

Whitelist-Based IoT Firewall for Mitigating Device Exploitation

IoT



The proliferation of IoT gives interconnectivity and automation of everyday objects that greatly increases productivity in various corners of life.

Security of IoT

Tight connectivity among IoT system

Easy spread among the IoT once one of the device is compromised.

Confined User Interface

Challenging to detect intrusions and recover from the malware softly

Limited Computing Power

Cannot run computationally intensive protocols to secure the communication or a vaccine program



IoT botnet

- Rapidly spreads among the IoT system in a worm-like fashion
- Exploits computing power and bandwidth of IoT for DDoS attack

Solution - Firewall Rules

- 01 MUD translation and Enforcement
- 02 Dynamic DNS Observation and whitelisting
- 03 Packet rate and Packet size limitation

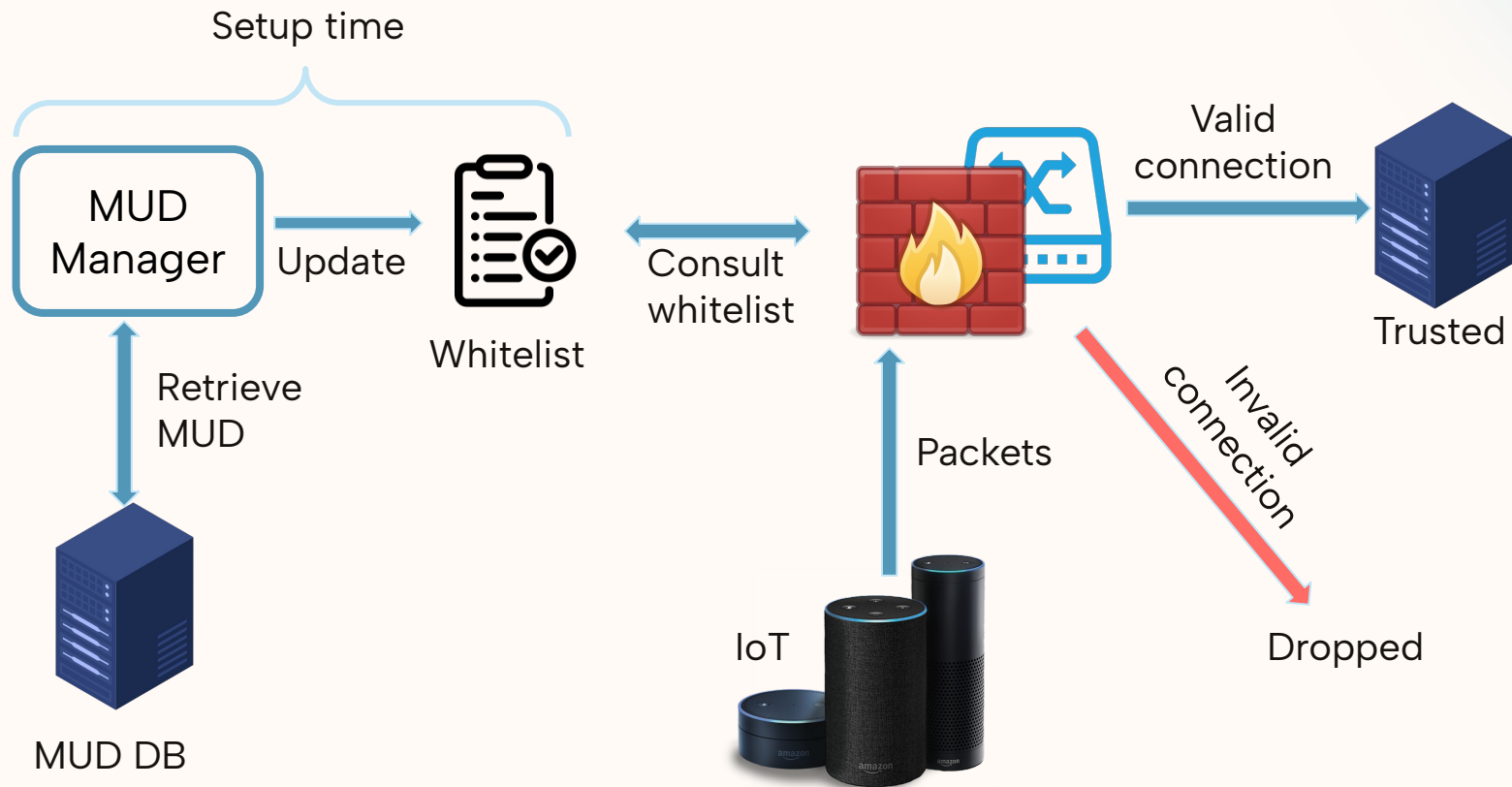
01 MUD (Manufacturer Usage Description)

- Embedded software standard for IoT Device makers to advertise device specifications
 - Intended communication patterns
 - Allowed URL / IP addresses
- Authoritative identifier and enforcer of policy for devices on the network
 - MUD is officially approved by IETF (Internet Engineering Task Force) as an Internet Standard, and Cisco is launching MUD1.0 to protect your IoT devices

```
{
  "name": "from-ipv4-amazonecho-0",
  "matches": {
    "ipv4": {
      "protocol": 6,
      "ietf-acldns:dst-dnsname": "dcape-na.amazon.com"
    },
    "tcp": {
      "destination-port": {
        "operator": "eq",
        "port": 443
      },
      "ietf-mud:direction-initiated": "from-device"
    }
  },
  "actions": {
    "forwarding": "accept"
  }
},
```

