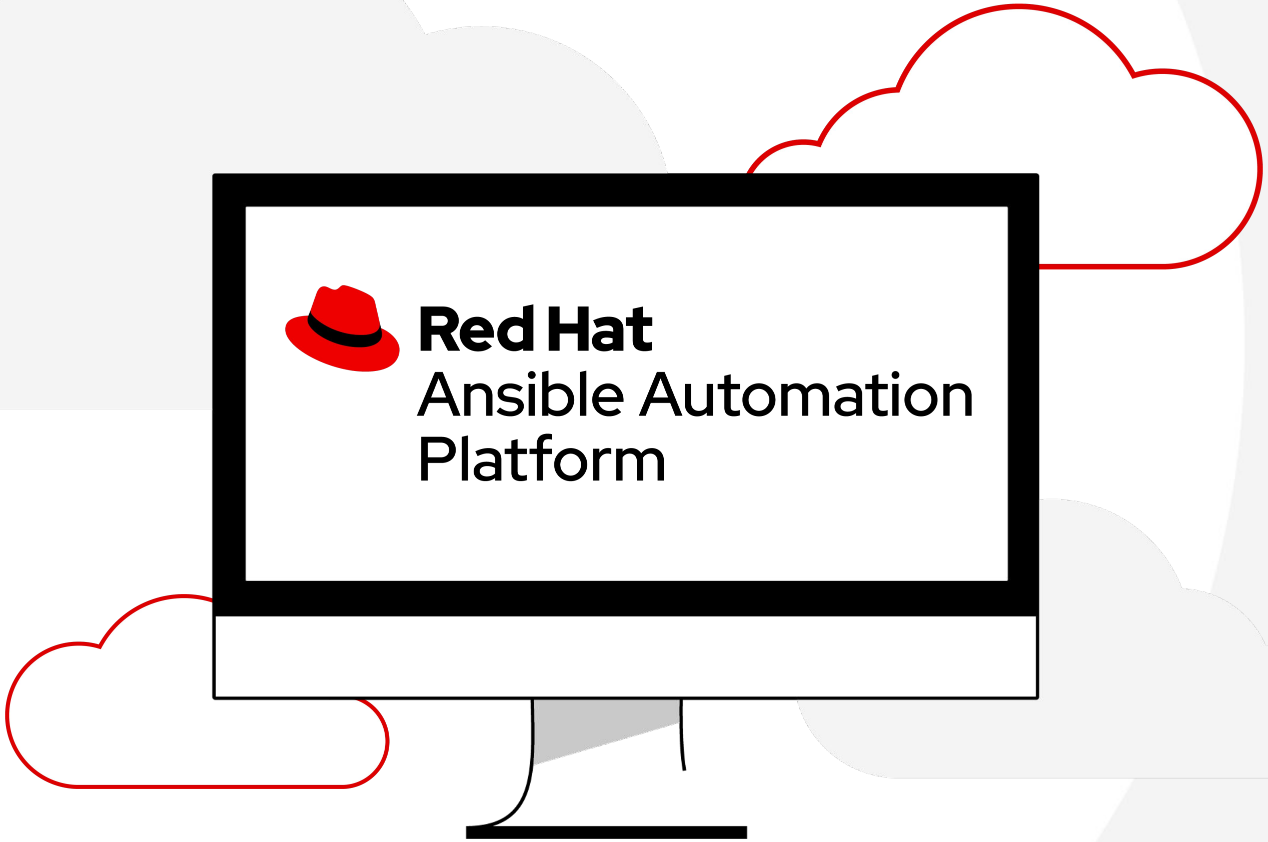
Red Hat
Ansible Automation
Platform

Ansible Contributor Summit 2021

Ansible security automation

Sumit Jaiswal
Principal Software Engineer
Ansible Content team

Craig Brandt
Principal Technical Marketing Manager
Ansible Automation Platform



What we’ll discuss...

