To ensure adequate protection for your network and devices, it is best to take a systematic approach.

**Control Visibility of Applications**
Consider which applications you want people within your network to be able to access as well as the visibility you need to achieve.

**Preventing Threats**
A next-generation firewall (NGFW) not only controls which applications are being used, but it can also scan applications to ensure they do not present a threat.

**Focus on Devices**
Focusing on devices instead of IP addresses is often a better way of protecting your network. You can use a next-generation firewall that can help you search for a device using a username. In this way, you can stop a malicious user, find the device, and prevent it from accessing the network.

**Adequate Throughput**
Applying filters and processing information can significantly limit throughput. If you opt for an NGFW, choose one that gives you at least one full gigabit of throughput.

**Beware of Remote Users**
Whether your organization uses remote employees who work from home or a co-working space, if they connect insecurely, they can present a significant threat.

For more details about firewall design principles read the full article “Firewall Design Principles in Network Security.”