Securing communication within a network by leveraging Internet Protocol Security Tunnels

In an era of greatly increased surveillance, by both our own government as well as foreign threat actors, it has become critically important to protect our communications. Whistleblowers such as Edward Snowden and Julian Assange have shown us that our communications are very much unprotected, despite the utilization of current technology. The problem lies in the implementation of the technology rather than the technology itself. Another problem is the lack of defense created around internal communication and the focus being on communications from outside into our networks. A more commercial usage of this program can be to prevent incidents like the Anthem medical data breech, or the attack on Target that occurred recently. IPSec is a protocol that exists at the IP layer, 2nd layer, on the 7 layer ISO network model. Much of the protections we use, TLS, SSH etc, operate at higher level, which makes the communication more vulnerable. IPSec is a technology that has existed for quite a while, however due to the possible complexities associated with the protocol; it is often either not used or used incorrectly. We aim to solve this problem by creating an easy to use program that presents simple options to the user. By utilizing the program created by us, you establish a tunnel between two computers that sends all communication between those two computers through a secured tunnel. The program can be run on any computer with a current version of the Windows operating system.