Grey team boxes that need internet connection will be connected to MAIN NAT and the router. Blue team boxes will be

Seperate router will hold the blue team and red team. Each will have an interface for their own subnet

This router will be connected to a black team box. This box will have access to the internet, but the blue team and red team boxes will not because this box is not a router.

Scavenger hunt - give red team credentials to mail server for social engineering

Mail server is untouchable - no locking blue team out

DNS names are the people