Amazon Echo's MUD file written in JSON format

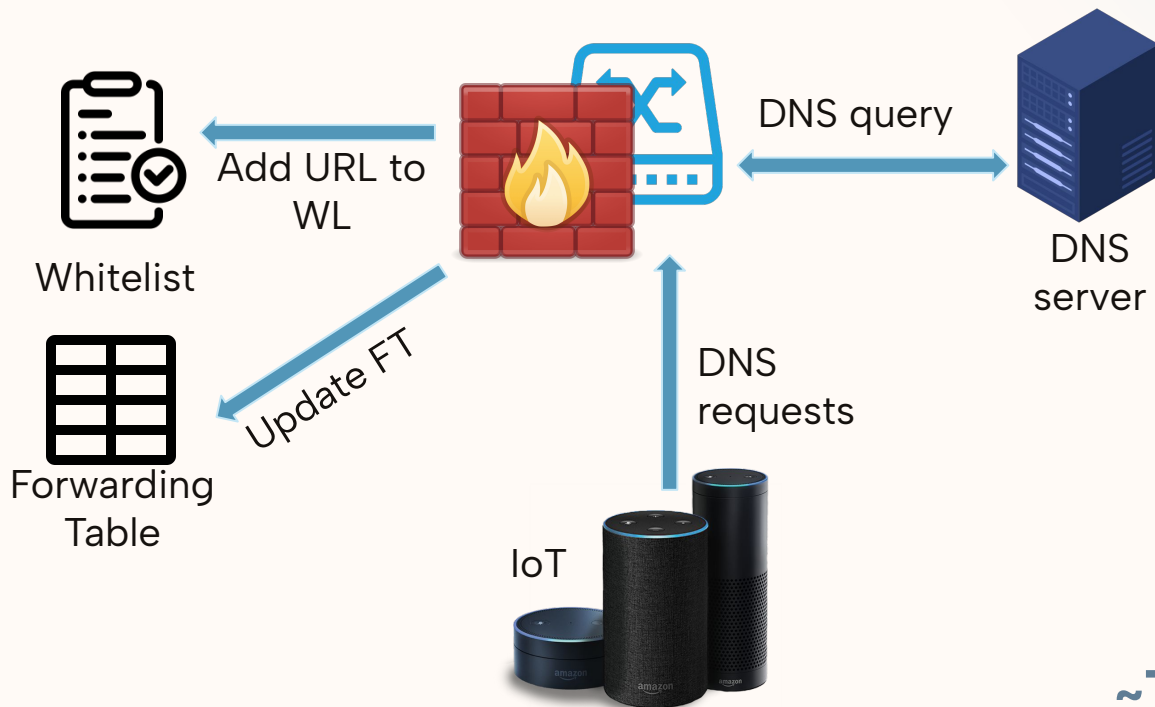
01 MUD-based Firewall Rules



02 Dynamic DNS Observation and Whitelisting

Whitelist build mechanism when MUD is not provided to IoT

Setup time
(Benign period)

