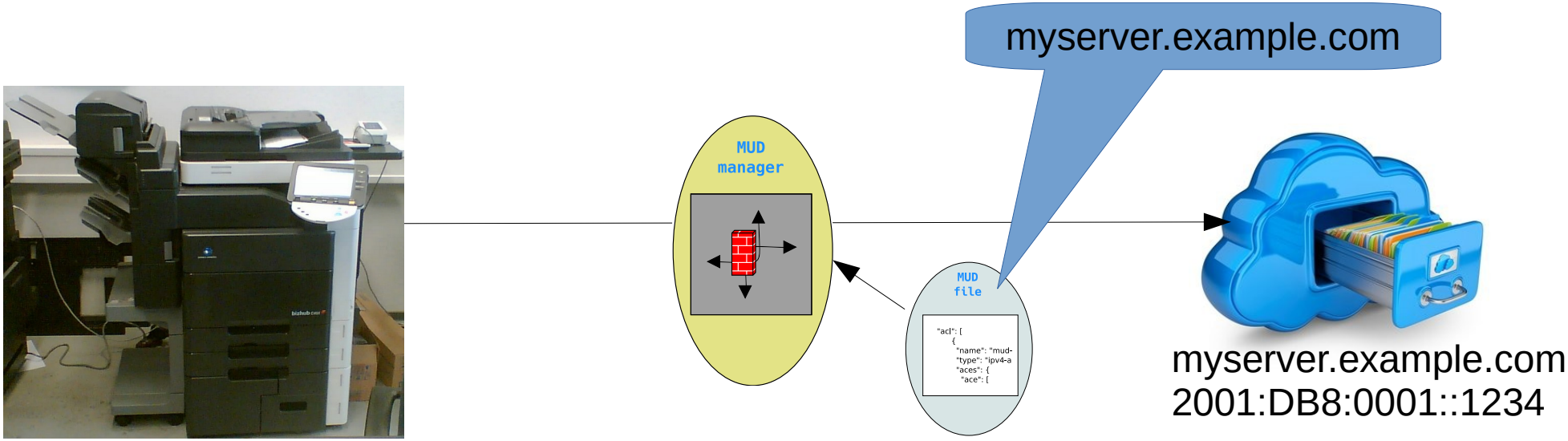
Operational Considerations for use of DNS in IoT devices

Michael Richardson
IETF110 DNSOP meeting
March 11, 2021

draft-opsawg-mud-iot-dns-considerations-01

https://github.com/mcr/iot-mud-dns-considerations

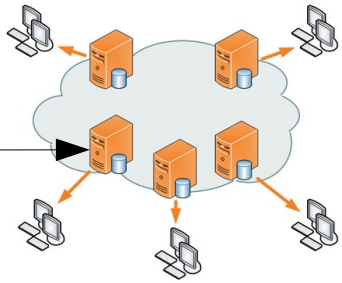
What is the problem?



- IoT devices makes legit connection to network service
  - myserver.example.com is some resource
- RFC8520, Manufacturer Usage Description, describes YANG specified, JSON serialized, CMS signed artifact that is a list of legitimate ACLs.
  - a device originating or receiving traffic outside that ACL is illegimate traffic, which should concern a MUD controller
- Applicable to devices with a few specific uses, not laptops/phones/etc.
  - Manufacturer asserts ACL, may get modified by additional local policies

We like to use DNS in ACLs, but this can present challenges

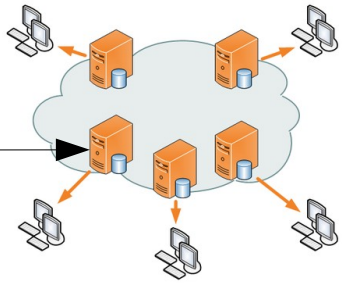
DNS in ACLs needs to use forward lookups... otherwise



myserver.example.com
2001:DB8:0001::1234

DNS in ACLs needs to use forward lookups... otherwise

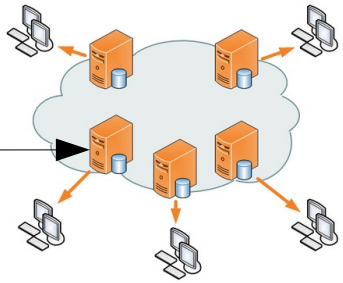
src: 2001:db8:1234::9999
dst: 2001:db8:0001::1234



myserver.example.com
2001:DB8:0001::1234

DNS in ACLs needs to use forward lookups... otherwise

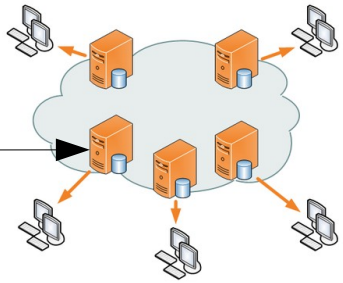
src: 2001:db8:1234::9999
dst: 2001:db8:0001::1234



myserver.example.com
2001:DB8:0001::1234

lookup IP addr to get name?

