Cisco live!
February 20 - 24, 2017 · Berlin

cisco

Your Time Is Now

Configuration Compliance Management with Prime Infrastructure

Gilles Clugnac – Technical Leader

BRKNMS 2036

Cisco live!

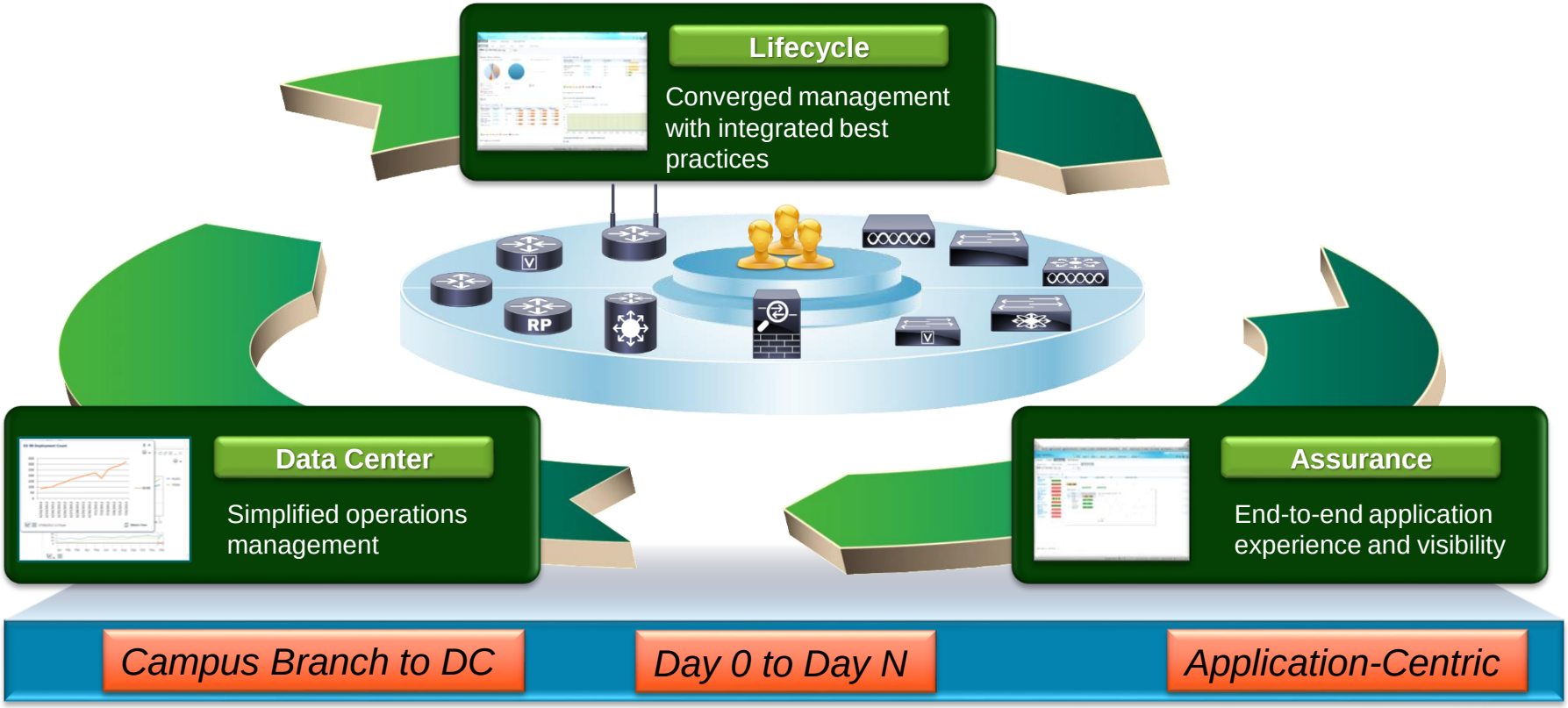
Agenda

- Introduction
- Prime Infrastructure Compliance Engine Concepts
- Getting started with compliance
- More realistic use cases
- Conclusion

Introduction

Cisco Prime Infrastructure

Realizing the Vision of One Management

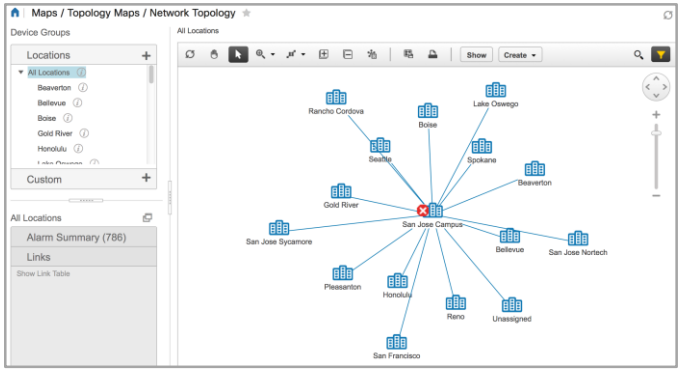


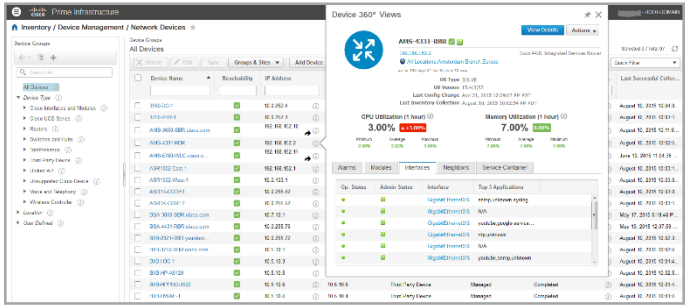
Enterprise Management (1 of

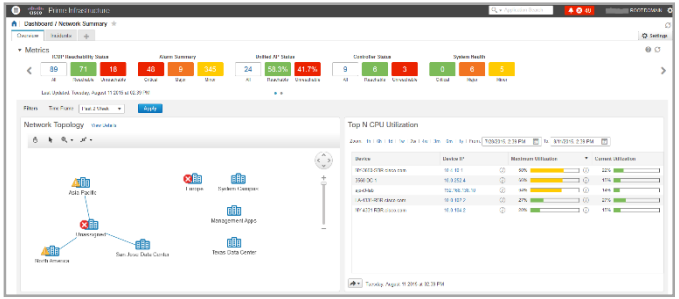
End-to-End Lifecycle Management

Lifecycle

- **Centralized lifecycle management** - discovery, inventory, configuration, SWIM, and proactive/reactive monitoring
- **Compliance Baseline**- Audit device configurations
- **Advanced troubleshooting** of wired and wireless infrastructure issues
- **Rapid device** support through Device Packs for new Cisco® devices, routers, switches, controllers, access points, Nexus® technology, and more
- **Customizable configuration templates** based on Cisco validated designs and guided workflows, including IWAN support
- **Cisco Unified Access™ management and client tracking**
  - Seamless integration with Cisco Identity Services Engine (ISE) for simplified troubleshooting
  - Seamless integration with Cisco Mobility Services Engine (MSE) for location-based services, rogue detection, etc.





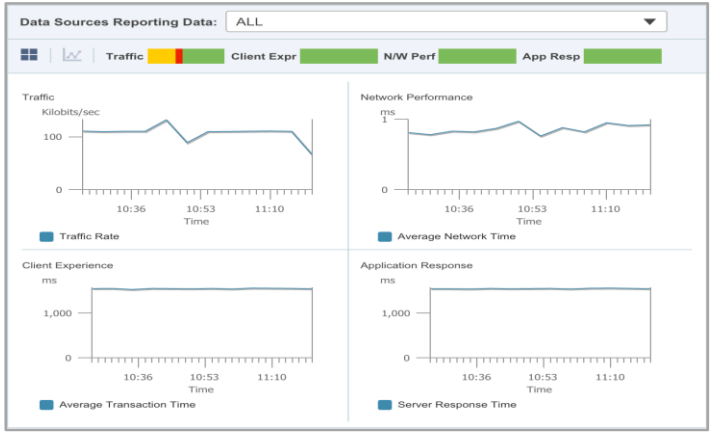


Enterprise Management (2 of 2)

Application Experience and End User Experience

Assurance

- **End-to-end visibility** for service-aware networking by applications, services, and end users
- **Out-of-the-box support** for Cisco® advanced technologies, including AVC , NetFlow, Flexible NetFlow, NBAR2, Performance Agent, Medianet, and more
- **Service health dashboard** allows quick health check on your business-critical applications
- **Simplified troubleshooting** of applications and client access issues
- **QoS Configuration / Monitoring** applied to and class-based traffic patterns
- **Multi-NAM management**
  - Traffic analysis
  - Application response time metrics
  - Packet capture and decode

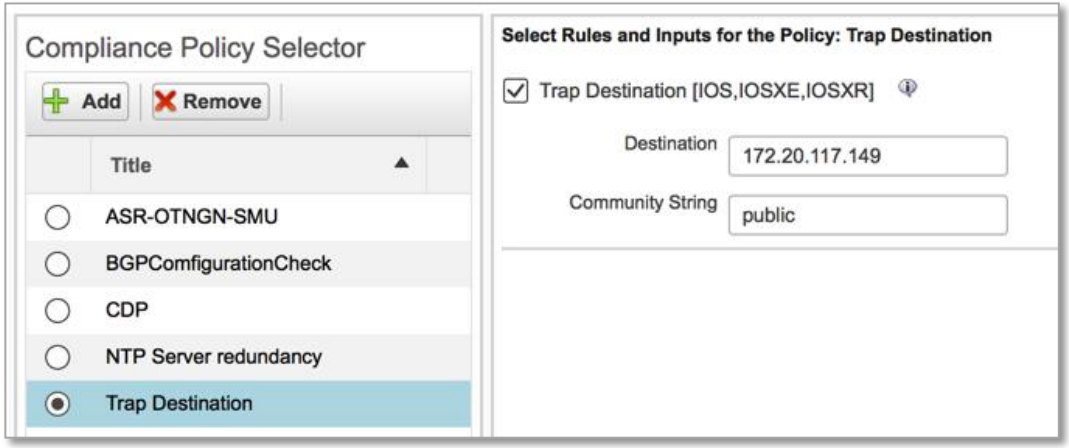


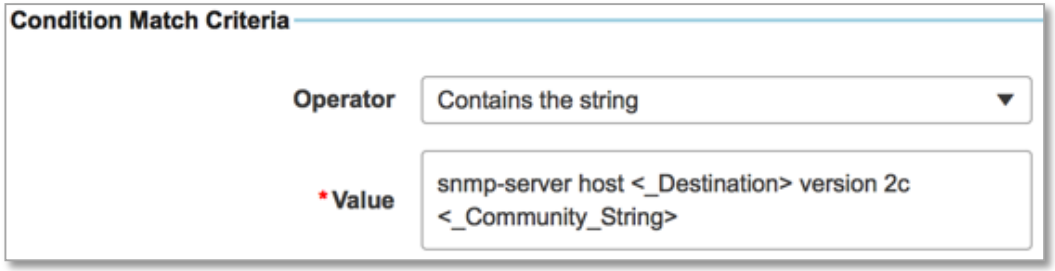
Site	telnet	http	snmp	rtp	cisco-jabber-control	cisco-jabber-audio
Asia Pacific	✓	✓	✗	✓	✓	✓
Europe	✓	✓	✓	✓	✓	✓
Management Apps	⚠	✗	✗	✓	✓	✓
North America	✗	⚠	✗	✗	✓	✓
San Jose Data Center	⚠	✓	✓	✓	✓	✓
Texas Data Center	✓	✗	✗	✗	✓	✓
Unassigned	✓	✗	✗	✗	✓	⊘

