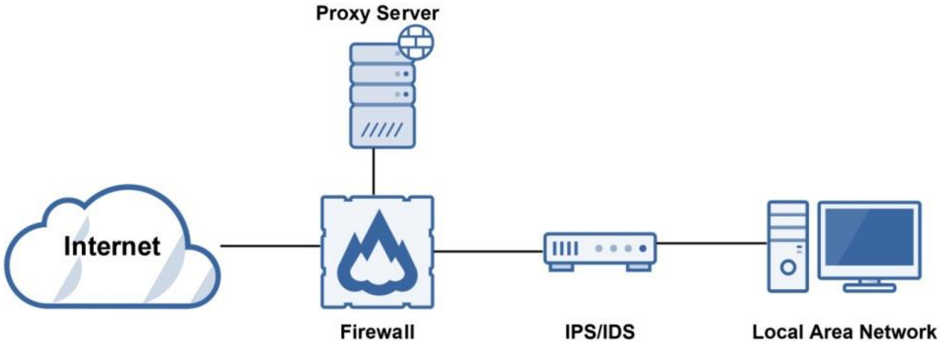
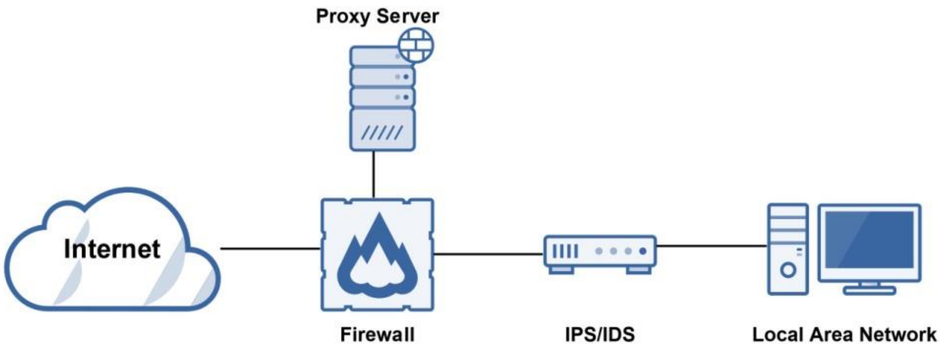
Intrusion Detection & Prevention Systems (IDS/IPS)

- Are designed to detect attacks on a network and respond passively or actively.
- Take a different approach than firewalls
- Basic firewalls will try to block network attacks using ACLs (rules), while IDS/IPS try to detect the attacks.



Intrusion Detection & Prevention Systems (IDS/IPS)

- An Intrusion Detection System (IDS) is **Passive**, meaning it’s response is logging and notifying.
- An Intrusion Prevention System (IPS) is **Active**, meaning it’ll change the network environment to stop an attack, such as changing ACLs or closing processes, sessions, or ports.


Proxy Server
Internet
Firewall
IPS/IDS
Local Area Network