



Internal Compliance Use Cases

Overview

The vast majority of IT and network teams have best practices or gold standards for network device configurations in order to maintain a stable and secure infrastructure when dealing with multiple devices spread across multiple locations. Since these are developed in-house, the term Internal Compliance (or Internal Standardization) is typically used. These standards typically focus on best practices such as:

- Logging server pointing to a specific IP address
- Access control to the device
- DHCP helper configuration pointing to a specific DHCP server
- Telnet disabled
- Standard VLAN numbers
- Standard routing protocol

Current Situation with Manual Processes

For many organizations, most teams attempt to maintain compliance via manual documentation and periodic spot checks. A major pain point is senior network staff is required to manually go device by device, standard by standard. And since your staff is likely overtaxed already, Internal Compliance often becomes an afterthought until something breaks or when a problem occurs. With each configuration change, the risk of non-compliance grows and drift eventually violates policy.

The challenge lies in the fact that inconsistent/non-standard networks tend to break more often. In fact, as Gartner notes, “80% of unplanned outages impacting mission-critical services will be caused by people and process issues, and more than 50% of those outages will be caused by change/configuration/release integration and hand-off issues.” (*Configuration Management for Virtual and Cloud Infrastructure – Gartner*)

Network Automation with Infoblox

Infoblox Network Automation helps ensure that your desired state actually matches your as-is state and does so continuously for each and every change made across the devices. Instead of manually digging through massive files one by one, the platform automates the process of comparing the current configuration to the internal standard and automatically notifies when violations occur. This ensures configuration parameters stay within your customizable, defined standards.

Best of all, the process is continuous. When a configuration change is made, the Network Automation platform detects the change and compares it to the standard. And if a violation is flagged, users can leverage the same platform and restore it to the proper configuration within 15 minutes.

Use Case

This use case document provides a sample of how to create and monitor for Internal Compliance. By following the instructions, you can create your own rule and policy for your specific environment. More importantly, you can easily broaden this to include other parameters by using the templates and customization options available within Infoblox Network Automation.

Instructions

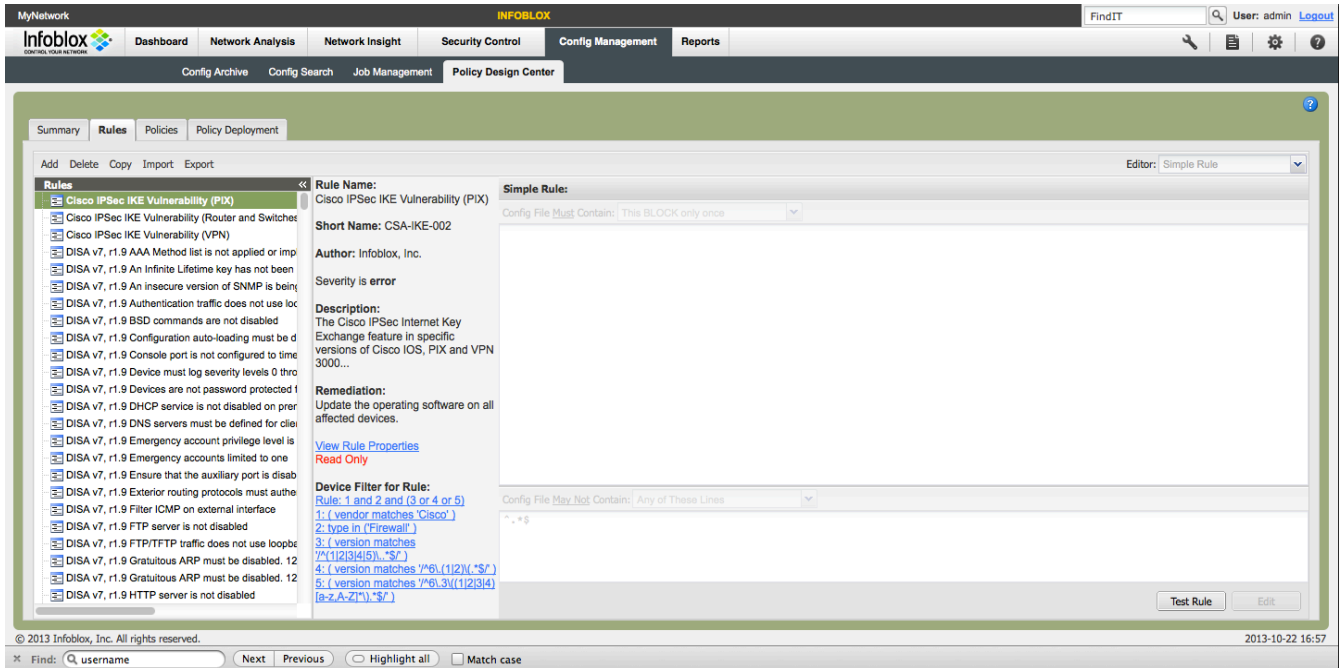
Creating a simple rule and policy to ensure the logging server IP address is in compliance

