Hyron

A Case Study in Automating Networks

@jacobneiltaylor

Agenda

- **Background:** Why should we automate?
- **Issues:** What’s stopping us today?
- **Design:** How could we automate networks?
- **Implementation:** What is Hyron and how is it better?
- **Demonstration:** Show us you aren’t full of it!

Background

Why things aren’t fine...

Networking is very different to what it was

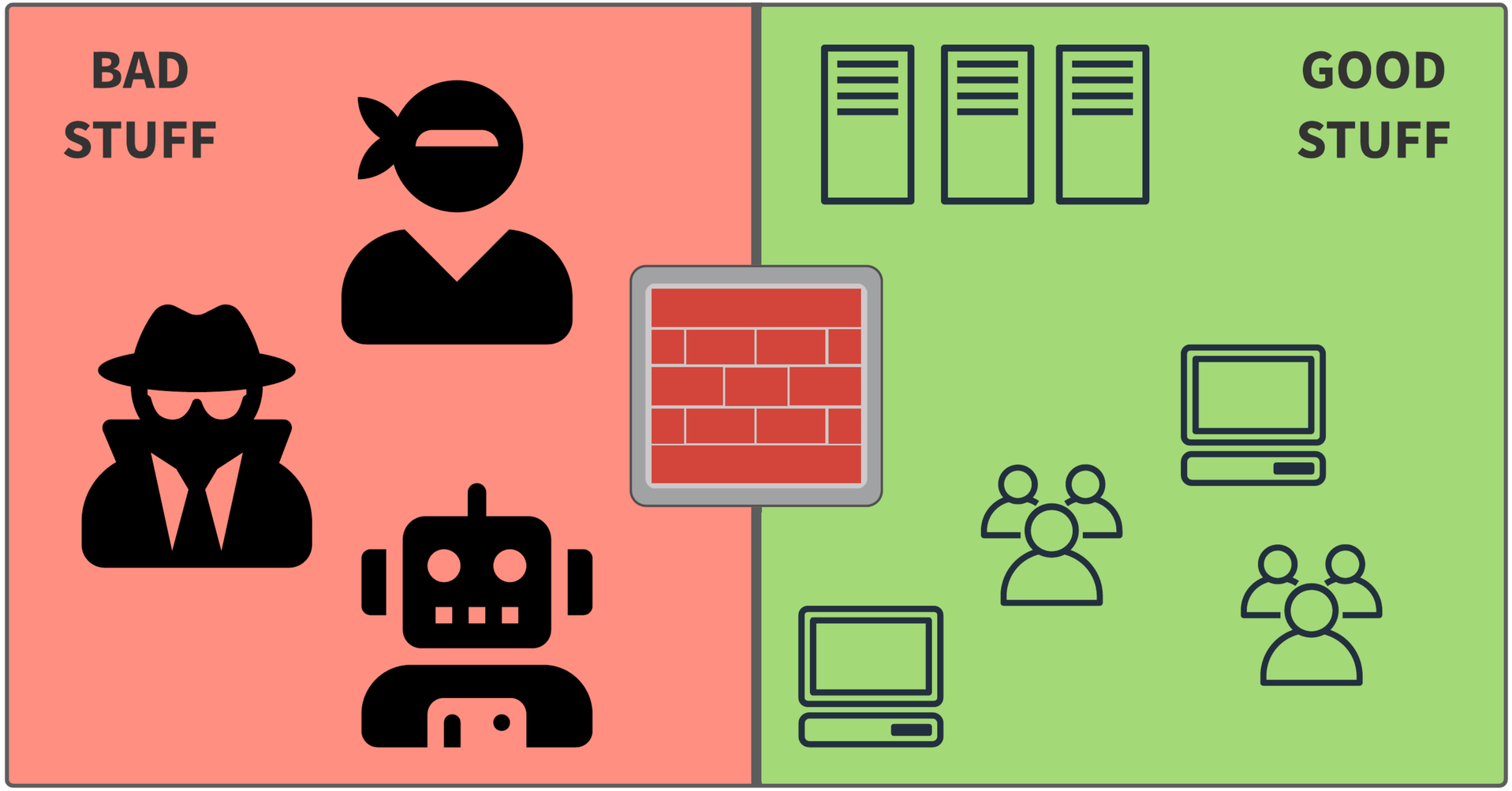
10 years ago

Why Automate?

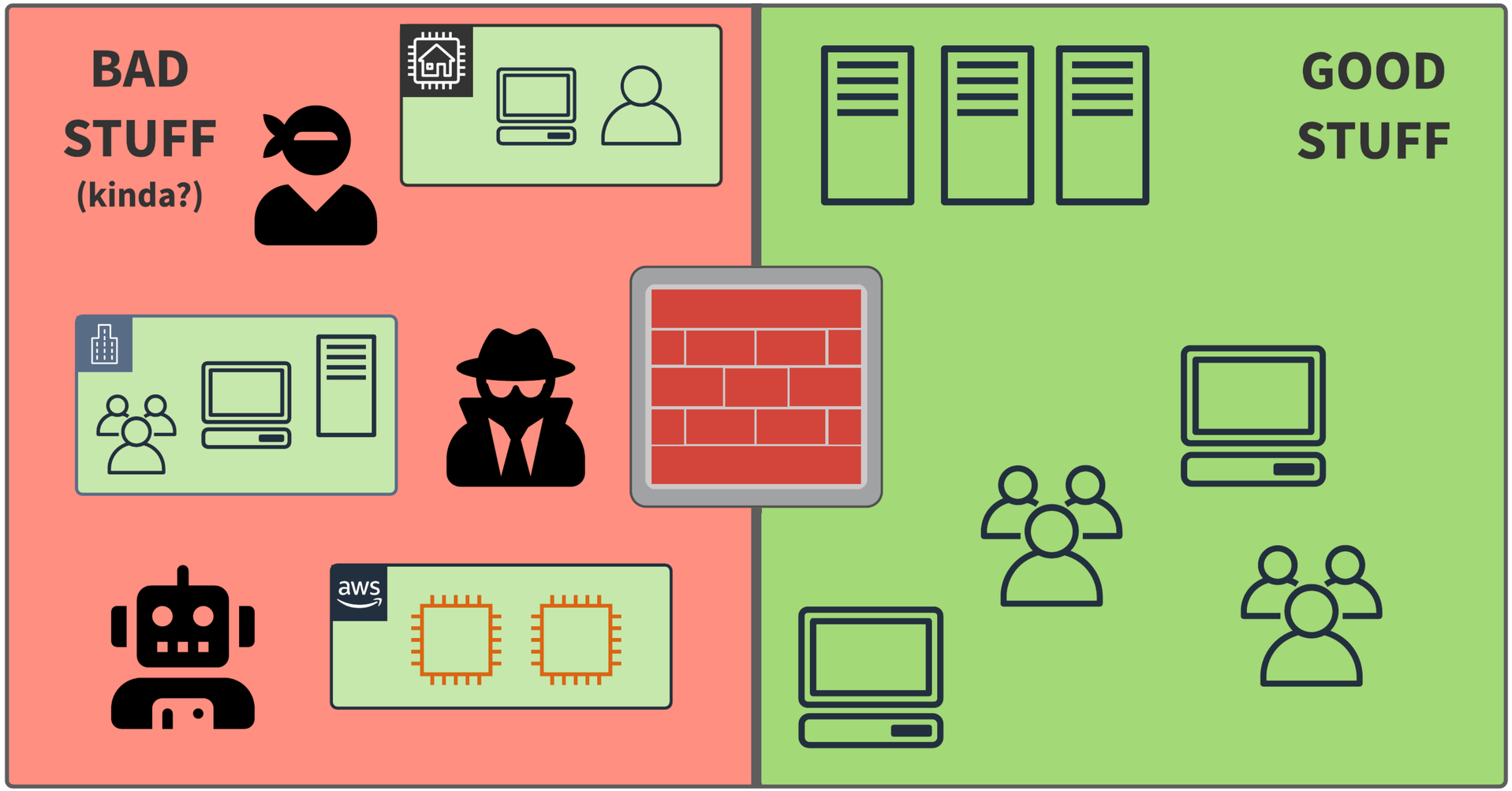
What's wrong with `conft`?

