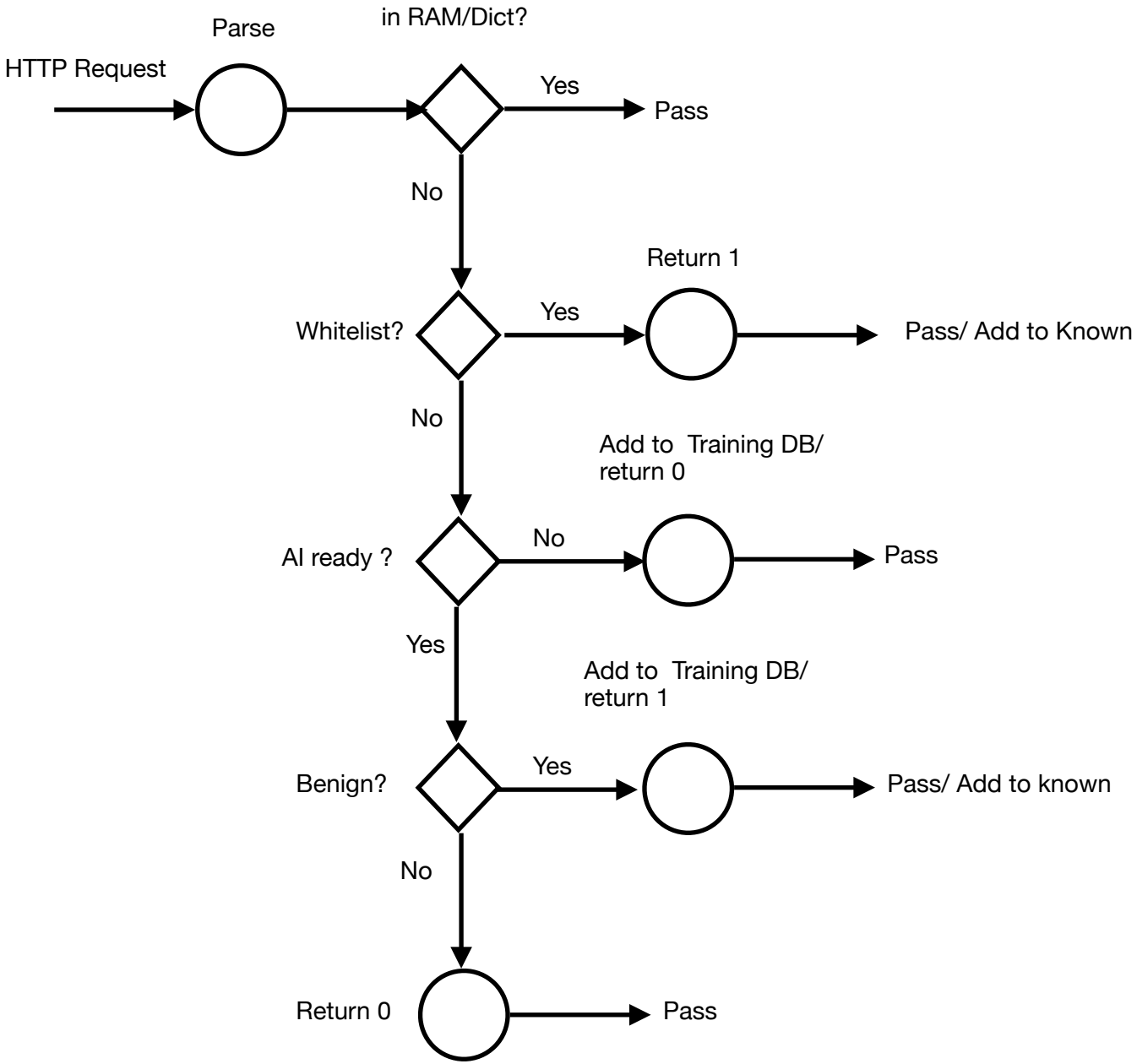
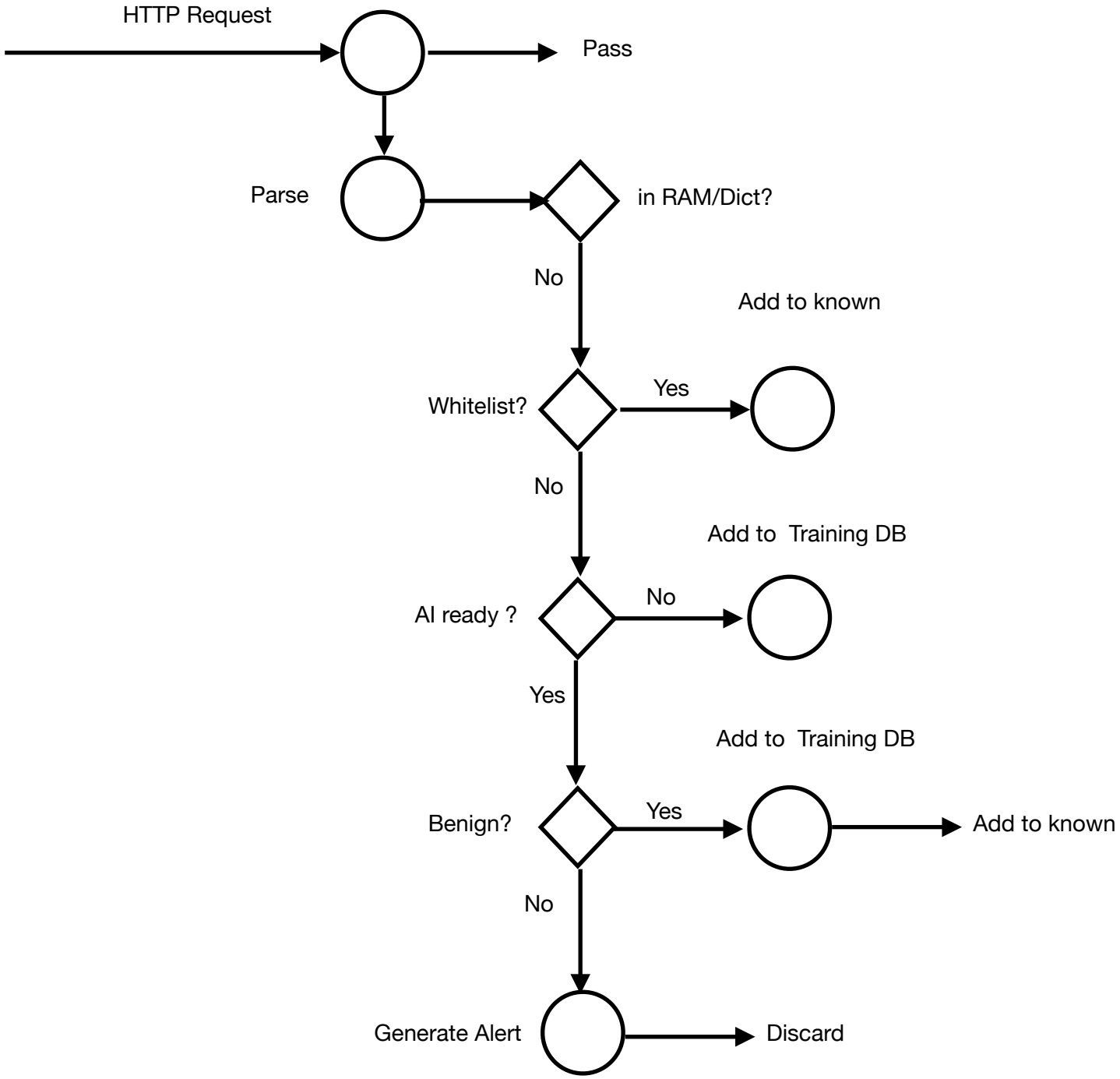
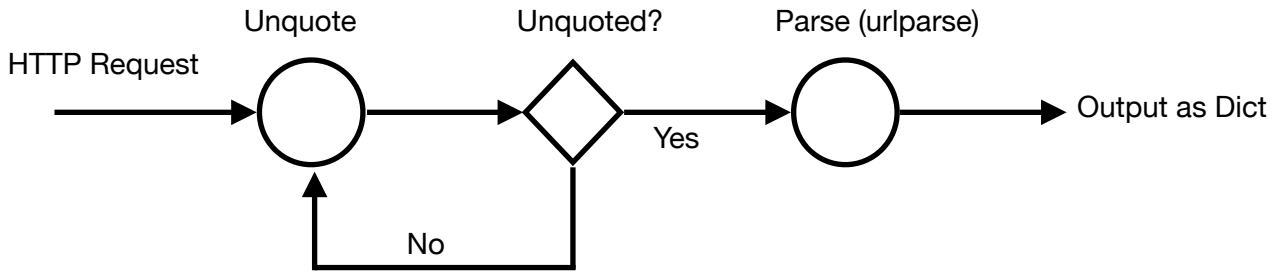
HTTP Request Flow Alternate 1



