Personal firewalling and Intrusion dection systems

1. Install Tiny Personal Firewall (pf.exe) accepting default settings („allow trusted ...”). After a restart warnings start to appear – accept them (permit). Later you will learn how to make filters to process such warnings automatically.
2. Run MSIE to see a web page (any one) – accept the warning **setting a checkbox** to make a filter
   - Run Firewall Aministration (right click on TPF icon on the taskbar), press advanced button, see present filters. Change the filter, which has been just created: it should allow connection only to port 80 and only within the school (remote endpoint: network/mask)
   - Try a connection with https://sekret, add a filter which allows using https worldwide.

3. In the Microsoft Networking tab unmark "For Microsoft Networking use this...." and observ messqages appearing on the screen (mainly warning about UDP packets to port 138- NetBios, it is a normal activity in a windows network)
   - Mark the option again to stop the messages

4. Start a telnet session with any host (you do not need to log on, a connection trial is enough). Accept a warning setting the checkbox to create a filter. Then stop telnet and run it again. Now it should work without firewall intervention.
   - Check that using the FTP program (from the command line) generates warnings (it tries to connect to port 21).
   - Change the filename telnet.exe to telnet.sav (folder \winnt\system32), then copy ftp.exe to telnet.exe in the same folder. Check if you can run FTP now, fooling the firewall program by the name change.
   - See the MD5 tab in Firewall Aministration window
   - Restore the files to their previous state.

Work in pairs:

5. make a shared folder, try to access it from a computer of your partner (it should work).
   - Block shared folder access in the Microsoft Networking tab. Check if the access is really blocked.
   - Add your partner’s computer to trusted computers (one IP address in „trusted address group”), check if it works.
6. Manually add a filter (tab „Filter rules” in Firewall Aministration window) for **ICMP Echo Request, direction:incoming**, action: **deny, log when this rule match**
   - In the miscellaneous tab check logging of unopened ports access
   - Try pinging your partner’s computer and scan its ports using any method (any program tool).
   - Open the Status Window : right click on the TPF icon on the taskbar, choose Firewall Status Window, see what processes are using what network resources
   - See the log file : menu Logs
7. Uninstall Tiny Personal Firewall

8. Install Sygate Firewall (spf.exe)
9. Configure the ping command – run it pinging e.g. z.pjwstk.edu.pl, accept firewall warnings **setting the checkbox** to create a rule and not to ask again
10. Open the **Application** window, find a line with **TCP/IP ping command,** then enter advanced window. Change the settings there leaving only „allow ICMP” (without options „server” i „client”)
11. Check if pinging e.g. z.pjwstk.edu.pl works now (it should). You can notice that the computers in the lab do not answer for pings. The firewall program display warnings on the pinged machines (do not accept these warnings). In the **Tools | Advance options** menu add rules which allow answering for pinging:
    rule 1 : allow incoming ICMP echo request all hosts
    rule 2 : allow outgoing ICMP echo reply all hosts, applications: \winnt\system32\ntoskrnl.exe

12. See if your computer now answers for pinging.

13. Watch the main window with graphs while your partner is scanning your machine. Then see entries in **Tools | Logs | security log** and .. **| traffic log**
14. Uninstall Sygate Firewall.

_____