- **Humans suck:** Humans make mistakes, deal with it.
  - What was the cost of your first `conft` booboo?
  - Delegating BAU work to junior staff doesn't scale
- **Those damn clouds:** Changes are increasing in two ways:
  - Frequency
  - Complexity

The Old World



The New World



Hasn’t This Been Done?

Can we copy our neighbours homework?

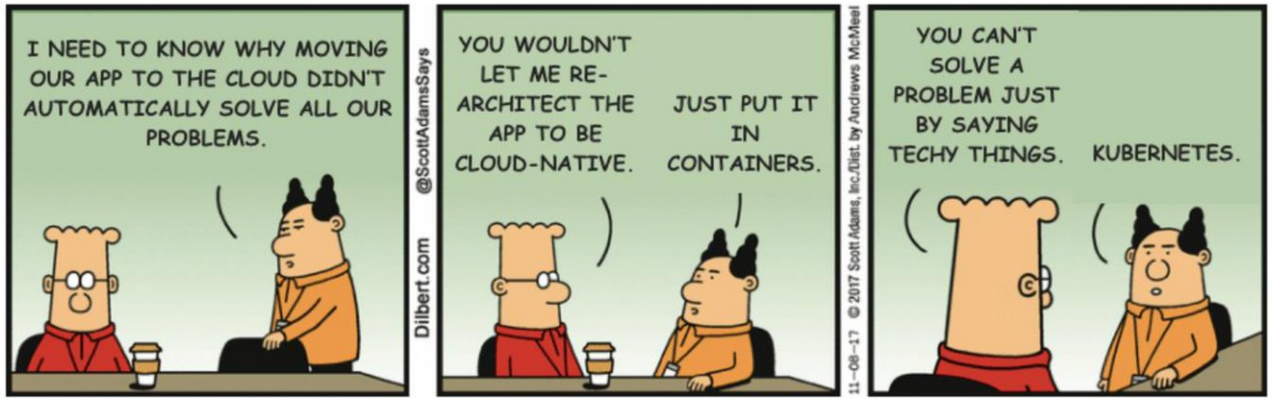
- **Version Control as Change Control:**
  - Use Git PRs as change mechanism
  - Store declarative configuration in Git repos
- **Pipelines as Change Deployment:**
  - Elimination of fat fingers
  - Focus less on process, more on delivery

What Solutions Exist?

ANSIBLE

CHEF

HashiCorp
Terraform



Issues

Why can’t we “just automate it”?

Most automation tools are
misaligned with our ***requirements***

Why Haven't We Automated?

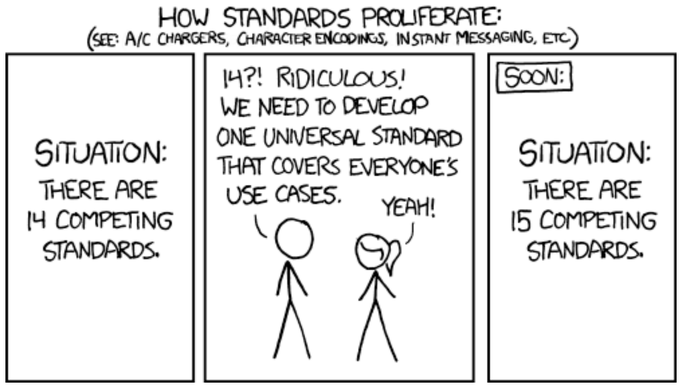
It's a conspiracy by big ASIC!

- **Vendors have Vested Interests:**
  - Vendors REALLY want you to use their automation solutions
  - Their solutions funnily enough require buy-in to their ecosystem
  - "Standards" like NETCONF are either ignored or subject to embrace-extend-extinguish
- **Integrated Generation and Deployment:**
  - Often, automation tools only resolve final configuration at the point of change
  - For network devices, we often want to know exact end-state prior to change

Why Haven't We Automated cont.

I blame the lizard people...

- **Network People with Dev Skills = 🦄:**
  - Finding the people with the skills to deploy and manage such systems is hard
  - Keeping them is even harder...
  - SysOps and Devs often have greater overlap so it's less problematic
- **Networking is a 2nd Class Citizen in Automation:**
  - Network support is often an afterthought, if implemented at all
- **It's just plain risky!**
  - If an automation system botches a host update, healthchecks will mark the node down
  - If an automation system botches a network update, BGP will mark your AS down!



