

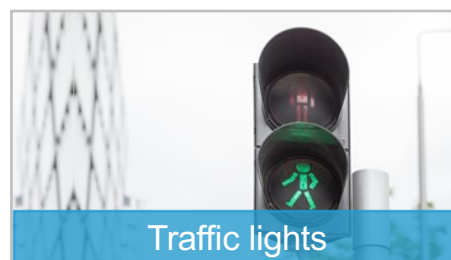
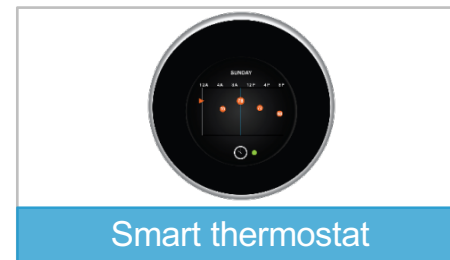


IoT Security and Horizontal Integration

Eliot Lear

Released: September 12, 2016

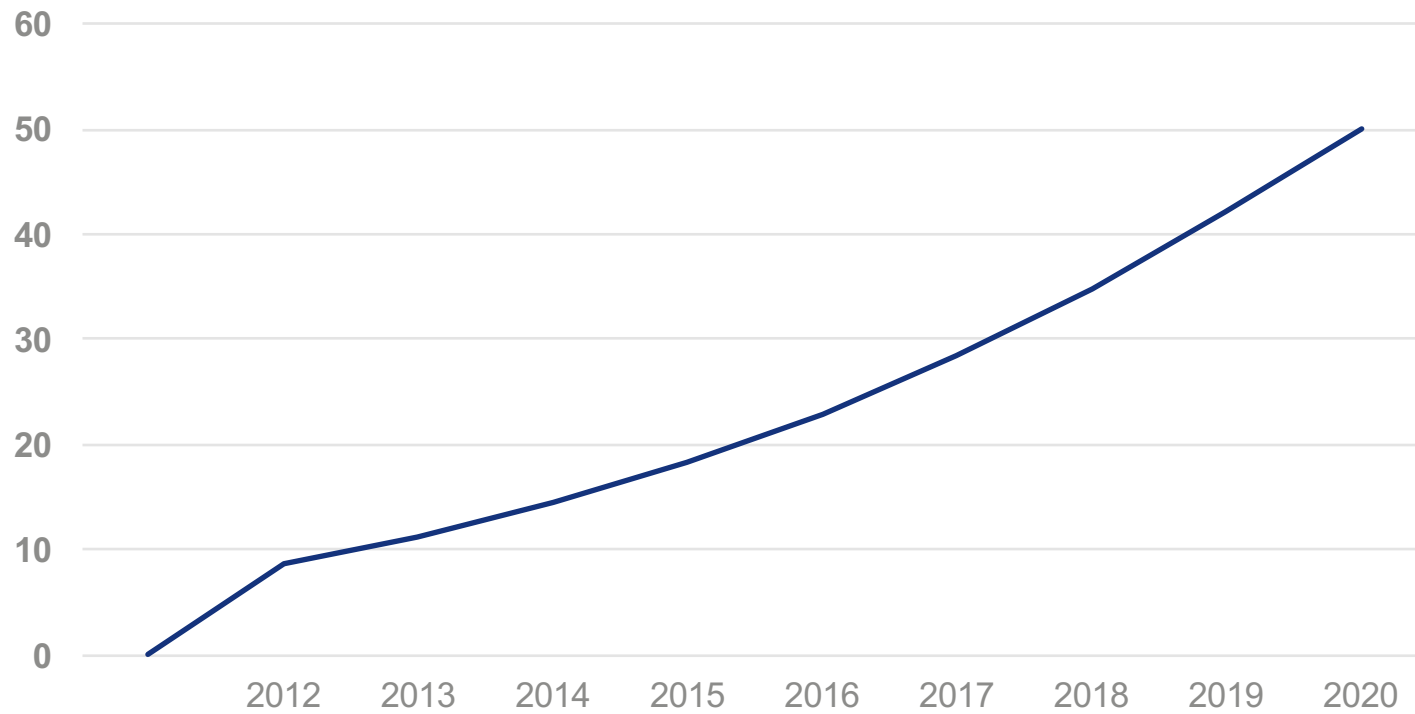
What's a Thing?



For Today

*A thing is a networked device that has a **single or small number** of intended uses.*

Number of connected devices (Billions)



Introducing Raul Rohas

- Entire house Internet-enabled
- A single lightbulb took down his IoT house.
- It was an SNMP bug.



From Fusion.net (3 March 2015)

It's not just lightbulbs

- Japanese Bluetooth toilet hacked
 - Remote flushing
 - Lid open and close
 - Bidet activation



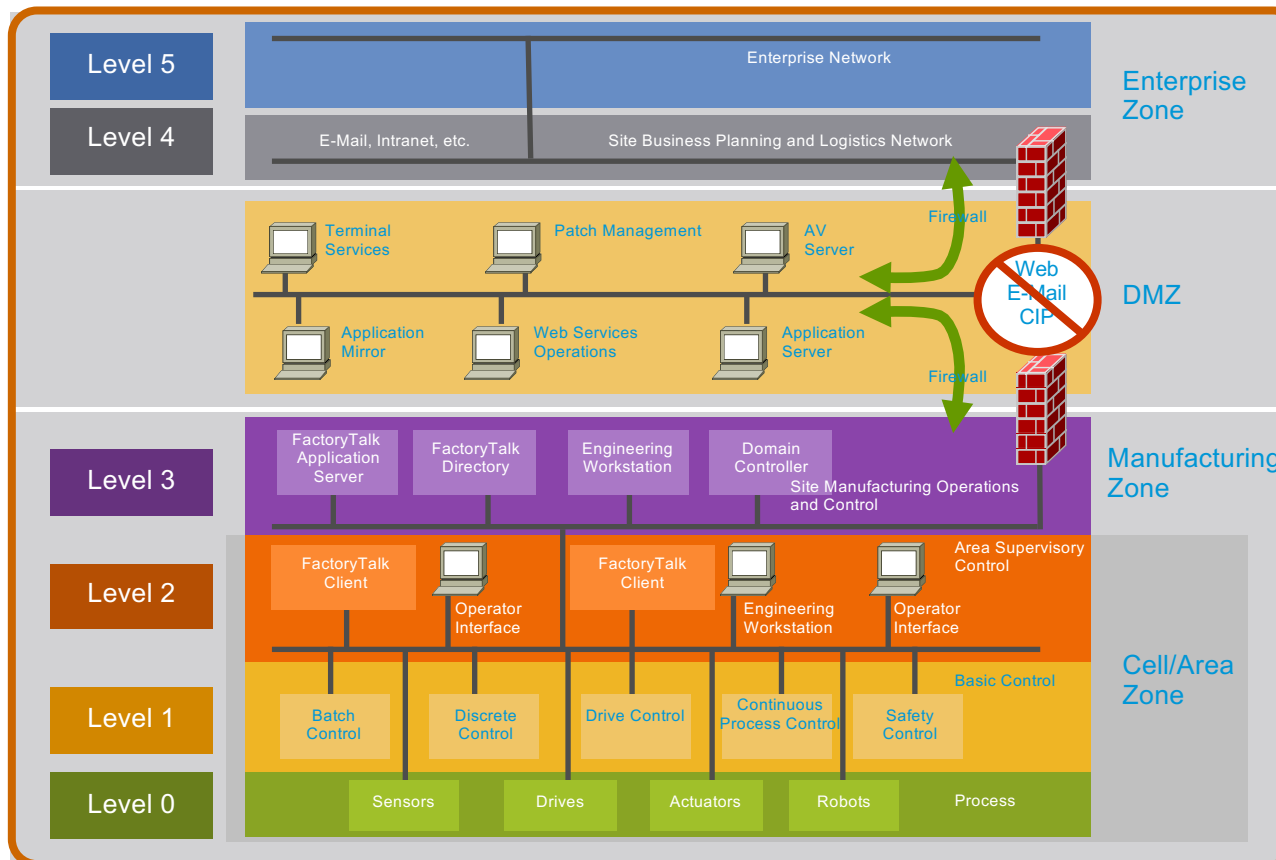
Not just the house

- German smelting plant was hacked
- Blast furnace was taken over
- Not able to be shut down



By AMIR MARINE - Own work, CC BY-SA 3.0,
<https://commons.wikimedia.org/w/index.php?curid=28937609>

Many vertical approaches: Here is industrial (ISA99)