- What is Ansible security automation?
- Introducing Ansible firewall policy automation
- Resource module basics
- Use-cases and examples
- Ansible security roadmap

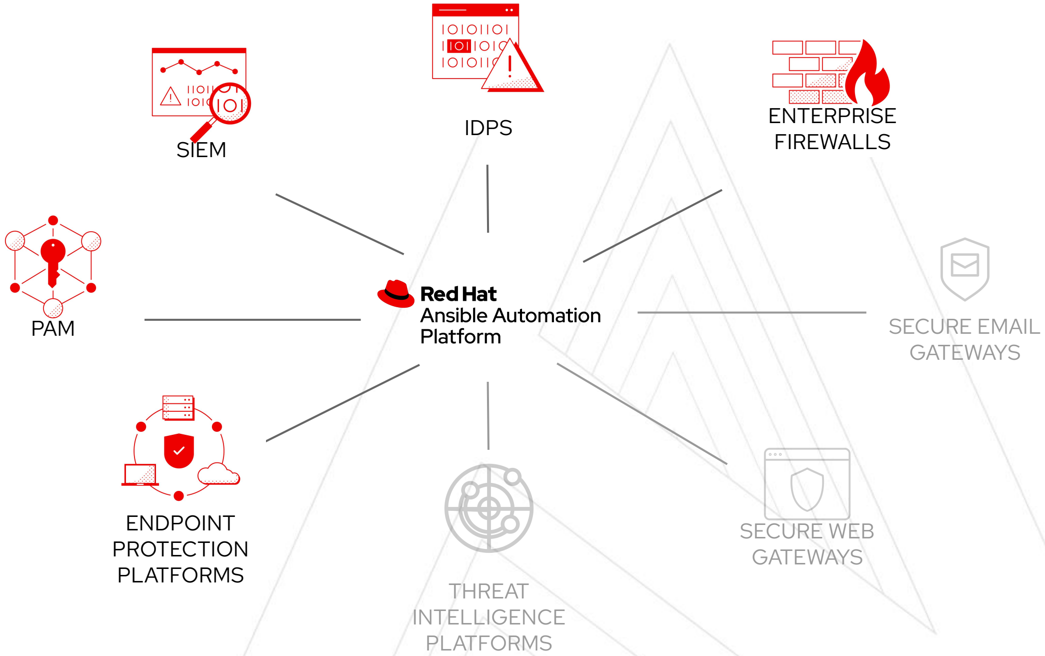
Ansible security automation

Red Hat
Ansible Automation
Platform

What is Ansible security automation?

Orchestrate threat response across domains

- Expansion of Ansible as the Enterprise automation platform
- Integrates & orchestrates multiple classes of security solutions
- Provides modules, roles, collections and playbooks to support security use cases across those solutions
- NOT a security solution


SIEM
IDPS
ENTERPRISE FIREWALLS
PAM
Red Hat Ansible Automation Platform
SECURE EMAIL GATEWAYS
ENDPOINT PROTECTION PLATFORMS
THREAT INTELLIGENCE PLATFORMS
SECURE WEB GATEWAYS

Red Hat
Ansible Automation Platform

What Does It Do?

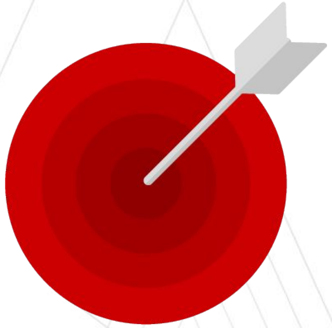
Ansible security automation use-cases

Investigation Enrichment

Enabling programmatic access to log configurations such as destination, verbosity, etc.

