Firewall

General Concept

A firewall is in general a piece of software or hardware, that is meant for blocking (unwanted) network communication. This is specifically important in sensitive areas, such as in companies or organizations and in general when being exposed to the internet. There are many variations of what exactly a firewall will be checking for, from simple port blockings to elaborate analysis of package inspection results.

Kinds of Firewalls

There are in general two types of firewalls, the hardware firewall (a dedicated device placed between a protected network and the rest of the network (e.g. the internet)) and software firewalls (also known as desktop firewalls). The latter have the advantage, that they can be deployed on every client. Windows since Windows XP has one on board, as well as Linux. The disadvantage is, that it can be tampered with client-side, e.g. by some malware infection. The hardware solution is usually not modifiable for the clients, so should be a lot more resilient to attacks, but usually also requires a lot more knowledge to maintain it.

Problems When Gaming

In the gaming context firewalls are both, useful and problematic. On the one hand side they provide additional security to the protected computers. On the other hand they can get in the way when trying to play via network. Especially when you have no access to their settings (e.g. hardware firewall maintained by another person) they may even make it impossible to play via network.

Troubleshooting

Software Firewalls can very often be adapted to allow certain applications, ports or IP addresses/ranges to be allowed through. They might still work differently for outgoing and incoming traffic. So when trying to get a game working, make sure to set the right settings. **In general it is not advised to turn off your firewall permanently.** You may of course turn it off for short periods of debugging (seeing, if the firewall has anything to do with encountered problems at all).

Depending on the situation, a firewall may or may not be the cause of problems when trying to play over a network. As there are many different solutions, it is not always quite clear, if the firewall is actually the problem. For instance, many games refuse to connect to (or even display) matches, that run under a different version of the game. Also routing issues can be a cause of impossible connections. Very often people tend to attribute this solely on firewalls, so turning them off

Misconceptions

A firewall should not be confused with a NAT. While the former can do many kinds of security checks and only the eventual result is a block, the NAT's job is a completely different one. It is only meant for facilitating network connections for many clients on a (private) network to other hosts on the internet, by using only one public IP address. This means, blocks of incoming connections are not a security measure in the conventional sense but more a question of where to send the data to. (See Port Forwarding on the matter.) Outgoing connections are usually not blocked at all (at least not on consumer routers) so the security aspect comes a lot more short for NAT then for firewalls. While a NAT may give a basic protection from accesses from the outside, it is not meant for that purpose.

See also

- Network Address Translation
- Port Forwarding

[games_database] [network_terms]