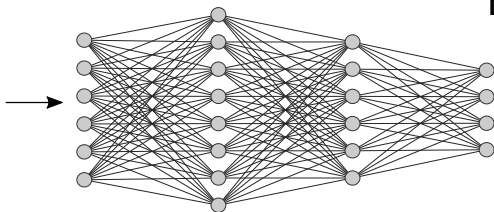


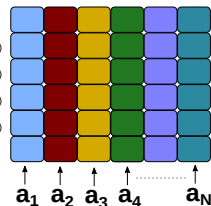
# Deep-TROJ Attack at Inference



Input



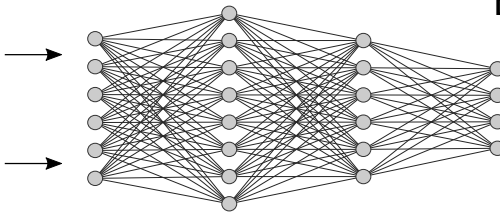
DNN Weight blocks



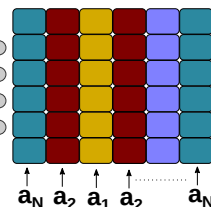
Dog



Input



DNN Weight blocks



Dog



Cat



Triggered Input



Attacker