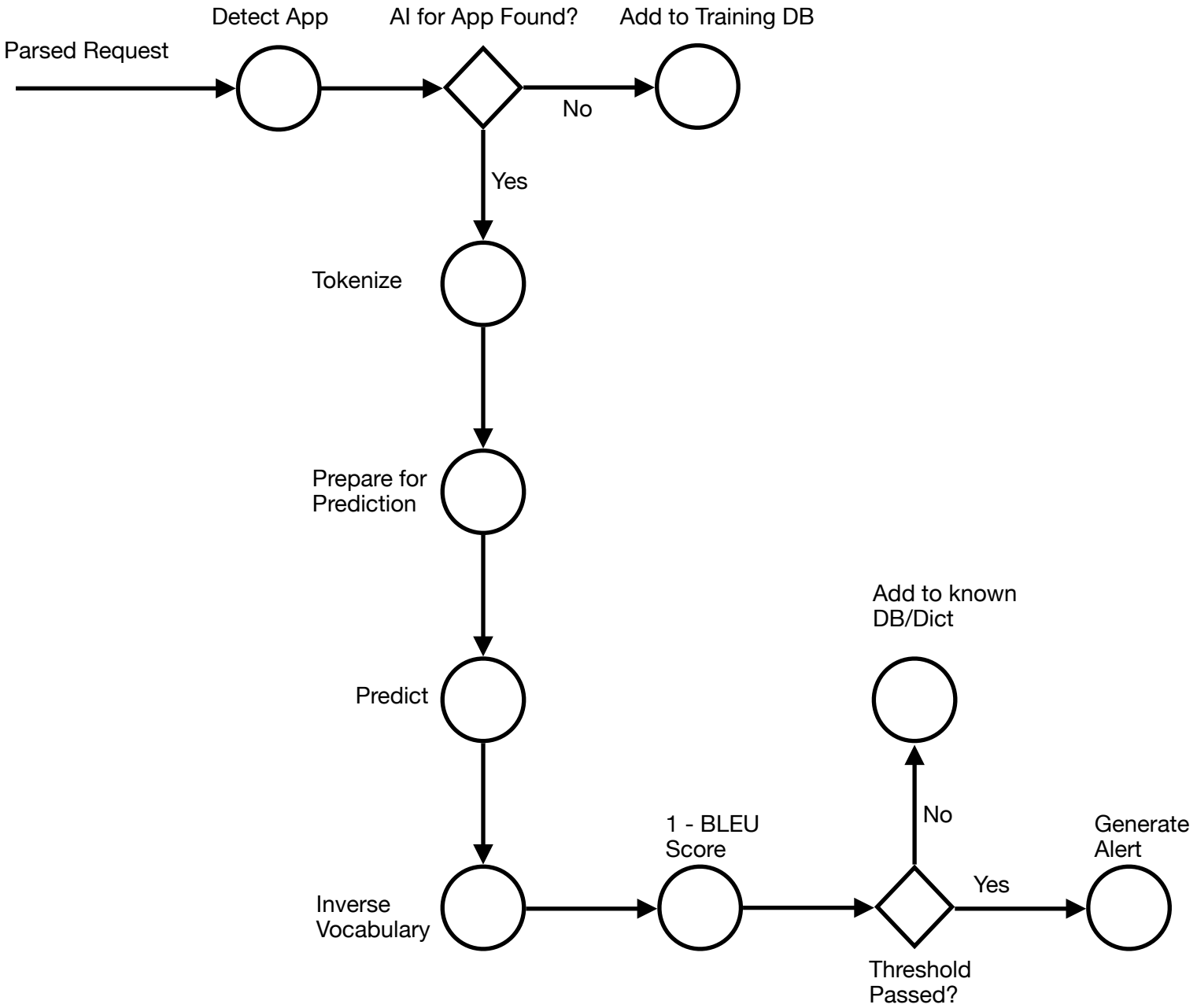
HTTP Request Flow Alternate 2

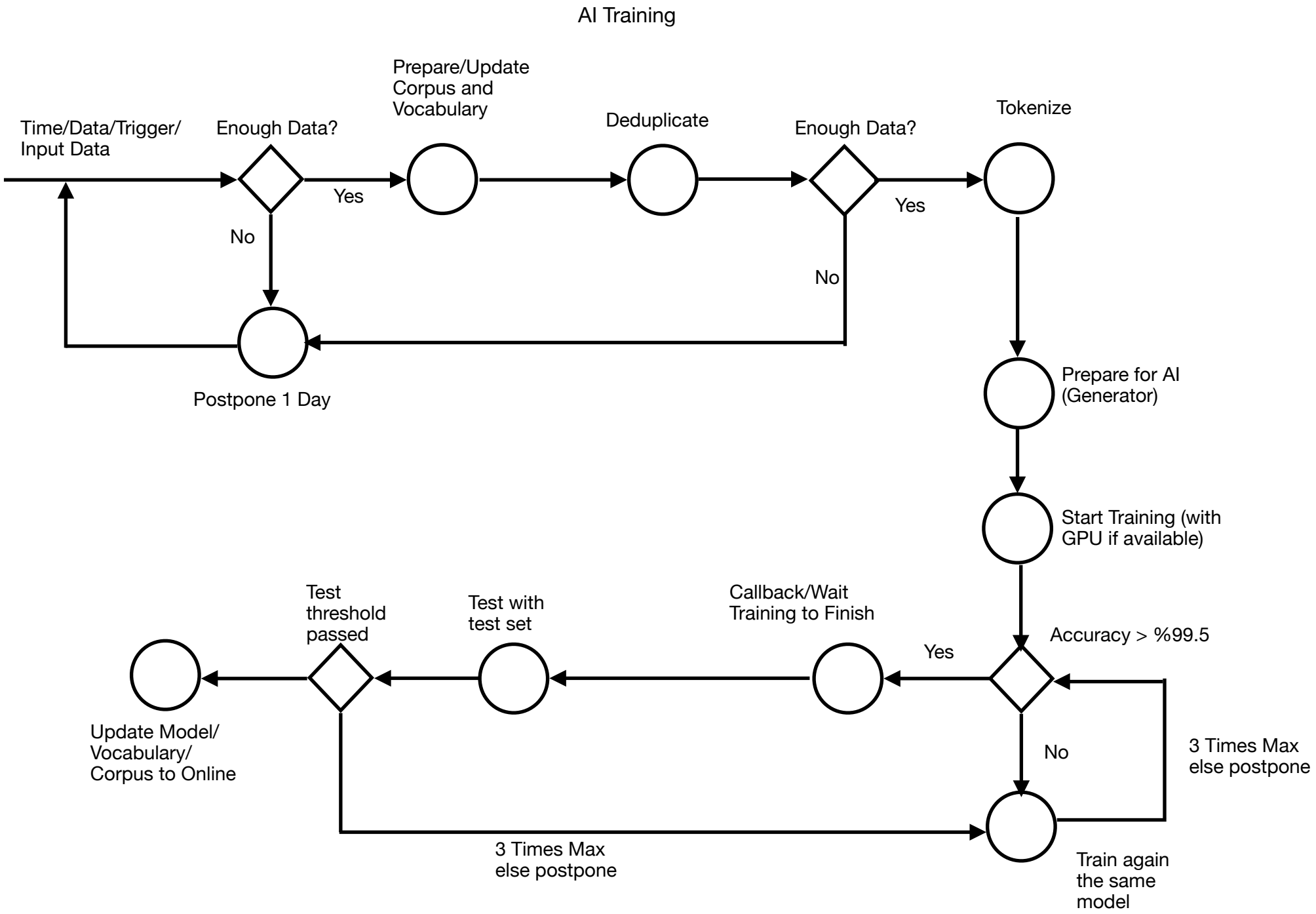


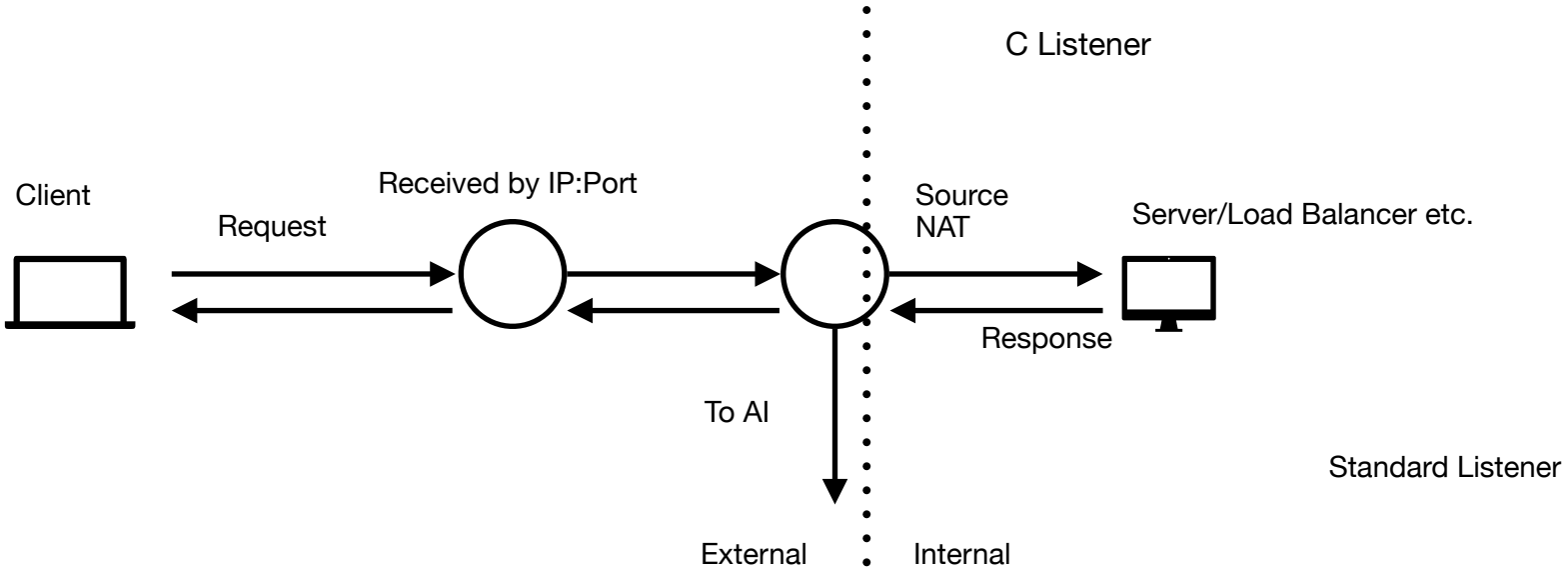
Request Parse

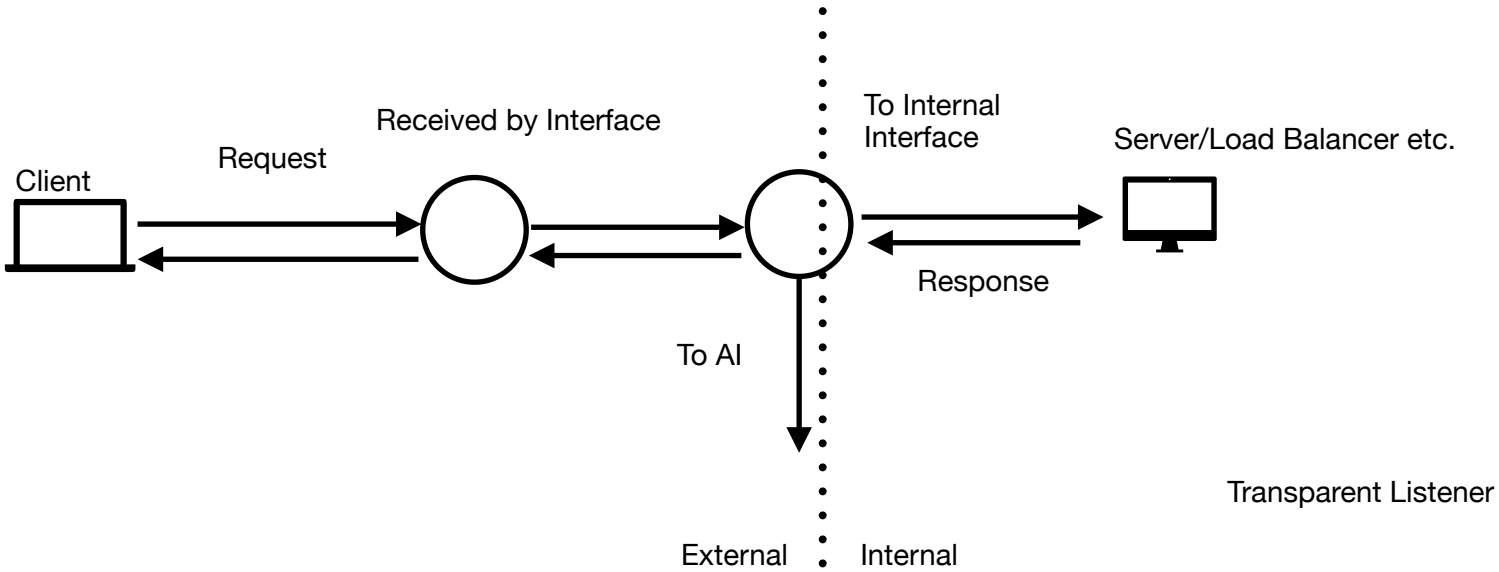


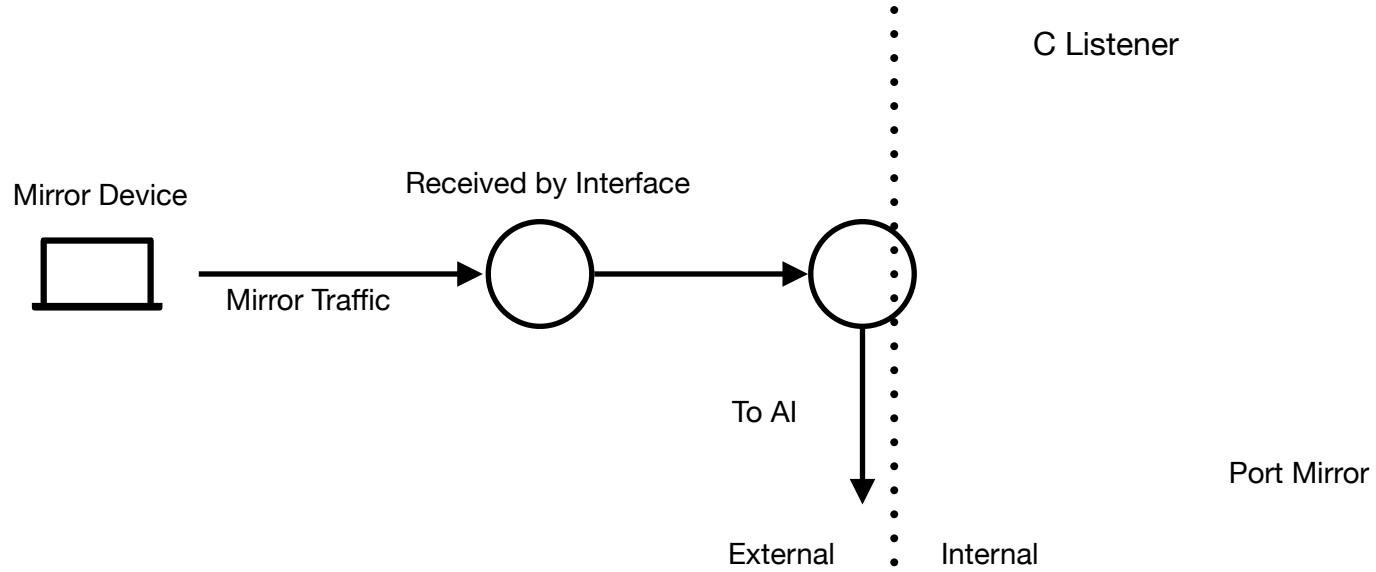
