靶场需求

网络靶场是通过对于网络进行模拟仿真，进行安全演练、安全评估的技术手段相当于目标网络空间的数字孪生。针对于目前我们对强化学习在网络安全中的研究需求，对于虚拟的网络靶场有着以下需求。

- 符合真实场景
- 支持强化学习训练
- 可视化
- 可配置

> 根据以及目前使用的开源靶场的情况，以及我们前期调研，目标大部分强化学习靶场都可以做到 1）部分符合真实场景 2）支持强化学习训练
>
> https://github.com/Limmen/awesome-rl-for-cybersecurity

1.符合真实场景：（可与网络安全专家再确认）

一般来说，作为对于网络空间的数字孪生，其需要尽量真实的还原网络的环境配置。总的来说需要描述好网络空间中的**网络拓扑结构，资产硬件配置，软件环境，以及应用服务。** 同时需要描述在网络空间中的各个参与者: **进攻方，防守方以及正常用户**。具体需求如下:

1.1 网络空间环境

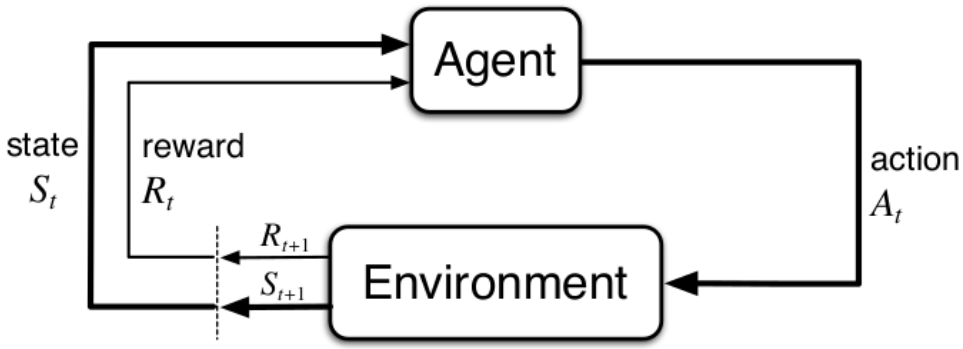
- 网络拓扑结构：靶场根据需求(可配置的)刻画出网络中不同设备的相连接的物理布局，主要包括以下
  - 节点之间的连接
  - 子网之间的关系
  - 子网/节点的物理地址
- 资产配置: 网络资产包括网络中的各种设备，比如主机、终端、路由器、交换机和安全设备（防火墙等），靶场中的资产配置信息需包括以下：
  - 各种设备的种类
- 各种设备的操作系统:Linux/Win/MacOS
  - 各种设备上运行的服务: Web/Database
- 各种设备上运行的应用：
  - **各种设备上的用户口令/权限信息**
- **以上不同配置对应的已知漏洞**