1. Go to Config Management -> Policy Design Center -> Rules.

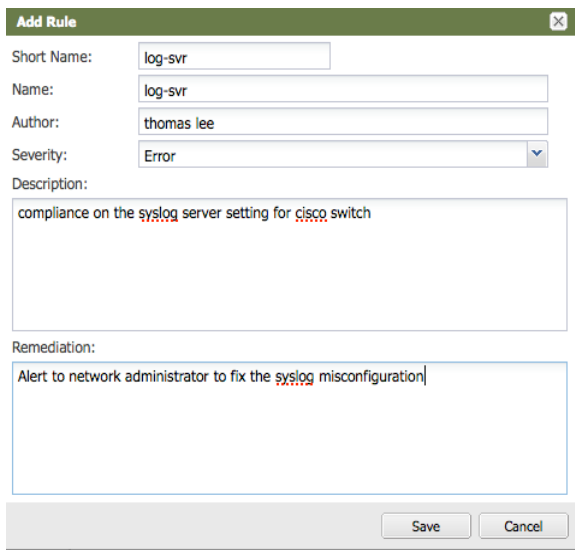


Internal Compliance Use Cases

Use Case | November, 2013



2. Click on the Add button to add a rule. A rule consists of one or more configuration file command matches and/or device attribute checks.



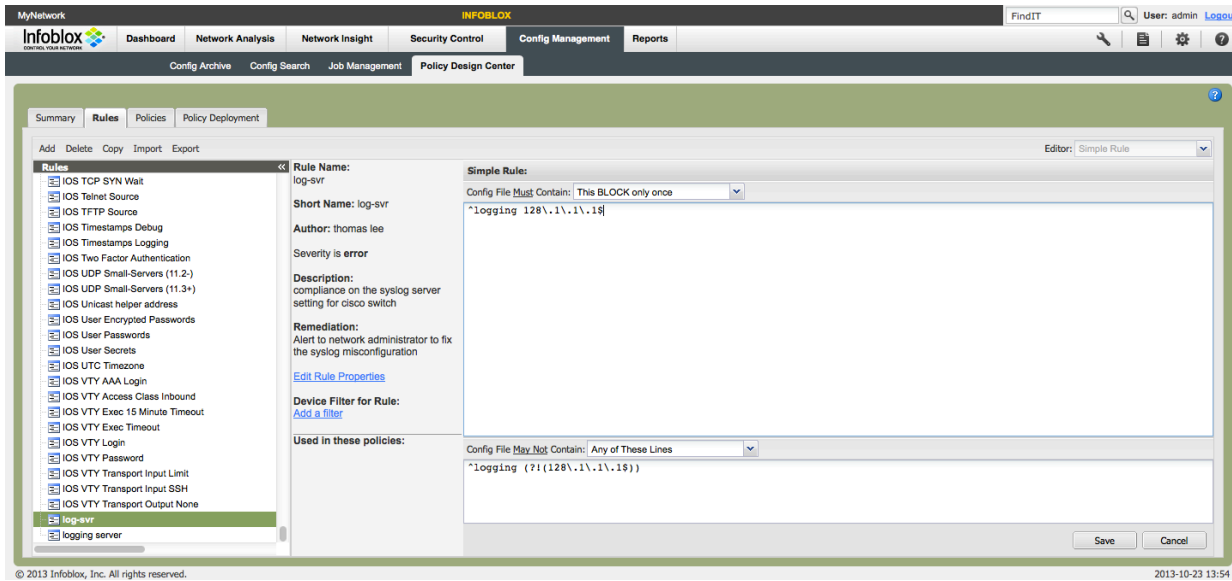
3. Enter a Short Name. The name is limited to 12 characters.
4. Enter author name.
5. Enter the severity. The choices are: Error, Info, or Warning.

A configuration Policy consists of one or more rules. Rules use different forms of regular expression pattern matching against configuration files—and tests of other data Network Automation has collected—to verify that the configuration of the device meets the rule(s). Each rule has a **severity** level, and may optionally define a device filter to limit the types of devices to which it applies. Rules may be freely re-used between



policies.