Design

Can we do better?

In any design exercise, we need to define ***goals*** and ***constraints***

Goals

What do we ***want*** network automation to be?

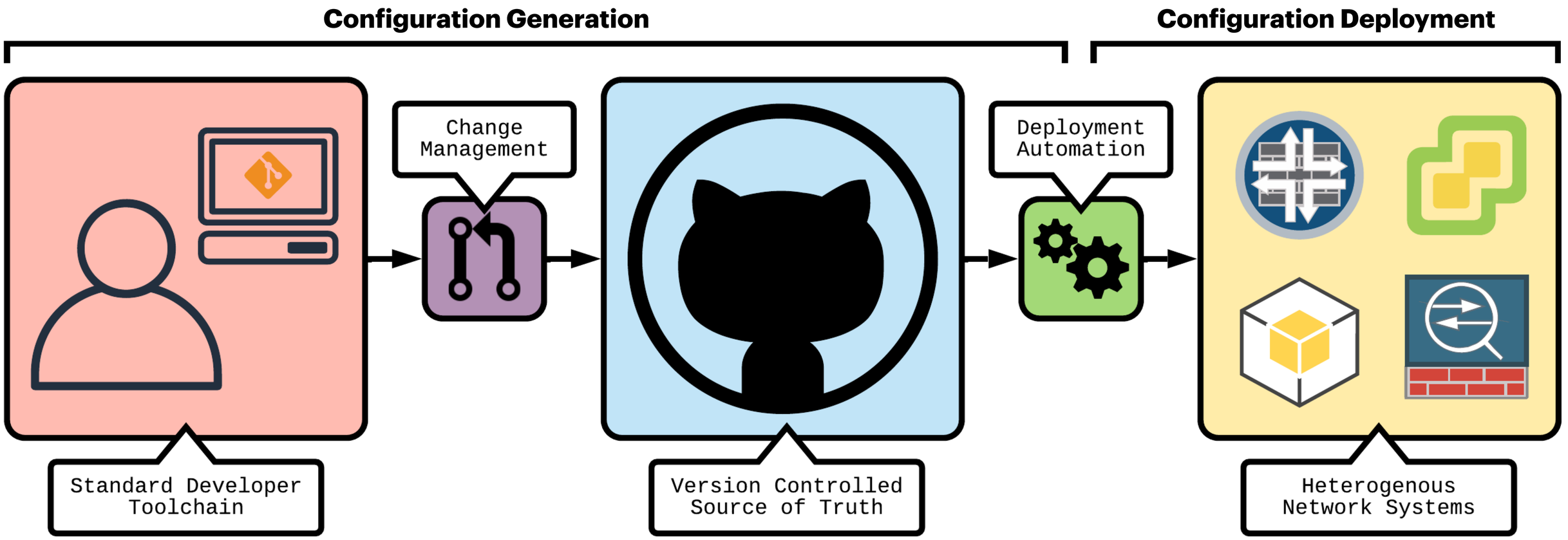
- **Idempotent:** The output should be the same when the input is the same
- **Descriptive:** The configuration intent should be clear from the source
- **Cross-platform:** It should support multiple device types/vendors/services
- **Modelled:** The source should model the intended state, not the path to it
- **Extensible:** Allow for integrations with custom data sources

Constraints

What does network automation ***need*** to be?

- **Simple:** You shouldn’t need a CompSci degree to author changes
- **Practical:** Cover the 95% case - less on exotic configuration
- **Decoupled:** Able to view actual configuration prior to deployment
- **Integrable:** Should be compatible with different deployment systems
- **Adoptable:** A pathway to allow users to slowly adopt the system

What does this look like?



Implementation

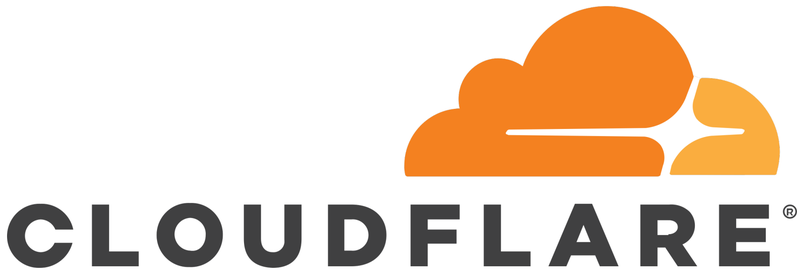
We CAN do better!

Why did you make *Hyron?*

The “Eureka” Moment

AKA: Updating ACLs is tedious

- I wanted only Cloudflare to talk to my EC2 instances on TCP 80/443
- Cloudflare can update it’s IP ranges at any time
- Cloudflare exposes an API to enumerate its current IP ranges
- I wanted to keep an EC2 SG in sync with CF



The Other Side of the Coin

AKA: Updating ACLs is unavoidable

Hey team,

Could you please implement the following firewall rules and revert to the same?

18.44.87.0/25 -> DMZ Network on TCP 443
OfficeNet -> OracleWeb on TCP 80
ANY -> DMZ on TCP 22

There will be additional requests coming today to support Cloud migration project.

Cheers,
Your Least Favourite Customer

Customer requests to change ACLs can be:

- **Ambiguous**
- **Insecure**
- **Frequent**
- **Wrong**

It Gets Even Better!

AKA: Humans suck at ACLs

- How many duplicate objects are in your corporate firewalls?
- When did you last audit/validate all your firewall rules?
- Do all your engineers adhere to the same naming standards?
- How many redundant rules do you have?
- If the customer asked for an ACL audit right now, could you deliver?

In short:

ACLs are something we ***need*** to manage,

but we really, really ***suck*** at it

What *Hyron* is not...

Have we seen this before?

Think again!

