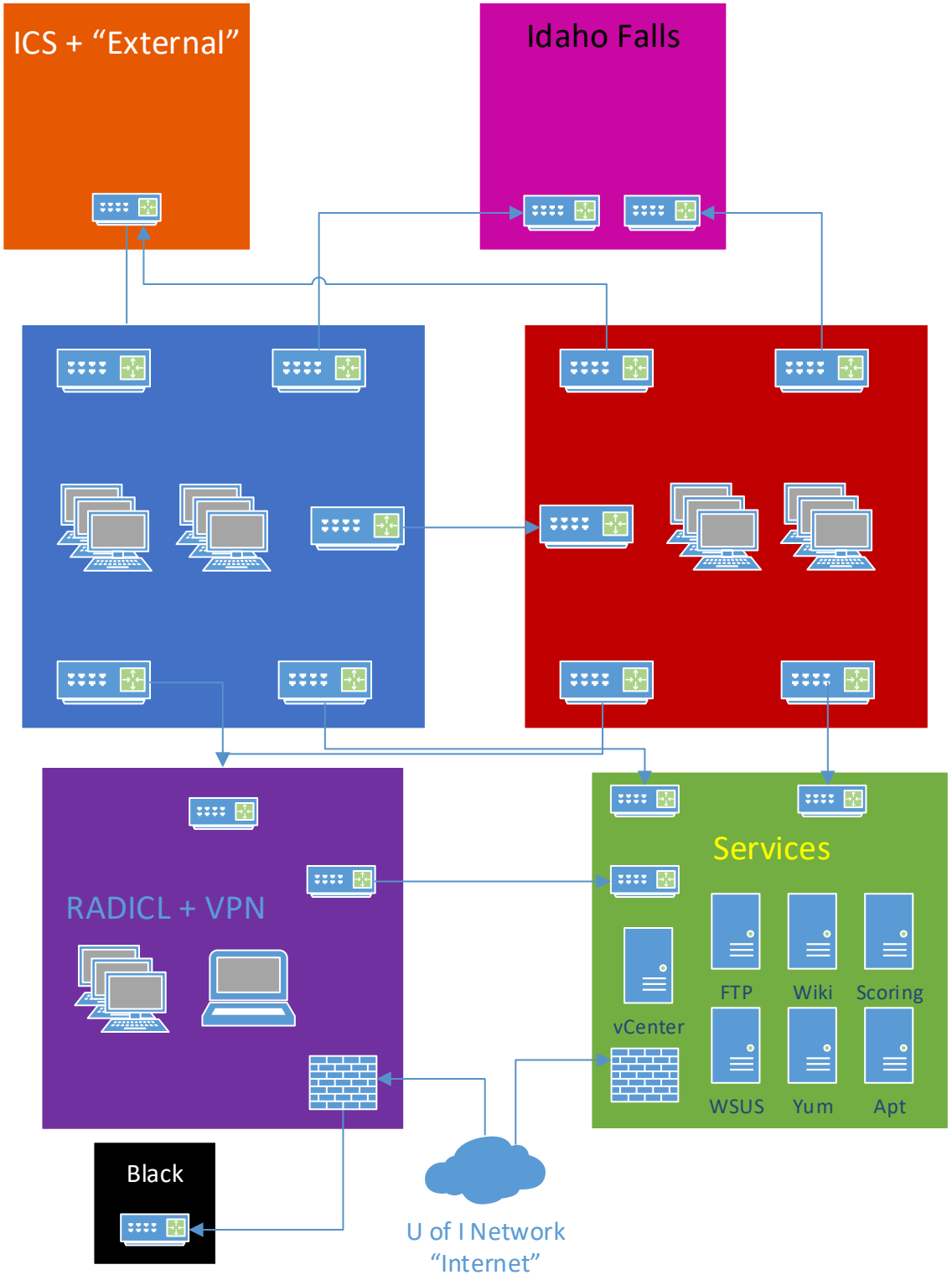

Red/Blue: Attacker/Defender networks. Isolated.
Green: Services for Red/Blue, use to setup and run scenarios. Use of Docker to isolate red/blue/purple without undue overhead (shared volume but separate containers).
Purple: Access to the environment. Isolated.
Orange: SCADA equipment + “External” services we want to simulate.
Pink: Idaho Falls red/blue network
Black (Not pictured): Infrastructure, e.g Management interfaces on servers, Pica8 switch, VRTX switches.

Red/Blue VMs have 3 interfaces: Green, Red/Blue, Purple
Green VMs have 2-4 interfaces: RedR, BlueR, External, PurpleR. (e.g vCenter from Purple only)

Green “Kill switch” to disable either specific services or the whole external interface.
Breaking isolation: Attack a service with active internet directly (since firewall), gain full control of it, then explicitly target external network. Essentially the same as attacking a student’s machine and using to launch attacks. (Unlike a student’s machine, our services are rigorously hardened)

Purple concerns: Students accessing over VPN or personal machines will need to use a VM with bridged access to the interface being used (VPN/Ethernet). The VM will be created using a Vagrantfile, so students don’t have to bother with configuration. That VM will need a private key + PW to access the SSH tunnel before it can access any VMs. (RDP/SSH/etc.) PW rotates by semester, key is distributed through email/bblearn,

Green services from Purple are accessed through the same interface, but a separate router.
Black is accessed through VPN port group, but with different key + user/pass + routing info. Firewalled separately from VPN router.