Network Security

Generally network security starts by separating the network into an inner and an outer part. The "inner" part has to be protected against the "outer" one. The inner is "good", the outer is suspected to be "bad".

This simple separation of the world does not solve all security problems. The model is getting more and more complicated as soon as remote access or mobile computing is used.

One solution is establishing a VPN, a virtual private network.
("The good ones own a common secret").

Only setting up a firewall doesn't solve the problems:
All concepts of security require the supervision of the rules (policies) defined. This task has to take place all over your network permanently and on all network layers.
This means we need a supervision of the network: which stations are up and running (MAC− and IP−addresses), are these stations known (intrusion detection) and if they are known, are they allowed in the watched segment. Who is talking to whom using which port, which VLAN, especially when using tunnelling protocols (PPTP, IPSec,..); not a simple task.

As today’s networks are switched or routed it isn't so easy to get access to the information needed. If e.g. a person makes its own connection to the internet through a cell phone, this would be very hard to detect. But if he provides a "routing service" to these forbidden networks you can "watch" him (ARPs spread like broadcasts through switches).

You can also watch the traffic passing through your WAN−connection. A perfect tool for this task is RzK's ***NetControl*** for Windows. RzK's ***Address Wizard*** can scan periodically certain addresses of your network (reachability tests) and additionally watch the net to detect foreign addresses (detection of old / new addresses).