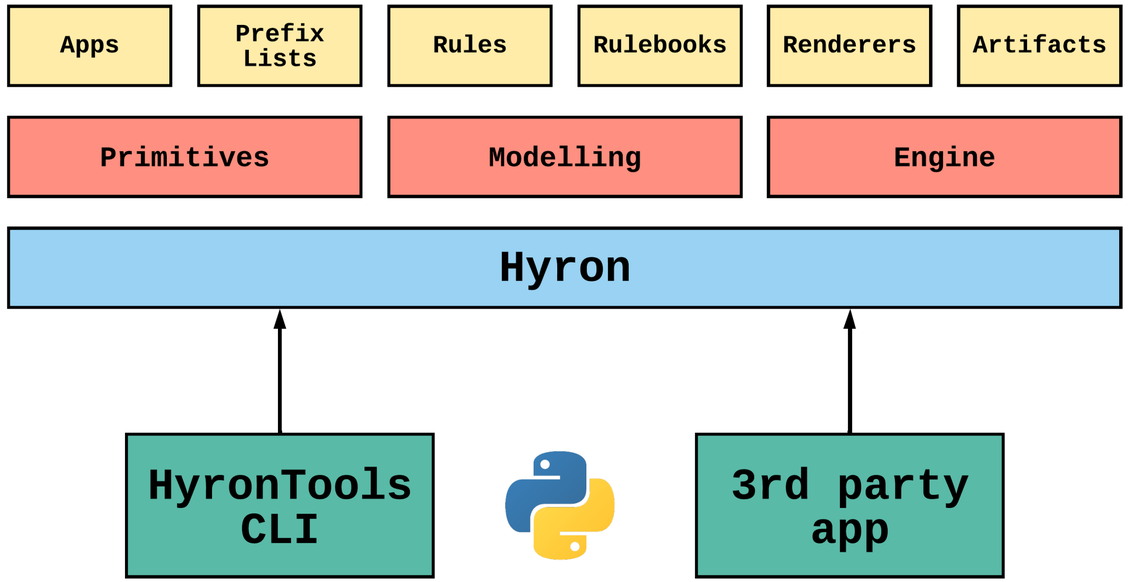
- Hyron is not **a templating engine**
- Hyron does not handle **deployment**
- Hyron is not **vendor-specific**
- Hyron is not a **proof-of-concept**
- Hyron is **not for sale**

So, what *is* this *Hyron* thing then?

Hyron from 10,000 Feet

What does automating ACLs look like?

- Hyron is a Python3 library - not a CLI tool
  - Try it yourself: `pip install hyron hyrontools`
- Hyron ***models*** ACLs before rendering them
  - This allows for intelligent inspection of rulesets
  - Currently supports prefix list deduplication
  - Planned support for redundant ACL detection
- Hyron can load prefix lists from remote sources
  - Built-in support for Cloudflare, Team Cymru Fullbogons
  - Supports region and service specific lists from AWS



What Does a Ruleset Look Like?

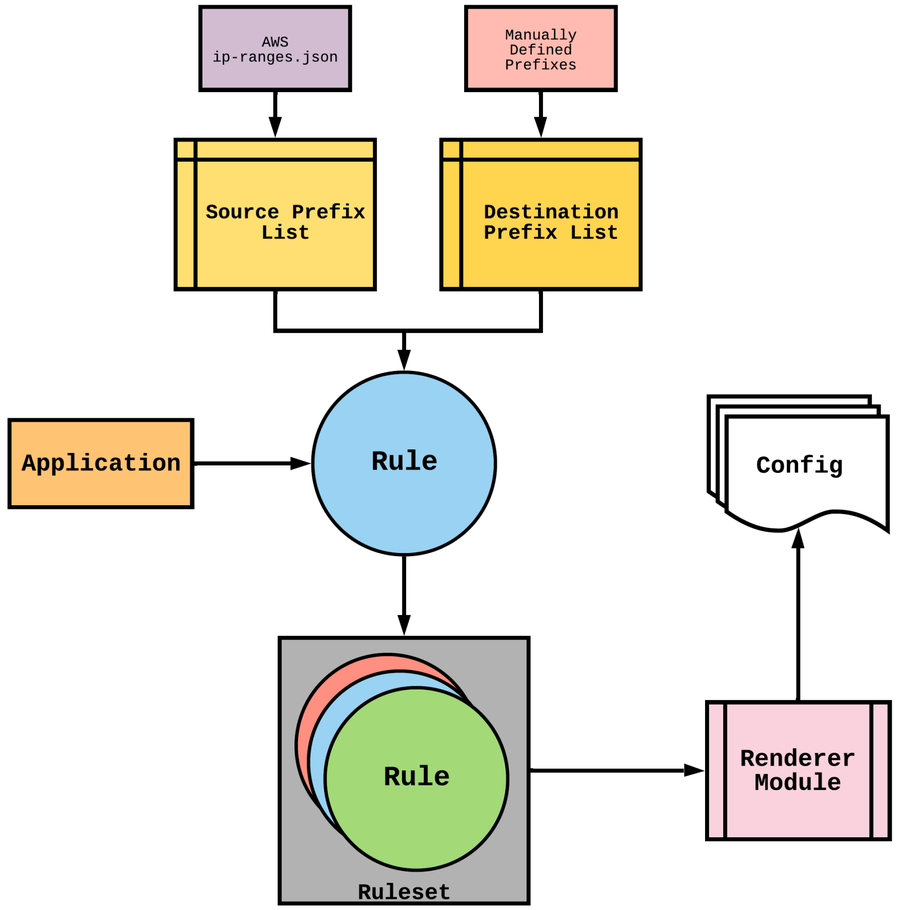
Yet another YAML DSL

```yaml
---
meta:
  title: Example
  owner: Jacob Neil Taylor
  import_builtin: true

objects:
  prefixlists:
    internal:
      type: static
      items:
        - 10.1.0.0/24
    dmz:
      type: static
      items:
        - 10.0.0.0/24

rules:
  permit-internet-access:
    src: internal
    dst: any
    app: any
    meta:
      jsrx_context: zonal
      jsrx_from_zones: inside
      jsrx_to_zones: outside
  permit-cloudflare-access:
    src: cloudflare
    dst: dmz
    app: https
    meta:
      jsrx_context: zonal
      jsrx_from_zones: outside
      jsrx_to_zones: dmz

artifacts:
  srxfwconf:
    meta:
      created: 26-02-2022
      apply_group: "HYRON_SECURITY_POLICY"
    files:
      config.txt:
        renderer: jsrx-cmd
        ruleset: example
        config:
          apply-group: "HYRON_SECURITY_POLICY"
```



What Does a Render Look Like?