Compliance

- Audit the configuration of devices to assess compliance with baseline policies
- Predefined library of policies for best practices audit
- User defined policies

Configuration Baseline Compliance





- Introduced in Prime Infrastructure 3.0
- Define configuration baseline policies
- Perform compliance audits
- View compliance audit violations
- Option to fix violations
- Support for IOS, IOS-XE, IOS-XR, NXOS, AireOS* and ASA devices
- Gen2 Appliance or Standard** OVA required

** 3.1 ** 3.1 MR3*

Prime Infrastructure Compliance Engine Concepts

Compliance Conceptual Model

Policies

Define granular “per-feature” level compliance rules

Profiles

Aggregate multiple compliance policies into larger sets of policies

Used when performing compliance **audits**

Jobs

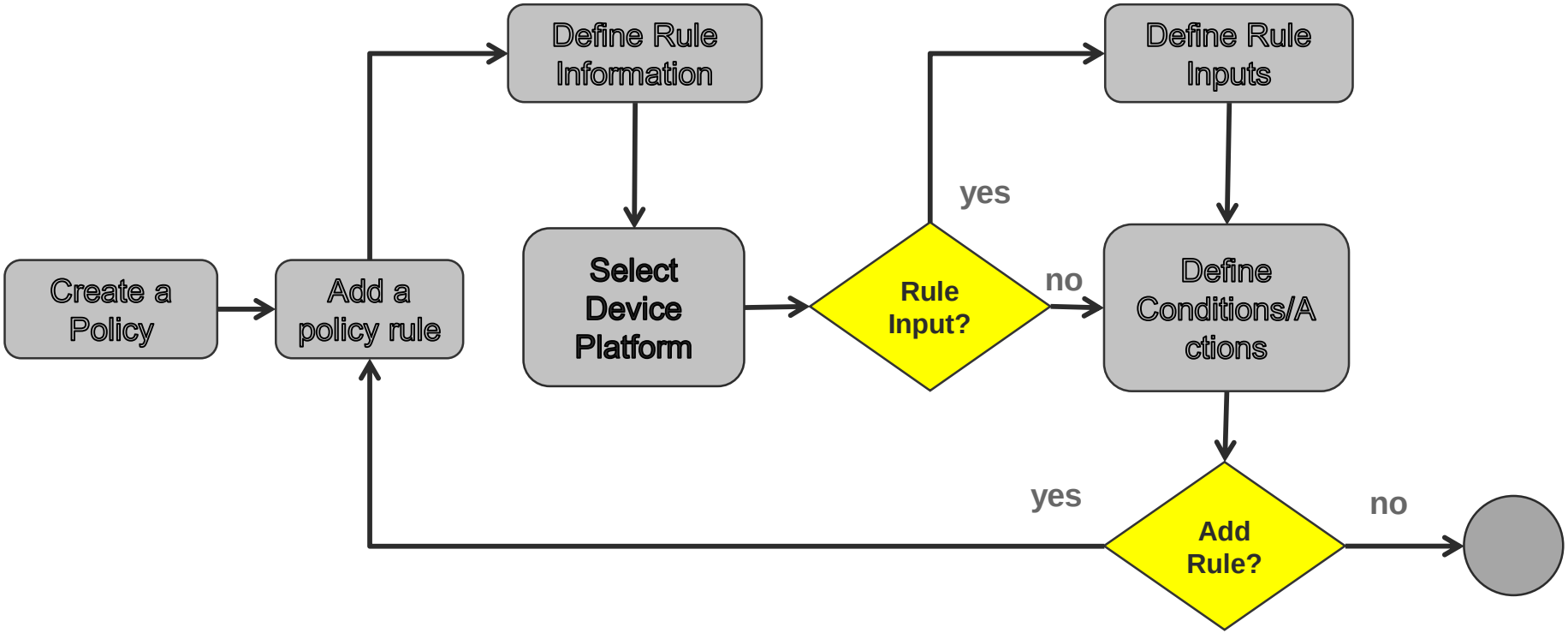
Maps a specific profile against a specific set of network devices

Perform compliance audits to detect compliance **violations**

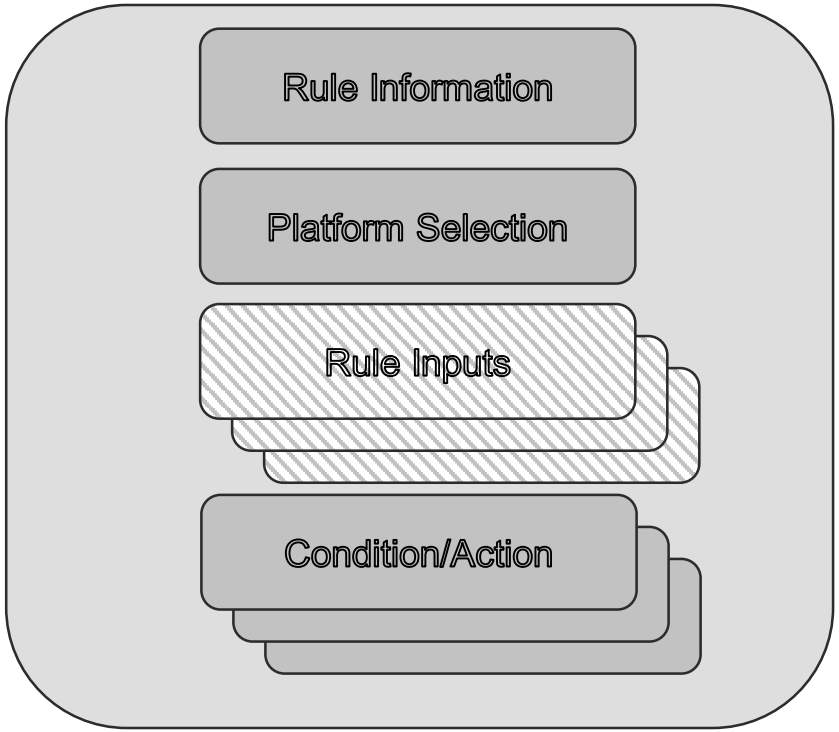
Compliance Process Overview

1. Configure Compliance Policies which contain Policy Rules
2. Configure a Compliance Profile which contains system provided and/or user defined Policies
3. Run Compliance Audit
4. Evaluate audit result
5. Based on results, make correction by running a fix job
6. Re-run the audit to validate

Summary of a Compliance Policy definition flow

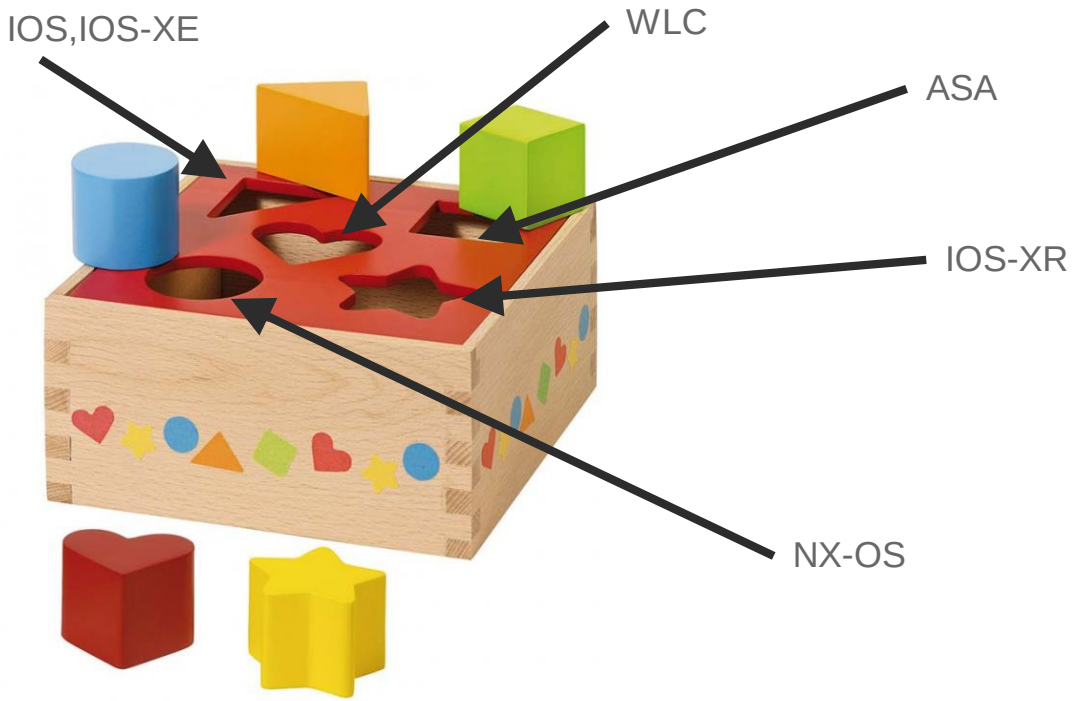


contains



- **Rule Information** – Name, Description, Impact, Suggested Fix
- **Platform Selection** – IOS, IOS-XE, IOS-XR, NXOS, ASA,AireOS
- **Rule Inputs** (optional) – string, IP address, boolean, etc
- **Conditions** and **Actions** – 1 or more (ordered list)