1.2 网络参与方

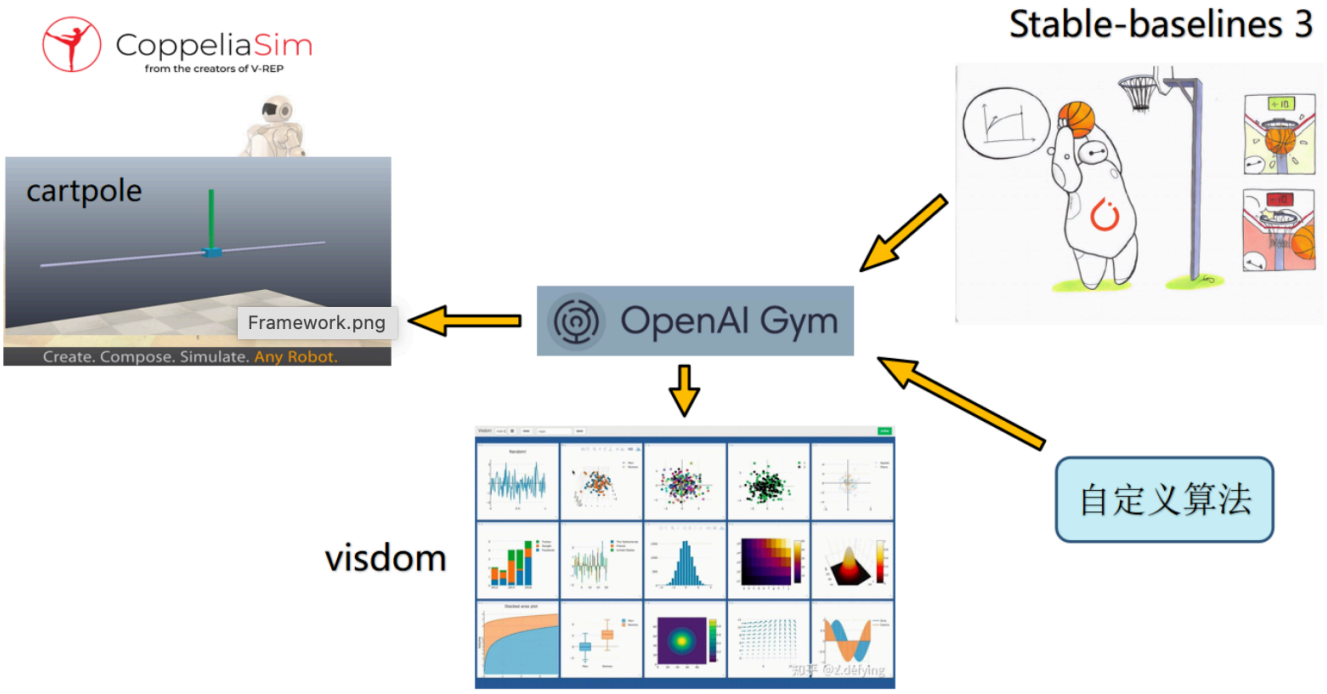
- 进攻方：
  - 需要可以包含其行为以及行为导致的网络中的变化
  - 需要表示其对网络信息的了解 (强化学习中的S--状态/观察)
    - 进攻方agent在进攻过程中对于网络的了解持续增加
  - **其行为可参考 ATT&CK**
    - 尽量做到可以包含里面的不同Techniques, e.g.:
      - Pre-OS Boot
      - Boot or Logon Initialization Scripts
  - 需要支持both on-host 攻击和 Remote 攻击
- 防守方：
  - 需要表示其对网络信息的了解 (强化学习中的S--状态/观察)
    - 防守方利用不同的防守设备中信息了解网络
  - 其具体行为也可以参考 **D3FEND** 或者 **Engage**
- 正常用户：
  - 正常用户的操作(Logon)也会对于防守方识别造成一些难度

2. 支持强化学习

因为强化学习是我们目前的研究重点，所以我们需要利用 **OpenAI Gym** 的框架进行训练。



首先强化学习中的Agent对应于网络空间中的 进攻方/防守方 ， 他们执行一些操作和环境交互，从而得到奖励和观察。



参考上图，我们需要的Gym接口来支持我们进行训练，因此对于每个靶场中的智能体来说，需要支持以下几个函数：

- action_space 表示智能体的动作空间，表示智能体可以支持的操作的集合。
  - e.g. 比如一般智能体的动作空间可以包含（nmap id:xxx ， ping id: xxx 之类的）
- state 表示智能体的当前状态，某种意义上来说，state是对observation的一次采样，每次step我们就能从observation中得到当前的state
  - e.g 比如智能体的状态代表着 目前 那些节点被攻占，那些节点的地址是已知的，那些漏洞可以被利用，那些动作不可以执行

总之，我们需要网络靶场提供Gym框架的接口，方便智能体进行训练。 具体可参考上面提供的框架

> https://github.com/tkn-tub/ns3-gym 可以参考一个网络模拟器和Gym的结合

3. 可视化的需求:

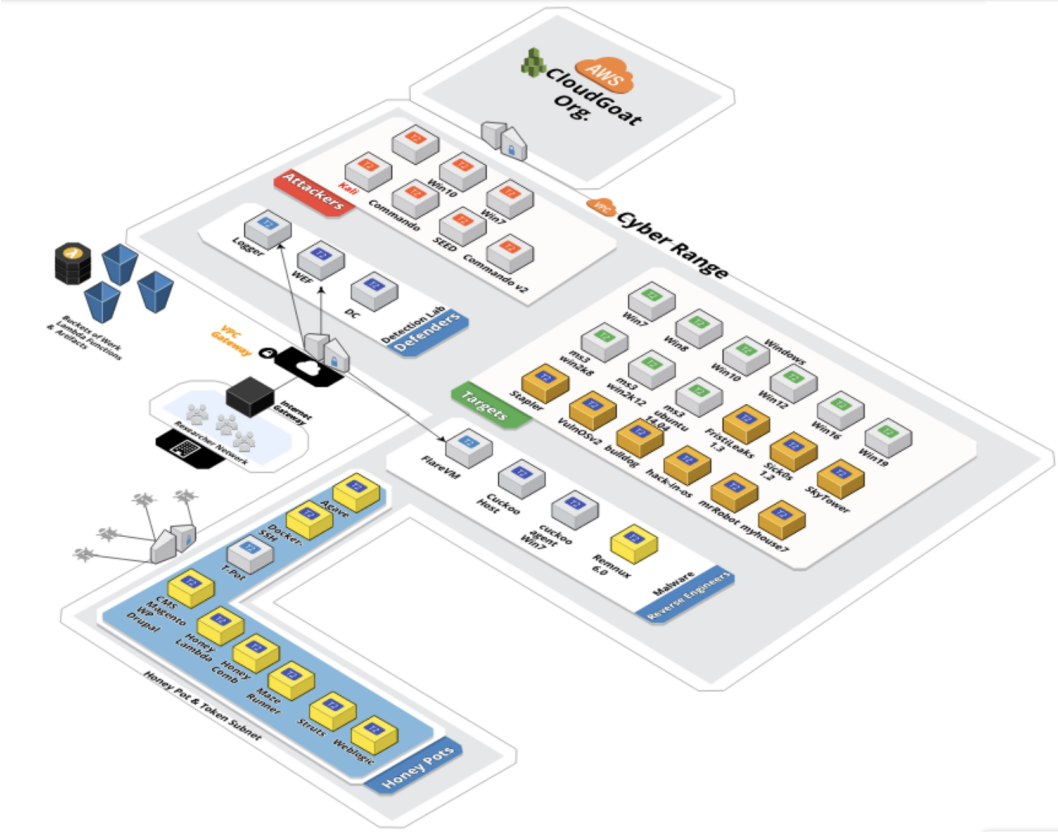
可视化的靶场环境可以帮助客户更好的更直观的了解网络资产的数目以及配置。同时加之动态化的展示可以帮助研究人员了解训练的过程。具体需要做到一下几点:

- 网络展示
  - 主机
  - 子网
  - 放火墙/蜜罐 (防守系统)
  - 其他

- 行为的动态展示

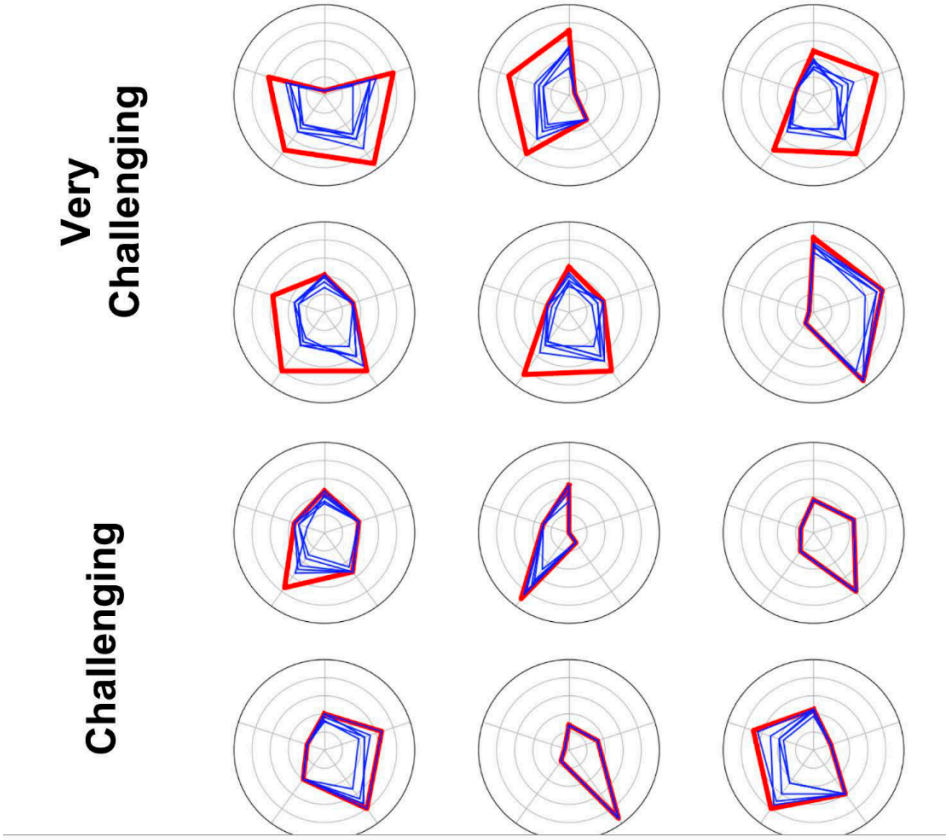
  应该可以高亮现实以下内容

  - 攻击/防守 的路径
  - 攻击/防守 的对象
  - 攻击/防守 所使用的工具
  - 正常用户的操作/流量（如果可行的话）
- 可交互 （如果可行的话）
  - 点击子网/节点 可以展示其配置
  - 点解某些高亮的操作可以展示其具体的操作以及对象