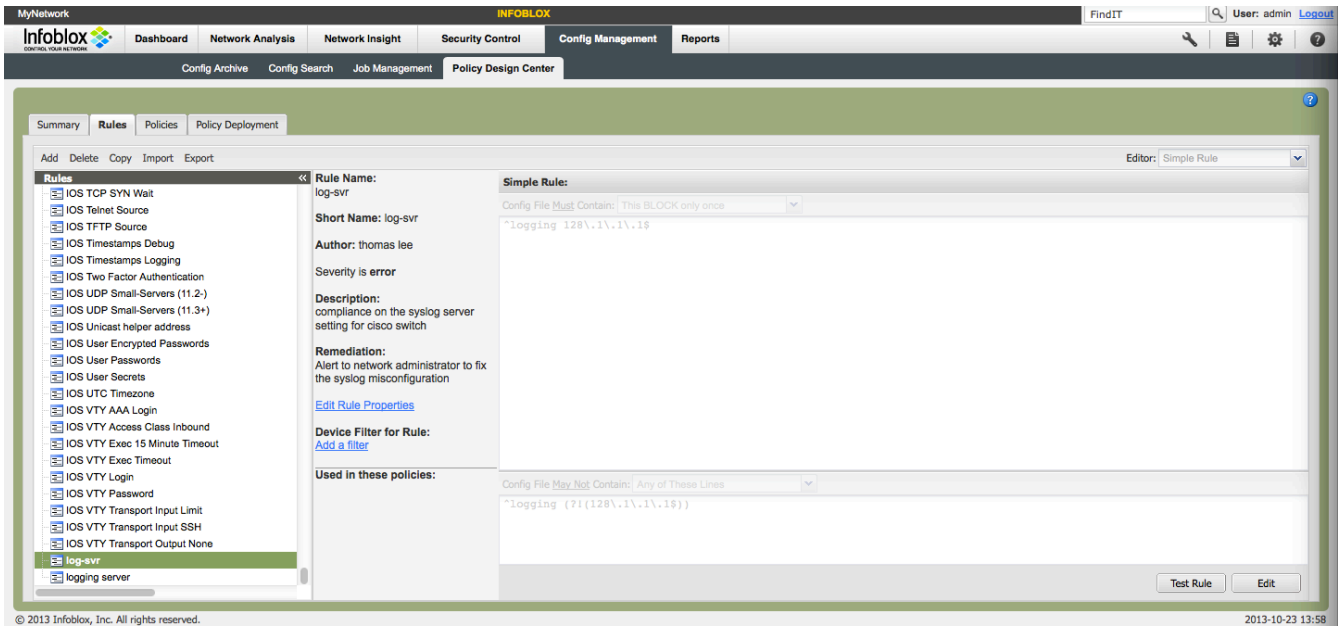
6. Enter a description of the rule.
7. Enter a remediation description. This text field describes what action should be taken when the policy fails.
8. Click Save to save the rule.



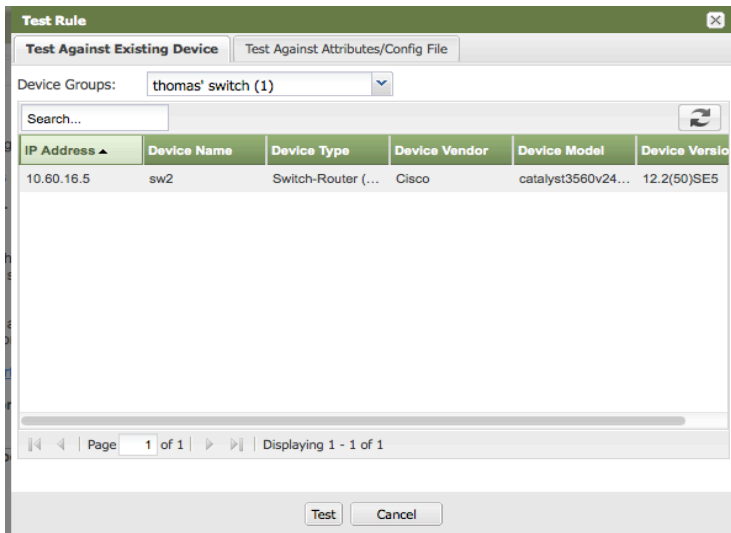
9. With the newly created rule highlighted on the left, select an editor on the upper right side. The choices are: simple editor, CPD, Rule Logic Builder, Raw XML. Refer to the Network Automation Administrator Guide for more information. For this example, simple editor is selected.
10. Enter the configuration line or block in the 'Config file must contain' section. In this case, it is `^logging 128\.\.1\.\.1$`. In the configuration file of the device, the command is `logging 128.1.1.1`. Network Automation uses Ruby-style regular expressions. The reason for using the '^', '\$', and the '\' characters is to ensure rules engine searches for this exact statement. The '^' character denotes the beginning of a line. The '\$' denotes the end of a line. The '\' character denotes treating the subsequent character as a literal character instead of a regular expression. Network Automation rules use Ruby-like regular expressions.