AI Prediction

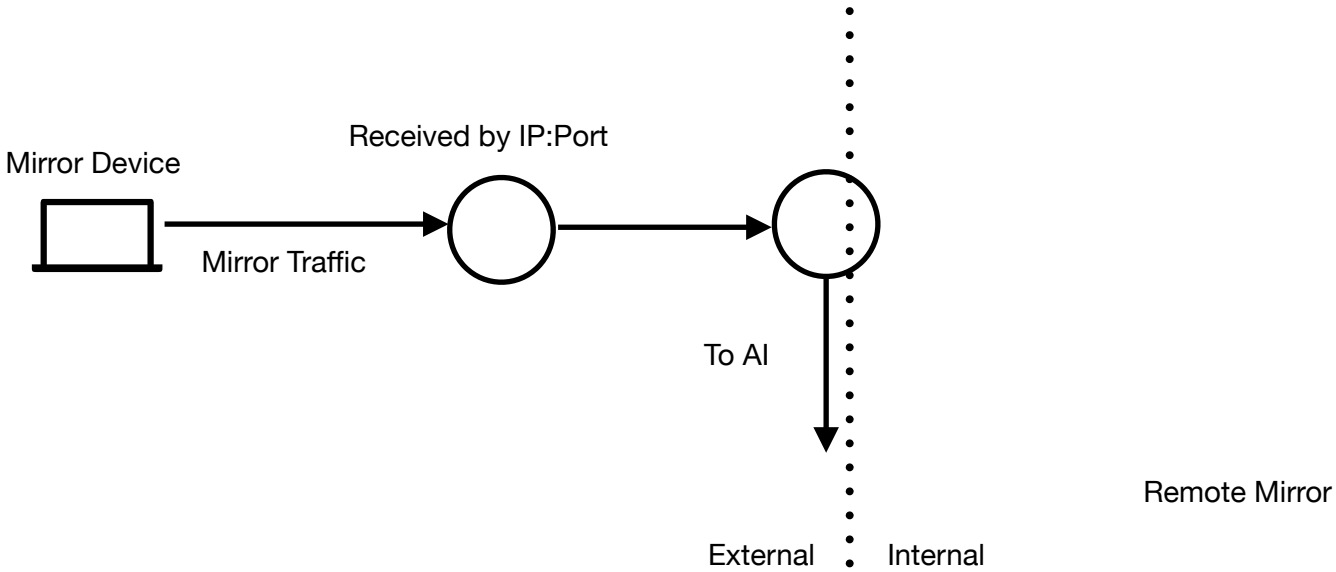



AI Training
Time/Data/Trigger/
Input Data
Enough Data?
Yes
No
Prepare/Update
Corpus and
Vocabulary
Deduplicate
Enough Data?
Yes
No
Tokenize
Postpone 1 Day
Prepare for AI
(Generator)
Start Training (with
GPU if available)
Accuracy > %99.5
Yes
No
3 Times Max
else postpone
Callback/Wait
Training to Finish
Test with
test set
Test
threshold
passed
Update Model/
Vocabulary/
Corpus to Online
3 Times Max
else postpone
Train again
the same
model


C Listener
Client
Request
Received by IP:Port
Source
NAT
Server/Load Balancer etc.
Response
To AI
Standard Listener
External
Internal


Received by Interface
To Internal
Interface
Server/Load Balancer etc.
Request
Client
Response
To AI
Transparent Listener
External
Internal


C Listener
Mirror Device
Received by Interface
Mirror Traffic
To AI
Port Mirror
External
Internal


Received by IP:Port
Mirror Device
Mirror Traffic
To AI
Remote Mirror
External
Internal

Server Configurations

Mgmt Port

- IP Address (x.x.x.x/x)
- VLAN (ex: 10)