DNS in ACLs needs to use forward lookups... otherwise

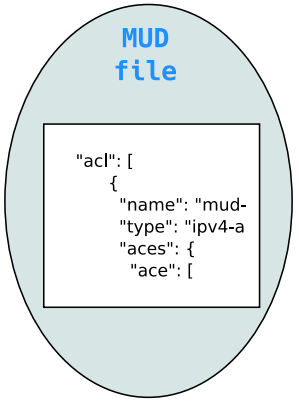


myserver.example.com
2001:DB8:0001::1234

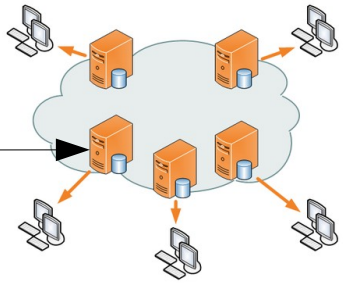
src: 2001:db8:1234::9999
dst: 2001:db8:0001::1234

lookup IP addr
to get name?

ACL says:
permit
src: IoTdevice (me)
dst: myserver.example.com



DNS in ACLs needs to use forward lookups... otherwise



myserver.example.com
2001:DB8:0001::1234

src: 2001:db8:1234::9[illegible]09
dst: 2001:db8:0001::123

FAIL!

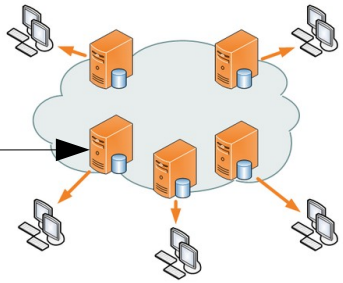
lookup IP addr to get name ?

ACL says:
permit
src: IoTdevice (m[illegible])
dst: myserver.example.com

MUD file

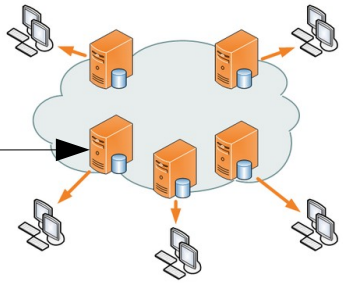
```
"acl": [
  {
    "name": "mud-
    "type": "ipv4-a
    "aces": {
      "ace": [
```

Only do Forward Lookups

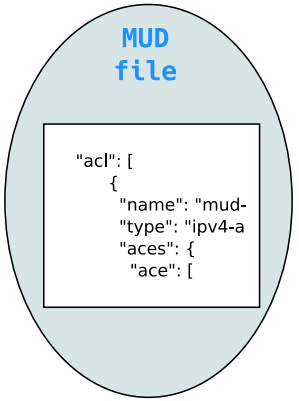


myserver.example.com
2001:DB8:0001::1234

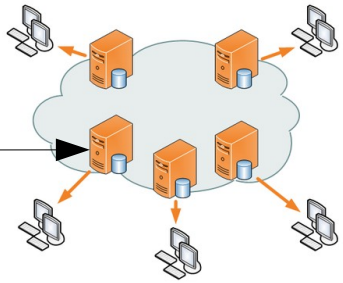
Only do Forward Lookups



myserver.example.com
2001:DB8:0001::1234

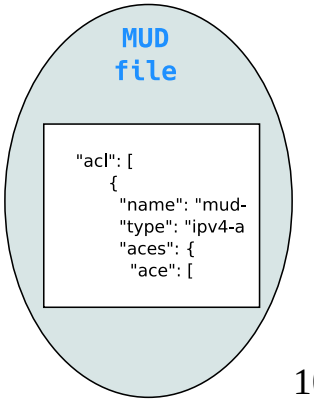


Only do Forward Lookups

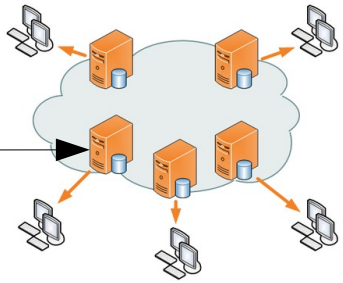


myserver.example.com
2001:DB8:0001::1234

ACL says:
permit
src: IoTdevice (me)
dst: myserver.example.com



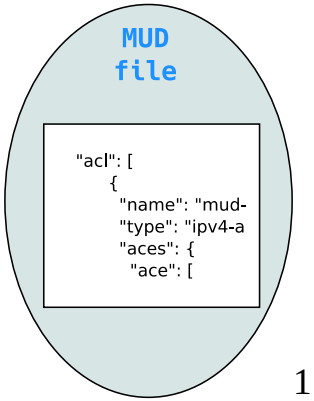
Only do Forward Lookups



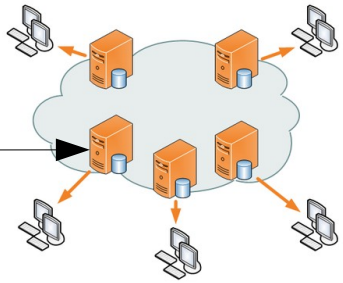
myserver.example.com
2001:DB8:0001::1234

lookup myserver.example.com
get 2001:db8:0001::1234

ACL says:
permit
src: IoTdevice (me)
dst: myserver.example.com



Only do Forward Lookups

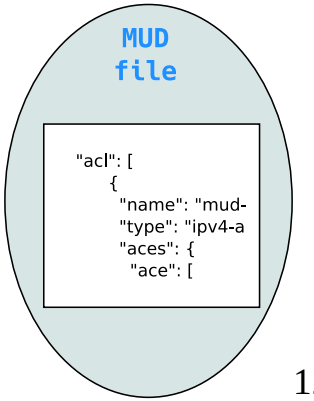


myserver.example.com
2001:DB8:0001::1234

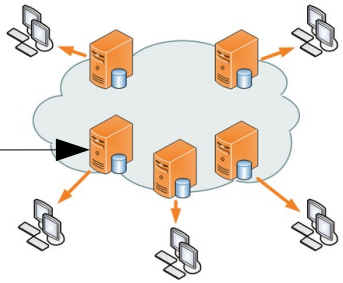
write FIB policy:
src: 2001:db8:1234::9999
dst: 2001:db8:0001::1234

lookup myserver.example.com
get 2001:db8:0001::1234

ACL says:
permit
src: IoTdevice (me)
dst: myserver.example.com



Only do Forward Lookups



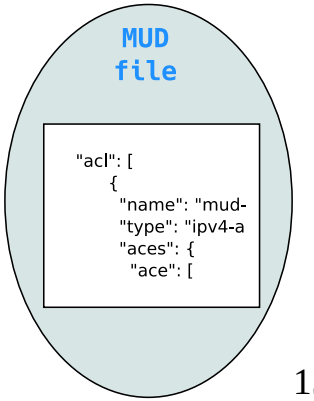
myserver.example.com
2001:DB8:0001::1234

write FIB policy:
src: 2001:db8:1234::9999
dst: 2001:db8:0001::1234

lookup myserver.example.com
get 2001:db8:0001::1234

need to get
TTL right,
geo-DNS,
and DoH/DoT!

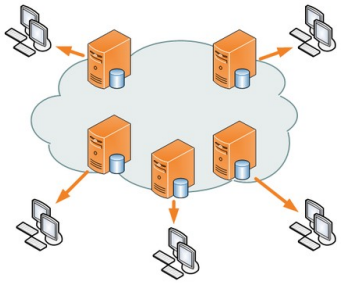
ACL says:
permit
src: IoTdevice (me)
dst: myserver.example.com



Best scenario: local cache

DNS lookup

DNS cache



myserver.example.com
2001:DB8:0001::1234

DNS lookup

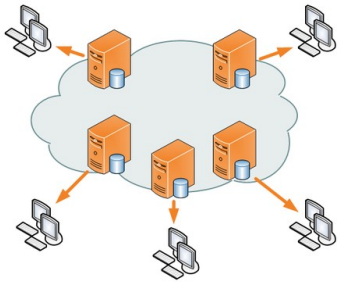
MUD controller does DNS

example.com DNS server

Best scenario: local cache

DNS lookup

DNS cache



myserver.example.com
2001:DB8:0001::1234

DNS lookup

MUD controller does DNS

example.com DNS server

more complicated in Enterprises!

mud-ios-dns-considerations

- implementation advice
- anti-patterns to avoid
- what things to do
- keeping queries private: don’t leak them

Table of Contents

1. Introduction

Use of Round Robin DNS vs geo-fenced DNS

- Two ways of answering DNS.
  - Return just the A/AAAA to be used
  - *Return all A/AAAA, but sort it so that first one is desired one.*

Advice

1) Always use DNS provided by DHCP

2) When doing round robin DNS, always arrange for all possible records to be returned

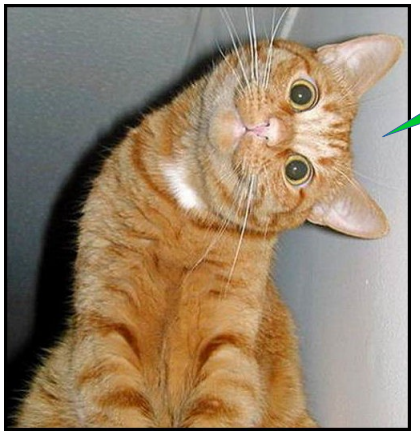
Advice

1) Always use DNS provided by DHCP

2) When doing round robin DNS, always arrange for all possible records to be returned

My Ask

- Review from DNSOP on sections:
  - Strategies to map names
  - Additional Anti-Patterns
    - particularly around RR-DNS, geo-fenced DNS
  - Additional advice for manufacturer
- QUESTIONS?



Is this an ADD issue?
Not directly.
ADD WG said no.
OPSAWG is home for MUD

Image Credits:

- Slides from Cisco
- Images from IoT-DIR IETF GITHUB
- https://en.wikipedia.org/wiki/Content_delivery_network#/media/File:NCDN_-_CDN.png
- https://starecat.com/content/wp-content/uploads/what-seems-to-be-the-problem-mary-doctor-it-hurts-when-i-do-this-then-dont-do-that.jpg