Cost of configuration

Static environments



Dynamic systems





The Network Needs Two Pieces of Information

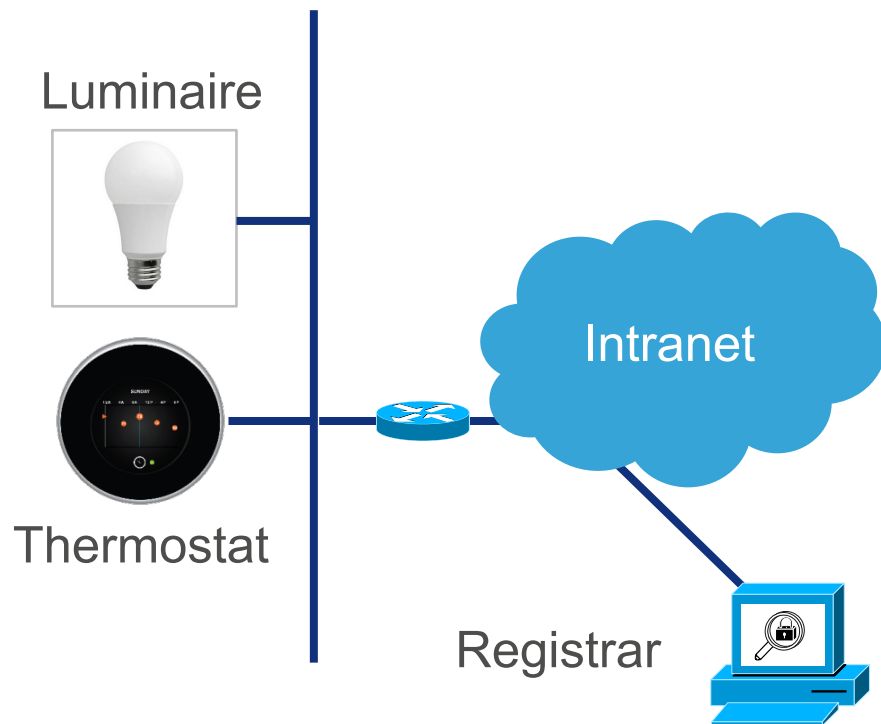
- What the device is
- How the network should protect it



The Network Needs Two Pieces of Information

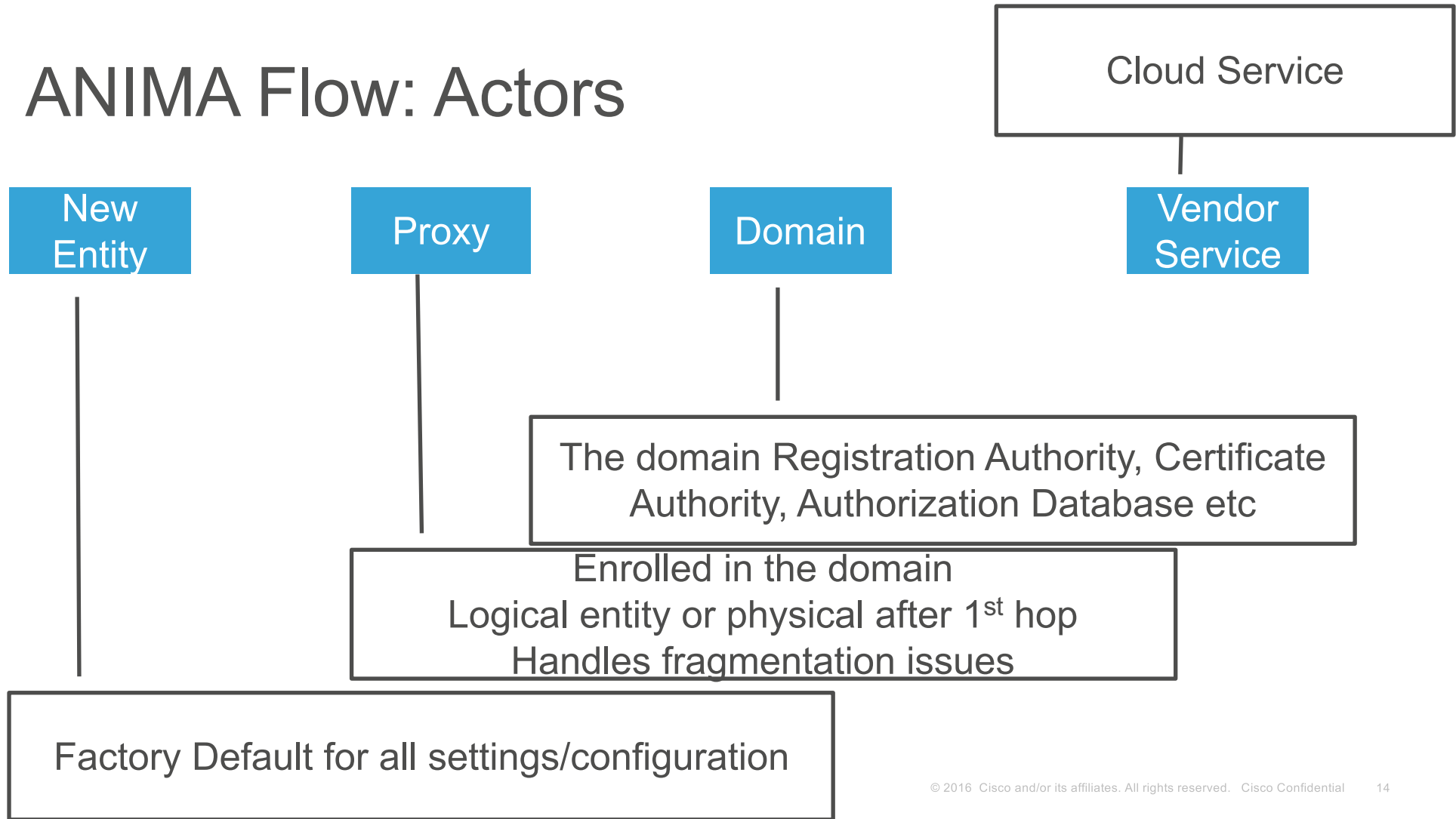
- What the device is  IEEE 802.1X/AR + ANIMA
- How the network should protect it  Manufacturer Usage Descriptions

IEEE 802.1X with EAP-TLS: a scalable approach

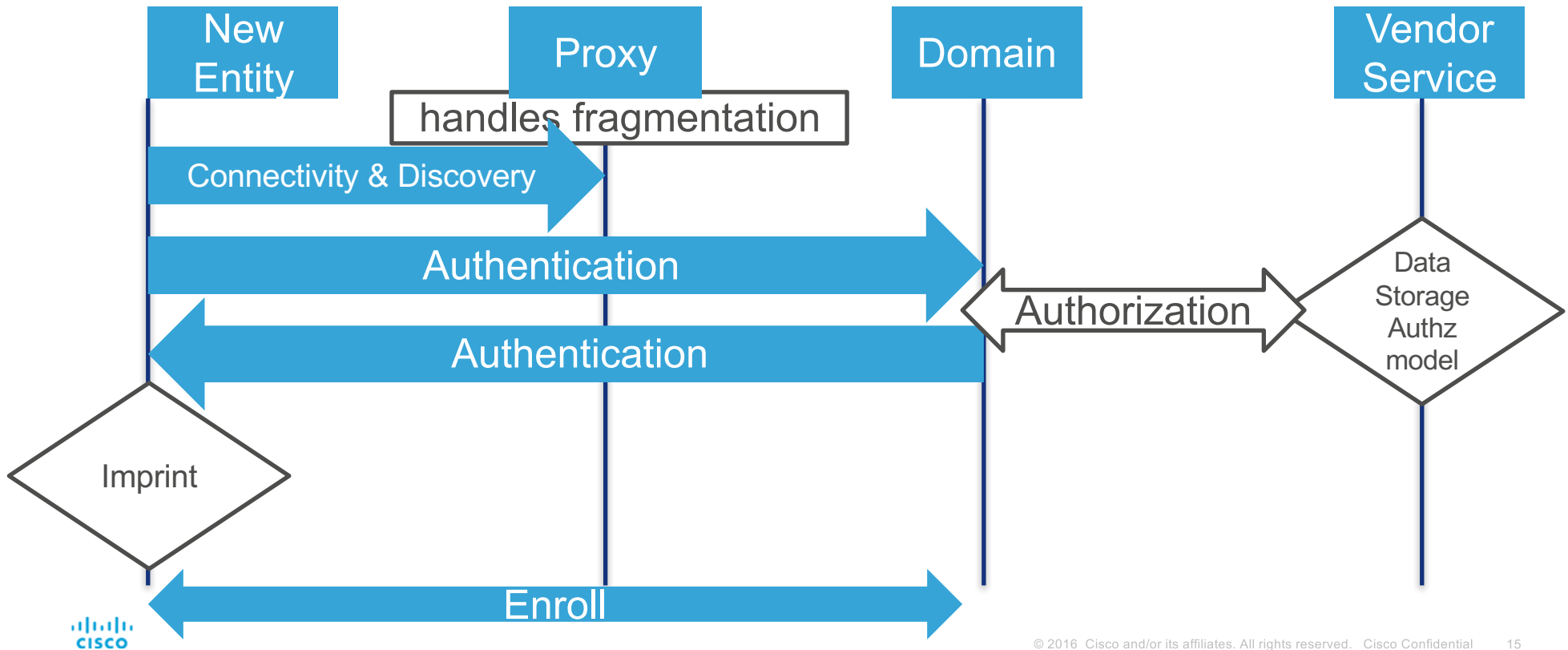


- EAP-TLS makes use of certificates to identify new elements
- IEEE 802.1AR specifies a device certificate format
- Assertion about device is initially from manufacturer, and then from administrator.
 - **NOT from the device!**
- Requires a common trust anchor
- Constrained devices lack capacity for common trust anchors

