Blocking

Snort

Intrusion detection system (IDS)

Rule based

Rules can alert, log, pass, **drop**, or **reject**

TCP Reset

Man in the middle

Send TCP RST message to each end of connection

Connection is stopped

TCP Reset

Put a diagram here

Problems with Snort

Snort was too slow!

IP addresses are not human friendly

Whitelist

Whitelist creation

Host name → IP address

Demo