Restricting Server Access with Squid

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe the criteria that can be used to filter traffic with the squid proxy server.
2. Configure access control lists in squid to restrict access.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Restricting Server Access with Squid
  - Access control types
  - Defining an ACL
  - Time-based restrictions
- Access control types
  - Domain name
    - `dstdomain`
  - IP Address
    - `src` / `dst`
  - Time
    - `time`
  - Full list
    - https://wiki.squid-cache.org/SquidFaq/SquidAcl
- Defining an ACL
  - Creating a list
    - `acl <name> <type> <values>`
  - Defining an action
    - `http_access <allow/deny> <list>`
    - Default action
      - Opposite of the last line
      - If the last line is an allow, the default is deny
      - Use `http_access allow all` to explicitly define
  - Example
    - `acl internal src 10.0.0.0/255.0.0.0`
    - `acl streaming dstdomain www.tiktok.com www.youtube.com`
    - `http_access deny streaming`
    - `http_access allow internal`
    - `http_access deny all`
- Time-based restrictions
  - http_access entries use **AND** not **OR**
  - Example
    - `acl streaming dstdomain www.tiktok.com www.youtube.com`
    - `acl workday MTWHF 08:00-17:00`
    - `http_access deny streaming workday`
    - `http_access allow all`