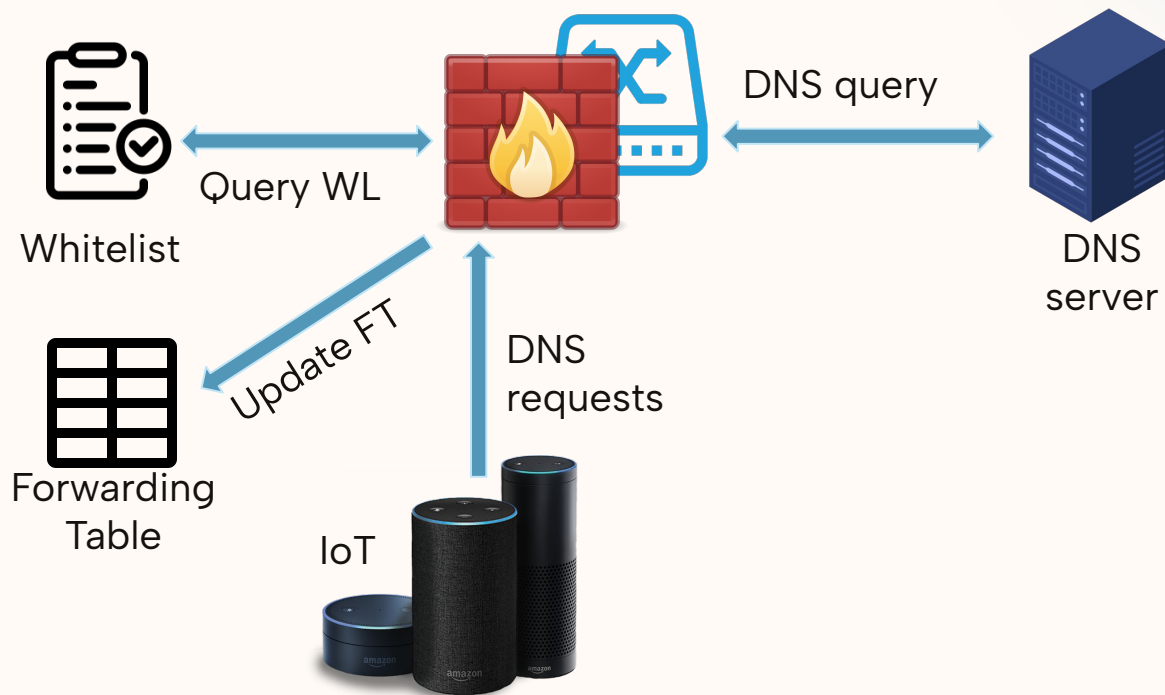


~10 sec

02 Dynamic DNS Observation and Whitelisting

IoT operation
time

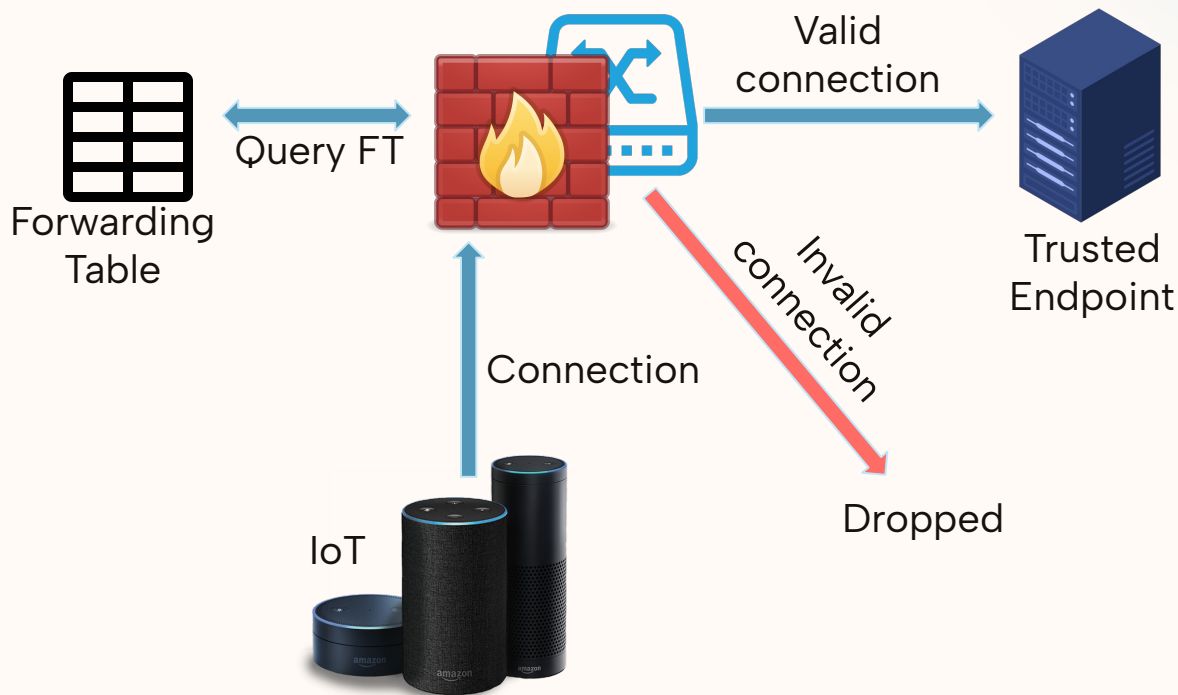
DNS Packets
(Update FT)



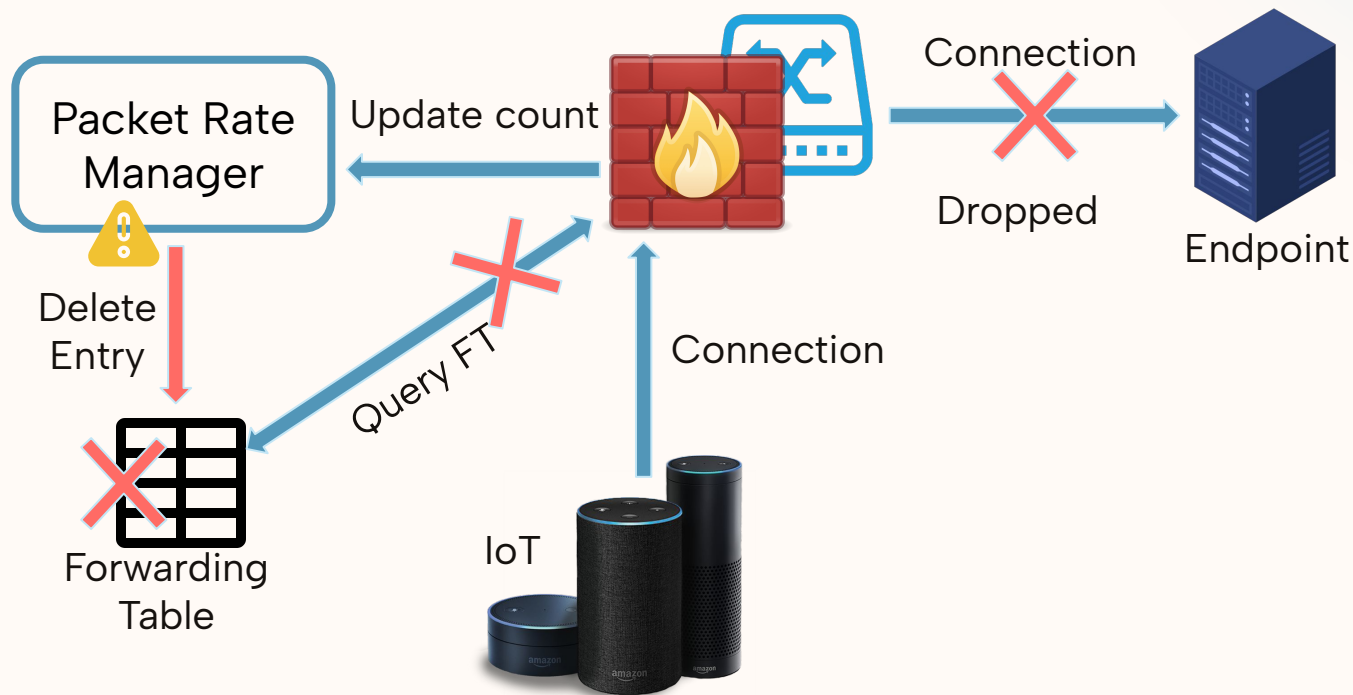
02 Dynamic DNS Observation and Whitelisting