Threat Hunting

Automate alerts, correlation searches and signature manipulation to preemptively identify threats

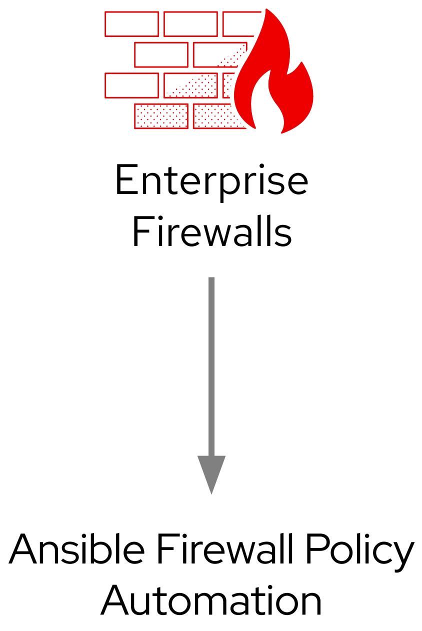


Incident Response

Creating new security policies to grant access, block or quarantine a machine

Ansible firewall policy automation

Expanding on Ansible security automation use-cases



Enterprise Firewalls

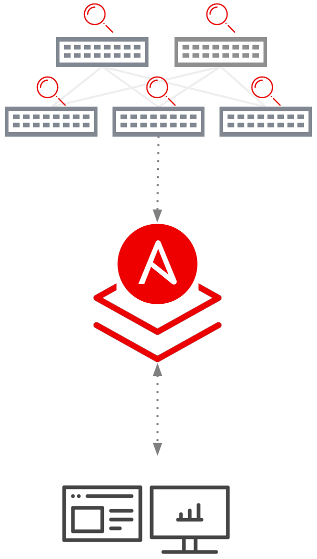
Ansible Firewall Policy Automation

Ansible firewall policy automation

Red Hat
Ansible Automation
Platform

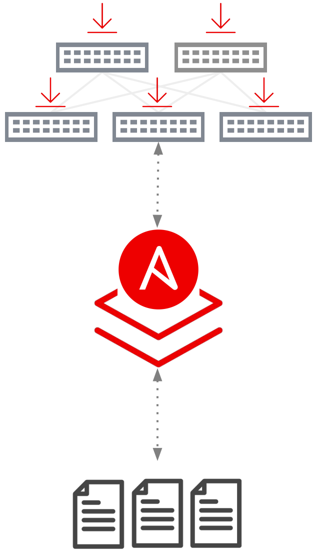
Firewall policy automation use-cases

Relevant throughout your automation journey



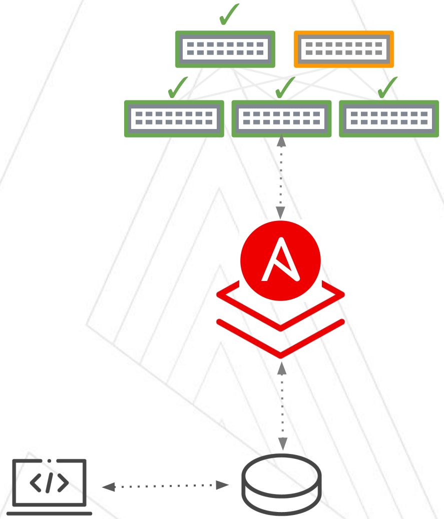
Policy visibility

- Read-only, no production config change
- Dynamic documentation and reporting
- Identify policy misconfigurations
- Create remediation plan



Policy hygiene

- Desired state policy definitions
- Single source of truth concepts
- Multi-vendor and multi-region
- Execute remediation plan



Policy life-cycle management

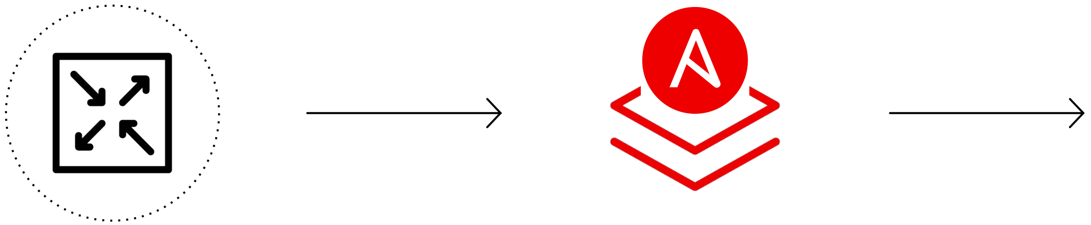
- Policy validation
- Event-driven enforcement (IaaC)
- Integration into security response plan
- SecOps