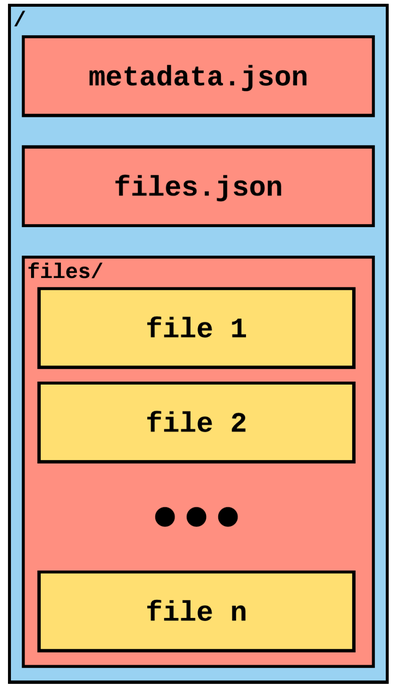
Game, set, match

```
delete groups HYRON_SECURITY_POLICY
set groups HYRON_SECURITY_POLICY security address-book global address pfx4-0.0.0.0-0 0.0.0.0/0
set groups HYRON_SECURITY_POLICY security address-book global address pfx4-10.0.0.0-24 10.0.0.0/24
set groups HYRON_SECURITY_POLICY security address-book global address pfx4-10.1.0.0-24 10.1.0.0/24
set groups HYRON_SECURITY_POLICY security address-book global address pfx4-103.21.244.0-22 103.21.244.0/22
... snip ...
set groups HYRON_SECURITY_POLICY security address-book global address pfx6-2c0f:f248::-32 2c0f:f248:0000:0000:0000:0000:0000:0000/32
set groups HYRON_SECURITY_POLICY security address-book global address pfx6-::-0 0000:0000:0000:0000:0000:0000:0000:0000/0
set groups HYRON_SECURITY_POLICY security address-book global address-set nets_any address pfx4-0.0.0.0-0
set groups HYRON_SECURITY_POLICY security address-book global address-set nets_any address pfx6-::-0
set groups HYRON_SECURITY_POLICY security address-book global address-set nets_cloudflare address pfx4-103.21.244.0-22
... snip ...
set groups HYRON_SECURITY_POLICY security address-book global address-set nets_cloudflare address pfx6-2c0f:f248::-32
set groups HYRON_SECURITY_POLICY security address-book global address-set nets_dmz address pfx4-10.0.0.0-24
set groups HYRON_SECURITY_POLICY security address-book global address-set nets_internal address pfx4-10.1.0.0-24
set groups HYRON_SECURITY_POLICY security policies from-zone inside to-zone outside policy inside_outside_1 match source-address nets_internal
set groups HYRON_SECURITY_POLICY security policies from-zone inside to-zone outside policy inside_outside_1 match destination-address nets_any
set groups HYRON_SECURITY_POLICY security policies from-zone inside to-zone outside policy inside_outside_1 match application junos-tcp-any
set groups HYRON_SECURITY_POLICY security policies from-zone inside to-zone outside policy inside_outside_1 match application junos-udp-any
set groups HYRON_SECURITY_POLICY security policies from-zone inside to-zone outside policy inside_outside_1 then permit
set groups HYRON_SECURITY_POLICY security policies from-zone outside to-zone dmz policy outside_dmz_1 match source-address nets_cloudflare
set groups HYRON_SECURITY_POLICY security policies from-zone outside to-zone dmz policy outside_dmz_1 match destination-address nets_dmz
set groups HYRON_SECURITY_POLICY security policies from-zone outside to-zone dmz policy outside_dmz_1 match application junos-https
set groups HYRON_SECURITY_POLICY security policies from-zone outside to-zone dmz policy outside_dmz_1 then permit
set apply-groups HYRON_SECURITY_POLICY
```

Deployment Artifacts

How do we “compile” configuration?

- Each target is different, so how can we remain independent?
- Put everything in a ZIP file!
- Metadata is needed for deployment systems
- Allows for comparison between packages



How do we actually *deploy* though?

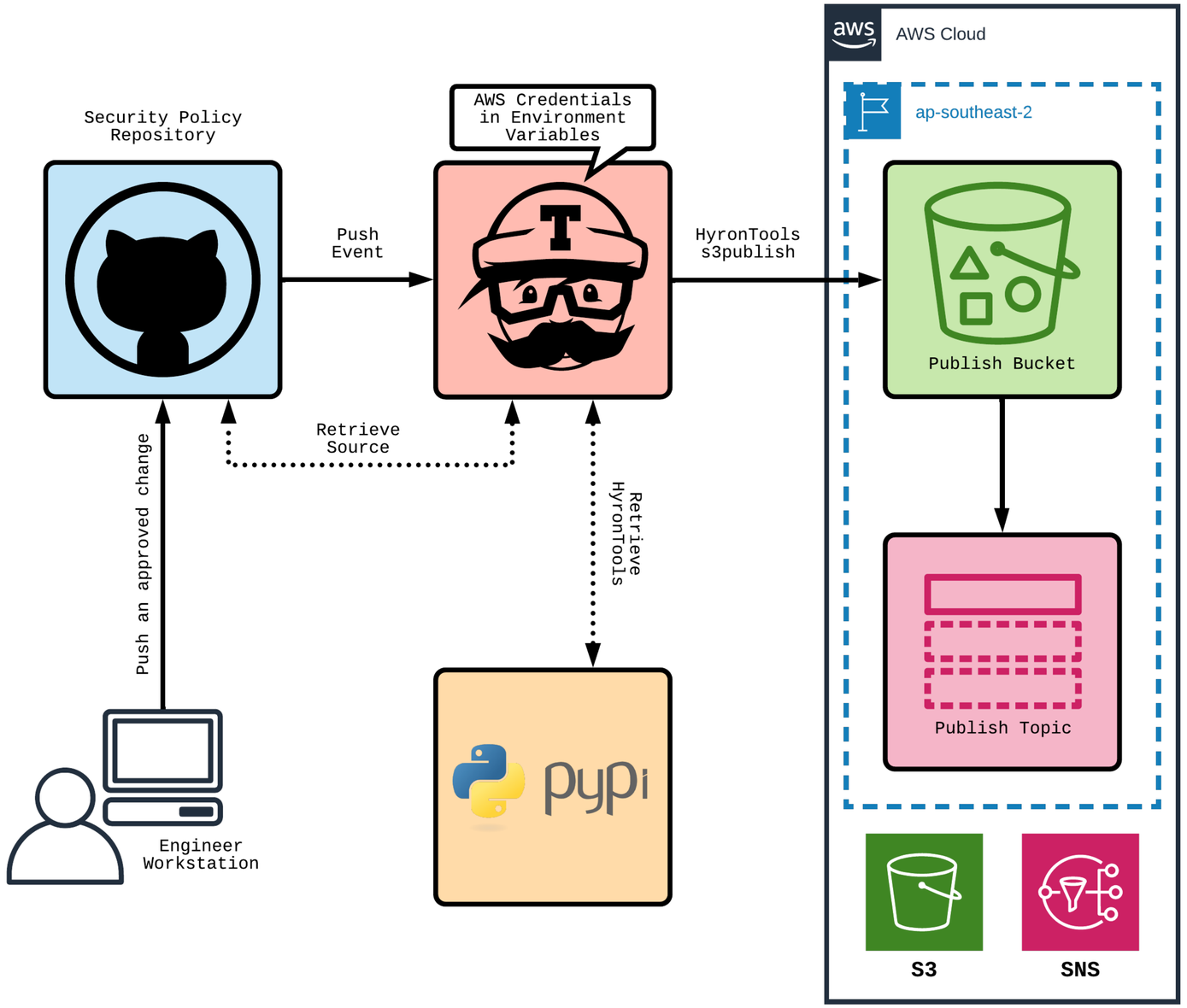
It’s up to you!