IoT operation
time

Non-DNS Packets
(Normal Packets)



03 Packet Rate and Packet Size Limitation



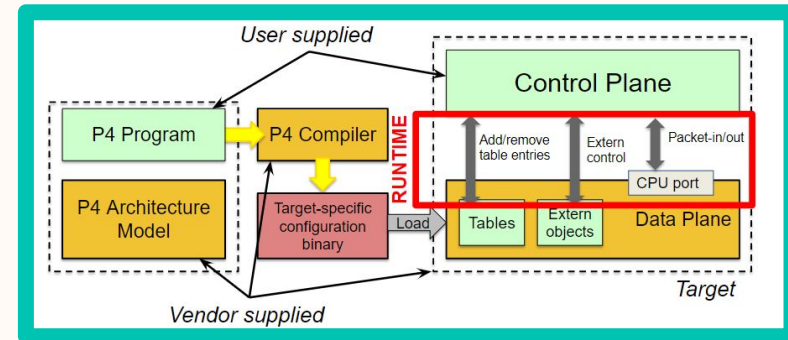
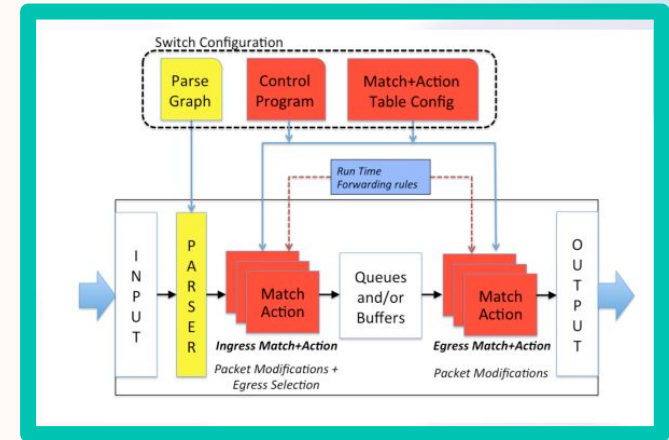


P4 is a language for **controlling packet forwarding planes** in networking devices such as routers and switches.