Interfaces

- Enable/Disable (Disabled by default)
- Mode (Access/Trunk)

VLANs

- Name (xxxxx)
- ID (ex: 10)
- Interface (1 for access interface, Can be multiple for Trunk)

IP Addresses

- IP Address (x.x.x.x)
- Netmask (x.x.x.x)
- VLAN (ex: 20)

Listener Configurations

Server

- External Part
    - Application Name: (ex: Alisa Application)
    - Mode: (Port Mirror/Remote Mirror/Transparent/Standard)
    - Interface: ethX (for Port Mirror/Transparent)
    - IP Address : x.x.x.x/x (for Remote Mirror/Standard)
    - Port: (ex: 8080) (for Remore Mirror/Standard)
    - Client IP: x.x.x.x/x
    - Destination Port: (ex : 80)
- Internal Part
    - Interface: ethX (for Transparent)
    - IP Address: x.x.x.x/x (for Standard)
    - Port: (ex: 8088) (for Standard)
    - SNAT: boolean yes/no (for Standard)

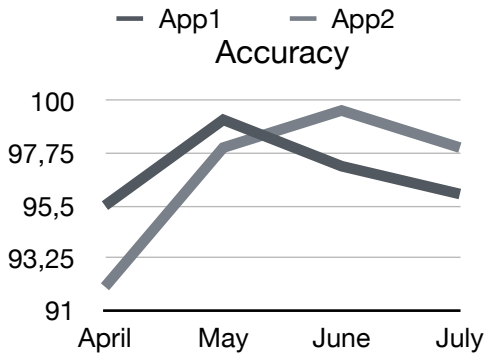
Alert Management

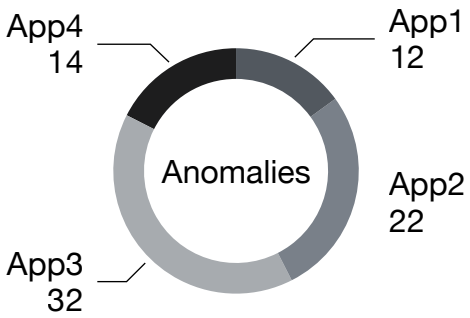
Date/Time	Application	Request	Anomaly Score	Source IP	Destination Port	Add to Whitelist
21.11.1983 08:50	Alisa Application	http://xxxxxxx/xxx/xx?xx=xx	0,568	195.175.44.33	80	Add

Whitelist Management

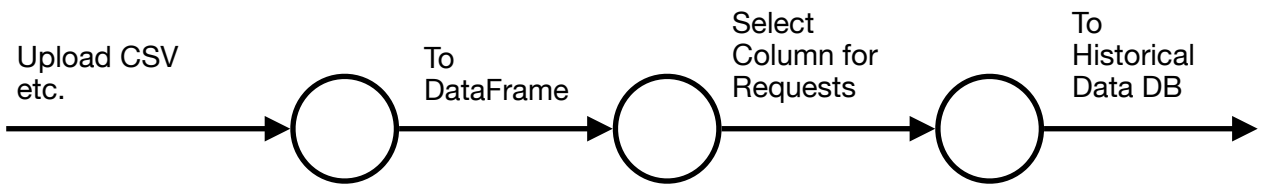
Added Time	Last Seen	Application	Request	Last Anomaly Score
21.11.1983 08:50	21.11.1983 08:50	Alisa Application	http://xxxxxxx/xxx/xx?xx=xx	0,568

AI Statistics





Historical Training Data



Files

base_conf - VLAN, IP, Interface, redundancy, management ip
db_conf - keys, passwords, ipaddresses for DB
x_conf - virtual ip, pool, mode, mirror ip
x-license - license

base_conf

Server configurations

db_conf
- ip_address
- dbuser
- dbpass
- dbport

alisa_license
- license:

alisa_conf {
- listener <name>
- Listener Configurations
- Creation Date
- Last Modified

DB Design

Applications Table

- Listener Configurations + ID

Training Data

- Requests + ID + Application ID

Known Benign

- Requests + ID + Application ID

Whitelist

- Requests + ID + Application ID + Score + Last Seen + Creation Date

Alerts

- Request + ID + Application ID + Date/Time + Score