Firewall Security Best Practices

A firewall protects your network in general and devices on the network in particular from malignant traffic by acting as the first respondent. A firewall keeps an eye on incoming data packets to block unwanted traffic based on a defined set of rules. A firewall also prevents the outgoing traffic from accessing bad nodes and sites. It can be installed as a software, which is usually a preferred method for individual devices, or a hardware can be installed to secure the network from unwanted traffic.

### Know your Data

The first and foremost step in ensuring firewall security is to know the information you need to protect and the threats to it. For example, you would need to have a different set of rules defined to protect financial data than visual data.

### Regular Monitoring and Management

Keep an eye on security protocols for your firewall to ensure enhanced firewall security. It is important due to the continuous evolution of threats. A firewall can make recommendations on basic rules, however, it is important to create and manage Acces Control Lists (ACLs) periodically.

### Follow Standards

Firewall Security rules need to be reviewed and updated based on the laws set by the local government and/or other regulatory authorities. This can help with understanding and avoiding unknown threats to your system. Thus, it is specially important for organizations that handle sensitive data, for example, banks, etc.

### Find Loopholes and Track

Backdoors can create a major loophole in your system firewall security hence making it vulnerable. Therefore, it is particularly important to keep testing and attacking your system internally. Record and manage the logs of all the updates to the firewalls for a periodic review and a complete system upgrade/update and the attacks on the system. Documenting small updates and tracking the known threats is a vital part to endure firewall security.

### Develop Trust

Every new source of traffic needs to be properly monitored and filtered multiple times before it is marked safe. Developing trust is the key instead of allowing incoming traffic at face value, hence, use a combination of firewalls at different levels to ensure this. This also includes the external devices connecting to your network that need to be monitored regularly and are in compliance with the set rules by your organization.

In conclusion, a firewall is your first line of defense against any threat you might face in the virtual world. Therefore, it is important to understand how to take full advantage of the available features. It is important to not only set up the firewall security of your network but regular review and monitoring of the set rules are also vital to your system’s health.