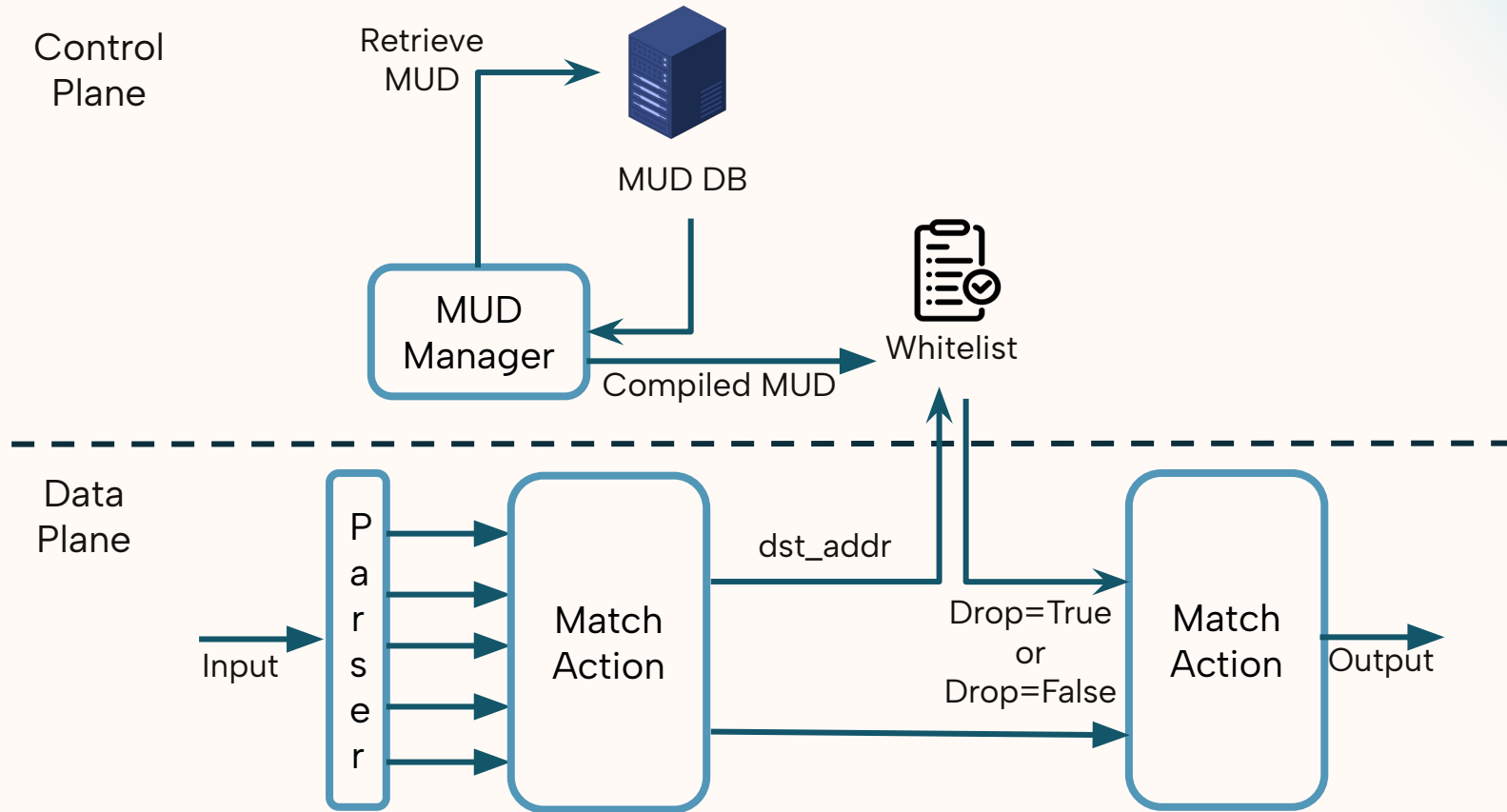
P4 implementation

P4 Programming Language

- **P4 Language:** Programmable language for network protocol control
 - Network Topology: Allows for the description of network layouts within P4 programs, hard-coded by json files or dynamically-generated by runtime
 - Ingress & Egress: Packet handling on entry and on exit to ensure protocol compliance
 - Parser & Deparser: Parses incoming packet structures for processing and reassembles them post-processing
 - Match-Action Tables: Core P4 construct for decision making; matches packets to actions based on headers, enabling dynamic rule application
- **P4 Runtime:** API to facilitate control plane interactions
 - Controller Programmability: Enables the modification of P4 match-action tables at runtime, providing real-time network adaptability.
 - API for Devices: Offers a standardized interface for managing various network device functions

