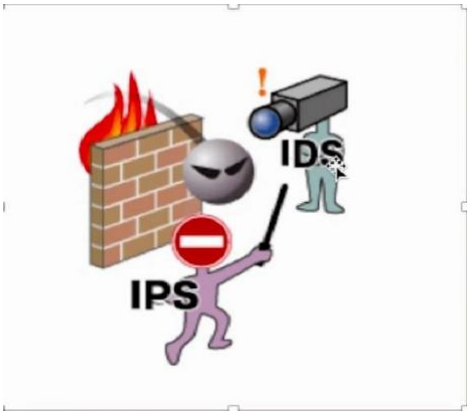
IDS 与 IPS

DS 与 IPS 异同点

IDS:入侵检测系统(IDS)是一种通过实时监控网络流量来定位和识别恶意流量的软件。在网中，IDS 所处的位置是一个非常关键的设计因素，IDS 一般会部署在防火墙之后当攻击发生时系统只能发出警报，它并不能防止攻击的发生。

而入侵防御系统(IPS)却能有效地组织攻击行为的发生，因为所有的网络流量在达到目标服务都需要流经 IPS。所以在没有得到允许的情况下，恶意软件是无法触及服务器的。

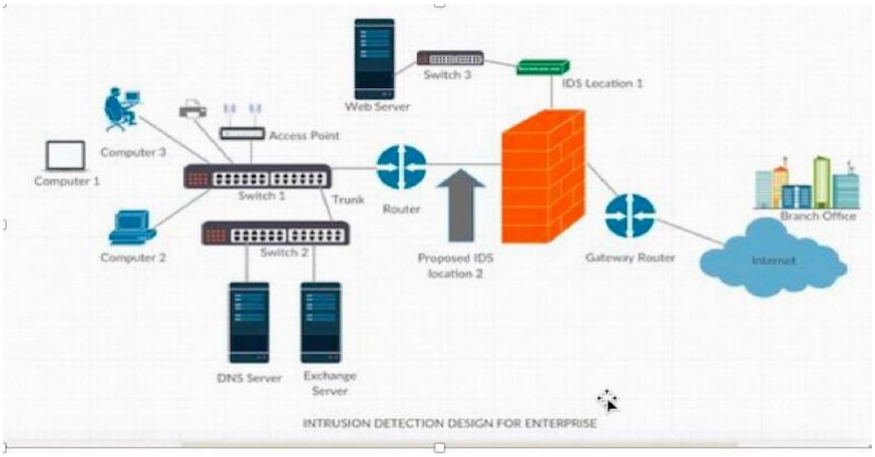


■ 流量收集

1)基于主机的 IDS/IPS:【HIDS】大规模部署麻烦；信任。
2)基于网络流量的 IDS/IPS【NIDS】
3)基于路由器的 IDS/IPS:收集路由器流量
4)基于防火墙的 IDS/IPS:收集防火墙流量
5)基于云环境下的 IDS/IPS 实现： 云 IDS
6)针对智能物联网设备的 IDS/IPS:
7)使用机器学习算法实现入侵检测

第一种：签名；
第二种：基于特征，特征码。判断准，缺点：误报比较高，效率下降
第三种：异常行为， 【基线判断】,>10 次/次。能发现未知恶意代码，

■ 旁路部署(也可以串联，但少)



■ BS 或者 CS 模式

■ 分析数据