Cassan

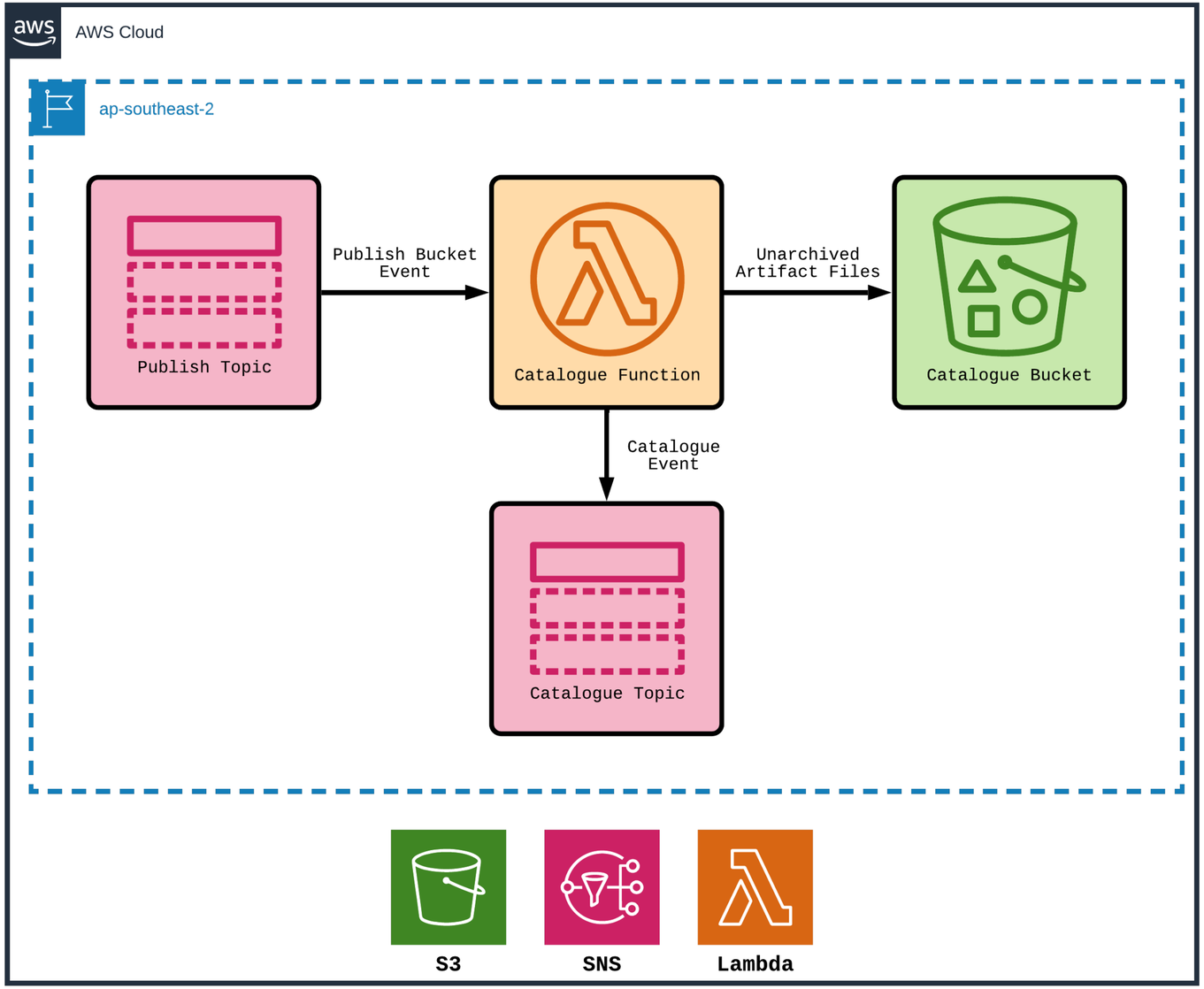
What does deploying ACLs look like?

- There is an existing deployment system in place
  - It’s called Cassan
  - It’s an MDP - Minimum Demonstrable Product
- Serverless solution based on AWS Lambda/S3
- Absolutely not ready for Prod
  - Needs features like deployment windows/scheduling

