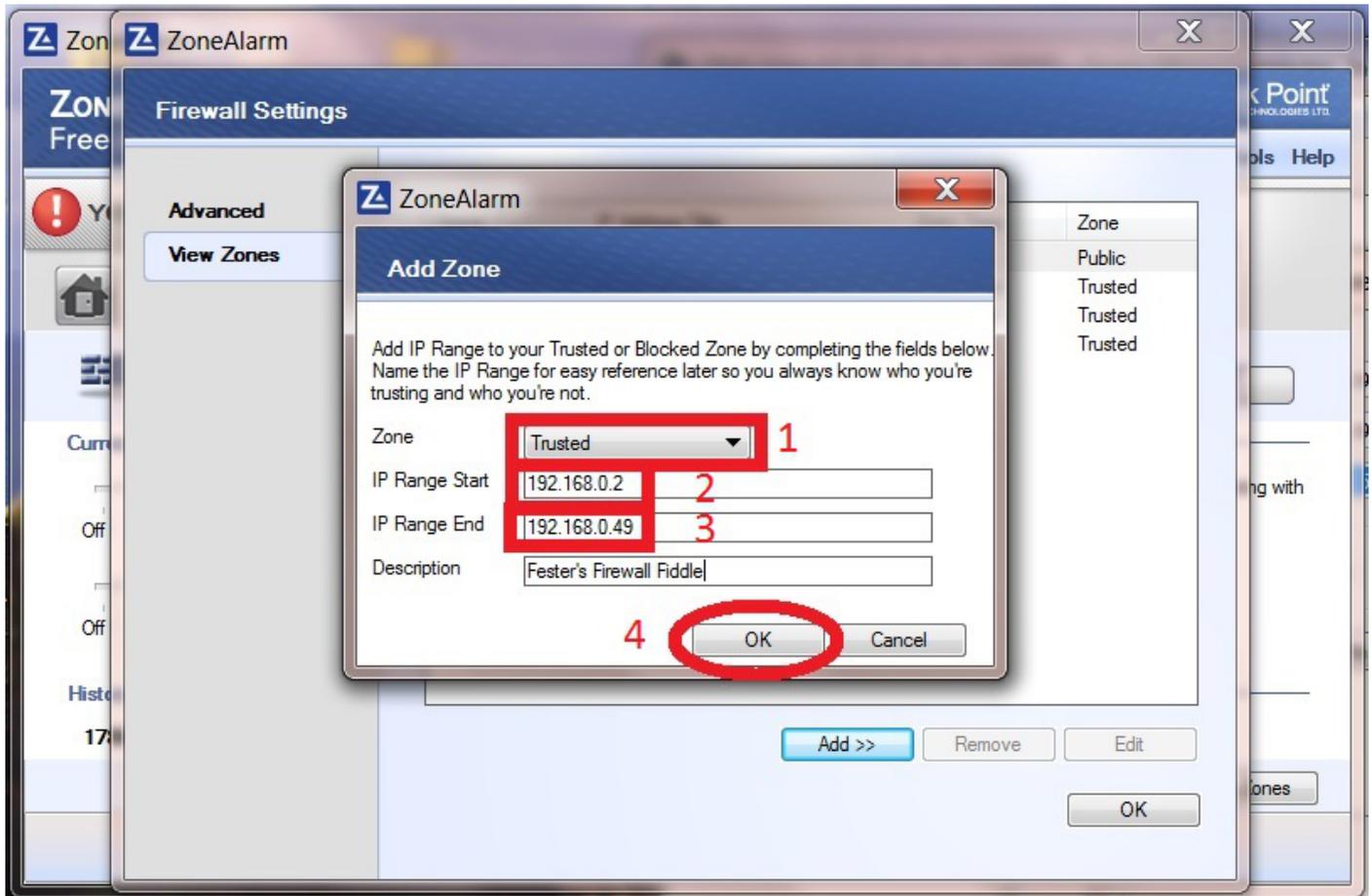
Click on "View Zones".



Click on "Add" (1) and chose "IP Range" (2).



Set the drop down selection box next to "Zone" to "Trusted" (1). Enter the first IP address of your server's IP address range in the "IP Range Start" text box (2) and then enter the last address in your server's range in the text box labelled "IP Range End" (3). Call it something meaningful in the "Description" text box and press OK (4).



That should be the firewall configured.

From:
<https://familybrown.org/dokuwiki/> - danb35's Wiki

Permanent link:
https://familybrown.org/dokuwiki/doku.php?id=fester:prelim_barrier

Last update: **2016/06/08 10:21**