Ansible Resource Modules and Firewall policy automation examples

Red Hat
Ansible Automation
Platform

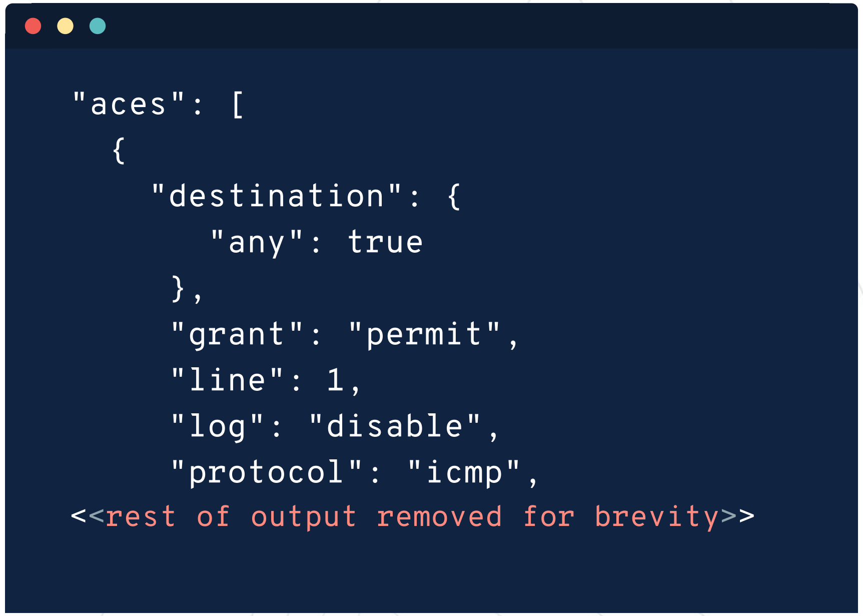
Resource modules

Firewall policy automation begins and ends with facts



Firewall native configuration

Convert to structured data

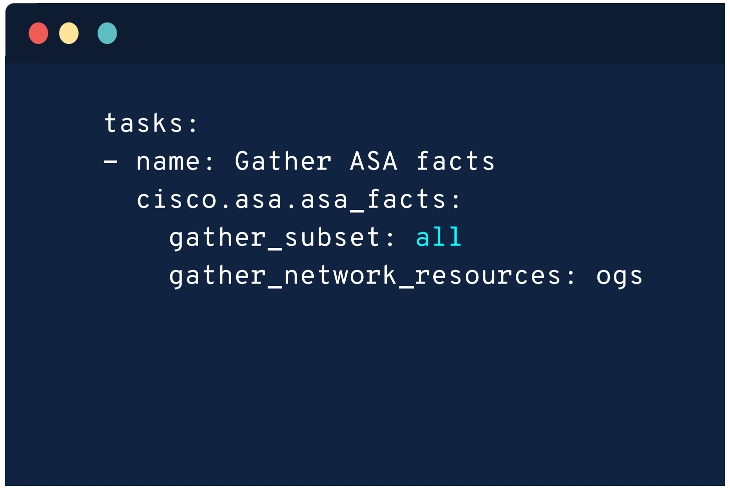


```
"aces": [
  {
    "destination": {
       "any": true
     },
     "grant": "permit",
     "line": 1,
     "log": "disable",
     "protocol": "icmp",
<<rest of output removed for brevity>>
```