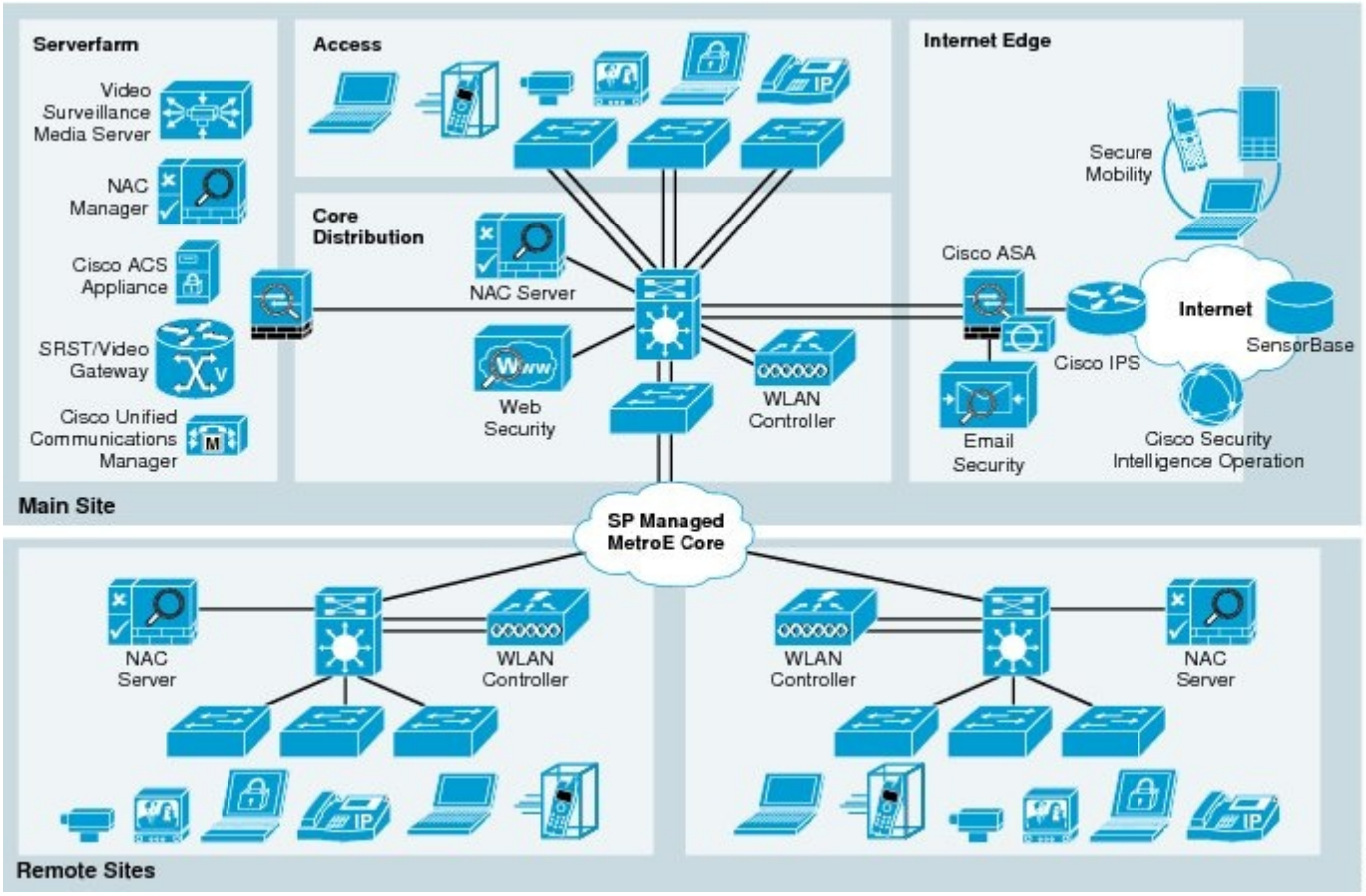


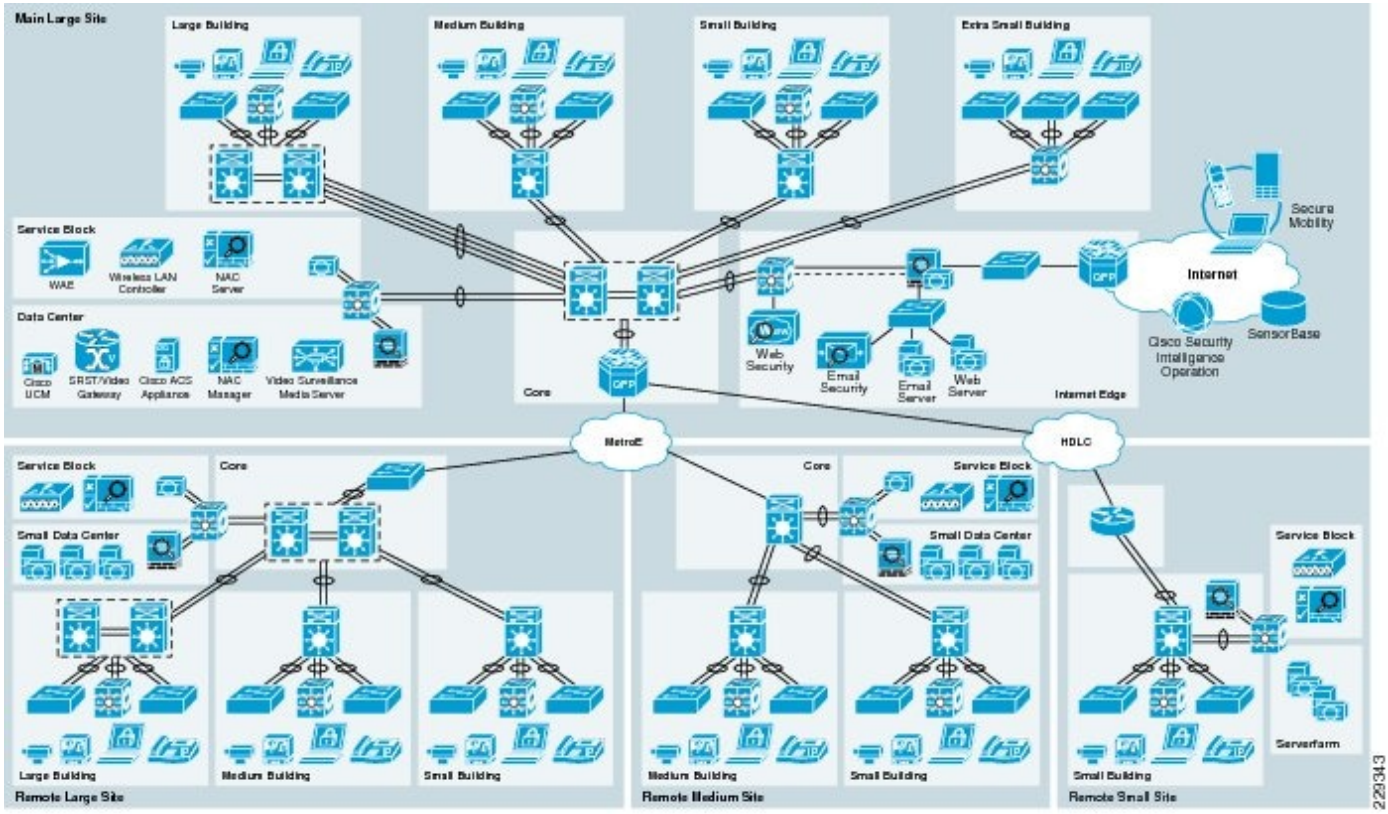
4. 可配置 (以训练攻防为例)

作为本研究的特色之一，我们需要更多的环境支持训练。所以我们希望的我们的靶场可以灵活自由的根据不同的配置生成不同模拟。这里我们定义一些难度指标，比如 **节点的数量，子网的数量，目标节点的数量(optional), 渗透的层数，防御的等级，漏洞的多少** 。



不同的难度指标代表着雷达图的不同的维度，通过挑战不同难度指标，我们可以控制总体的环境渗透难度。同时对于防守方来说，也可以设计另外一套不同的难度指标。**总之，需要做到仅改变少数网络参数即可生成新的靶场环境。**





举例说明比如上图对应的就是一个简单的网络，对应于:

- 节点数：20

- 子网数：5
- 渗透级数：2
- 防护等级：弱
- 目标节点数：1
- 漏洞数：100

通过改变参数为：

- 节点数：100
- 子网数：20
- 渗透级数：4
- 防护等级：中
- 目标节点数：3
- 漏洞数：1000

我们可以将网络靶场变为下图的靶场，提升了渗透的难度。