Firewall policies

12. Mai 2011

These are the policies we settled on in class:

a) Flush all existing rules
b) Consider logging for each ruleset where appropriate
c) Use a blacklist
d) Limit the number of outbound connections per time for each host for given protocols
e) Allow anything *inbound*
f) Allow RELATED,ESTABLISHED
g) Throttle each connection accordingly
h) Do not allow SMTP from the honeynet
i) Allow DNS to known DNS servers
j) Drop IPv6 packets
k) Make sure you are using fail-safe defaults
l) Keep the firewall manageable via eth2 from one single host IP (use an arbitrary one for this task)
m) Restrict traffic from and to the logging server