Platform Selection

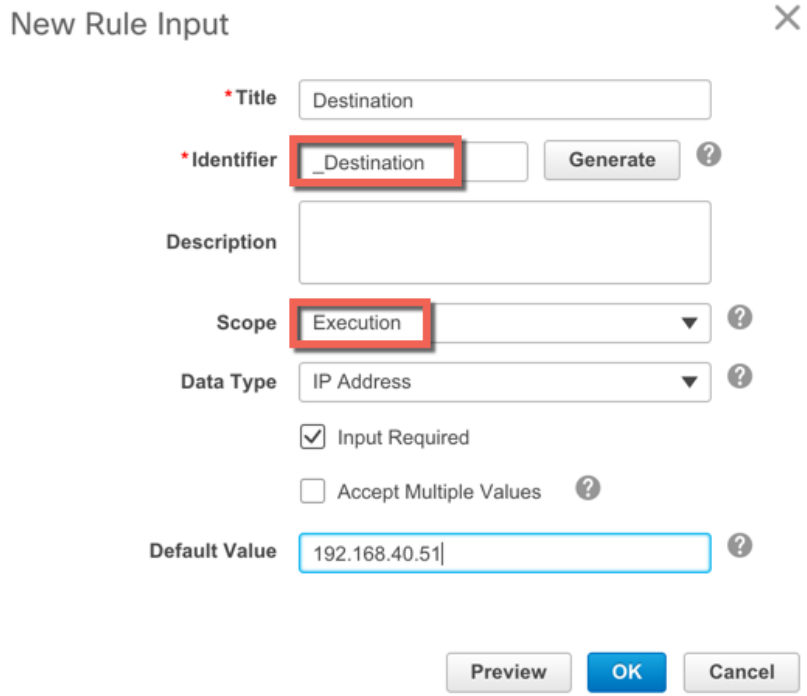


A single Policy with multiple rules for different platforms

Devices will be audited only with the policies matching their platform type

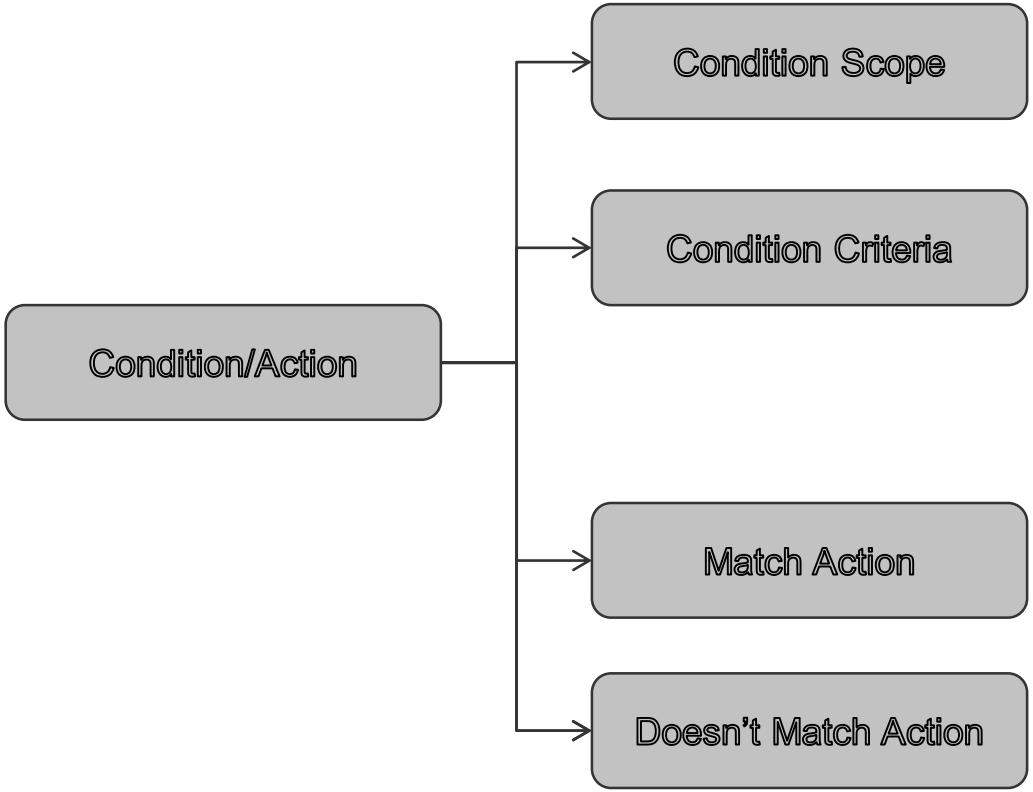
Rule Inputs

Parameters provided to a rule



- Identifier used in :
  - Condition match
  - Message
  - Fix CLI
- Scope can be:
  - Execution
  - Fix

A rule contains one or more Condition/Action



Regex survival kit : the minimum to understand this presentation (1/2)

- . : matches any character except newline
- * : any repetition. Example .* : matches any character, any repetition
- ^ : starts with
- $: ends with
- (exp) : when matches, creates a **capture a group** which can be reused in a **back reference**
- *<x.y> : uses a back reference: x = condition number of the capture group, y = capture group number in the condition*

Regex survival kit : the minimum to understand this presentation (2/2)

- (st1|st2) : match of st1 or st2 with capture
- \n : new line
- \s : space or tab
- \S : any character except space, tab or new line
- \d : digit

Regex survival kit : the minimum to understand this presentation (2/2)

PCRE

```
/ ^\s*((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa /
  -f]{1,4}|((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-
  9][0-9]|[1-9]?[0-9])){3})|:))|(([0-9A-Fa-f]{1,4}:){5}((:[0-9A-Fa-f]{1,4}){1,2})|:(
  (25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1
  -9]?[0-9])){3})|:))|(([0-9A-Fa-f]{1,4}:){4}((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-
  f]{1,4})?:((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0
  -9][0-9]|[1-9]?[0-9])){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}((:[0-9A-Fa-f]{1,4}){1,4})|
  ((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])(\.(25[0-5]
  |2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}((:[0-9A-Fa
  -f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[
  0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])){3}))|:))|(([0-9A-Fa-f]{1,4}:
  ){1}((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4][0-9]|1[0
  -9][0-9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])){3}))|:))|(:(
  ((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4][0-9]|1[0-9][0
  -9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])){3}))|:))(%.+)?\s
  *$
```

open regex in editor

Regex survival kit : the minimum to understand this presentation (2/2)

IPV6 PCRE

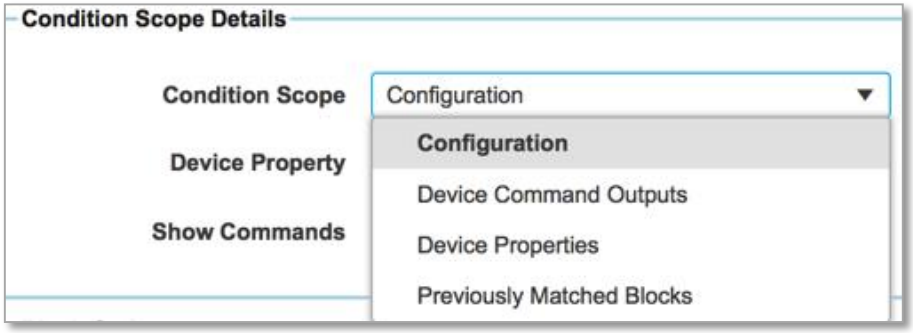
```
/ ^\s*((([0-9A-Fa-f]{1,4}:){7}([0-9A-Fa-f]{1,4}|:))|(([0-9A-Fa-f]{1,4}:){6}(:[0-9A-Fa /
  -f]{1,4}|((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-
  9][0-9]|[1-9]?[0-9])){3})|:))|(([0-9A-Fa-f]{1,4}:){5}(((:[0-9A-Fa-f]{1,4}){1,2})|:(
  (25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1
  -9]?[0-9])){3})|:))|(([0-9A-Fa-f]{1,4}:){4}(((:[0-9A-Fa-f]{1,4}){1,3})|((:[0-9A-Fa-
  f]{1,4})?:((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0
  -9][0-9]|[1-9]?[0-9])){3}))|:))|(([0-9A-Fa-f]{1,4}:){3}(((:[0-9A-Fa-f]{1,4}){1,4})|
  ((:[0-9A-Fa-f]{1,4}){0,2}:((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])(\.(25[0-5]
  |2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])){3}))|:))|(([0-9A-Fa-f]{1,4}:){2}(((:[0-9A-Fa
  -f]{1,4}){1,5})|((:[0-9A-Fa-f]{1,4}){0,3}:((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[
  0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])){3}))|:))|(([0-9A-Fa-f]{1,4}:
  ){1}(((:[0-9A-Fa-f]{1,4}){1,6})|((:[0-9A-Fa-f]{1,4}){0,4}:((25[0-5]|2[0-4][0-9]|1[0
  -9][0-9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])){3}))|:))|(:(
  ((:[0-9A-Fa-f]{1,4}){1,7})|((:[0-9A-Fa-f]{1,4}){0,5}:((25[0-5]|2[0-4][0-9]|1[0-9][0
  -9]|[1-9]?[0-9])(\.(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9]?[0-9])){3}))|:))(%.+)?\s
  *$
```

open regex in editor


[^\?:(#)\.*@|\S!!$]

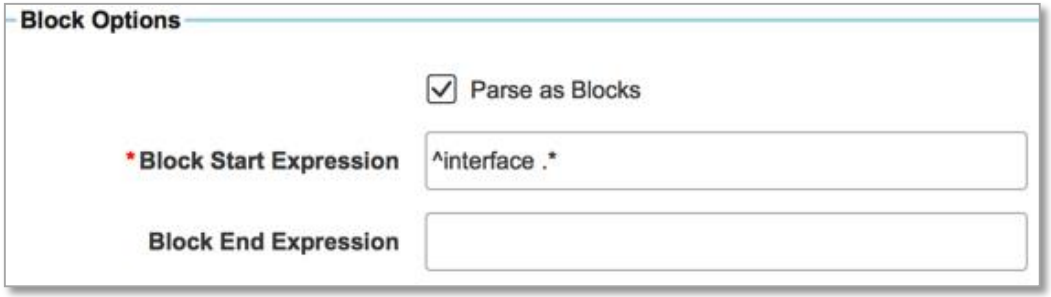
Tip: use Online Regex tester like https://regex101.com/

Rule Condition Scope & Block Options



Scope controls what information is checked

- **Configuration**
- **Command Outputs**
  - Show commands, etc
- **Device Properties**
  - Device Name, IP Address, OS Name, OS Version
- **Previously Matched Block**



