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 illegitimate 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

lookup IP addr to get name?

myserver.example.com
2001:DB8:0001::1234
DNS in ACLs needs to use forward lookups... otherwise

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

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

lookup IP addr to get name?

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

MUD file
*ad*: [ 
  *name*: "mud-" 
  *type*: "ipv4-a" 
  *aces*: [ 
    *ace*: [ ....] ] ]
DNS in ACLs needs to use forward lookups... otherwise otherwise

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

FAIL!

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

lookup IP addr to get name?

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

MUD file

`"ace": [
  "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

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

lookup myserver.example.com
get 2001:db8:0001::1234
Only do Forward Lookups

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

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

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

myserver.example.com
2001:DB8:0001::1234
Best scenario: local cache

- DNS lookup
- DNS cache
- MUD controller does DNS
- example.com DNS server
- 2001:DB8:0001::1234
- myserver.example.com
Best scenario: local cache

MUD controller does DNS

more complicated in Enterprises!

DNS cache

DNS lookup

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

does DNS

dns.lookup

DNS

example.com DNS server
mud-ios-dns-considerations

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