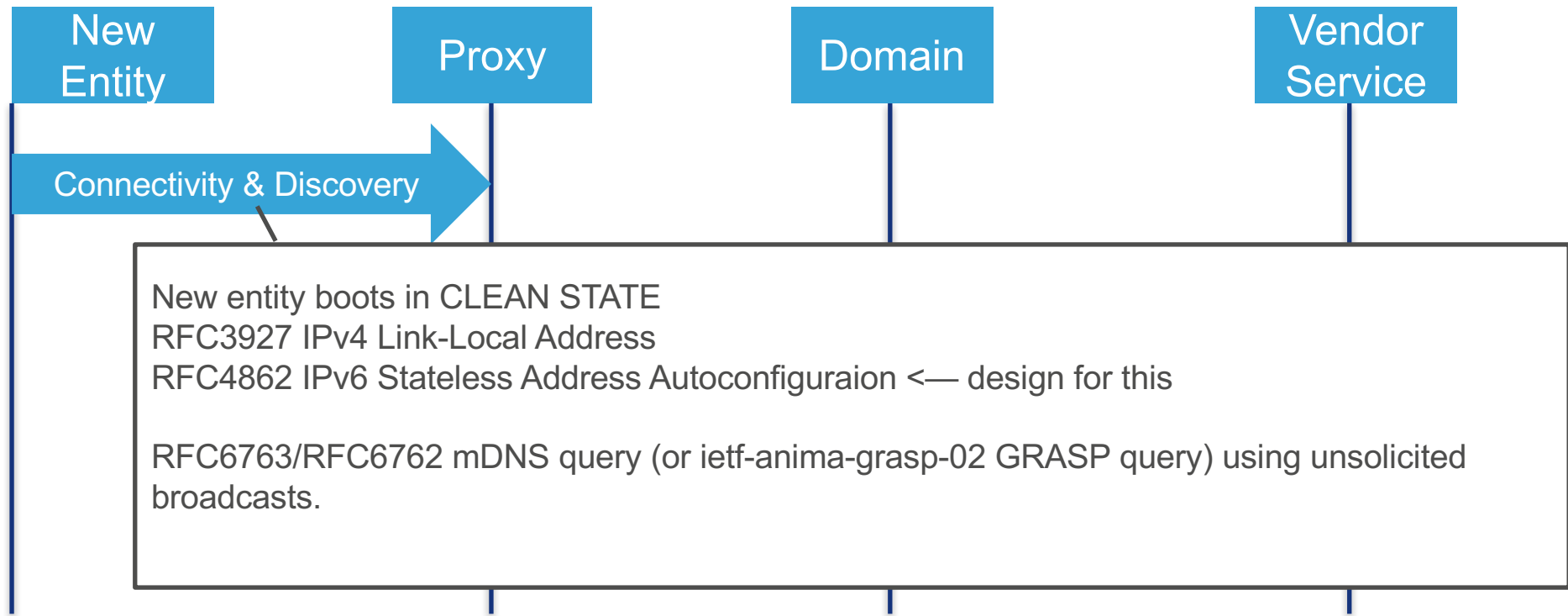
ANIMA Flow: Actors



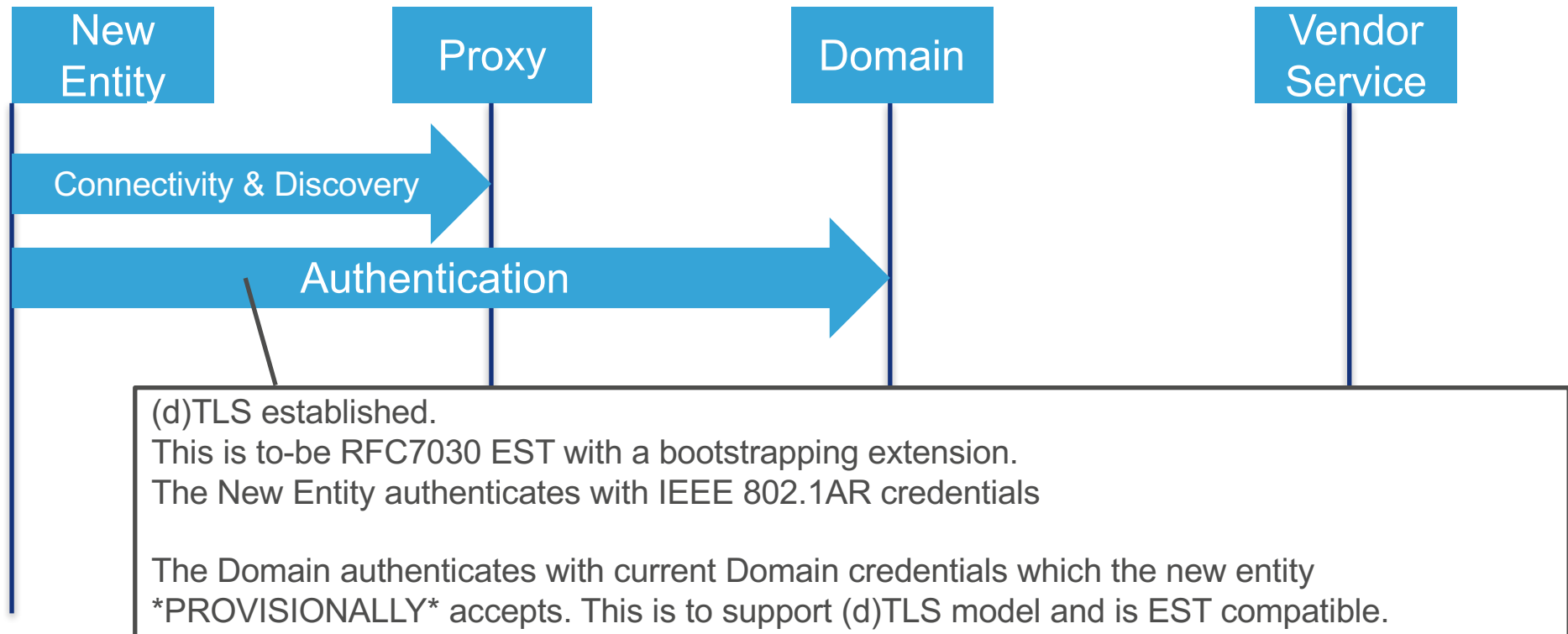
Problems to solve



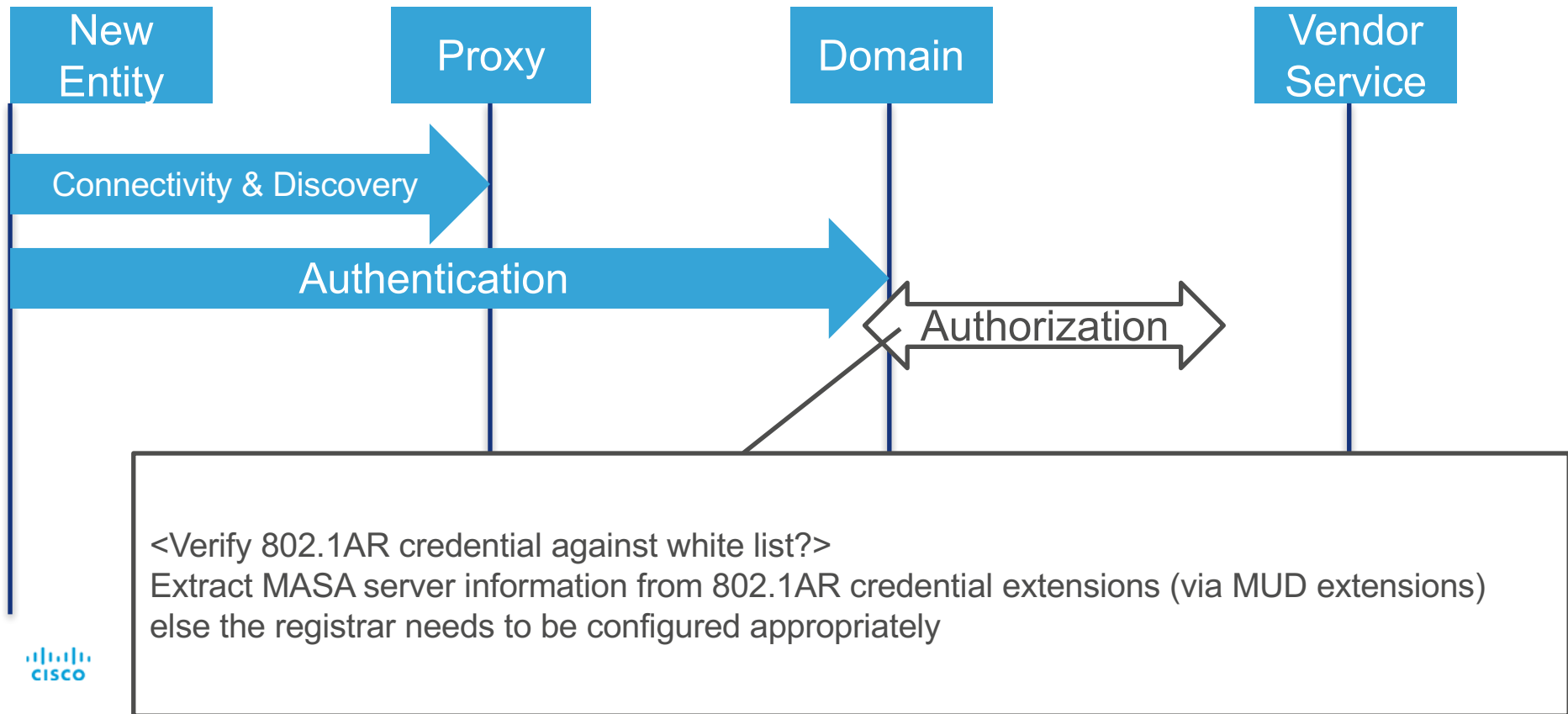
Discovery, Connectivity



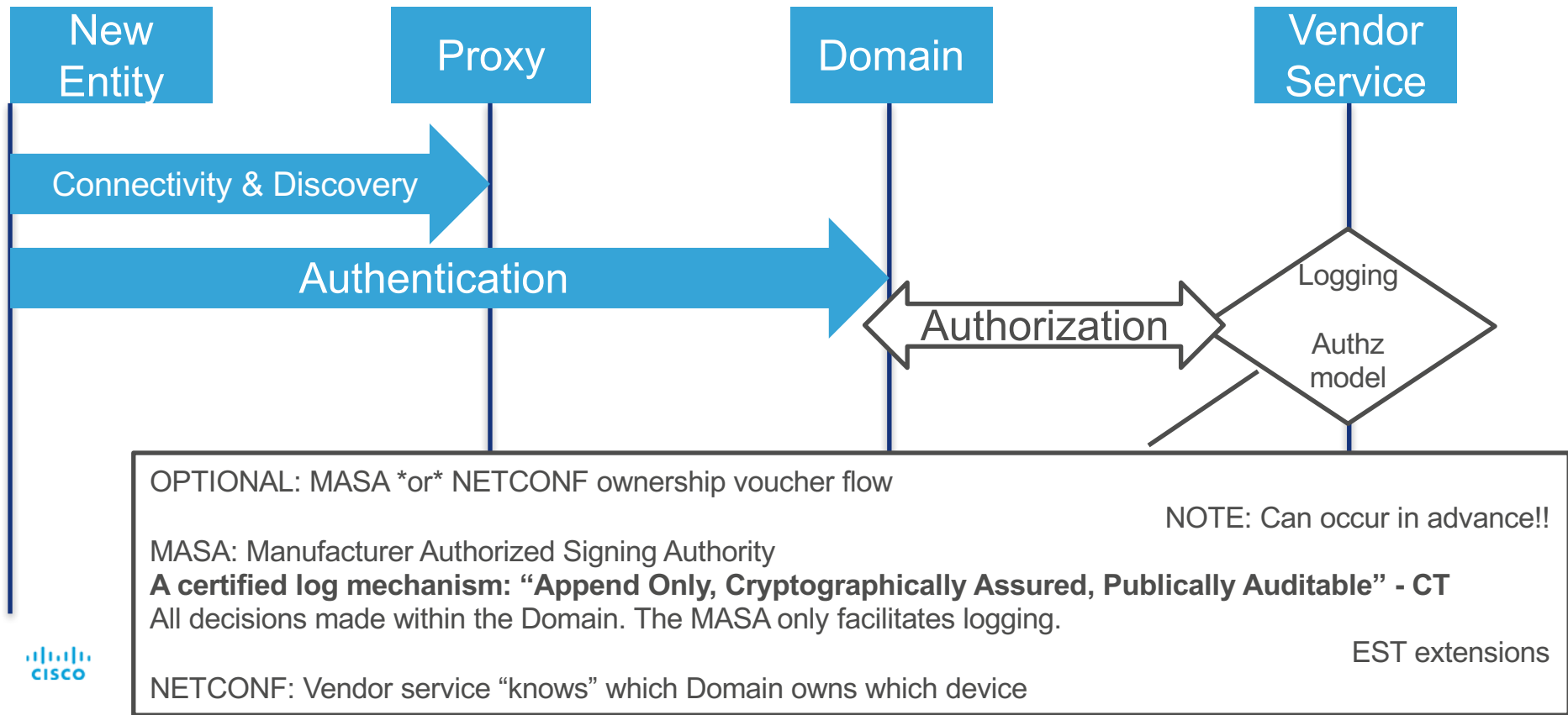
New Entity Authentication



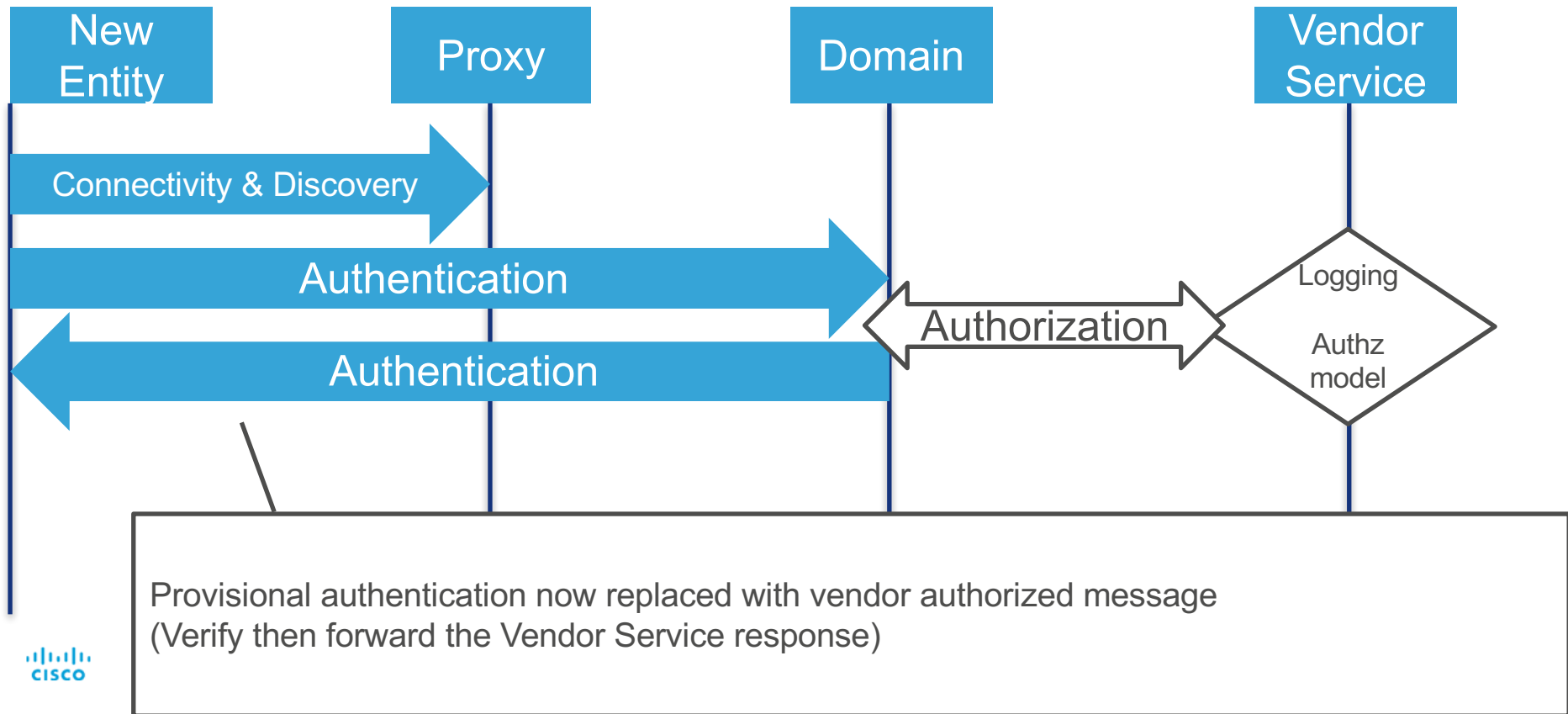
Authorization by the Domain