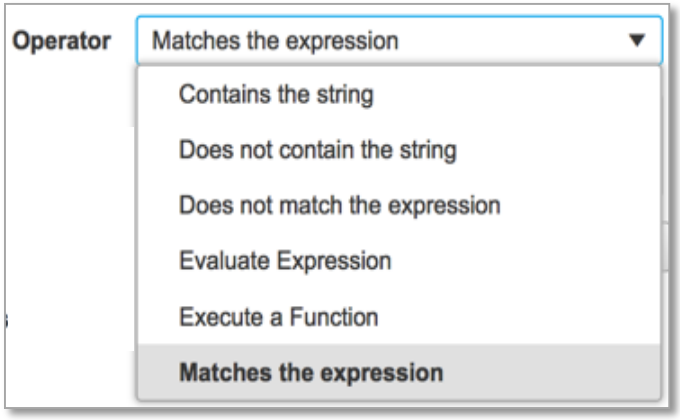
Block Options

Check inside config sub-mode blocks

Typical uses:

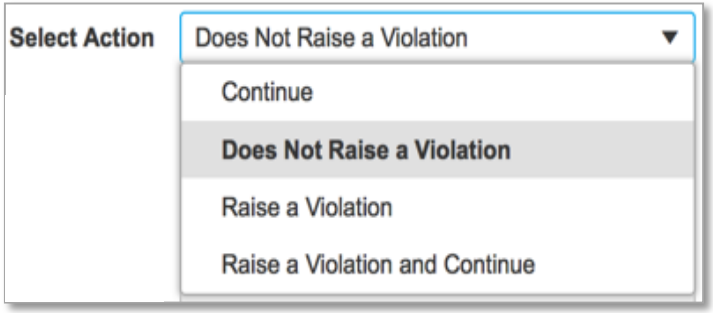
- Interface
- Router

Conditions and Actions



Condition operations

- String compare (contains / does not contain)
- Regular Expressions (match / doesn't match)
- Evaluate Expression
- Execute Function



Actions

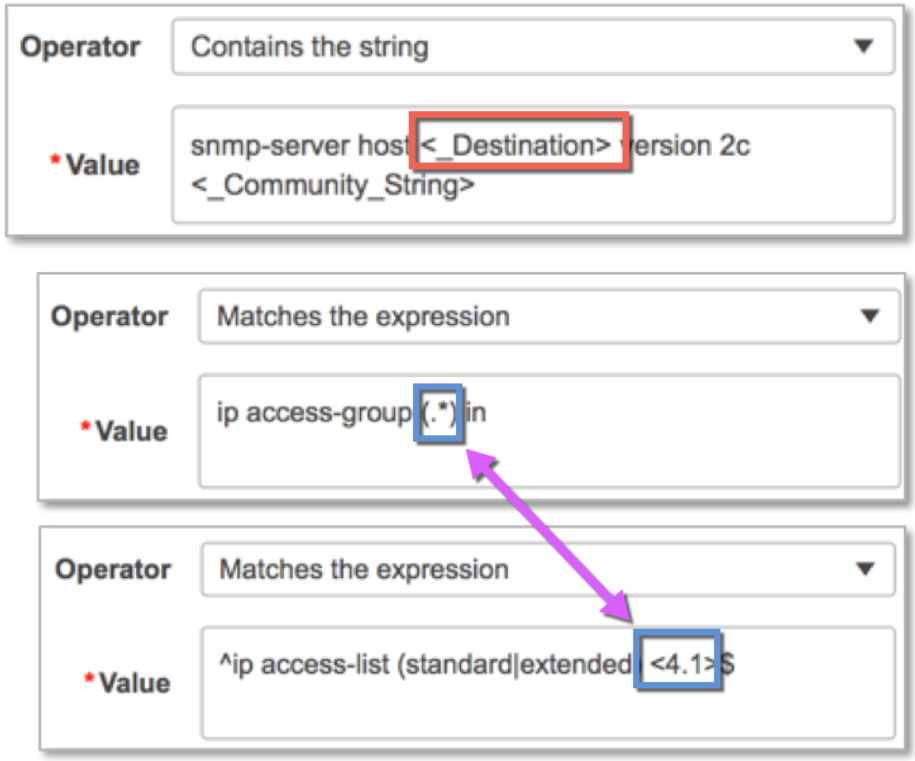
Continue – keep checking, go on to succeeding Condition

Does Not Raise a Violation – stop checking, all is good, no more checking needed

Raise a Violation – raise a violation and stop checking

Raise a Violation and Continue – raise a violation and keep checking, go on to succeeding Condition

Conditions: String and Expression Matching



String Compare

Checks that line contains string

Rule Inputs can be inserted

Regular Expression Support

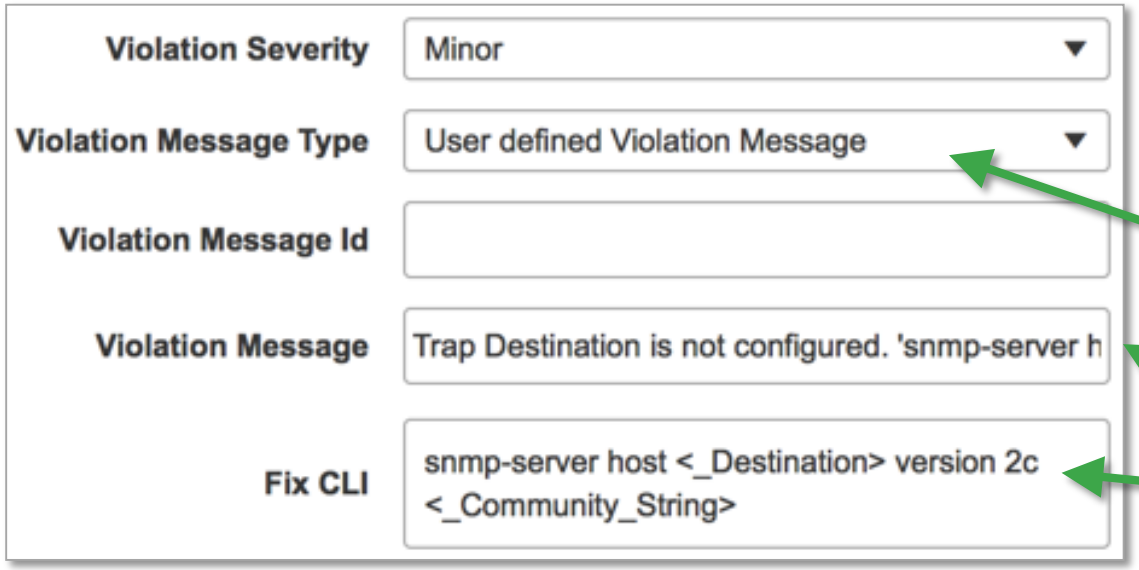
Single line regular expression

Parenthesis capture values

Back Reference previously captured values <condition#.value#>

Actions: Violation Handling

Either “Match” or “Does Not Match” Condition could be a Violation



User definable **Severity**

Default or **User Defined** Message Type

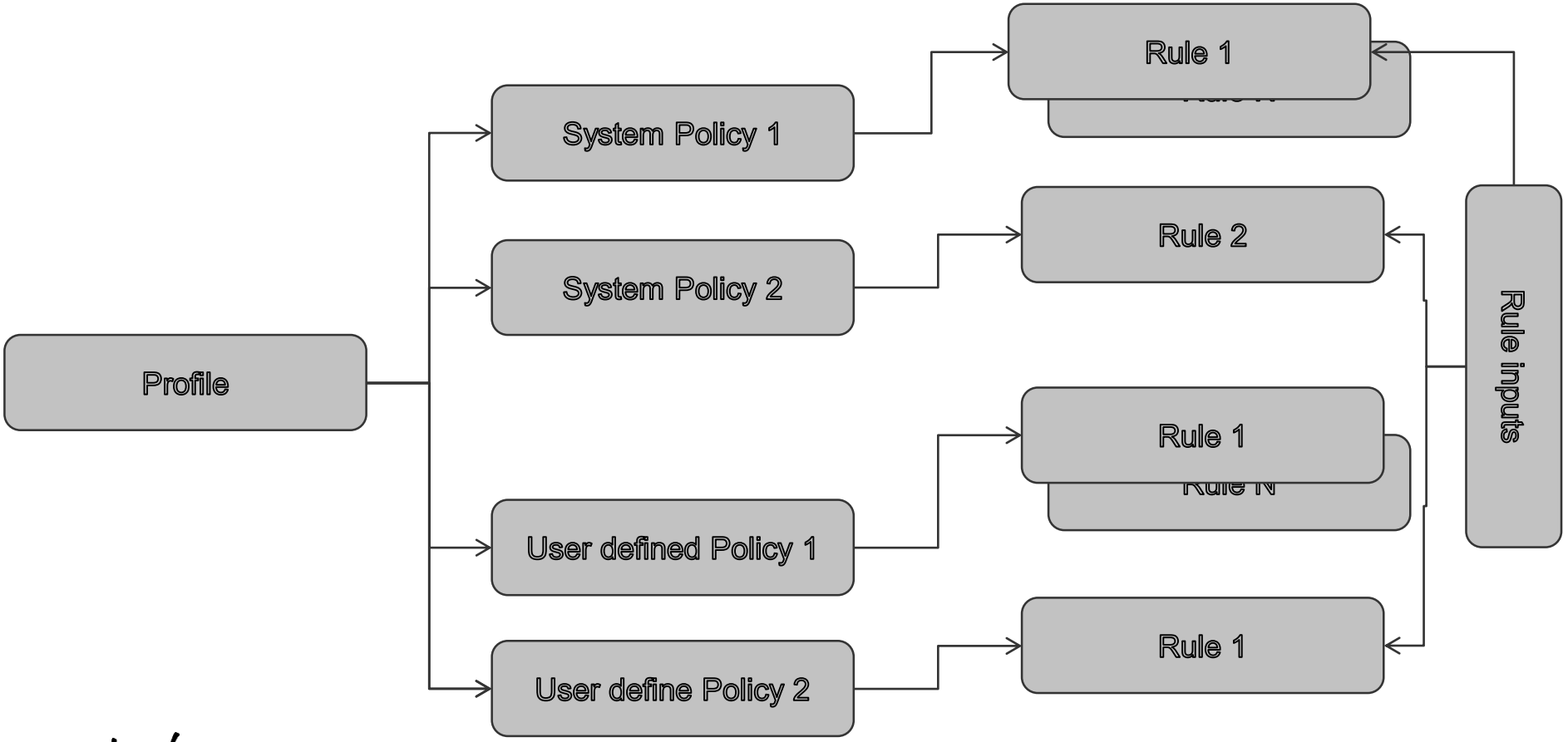
User Defined Violation Message option enables additional fields:

Violation Message text

Fix CLI (optional)

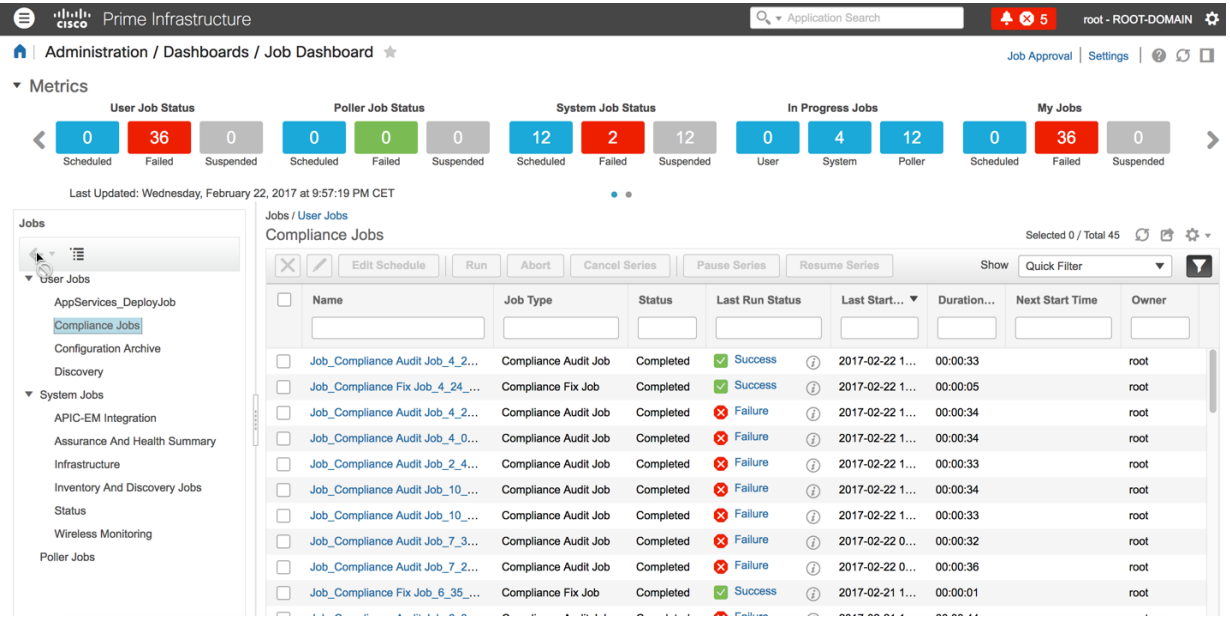
Fix CLI can be invoked from Audit Job Result (to generate Fix Job)

Profile, Policies and Rules



Compliance Jobs

Audit Jobs, Fix Jobs



Audit Jobs perform audit

- Select Profile
- Select Devices
- Perform Audit
- Results show **violations**

Fix Jobs apply Fix CLI

- Generate from Audit Job
- Preview Fix CLI commands
- Schedule Fix Job

Getting started with Compliance

Example 1: A profile with predefined policies

What did you learn in the previous example ?

- How to create a compliance profile
- How to use predefined policies in a profile
- How to send an audit job
- How to visualize the result of an audit job

Example 2
Testing SNMP community: A basic policy using string match

What did you learn in the previous example ?

- How to create a user defined compliance policy
- How to use string match in a condition
- How to generate a custom violation message and customize the severity

Example 3
Testing SNMP community:
Define the community as a parameter

What did you learn in the previous example ?

- How to create a parameter (rule input) in a rule
- How to use a rule input in a condition and in a message

Example 4
Testing and fixing SNMP community
A basic policy with fix CLI

Objective

- Reuse the previous policy to check another community called “dummy”
- If this community exist, apply cli to remove it

```
SW2-acc-demo#show run | inc community
snmp-server community private RW
snmp-server community public RO
snmp-server community cl17-acl RO 11
snmp-server community cl17_ro RO
snmp-server community dummy RO
SW2-acc-demo#
```

What did you learn in the previous example ?

- How to clone a policy
- How to edit a policy
- How to create fix cli
- How to change the value of a parameter in a profile
- How to execute a profile on the device running configuration and what happens in reality

Example 5:
Testing SNMP community and ACL:
A basic policy with simple regex and back reference

```
SW2-acc-demo#sho run | inc snmp-server
snmp-server community private RW 10
snmp-server community public RO 10
snmp-server community cl17-acl RO 11
snmp-server community cl17_ro RO
snmp-server location Berlin
SW2-acc-demo#
```

No violation: ACL 10 exists

Violation: ACL 11 doesn't exist

violation:

No ACL

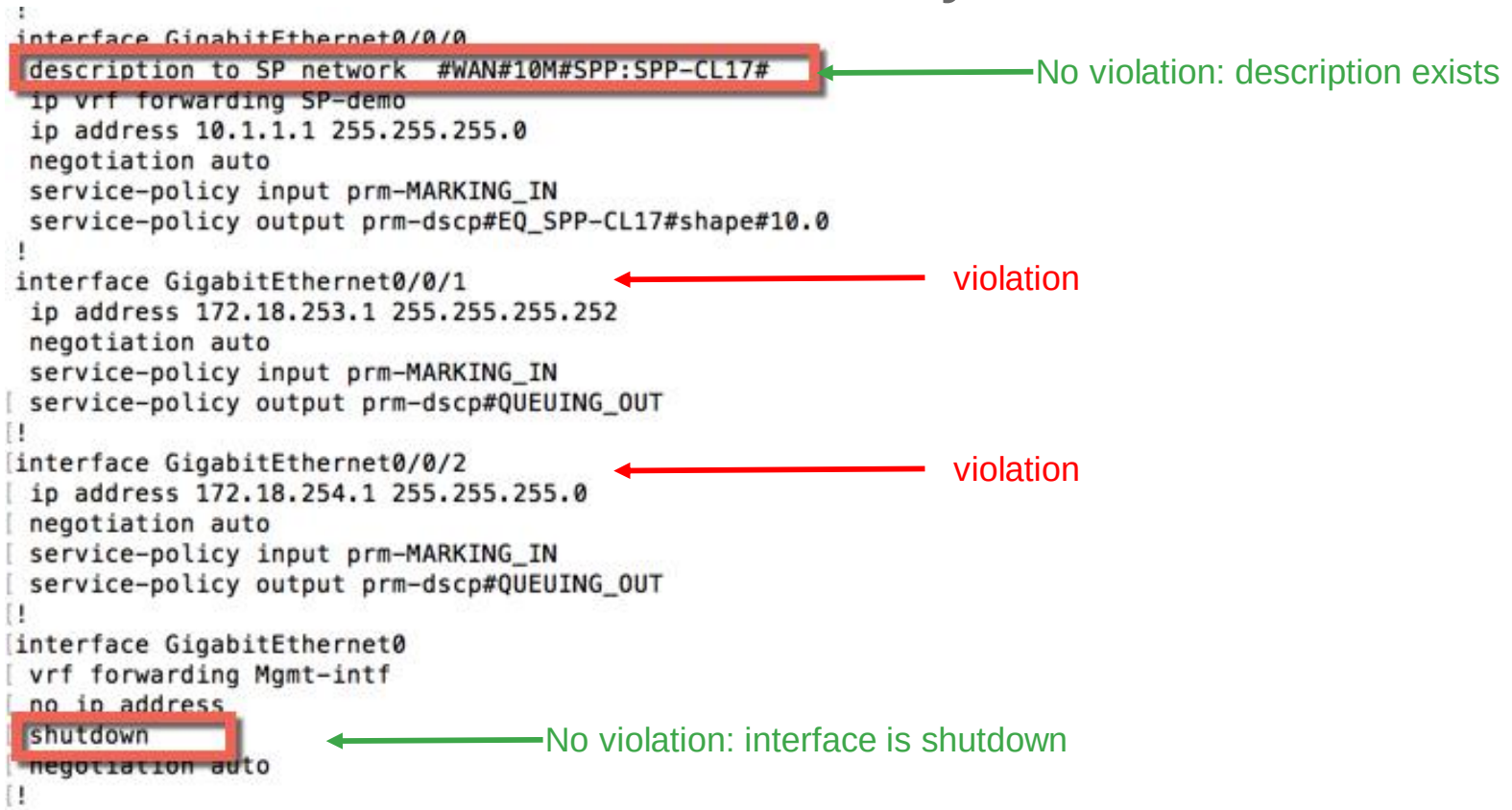
```
SW2-acc-demo#sho run | inc access-list 10
access-list 10 permit 172.0.0.0 0.255.255.255
access-list 10 permit 192.0.0.0 0.255.255.255
access-list 10 permit 10.0.0.0 0.255.255.255
SW2-acc-demo#sho run | inc access-list 11
SW2-acc-demo#
```

What did you learn in the previous example ?

- How to use multiple conditions/actions in a rule
- How to test compliance using regex
- How to capture elements in regex and how to use them with back reference

Example 6
All interfaces “no shutdown” must have a description

Each interface block must be analyzed



What did you learn in the previous example ?

- How to parse a configuration per block

More advanced use cases

Example 7
Report Ethernet interfaces with status Admin Up / Oper Down

Policy should apply to the output of a show command

```
SW1-acc-demo#sho ip inter br
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  unassigned      YES NVRAM  up                    up
Vlan100                172.18.0.250    YES NVRAM  up                    up
                       unassigned      YES NVRAM  down                  down
GigabitEthernet1/0/1   unassigned      YES unset  down                  down
                       unassigned      YES unset  down                  down
                       unassigned      YES unset  down                  down
GigabitEthernet1/0/4   unassigned      YES unset  administratively down down
                       unassigned      YES unset  administratively down down
GigabitEthernet1/0/6   unassigned      YES unset  administratively down down
GigabitEthernet1/0/7   unassigned      YES unset  administratively down down
GigabitEthernet1/0/8   unassigned      YES unset  administratively down down
GigabitEthernet1/0/9   unassigned      YES unset  down                  down
GigabitEthernet1/0/10  unassigned      YES unset  down                  down
GigabitEthernet1/0/11  unassigned      YES unset  down                  down
GigabitEthernet1/0/12  unassigned      YES unset  down                  down
                       unassigned      YES unset  up                    up
GigabitEthernet1/0/14  unassigned      YES unset  up                    up
                       unassigned      YES unset  down                  down
GigabitEthernet1/0/16  unassigned      YES unset  down                  down
GigabitEthernet1/0/17  unassigned      YES unset  down                  down
GigabitEthernet1/0/18  unassigned      YES unset  down                  down
GigabitEthernet1/0/19  unassigned      YES unset  up                    up
GigabitEthernet1/0/20  unassigned      YES unset  down                  down
                       unassigned      YES unset  down                  down
```

What did you learn in the previous example ?

- How to analyze the output of a “show command”
- How to evaluate a regular expression in a condition

Example 8
Cleaning a configuration

Cleaning configuration

- For example, you want to verify that:
  - community cl17_ro is defined as Read Only
  - Community cl17_rw is defined as Read Write
  - No other community exists

```
SW1-acc-demo#sho run | inc snmp-server
snmp-server community private RW
snmp-server community public RO
snmp-server community cl17 RO
snmp-server community cl17-acl RO 10
snmp-server location Paris
```

6 violations:
- 4 unexpected communities
- cl17_ro and cl17_rw missing

```
SW2-acc-demo#sho run | inc community
snmp-server community private RW 10
snmp-server community public RO 10
snmp-server community cl17-acl RO 11
snmp-server community cl17_ro RO
snmp-server community cl17_rw RW
```

3 violations:
- 3 unexpected communities

How to do that ? 1 policy, with 2 rules and 3 conditions in each. (below the first rule)

- Define Rule Input for the expected snmp community RO <_RO>
- Condition 1: Parse the configuration
  - Match string which contains the expected community RO
  - action if no match: raise an error and fix
  - Fix : add the snmp community : snmp-server community <_RO> RO
- Condition 2: Parse the configuration as **blocks (snmp-server community as block of 1 line)**
  - Matches Read Only and capture the community name : <2.1>
- Condition 3: Evaluate the Expression :
  - Does the captured community in condition 2 matches the rule input (expected community)
  - action if no match: raise an error and fix
  - Fix: remove the non valid snmp community

What did you learn in the previous example ?

- How to audit ”multiple commands” like snmp-server community, ntp server, name server, logging host ….
- How to create a policy with multiple rules
- How to clone a rule
- How to re-run an audit job after fixing

Example 9
Check if ports connected to Cisco IP Phones are correctly configured

You want to check if interfaces where an IP Phone is connected have a voice vlan

```
SW1-acc-demo#
SW1-acc-demo#show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
AP1-site1-demo   Gig 1/0/13        127             T B I  AIR-CAP27 Gig 0
AP2-site1-demo   Gig 1/0/14        129             T B I  AIR-CAP17 Gig 0
SW1-demo         Gig 1/0/25        162             R S I  WS-C3650- Ten 1/1/4
SEP00115C4076C3  Gig 1/0/19        141             H P M  IP Phone  Port 1
005056906b46     Gig 1/0/20        160               H    cisco-vm- eth0

Total cdp entries displayed : 5
SW1-acc-demo#sho run inter g1/0/19
Building configuration...

Current configuration : 270 bytes
!
interface GigabitEthernet1/0/19
 description IP Phone
 switchport access vlan 16
 switchport voice vlan 18
 ip device tracking maximum 10
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 spanning-tree portfast edge
 service-policy input prm-APIC_QOS_IN
end

SW1-acc-demo#
```

```
SW2-acc-demo#show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SW2-demo         Gig 1/0/25        161             R S I  WS-C3650- Gig 1/1/2
AP-site2-demo    Gig 1/0/13        158             T B I  AIR-CAP26 Gig 0
SEP00115C0E5254  Gig 1/0/19        164             H P M  IP Phone  Port 1

Total cdp entries displayed : 3
SW2-acc-demo#sho run inter gig1/0/19
Building configuration...

Current configuration : 222 bytes
!
interface GigabitEthernet1/0/19
 switchport access vlan 18
 ip device tracking maximum 10
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 spanning-tree portfast edge
 service-policy input prm-APIC_QOS_IN
end
```

no voice vlan

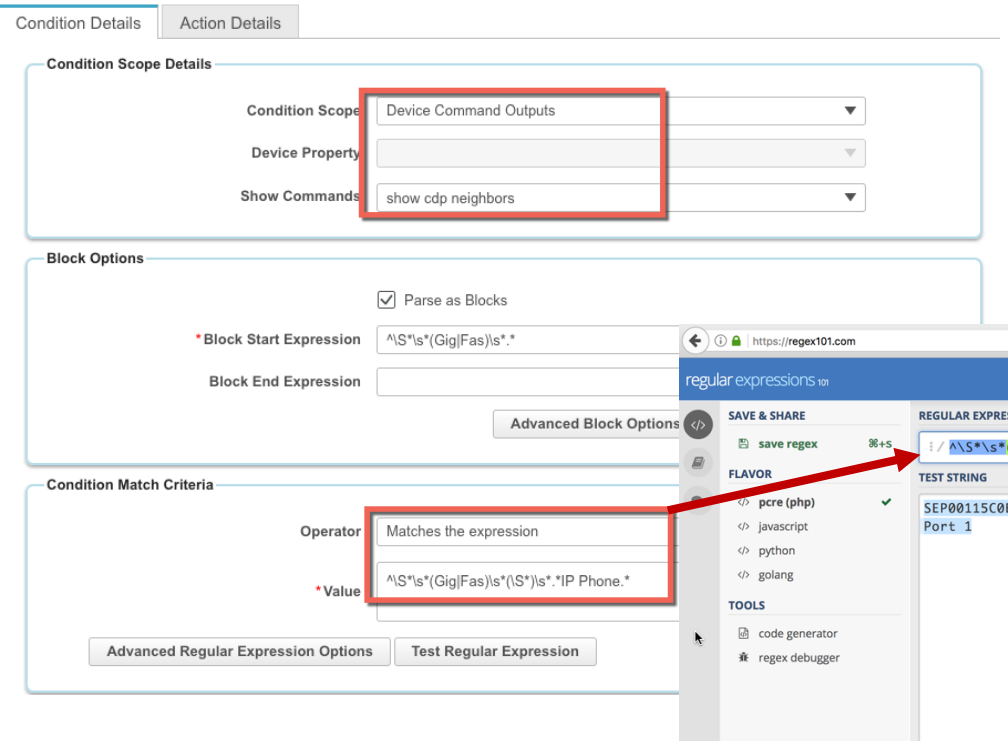
How to do that ? 1 policy with 1 rule and 3 conditions

- Condition 1: Parse the output of ”show cdp neighbors”
  - Matches lines which contains “IP Phone” at the appropriate expression , and capture the interface name and number (using Regex)

- Condition 2: Parse the configuration as **blocks (interface block in this case)**
  - Matches the interface name and number found in condition 1 only

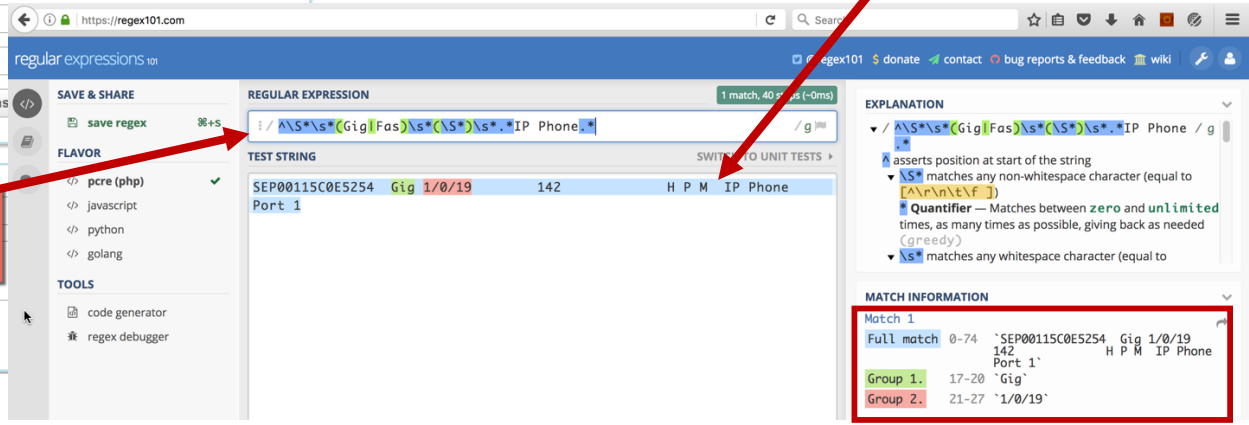
- Condition 3: Parse ”inside the previously matched block”
  - Matches the string “switchport voice vlan”

Condition 1 ”show cdp neighbors”

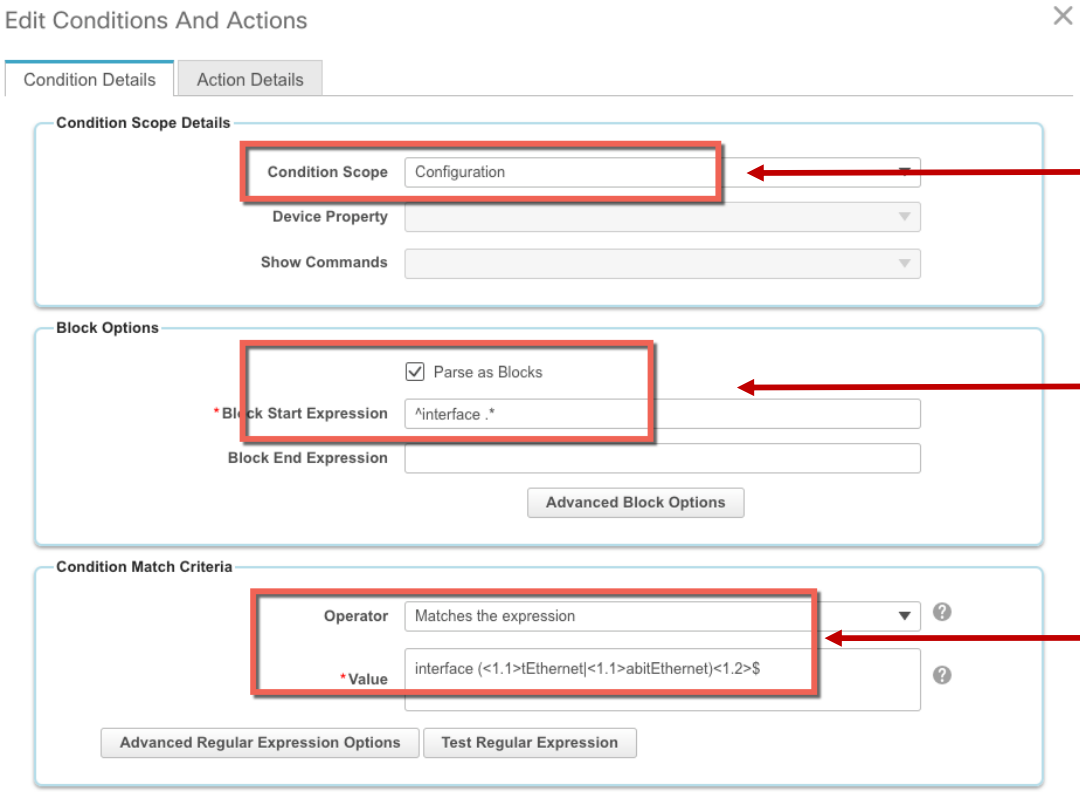



```
SW2-acc-demo#show cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
SW2-demo         Gig 1/0/25        126             R S I  WS-C3650- Gig 1/1/2
AP-site2-demo    Gig 1/0/13        154             T B I  AIR-CAP36 Gig 0
SEP00115C0E5254  Gig 1/0/19        142             H P M  IP Phone  Port 1
```