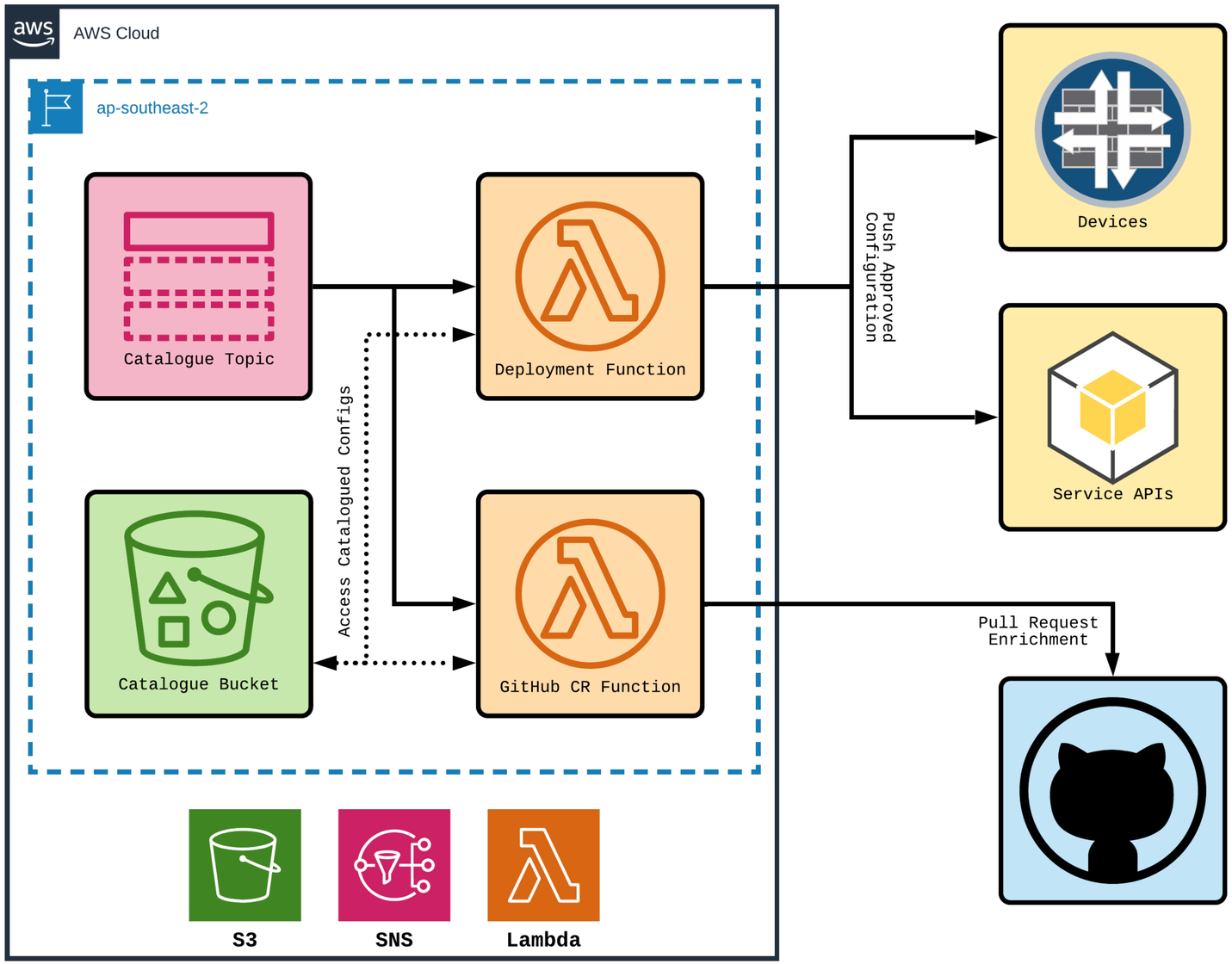
Generation


Security Policy
Repository
AWS Credentials
in Environment
Variables
Push
Event
HyronTools
s3publish
AWS Cloud
ap-southeast-2
Publish Bucket
Retrieve
Source
Push an approved change
Retrieve
HyronTools
Publish Topic
Engineer
Workstation
pypi
S3
SNS