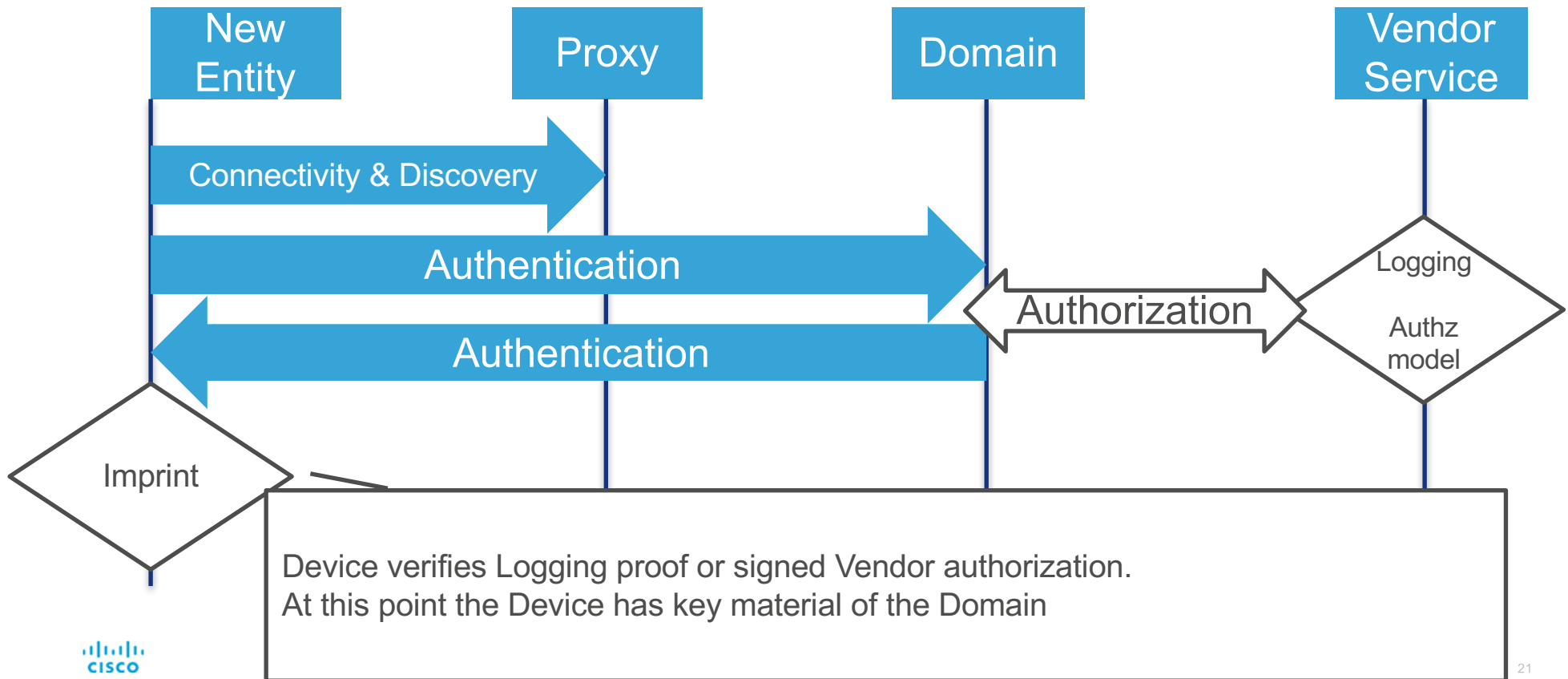
Logging or Decision by the Vendor



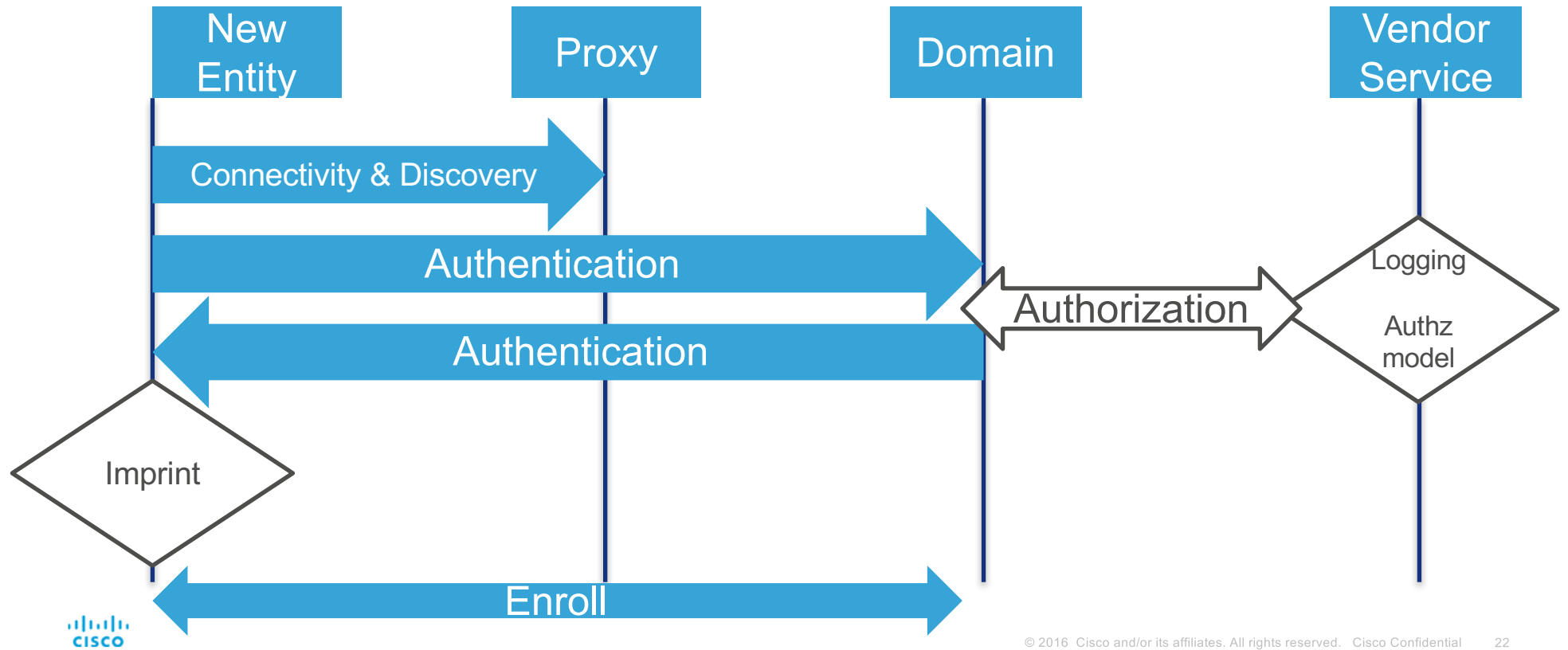
Transmit back to device



Imprint



Device Enrolls: Joins domain



What you get and don't with all of that...

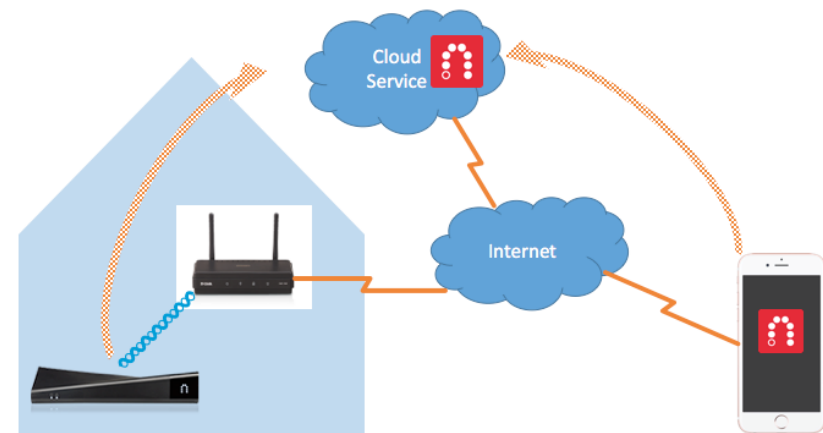
- What you get
 - Device gets a trust root and a certificate for the local deployment
 - Local deployment now has authenticated the device
 - Device can connect to network using certificate
- What you don't get
 - Automated selection of network
 - Automated profiling of the device
 - Application-specific authorization model
(but you have an identity anchor to build such a thing)

A word about the cloud and IoT...

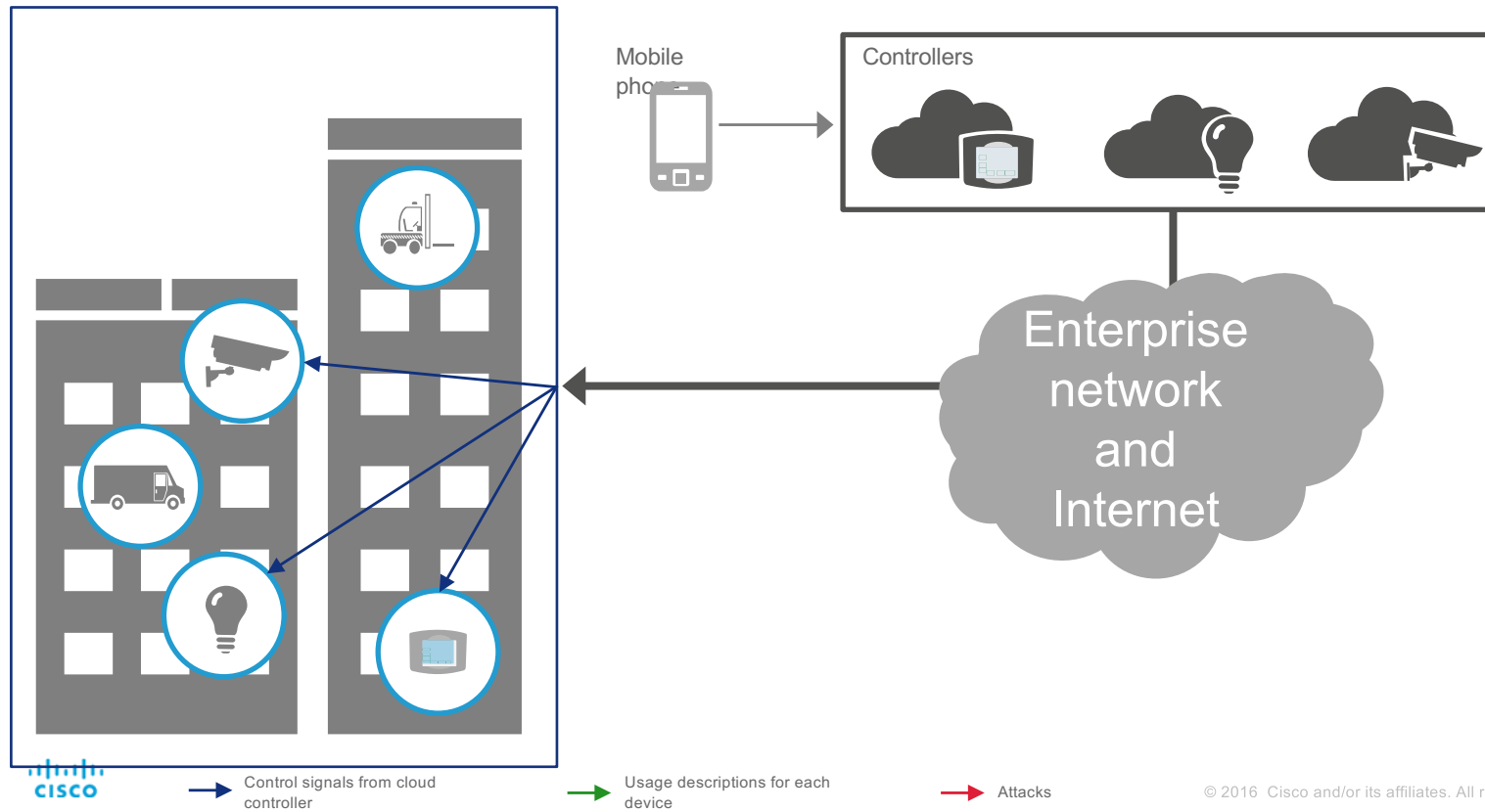
Clouds offer-

- A rendezvous point
- Substantial processing power

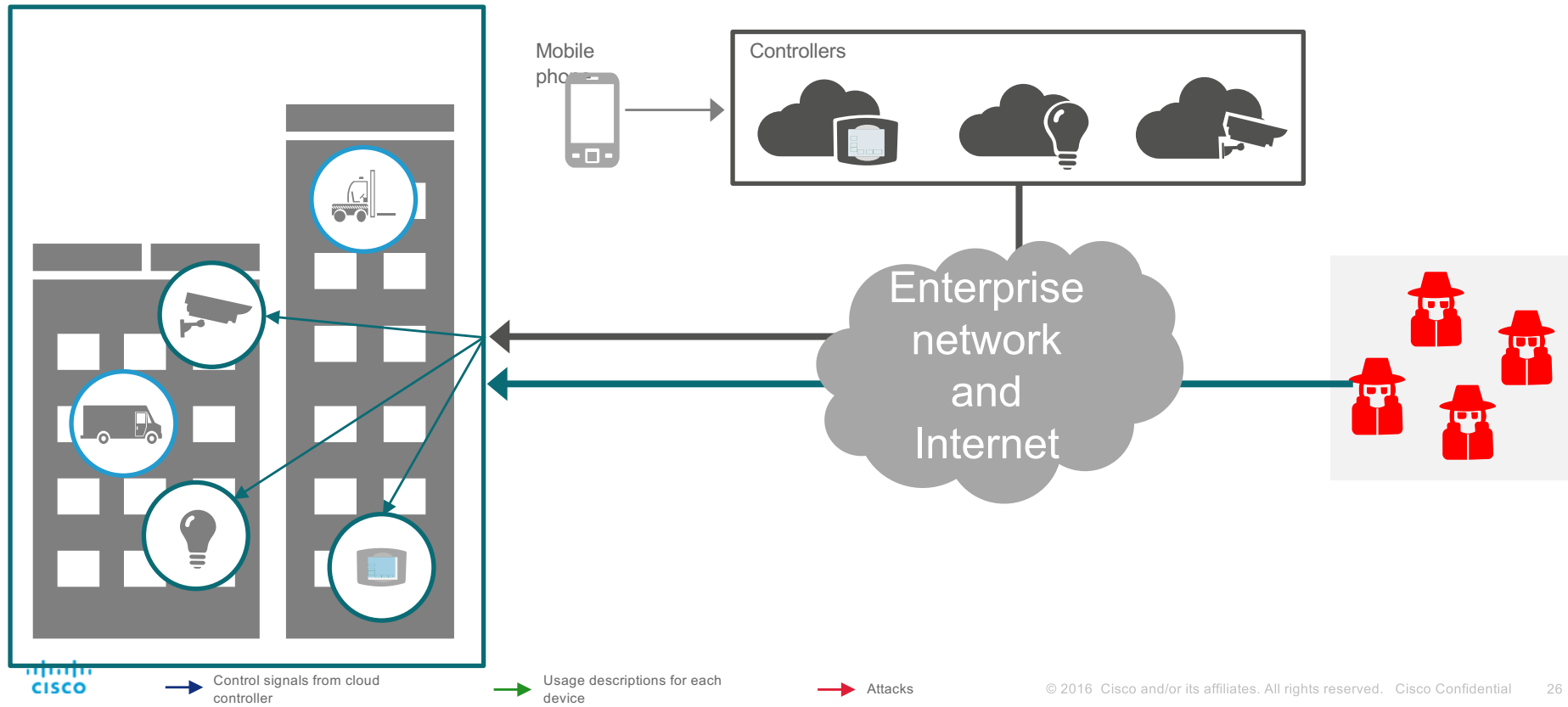
Cloud capabilities will continue to expand.



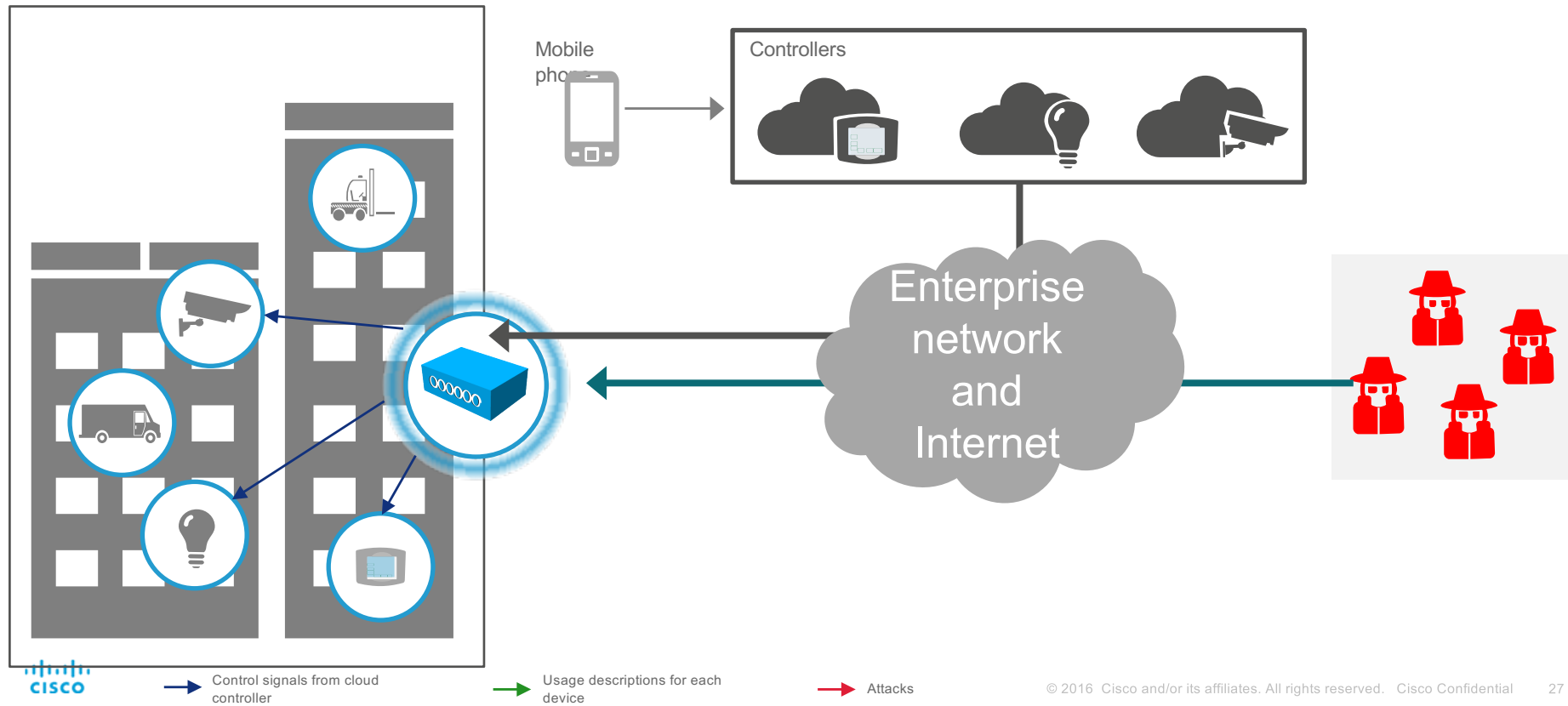
Many things need talk only to a few things