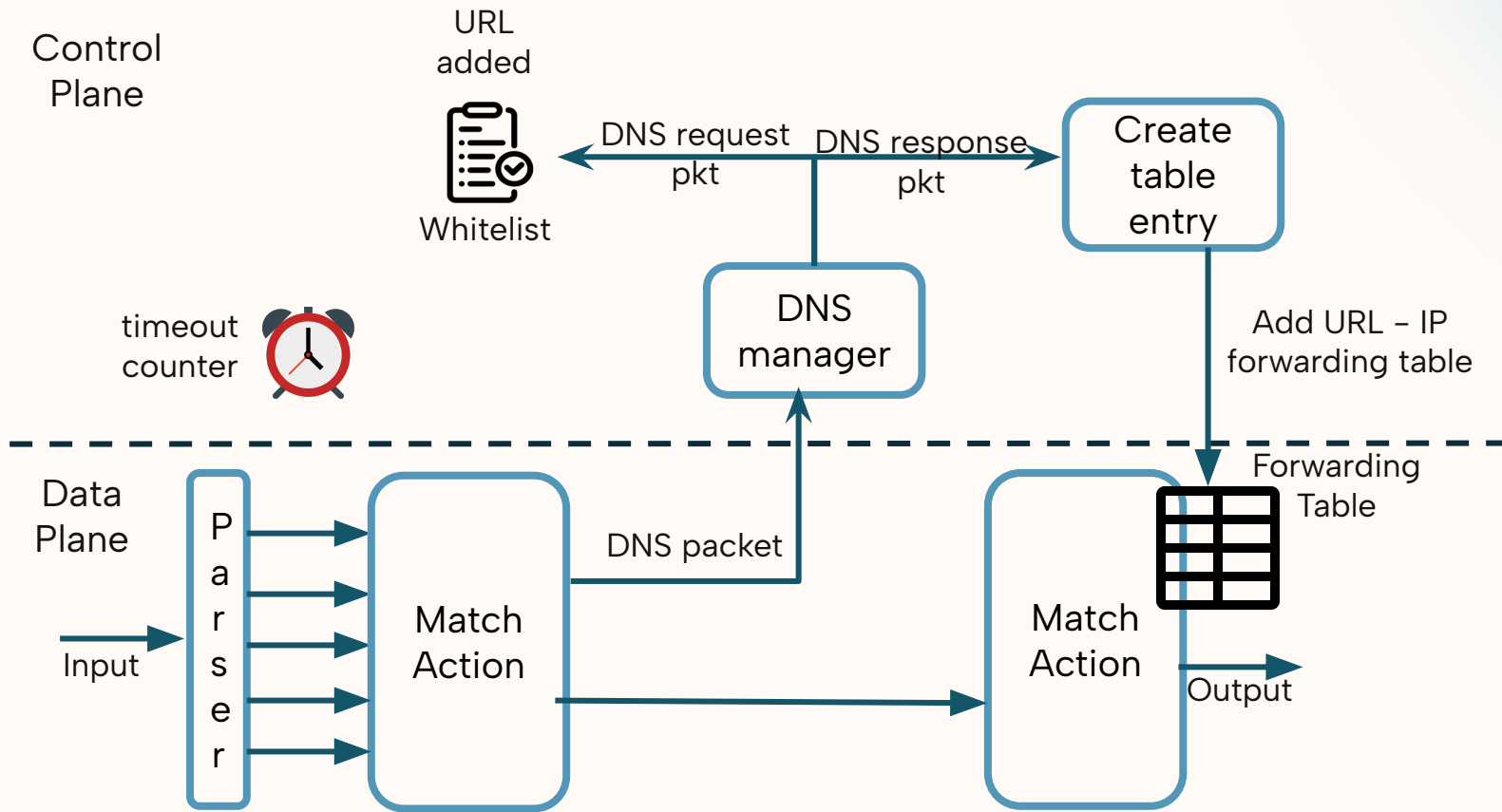


01 P4 Implementation of MUD based WL

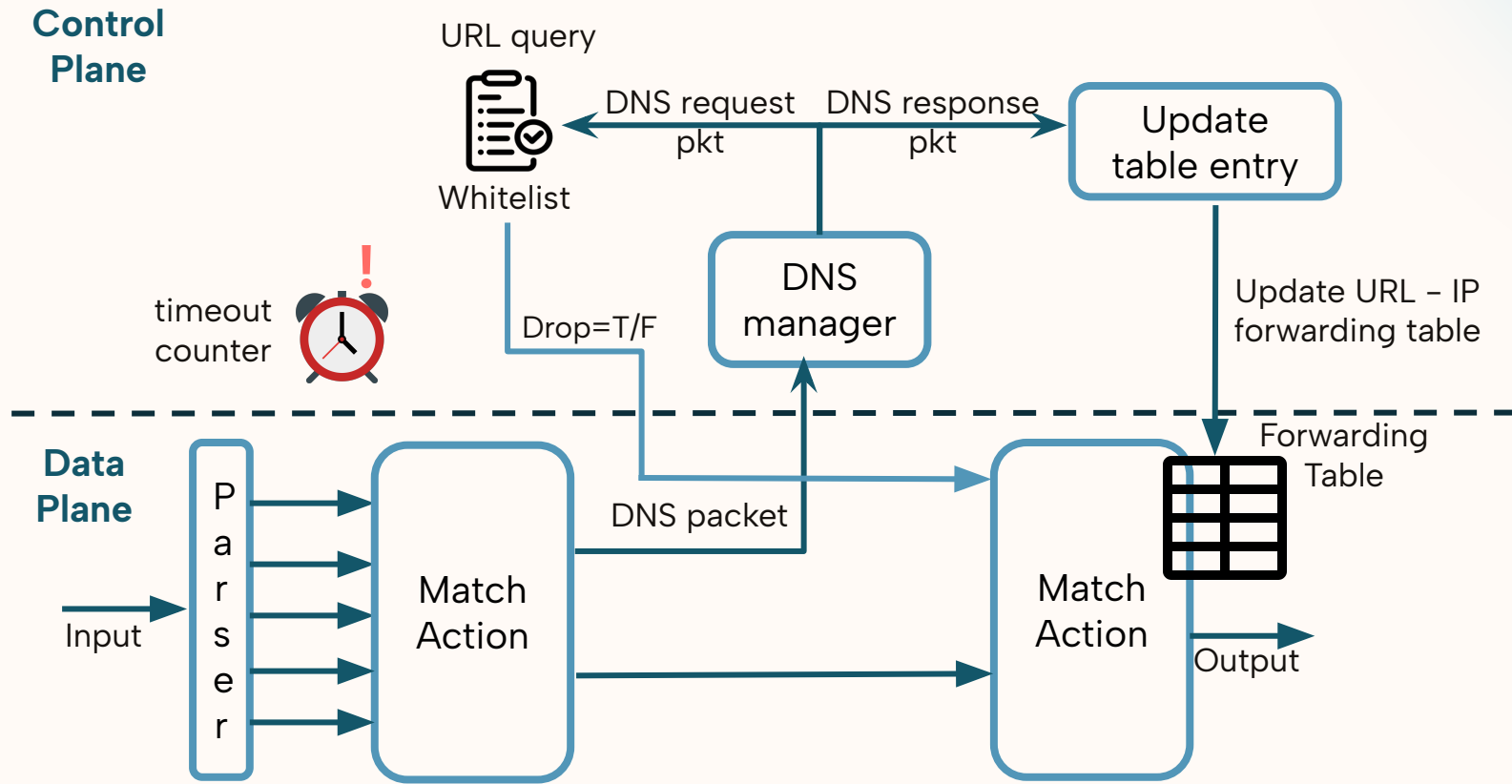


02 P4 Implementation of DNS based WL

Setup time
(Benign period)

