Collegiate Cyber Defense Competitions

Inject Name	Define Firewalls on Windows & Linux Servers
Inject ID	TOOL24T

Description	Define software firewalls on each Windows & Linux server. The security policy should be default-deny with specific exceptions for expected inbound and outbound traffic. Be sure to log dropped packets, so these can be reviewed in order to find flows that should be allowed as well as unexpected flows that need to be investigated. In Windows a good choice is to use Windows Defender Firewall. For Linux either UFW or iptables are good choices.
Deliverables	Respond with a business memo that documents the installation, via screen shots, of the working firewalls and security policy configuration. For each server verify what was found among the denied packets and if legitimate packet flows were discovered and the policy modified accordingly. Further, identify suspicious packet flows and what the investigation of these found.