Scenario 1

A department of NCSU needs to set up a firewall policy for their new building. The building hosts 20 research labs, two computer labs, 30 faculty offices, 10 classrooms, and the department administrative office. Each department member may have multiple computing devices including desktops, laptops, tablets, smart phones, and so on.

For security reasons, all desktop systems are managed by the department. Any daemon service, except secure shell (SSH), requires approval to run. All SSH services, running at port 22, only allow on-campus access (*.ncsu.edu, 192.168.3.*). Off-campus traffic must connect through virtual private network (VPN) at vpn.ncsu.edu (192.168.2.2) with university login. The department has a public HTTP server (www.csc.ncsu.edu, 192.168.2.1) for hosting department member's web pages.

The AI lab (192.168.2.10) requests to host a database service at port 3306 for their re-search collaborators from University 1 (*.university1.example.edu, 10.1.1.2) and University 2 (*.university2.example.edu, 10.1.2.2) to share their datasets. The gaming lab (192.168.2.11) requests to host a multiplayer game server for general public on port 1080. During the past week, malicious activities were reported from taipei.csc.ncsu.edu (192.168.3.9) (SSH login attempts) and attack.example.com (10.2.1.1) (port scans).

Define firewall packet filtering rules based on the requirements and the evidence described above. List requirements and associate a strength value with each based on your intuition.