

Zone and Program Expert Rules, Program Permissions, and Zone Rules and how they Interact.

You have several different layers of permissions and rules that can be used to modify how your computer and / or a program can connect to or be connected to, the internet.

Zone Rules and Zone Expert Rules

To begin with there are the global rules. These are the Zone expert rules, and the Zone rules (internet, trusted, and blocked)

The main type of global rules are Zone Expert Rules. They are enforced in order that they are listed in the expert tab. If the incoming packet doesn't match the first rule, then it continues to be compared to each rule until it finds a match, and then the rule is followed. If no match is found then it continues on to the Zone Rules. Once its determined where this packet falls in it is either passed on to the program section of enforcement, (in the case of trusted and internet zone) or is blocked by a blocked Zone rule. The thing to remember about the global rules are that a packet is only applied to a single rule, so if a Zone Expert rule is applied to the packet, then it skips the Zone rules (trusted, internet, and blocked).

Program Permissions and Program Expert Rules

Now we get to the program enforcement. There are two sections to this also. Program Permissions and Program Expert Firewall rules. The main part of program enforcement is program permissions, they are

the general permissions for the program. One type of Program permissions is access rights. This means a program can request information from a particular zone, either trusted or internet, depending on which kind of access you let it have. Then is Server rights to the trusted zone or the internet zone. This means that the program can listen to the internet or trusted zone for connection requests. If you allow this, then someone on the internet (or the trusted zone) can talk to this program all day long without your permission. So you can see that allowing this may not be in your best interest. Not many programs need to have server rights. If you are using an IM client, they need internet server rights. To this general rule there are exceptions, even all IM clients don't require internet server rights. A few others also need it. The best thing to do with this is deny it the first time a program asks for it, then if the program fails, then you can approve it.

Now we get to the Program Expert Rules. These only modify the Program permissions. So if you do have to give a program any rights, you can modify the rights to only be able to connect to certain servers, ports or at certain times by creating expert rules.

The way they are enforced is that all Program Expert Rules all equally apply to the packet. So an incoming (or outgoing) packet will go to each rule, and if it applies then the rule will be performed, and then move to the next rule. So if you have 10 Program Expert rules, the packet will be compared to all ten rules. This is the reason that you have to place a blocking rule at the end of each set of program rules, that way if the packet doesn't apply to the rules above then it will be blocked. Adding rules after a blocking rule will have no affect as the packet has already been blocked from doing anything.

One other thing that you need to be aware of is some programs tell you that you need to open ports for them to work. Opening ports is not the wisest choice in the world, and if you have to do it, you need to be careful how you do this. To open a port to the entire system you have to do it in the Zone Expert Rules. To do it for a single program you do it in the Program Expert Rules, but the port isn't always open unless the program is running AND you have given the program Internet server rights. So chose wisely on how you open ports. Always pick the most restrictive way of doing it, that way it is controlled better.