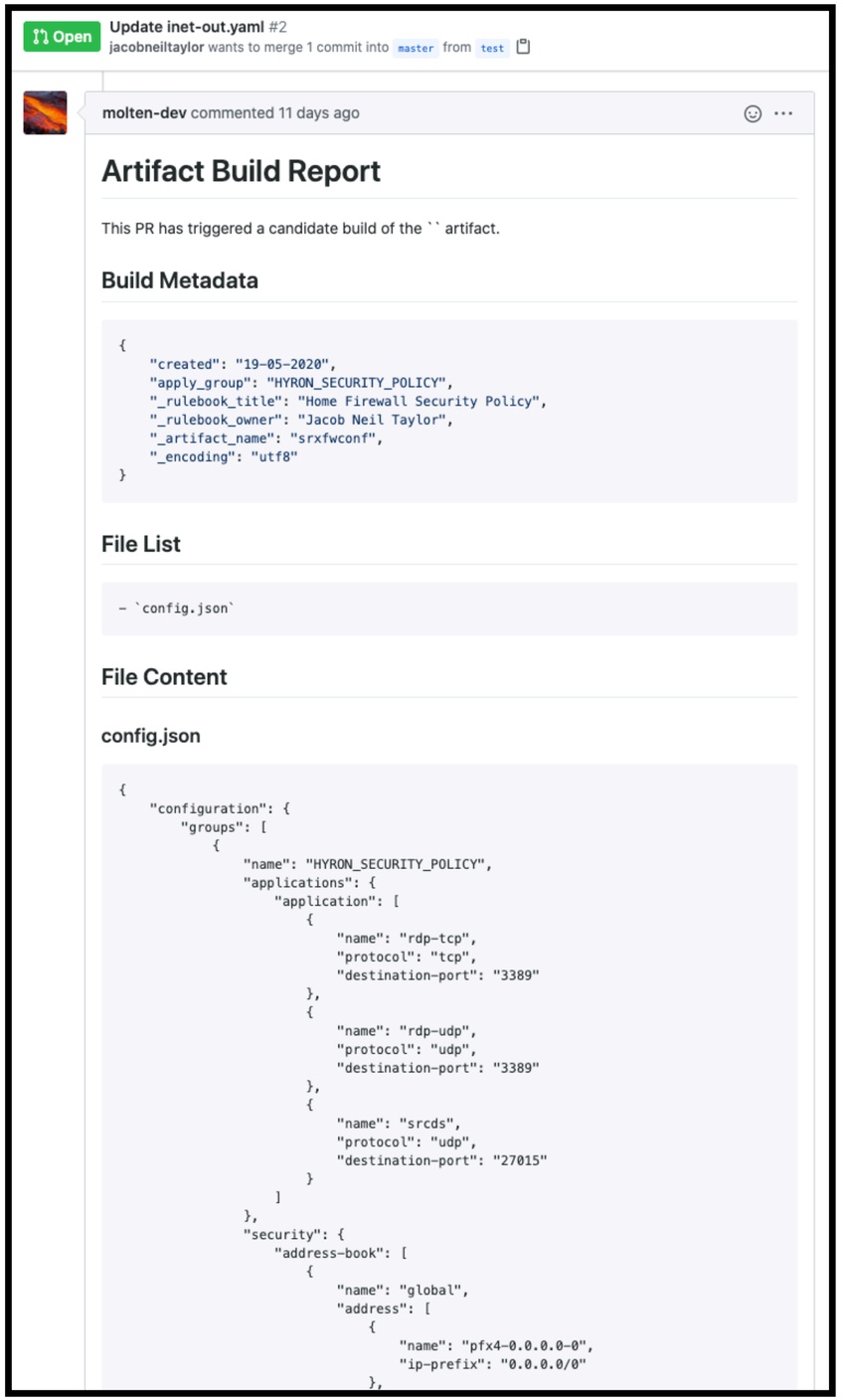
Ingest


AWS Cloud
ap-southeast-2
Publish Topic
Publish Bucket Event
Catalogue Function
Unarchived Artifact Files
Catalogue Bucket
Catalogue Event
Catalogue Topic
S3
SNS
Lambda

Deployment


AWS Cloud
ap-southeast-2
Catalogue Topic
Deployment Function
Catalogue Bucket
GitHub CR Function
Access Catalogued Configs
Push Approved Configuration
Devices
Service APIs
Pull Request Enrichment
S3
SNS
Lambda

PR Enrichment



Open **Update inet-out.yaml** #2

jacobneiltaylor wants to merge 1 commit into `master` from `test`

molten-dev commented 11 days ago

Artifact Build Report

This PR has triggered a candidate build of the `` artifact.

Build Metadata

```
{
    "created": "19-05-2020",
    "apply_group": "HYRON_SECURITY_POLICY",
    "_rulebook_title": "Home Firewall Security Policy",
    "_rulebook_owner": "Jacob Neil Taylor",
    "_artifact_name": "srxfwconf",
    "_encoding": "utf8"
}
```

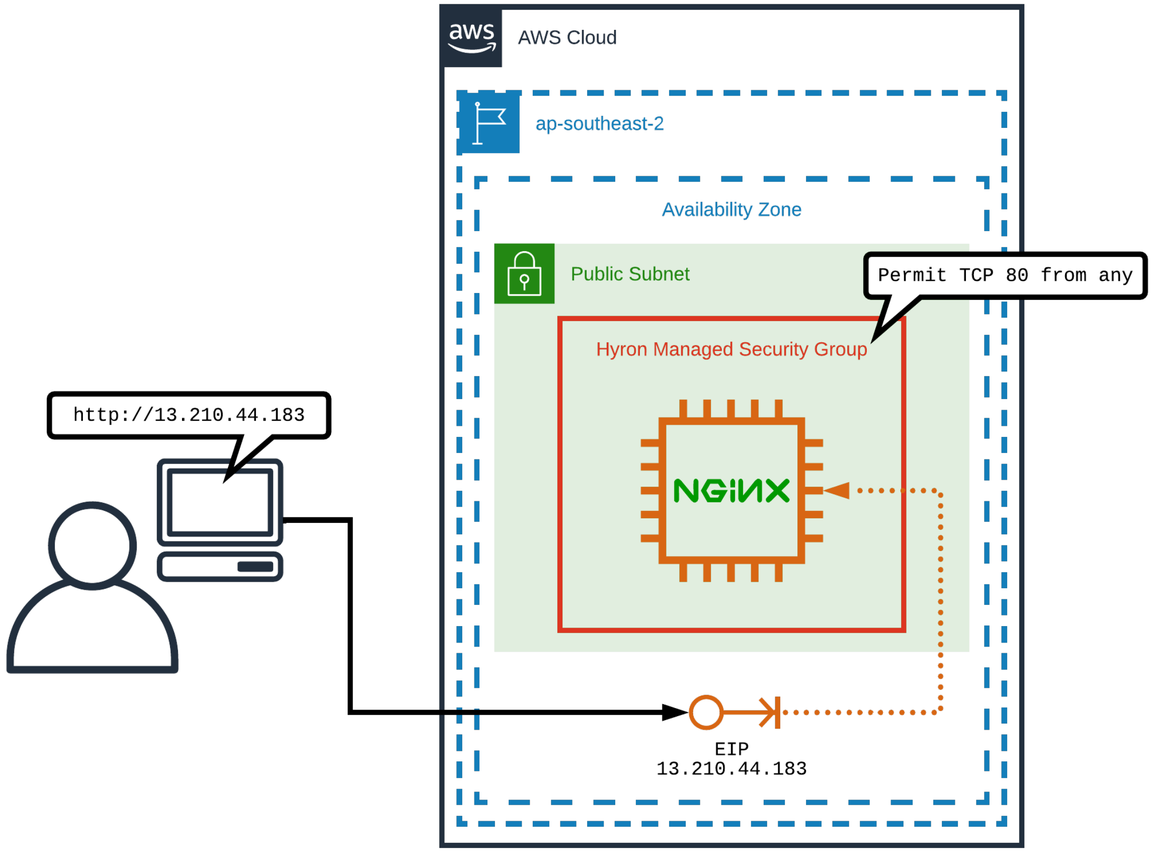
File List

```
- `config.json`
```

File Content

config.json

```
{
    "configuration": {
        "groups": [
            {
                "name": "HYRON_SECURITY_POLICY",
                "applications": {
                    "application": [
                        {
                            "name": "rdp-tcp",
                            "protocol": "tcp",
                            "destination-port": "3389"
                        },
                        {
                            "name": "rdp-udp",
                            "protocol": "udp",
                            "destination-port": "3389"
                        },
                        {
                            "name": "srcds",
                            "protocol": "udp",
                            "destination-port": "27015"
                        }
                    ]
                },
                "security": {
                    "address-book": [
                        {
                            "name": "global",
                            "address": [
                                {
                                    "name": "pfx4-0.0.0.0-0",
                                    "ip-prefix": "0.0.0.0/0"
                                },
```



Demonstration

Do you believe in magic?

Join us @ Atlassian

AKA manager-initiated plea for candidates

Any questions?