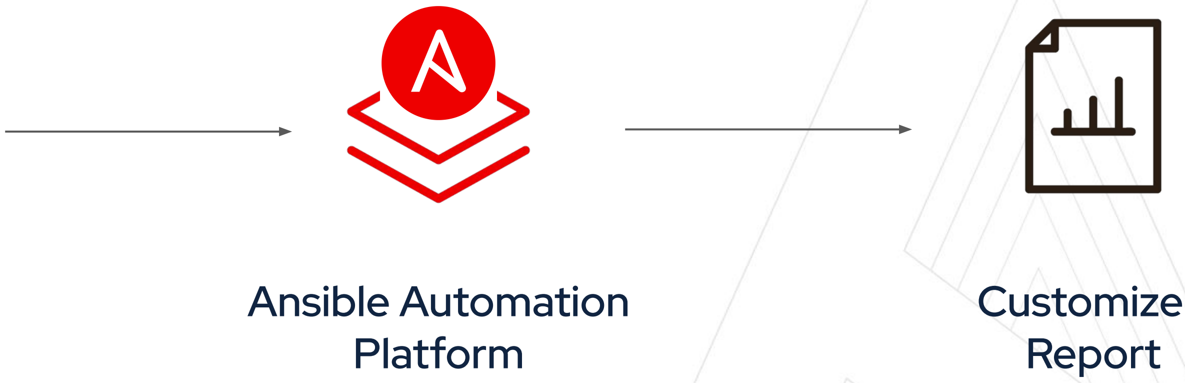
`Gathered` - no changes
`Merged` - add/increment
`Replaced` - template/diff
`Overridden` - force/policy
`Deleted` - destroy/remediate

Firewall policy visibility

Data output is flexible



```
tasks:
- name: Gather ASA facts
  cisco.asa.asa_facts:
    gather_subset: all
    gather_network_resources: ogs
```



Ansible Automation Platform

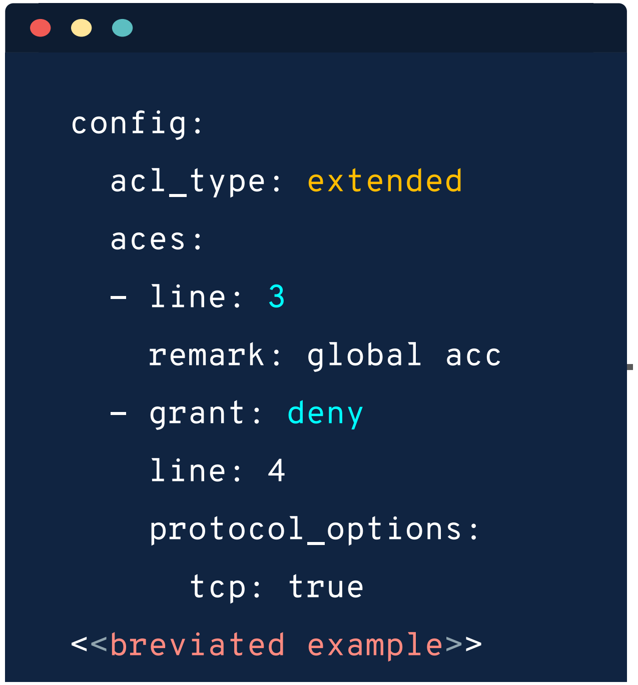
Customized Report

State:

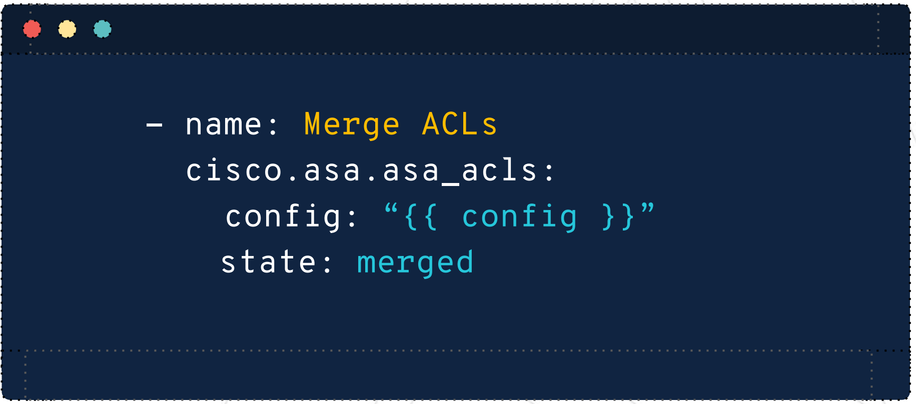
`Gathered` - Current policy state

Firewall policy hygiene

Managing firewall policy state - practical example using module



```
config:
  acl_type: extended
  aces:
  - line: 3
    remark: global acc
  - grant: deny
    line: 4
    protocol_options:
      tcp: true
<<breviated example>>
```



```
- name: Merge ACLs
  cisco.asa.asa_acls:
    config: “{{ config }}”
    state: merged
```

State:

`Merged` - add/increment

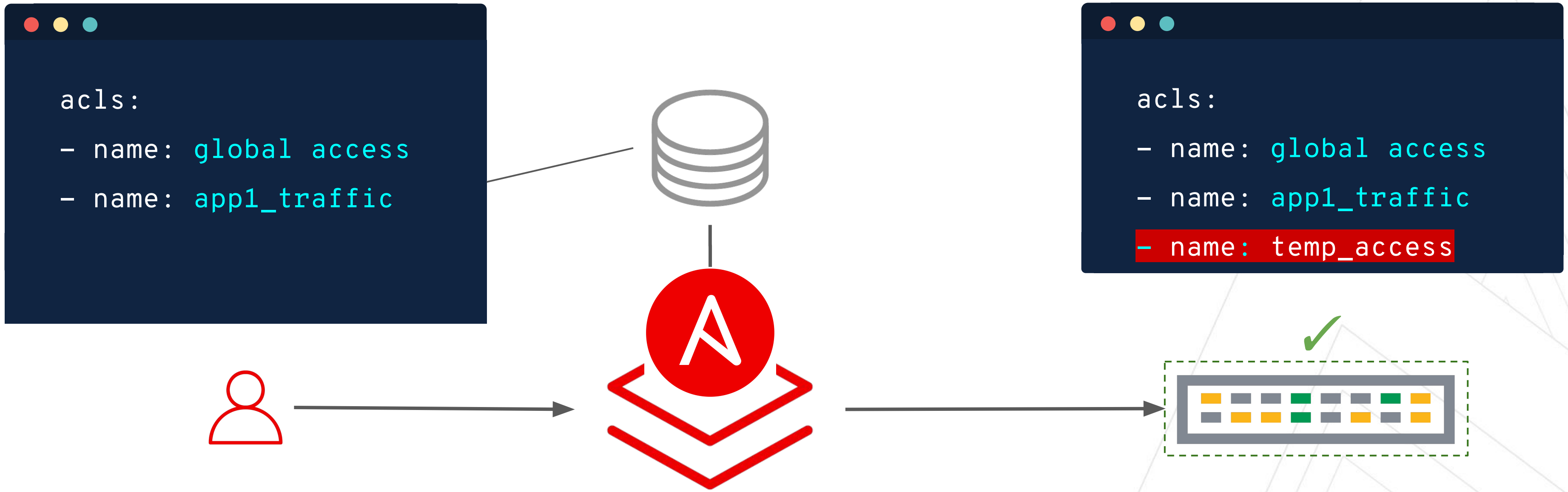
`Replaced` - template/diff

Firewall policy life-cycle management

Keep your firewall policies in the desired state

Source Of Truth

Running Configuration



```
acls:
- name: global access
- name: app1_traffic
```

```
acls:
- name: global access
- name: app1_traffic
- name: temp_access
```

Ansible Automation Platform

State:

`Replaced` - template/diff

`Overridden` - force/policy

Ansible Security Roadmap

https://github.com/ansible/community/wiki/Security-Automation

Red Hat
Ansible Automation
Platform

Thank you

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat