Application-Level Gateway = Application proxy
- relay for application traffic
- uses TCP/IP authentication
- Each app has a proxy code
- more secure than packet filters

Circuit Level Gateway
- SOCKS
  - RFC1928
  - uses TCP UDP to conveniently use a network firewall
  - Server decides if client can connect

Bastion hosts
- Critical to network security
- works with either application-level or circuit-level gateways
- runs only essential services
- each prox can restrict features, hosts accessed
- proxies are small, simple, and non-privileged
- read-only code

Intrusion Prevention System
- extension of IDS can attempt to block or prevent malicious activity
- can be host, network, or distributed
- can use anomaly detection and signature detection

HIPS
- host-based
- can use signature or anomaly detection
  - signature checks already known malware
  - anomaly checks behavior that indicated malware
  - can detect modification or system resources, privilege exploits, buffer overflows, directory traversal
  - can use a sand-box

NIPS
- uses signature and anomaly detection
- network-based
- filters packet by packet

Snort Inline
- tool kit to modify packets instead of drop them
- useful for honeypots
- attackers can’t figure out why the attack fails