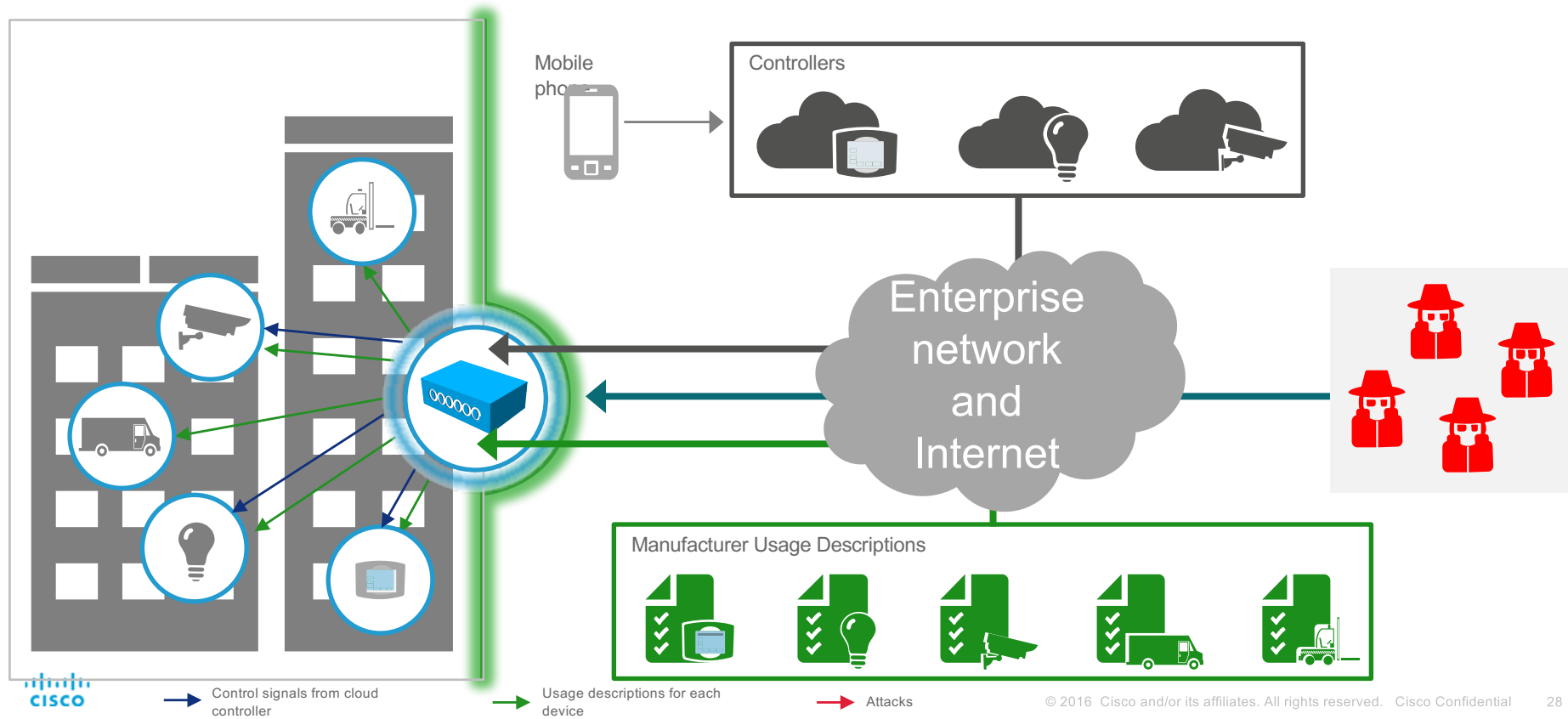
Expanding the attack surface



Cisco Routers are in the right place to defend these devices



Manufacturer usage descriptions can improve this security



Assumptions and Assertions

Assumptions

A Thing has a single use or a small number of uses.

Things are tightly constrained. Very **VERY** dumb. Resource constraints are tight.

Even those Things that can protect themselves today may not be able to do so tomorrow

Network administrators are the ultimate arbiters of how their networks will be used

Assertions

Because a Thing has a single or a small number of intended uses, it all other uses must be unintended

Any intended use can be clearly identified by the manufacturer

All other uses can be warned against in a statement by the manufacturer

Manufacturers are in a generally good position to make the distinction

| Drug Facts | |
|--|---------------------------------|
| Active Ingredient (in each tablet) Aspirin 81 mg | Purpose Pain reliever |
| Uses for the temporary relief of minor aches and pains or as recommended by your doctor. Because of its delayed release action, this product will not provide fast relief of headaches or other symptoms needing immediate relief. | |
| Do not use if you have ever had an allergic reaction to any other pain relievers/fever reducers. | |
| Warnings Reyes syndrome: Children and teenagers who have or are recovering from chicken pox or flu-like symptoms should not use this product. When using this product, if changes in behavior with nausea and vomiting occur, consult a doctor because these symptoms could be an early sign of Reyes syndrome, a rare but serious illness. | |
| Ask a doctor before use if you have stomach problems (such as heartburn, upset stomach, or stomach pain) that last or come back -bleeding problems -ulcers -asthma | |
| Ask a doctor or pharmacist before use if you are taking a prescription drug for -diabetes -gout -arthritis | |
| Allergy alert: Aspirin may cause a severe allergic reaction which may include: -facial swelling -asthma (wheezing) -shock -hives | |
| Alcohol warning If you consume 3 or more alcoholic drinks every day. Ask your doctor whether you should take aspirin or other pain relievers/fever reducers. Aspirin may cause stomach bleeding. | |
| Stop use and ask doctor if an allergic reaction occurs. Seek medical help right away. -Pain gets worse or lasts more than 10 days -redness or swelling is present -new symptoms occur -the ears or loss of hearing occurs | |
| If pregnant or breast-feeding ask a health professional. It is especially important not to use aspirin during the last 3 months of pregnancy unless definitely directed to do so because it may cause problems in the unborn child or complications during delivery. | |
| Keep out of the reach of children. In case of emergency, call for help or contact a Poison Control Center immediately. | |
| Directions -drink a full glass of water with each dose. -At 12 years of age and over: take 4 to 8 tablets every 4 to 6 hours. Do not exceed 48 tablets in 24 hours unless directed otherwise. -Children under 12 years: consult a doctor | |
| Other information -store at room temperature | |
| Inactive ingredients colloidal silicon dioxide, sodium, FD&C Yellow #10 lake, FD&C Yellow #6 lake, methacrylic acid copolymer, microcrystalline cellulose, talc, titanium dioxide, triethyl citrate | |

Translating intent into config

Any intended use can be clearly identified by the manufacturer



```
access-list 10 permit host  
controller.mfg.example.com
```