Condition 2: find the appropriate interface blocks in configuration

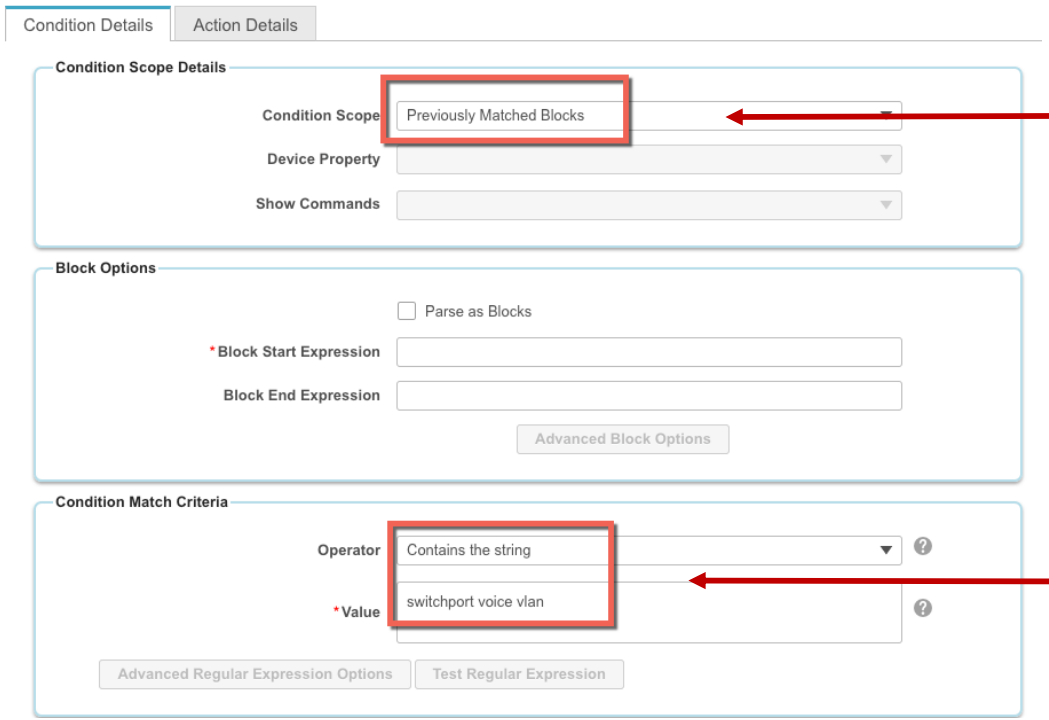


Parse the configuration

As interface blocks

Match the interfaces previously found in “show cdp neighbors”

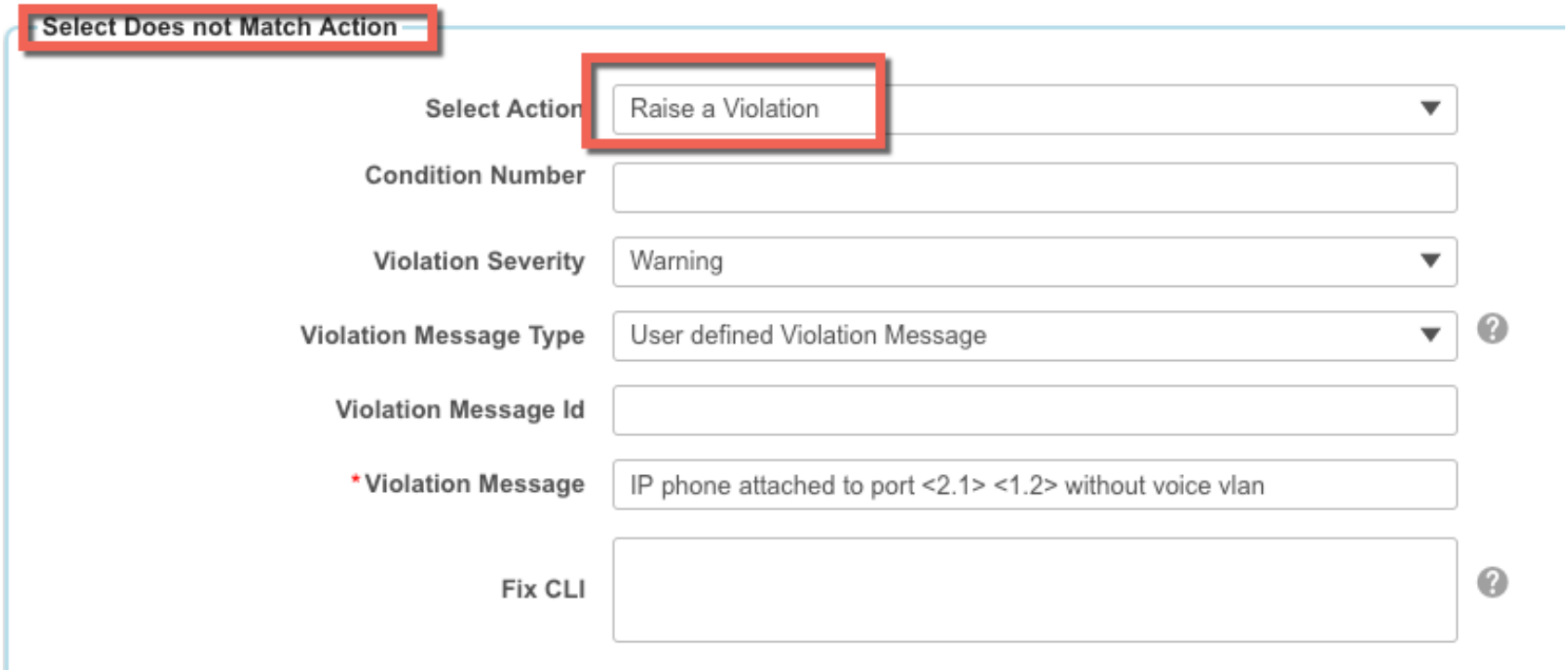
Condition 3: match “switchport voice vlan “ in the interface block



Stay in the interface block

Match the string

Condition 3: match “switchport voice vlan “ in the interface block



Cisco Prime Infrastructure - Le | Prime Infrastructure - 172.18 | Prime Infrastructure - 192.16 | https://192.168.193.11/webe | Gilles

Non sécurisé https://192.168.193.11/webacs/loginAction.do?action=login&product=wcs&selectedCategory=en#pageId=compliance_audit_policy_output_page&forceLoad=true

Prime Infrastructure | Application Search | 13 | root - ROOT-DOMAIN

Configuration / Compliance / Policies

Compliance Policies

Search All

- Example - All interfaces should restrict traffic
- Example - Block incoming telnets using un-authorized protocols
- Example - Check DNS Servers are configured
- Example - NTP Server redundancy
- Example - OSPF MD5 Check
- Example - SMU verification on ASR
- Example - SNMP prohibit well known community strings
- Example - Trap Destination
- PHONES
- STM access port
- STM access STP
- STM dhcp snooping trust
- STM etherchannel
- STM HSRP
- STM no ip routing
- STM NTP
- STM Power redundancy
- STM STP root

PHONES : Rules

Selected 1 / Total 1

New | Edit | Duplicate | Delete | Show All

Title	Description
voice vlan	ip phones must have a voice vlan

PHONES.xml | Tout afficher

Other Monitoring compliance operations available Prime Infrastructure

- Monitor PSIRT
  - ensure that you network is not expose to security threats:
- Monitor EoX
  - avoid obsolescence, plan for network upgrade:

Run Periodically EoX report

Reports / Reports / PSIRT and EOX

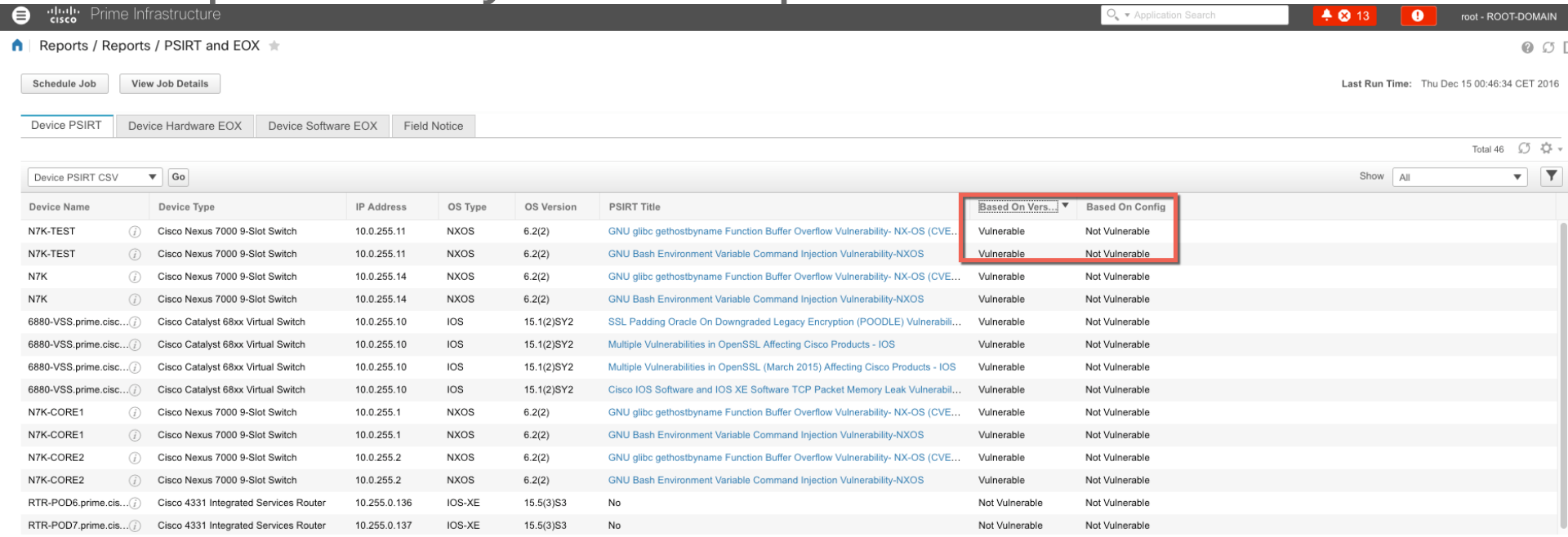
Schedule Job | View Job Details

Device PSIRT | Device Hardware EOX | Device Software EOX | Field Notice

Device HW EOX CSV ▼ Go

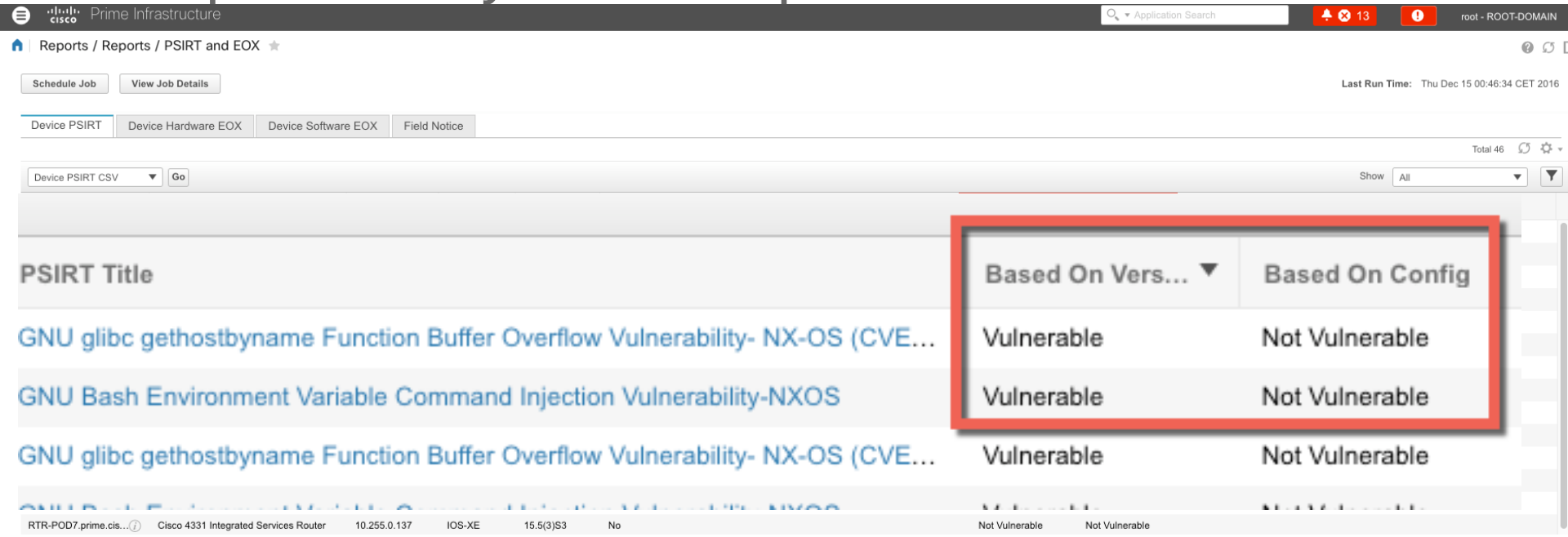
Device Name	Device Type	IP Address	Model Name	End of Life ▼	End of Support	End of Sale	End of Engineering	End of Contract Renewal
Traffic-Gen-West	Cisco 2851 Integrated Services Router	10.14.89.210	CISCO2851	Yes	Oct 31, 2016	Nov 01, 2011	Oct 31, 2014	Jan 30, 2016
SW-POD99-W-Acce…	Cisco Catalyst 3560V2-24PS Switch	10.14.89.200	WS-C3560V2-24P…	Yes	May 31, 2021	May 14, 2016	May 13, 2018	Aug 12, 2020
SW-SP-West	Cisco Catalyst 3850 24P 10/100/1000 …	10.0.255.6	WS-C3850-24P-E	No				
DC-2	Cisco Nexus 5548UP Switch	10.0.255.8	Fabric Extender M…	No				
SW-SP-East	Cisco Catalyst 3850 24P 10/100/1000 …	10.0.255.5	WS-C3850-24P-E	No				
DC-1.prime.ciscofra…	Cisco Nexus 5548UP Switch	10.0.255.7	Fabric Extender M…	No				

Run periodically PSIRT report



Device Name	Device Type	IP Address	OS Type	OS Version	PSIRT Title	Based On Vers...	Based On Config
N7K-TEST	Cisco Nexus 7000 9-Slot Switch	10.0.255.11	NXOS	6.2(2)	GNU glibc gethostbyname Function Buffer Overflow Vulnerability- NX-OS (CVE...	Vulnerable	Not Vulnerable
N7K-TEST	Cisco Nexus 7000 9-Slot Switch	10.0.255.11	NXOS	6.2(2)	GNU Bash Environment Variable Command Injection Vulnerability-NXOS	Vulnerable	Not Vulnerable
N7K	Cisco Nexus 7000 9-Slot Switch	10.0.255.14	NXOS	6.2(2)	GNU glibc gethostbyname Function Buffer Overflow Vulnerability- NX-OS (CVE...	Vulnerable	Not Vulnerable
N7K	Cisco Nexus 7000 9-Slot Switch	10.0.255.14	NXOS	6.2(2)	GNU Bash Environment Variable Command Injection Vulnerability-NXOS	Vulnerable	Not Vulnerable
6880-VSS.prime.cisc...	Cisco Catalyst 68xx Virtual Switch	10.0.255.10	IOS	15.1(2)SY2	SSL Padding Oracle On Downgraded Legacy Encryption (POODLE) Vulnerabili...	Vulnerable	Not Vulnerable
6880-VSS.prime.cisc...	Cisco Catalyst 68xx Virtual Switch	10.0.255.10	IOS	15.1(2)SY2	Multiple Vulnerabilities in OpenSSL Affecting Cisco Products - IOS	Vulnerable	Not Vulnerable
6880-VSS.prime.cisc...	Cisco Catalyst 68xx Virtual Switch	10.0.255.10	IOS	15.1(2)SY2	Multiple Vulnerabilities in OpenSSL (March 2015) Affecting Cisco Products - IOS	Vulnerable	Not Vulnerable
6880-VSS.prime.cisc...	Cisco Catalyst 68xx Virtual Switch	10.0.255.10	IOS	15.1(2)SY2	Cisco IOS Software and IOS XE Software TCP Packet Memory Leak Vulnerabil...	Vulnerable	Not Vulnerable
N7K-CORE1	Cisco Nexus 7000 9-Slot Switch	10.0.255.1	NXOS	6.2(2)	GNU glibc gethostbyname Function Buffer Overflow Vulnerability- NX-OS (CVE...	Vulnerable	Not Vulnerable
N7K-CORE1	Cisco Nexus 7000 9-Slot Switch	10.0.255.1	NXOS	6.2(2)	GNU Bash Environment Variable Command Injection Vulnerability-NXOS	Vulnerable	Not Vulnerable
N7K-CORE2	Cisco Nexus 7000 9-Slot Switch	10.0.255.2	NXOS	6.2(2)	GNU glibc gethostbyname Function Buffer Overflow Vulnerability- NX-OS (CVE...	Vulnerable	Not Vulnerable
N7K-CORE2	Cisco Nexus 7000 9-Slot Switch	10.0.255.2	NXOS	6.2(2)	GNU Bash Environment Variable Command Injection Vulnerability-NXOS	Vulnerable	Not Vulnerable
RTR-POD6.prime.cis...	Cisco 4331 Integrated Services Router	10.255.0.136	IOS-XE	15.5(3)S3	No	Not Vulnerable	Not Vulnerable
RTR-POD7.prime.cis...	Cisco 4331 Integrated Services Router	10.255.0.137	IOS-XE	15.5(3)S3	No	Not Vulnerable	Not Vulnerable

Run periodically PSIRT report



Conclusion/Take away

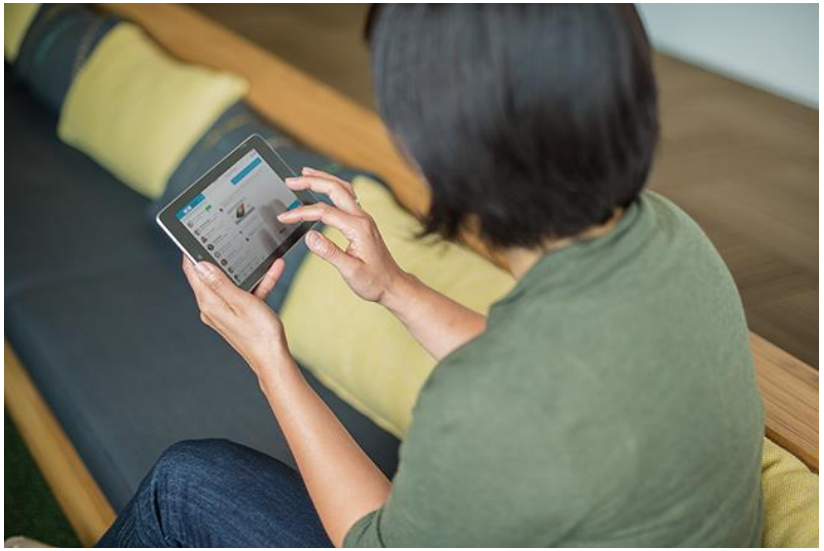
Conclusion/Takeway

- Powerful compliance engine
- 100+ pre-defined policies
- Supports IOS, IOS-XE, IOS-XR, NX-OS, AireOS*, NX-OS
- One policy can have rules for different OS
- Works on Standard OVA**, PRO OVA and GEN2 appliance
- Policy can be exported/imported (XML format)
- Available through API*

- Since 3.1
- Since 3.1 MR4

Complete Your Online Session Evaluation

- Please complete your Online Session Evaluations after each session
- Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations



Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Lunch & Learn
- Meet the Engineer 1:1 meetings
- Related sessions

Thank You

Cisco live!
February 20 - 24, 2017 · Berlin

cisco

Your Time Is Now