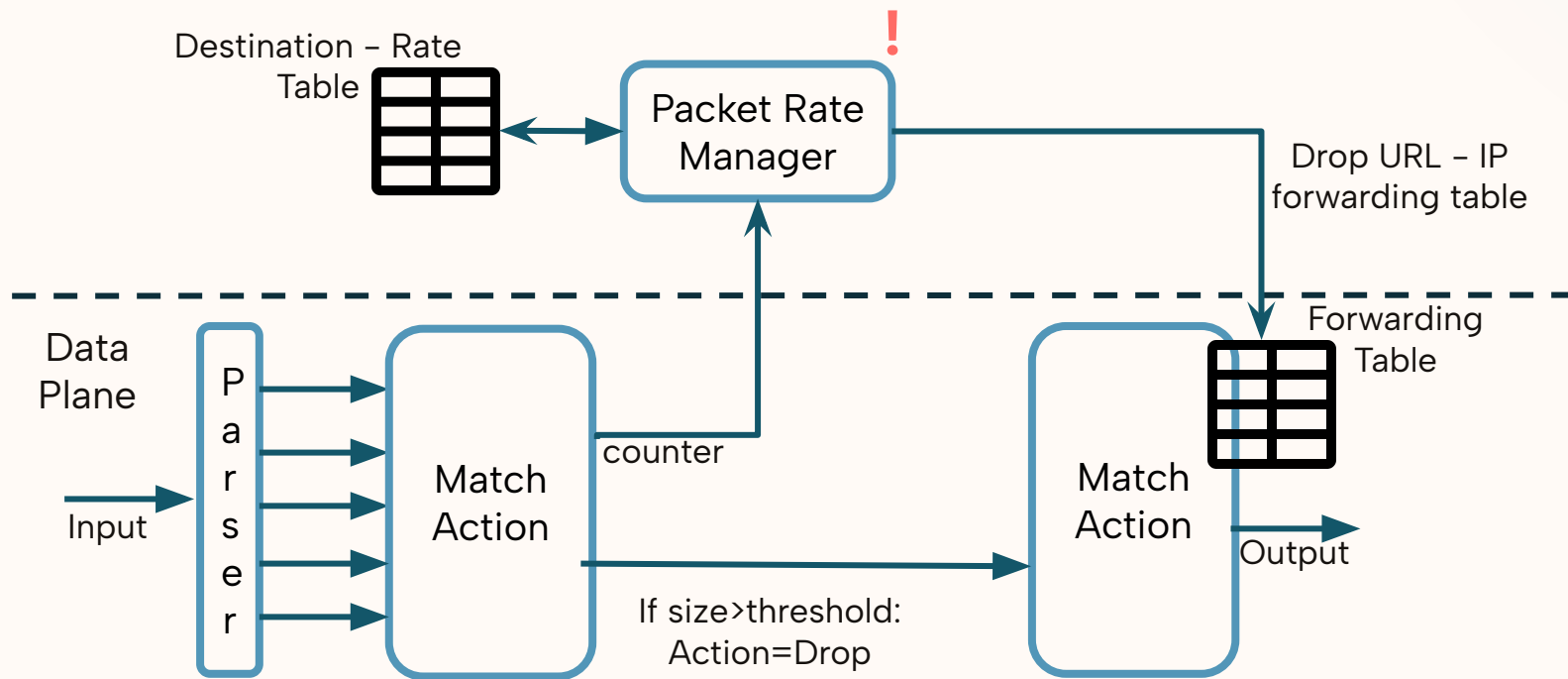


02 P4 Implementation of DNS based WL IoT Operation time

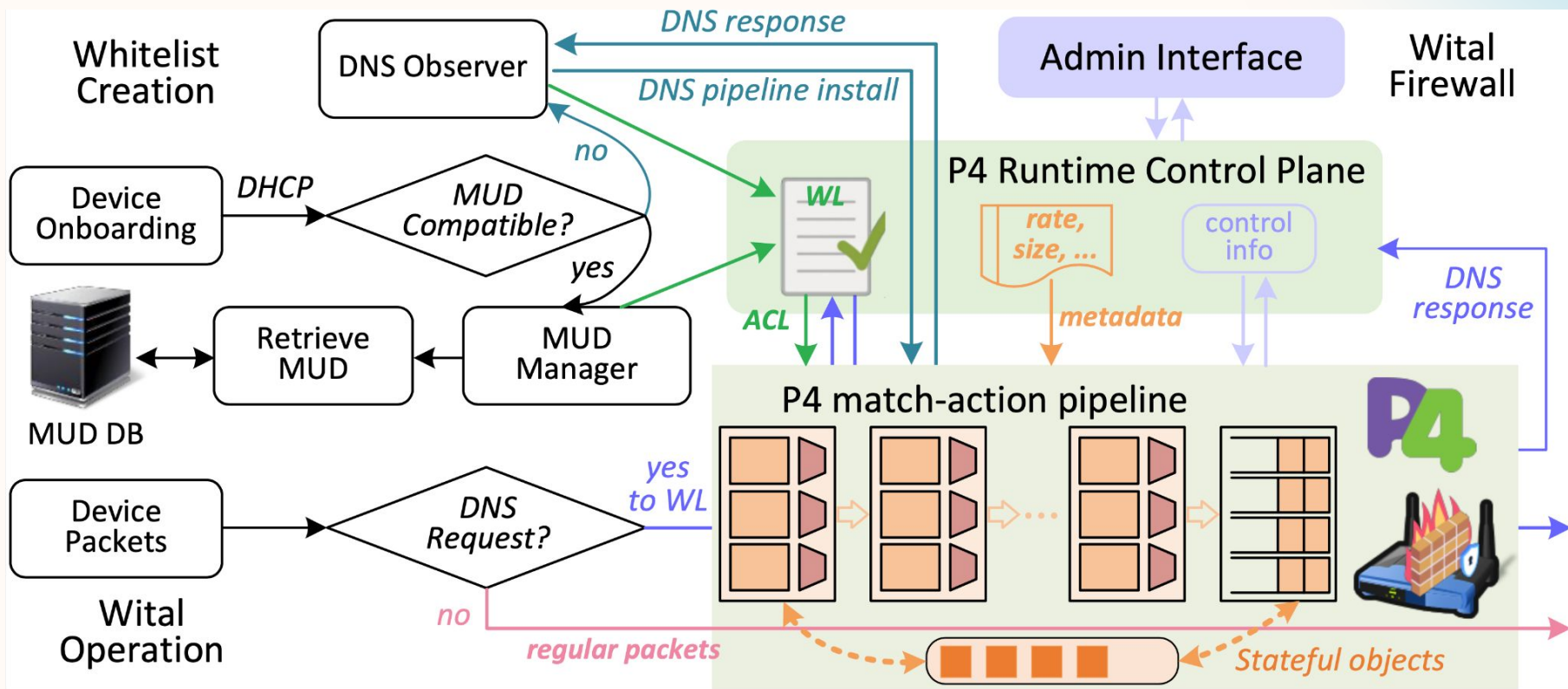


03 Packet Rate and Packet Size Limitation

Control
Plane

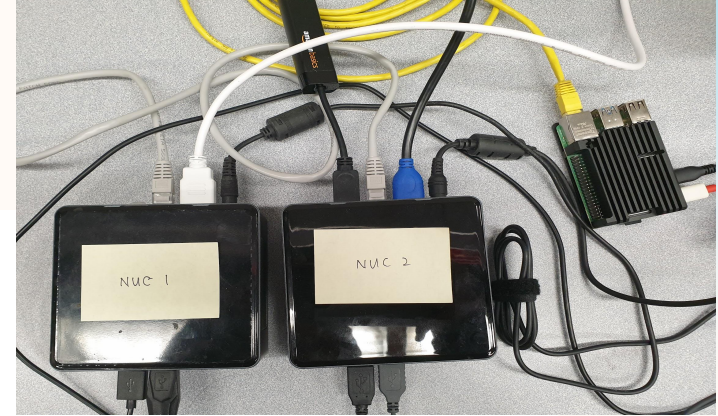
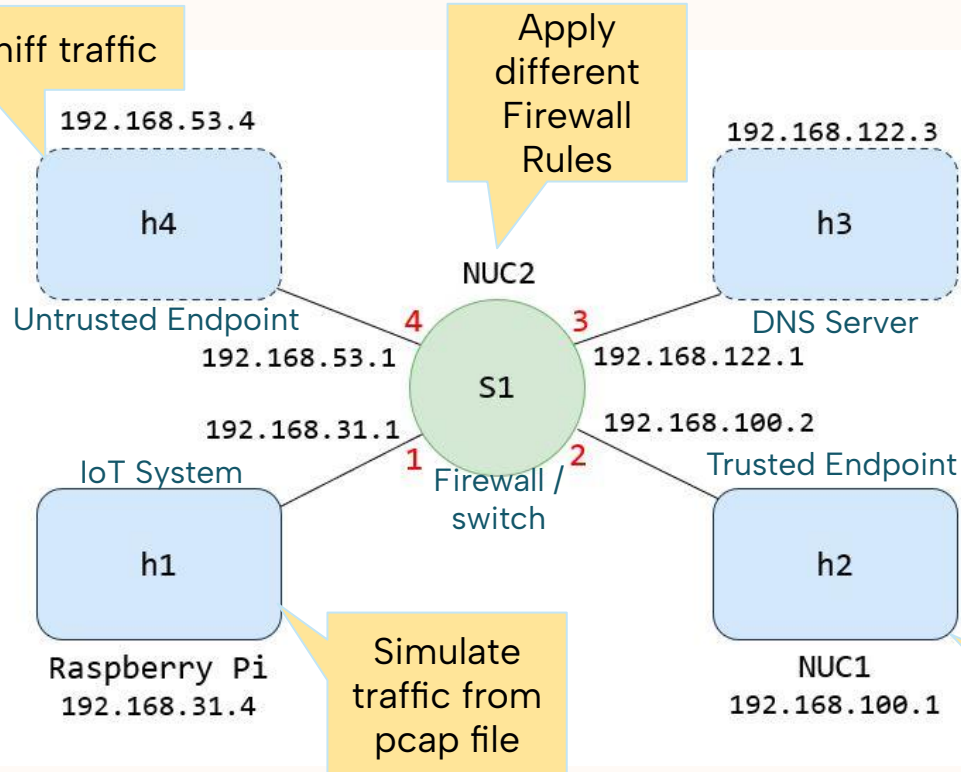


Overall Workflow



Testbed

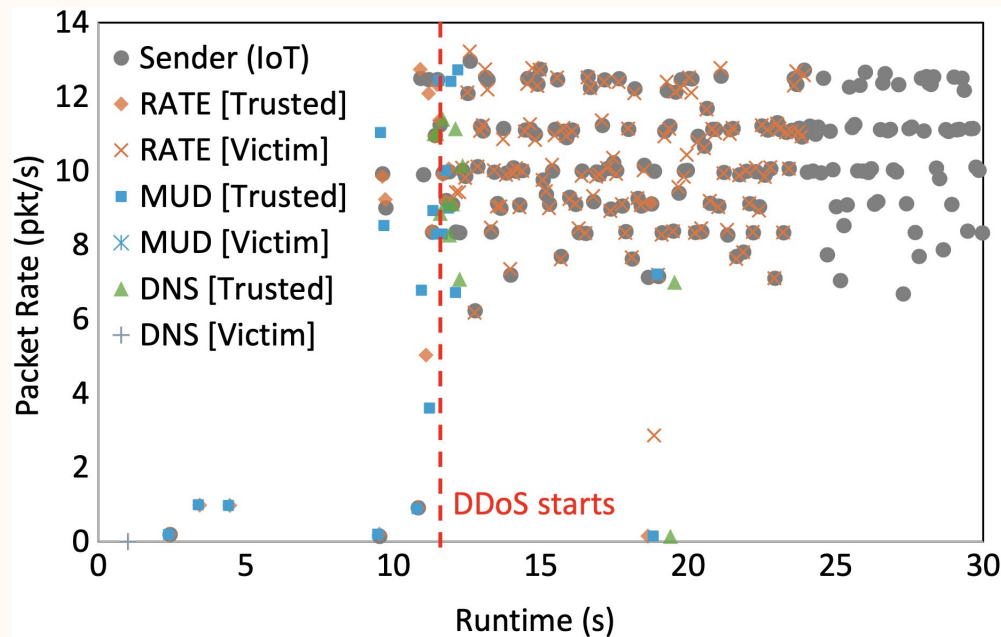
Sniff traffic



Legend

- Switch - port number
- Virtual endpoint
- Physical endpoint

Evaluation



**Effective in mitigating
the impact of botnet
attacks!**


Future Work

Mitigate spreading of botnet within the internal network

This firewall rule effectively mitigates botnet impacts on external networks by blocking DDoS attacks. However, its ability to prevent the spread within the local network has not been tested yet.

IDS alert system

While the firewall blocks suspicious activity, it does not alert IoT devices about potential compromises. Integrating an Intrusion Detection System (IDS) would help address and fix compromised IoT devices.



Heeyun Kim

Thanks!