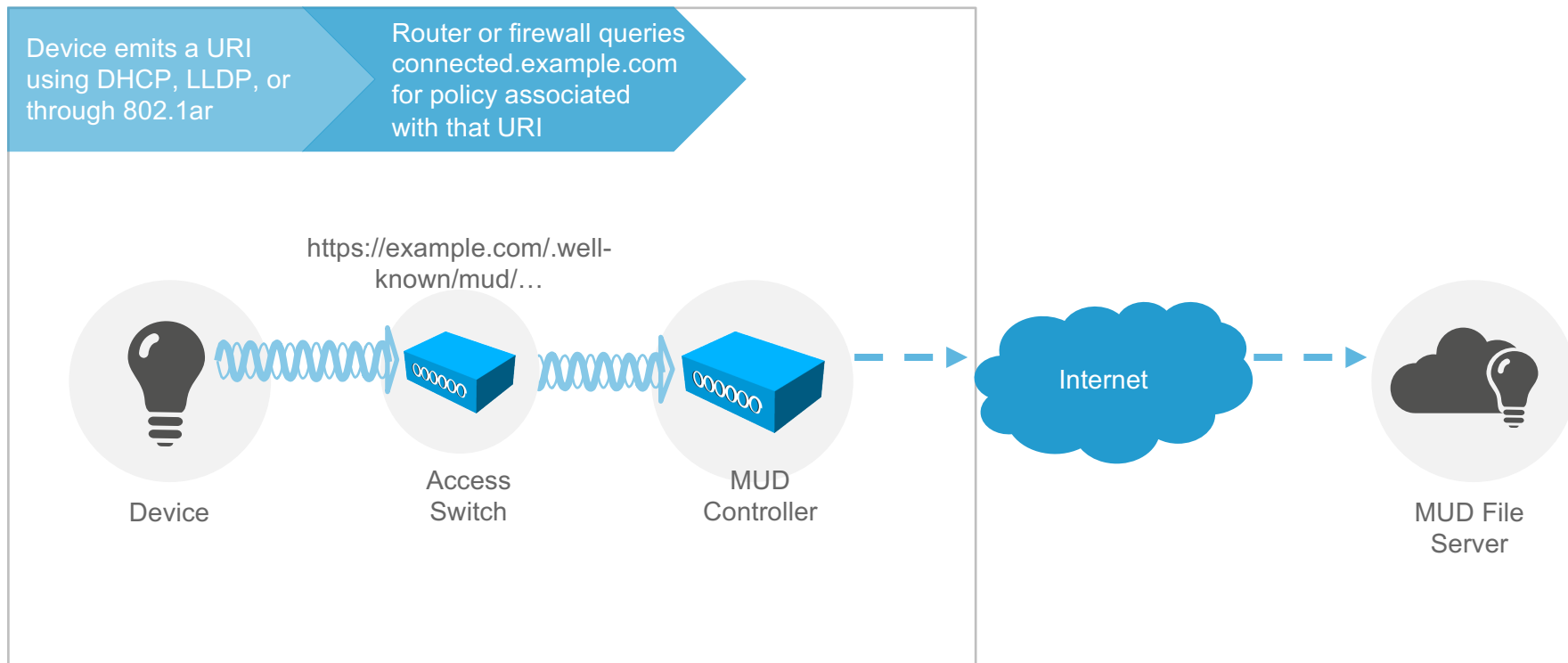
All other uses can be warned against in a statement by the manufacturer



```
access-list 10 deny any any
```



Expressing Manufacturer Usage Descriptions



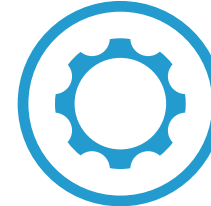
How to locate the policy? A URL

<https://mud.mfg.example.com/.well-known/mud/v1/CAS11LCDLversion2.12>

“Manufacturer”



Model

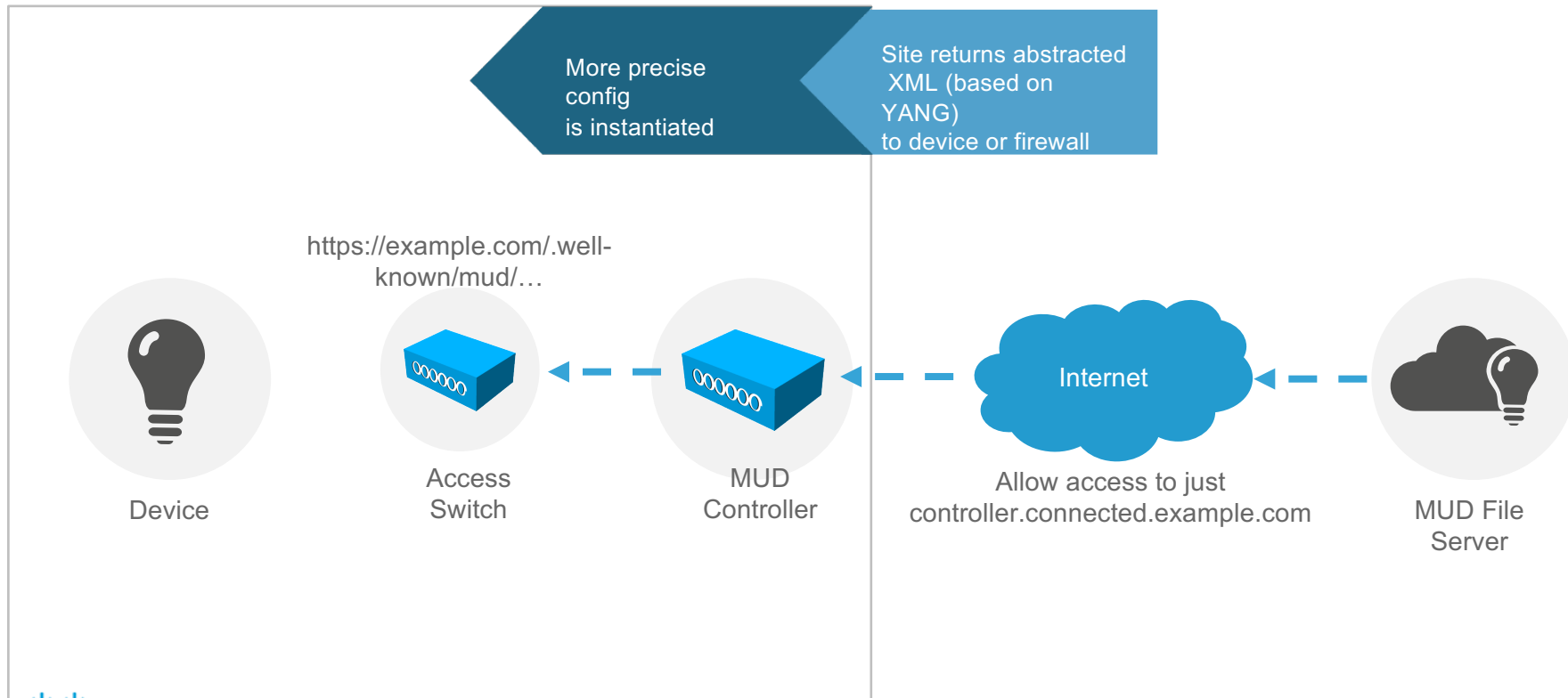


The MUD File

```
{
  "ietf-mud:support-information": {
    "last-update": "2016-05-18T20:00:50Z",
    "cache-validity": 1440
  },
  "ietf-access-control-list:access-lists": {
    "acl": [ {
      "acl-name": "inbound-stuff",
      "acl-type": "ipv4-acl",
      "ietf-mud:packet-direction": "to-device",
      "access-list-entries": {
        "ace": [
          {
            "rule-name": "access-cloud",
            "matches": {
              "ietf-acl-dnsname:source-hostname": "lighting-system.example.com",
              "protocol": 8,
              "destination-port-range": {
                "lower-port": 443,
                "upper-port": 443
              }
            },
            "actions": {
              "permit": [null]
            }
          }
        ]
      }
    }
  ]
}

},
{
  "acl-name": "outbound-stuff",
  "acl-type": "ipv4-acl",
  "ietf-mud:packet-direction": "from-device",
  "access-list-entries": {
    "ace": [
      {
        "rule-name": "access-cloud",
        "matches": {
          "ietf-acl-dnsname:destination-hostname": "lighting-system.example.com",
          "protocol": 8,
          "source-port-range": {
            "lower-port": 443,
            "upper-port": 443
          }
        },
        "actions": {
          "permit": [null]
        }
      }
    ]
  }
}
]
```

Expressing Manufacturer Usage Descriptions



This approach...

Does



Extend defense in depth



Reduces the threat surface of a Thing by preventing lateral infection



Provide the first effective security solution for IoT

Does not



Authenticate devices to the network
(Use 802.1x and 802.1AR)



Protect against introduction of devices that are already 0wn3d
(Use Cisco ISE or AMP)

Benefits

Customer



- Reduces target surface of exploding number of devices
- No additional CAPEX
- Helps to reduce OPEX through efficiency gains
- Standards-based approach uses existing equipment

Manufacturer



- Reduces product risk at almost no cost
- Will increase customer satisfaction and reduce support costs
- Easy service location of on-premises controllers
- Standards-based approach
- Reduces risk of government technology mandates

Where to go for more information

- IEEE standards 802.1x, 802.1ar, 802.11i for link layer protection
- IETF ANIMA group for trusted introduction
draft-ietf-anima-bootstrap-keyinfra-03
- IETF OPSAWG group for Manufacturer Usage Descriptions
draft-ietf-opsawg-mud-00.txt
- mud-interest@cisco.com for more information from Cisco