In the 'Config file may not contain' section, input `^logging (?!(128\.\.1\.\.1$))`. The '?' means do not match 128.1.1.1. However, this section states must not contain the following statement. The overall effect is that if the logging statement IP address differs from 128.1.1.1, an error will be flagged. Refer to the following link on Ruby regex characters: <http://www.ruby-doc.org/core-2.0.0/Regexp.html> to get more information on regex characters.

11. Click Save. You can now test the rule to ensure the rule is working correctly.



1. Click on the Test Rule button to test the rule. By testing the rule before deploying, you can ensure the rule is written properly without having to deploy a policy.



2. Click 'Test Against Existing Device' tab.
3. Select and highlight the device from the device groups.
4. Click on the Test button.



Internal Compliance Use Cases

Use Case | November, 2013

Infoblox Configuration Rule Test Results
2013-11-06 15:41:23

Rule log-svr
compliance on the syslog server setting for cisco switch

Pass

Device sw2
IP: 10.60.16.5
Model: catalyst3560v248ps
Version: 12.2(50)SE5
Last Check: 2013-11-06 15:39:41

Remediation:
Alert to network administrator to fix the syslog misconfiguration

Logic:

```
(
  Config file contains one block:
  ^logging 128\.\1\.\1$.
  Config file does not contain any:
  ^logging (?!(128\.\1\.\1$.))
)
```

5. It should come back as Pass if the configuration in the configuration file is correct.

The screenshot shows the Infoblox web interface. The 'Policies' tab is selected. On the left, there is a list of policies including 'IAVA 2009-A-0022' and various DISA and NSA rules. The main area shows details for 'IAVA 2009-A-0022', including its short name, author (Infoblox, Inc.), and description. On the right, a table titled 'Rules in this Policy' lists several rules with their names and severity levels, all set to 'error'.

Now that you have created your rule and tested it successfully, you can automate the process of monitoring compliance by placing this rule into a policy and deploy the policy against a device or a group of devices. When a policy is deployed against a device or device group, any detect changes to the configuration file will be examined by this policy. If the change is against this policy, then an error/issue will be posted and if configured, relevant users will be notified.

1. Click on the Polices Tab from the previus screen.
2. Click on the Add button to a policy.
3. Enter Policy Name, Short Name, Author, and Description.



4. Click on the Save button.

5. Highlight the policy was you just created and saved.
6. Click on the Edit button to add the rule that was created previously. In this example, it's the swlog-svr policy.
7. Click on the rule or rules to be placed into this policy. In this case, we click on the rule called log-svr.
8. Click the Save button.



Internal Compliance Use Cases

Use Case | November, 2013

Policy: swlog-svr
Description: ensure compliance for logging 128.1.1.1 syslog command on switch
Device Filter:

Device Groups	Count	Rank	Criteria
Security Control	15	92	\$Assurance > 75 and \$Access = "on..."
Switching	13	85	\$Assurance > 75 and \$Type in ["Switch", "Switch-Rou...]
Network Management	8	55	\$Assurance >= 20 and \$Type in ["NetMRI", "NMS", "Net...]
App Servers	7	35	\$Assurance >= 20 and \$Community ne "" and \$Typ...
Security	5	80	\$Assurance > 75 and \$Type in ["Firewall", "VPN", "Se...
thomas' switch	1	86	\$IPAddress = 10.60.16.5...
Optimizers	0	80	\$Assurance > 75 and \$Community ne "" and \$Type in ...
Video	0	80	\$Assurance > 75 and \$Type in ["CMTS", "Video QAM", "...]
Voice	0	75	(\$Assurance > 75 and \$Type in ["VoIP Gateway", "C...]
Webcams	0	76	\$Assurance > 75 and \$Type in ["Miscellaneous APD...

The last step is to deploy the policy. This means you are assigning the policy to the device or device group.

1. Click on the Policy Deployment Tab. Select the device group that you want the policy to enforce.
2. Click on the Save button.
3. Now the policy will examine the latest configuration file for this device or device group to ensure the logging statement is correct.

thomas' switch 2013-10-23 / Daily

Overall Score: **9.9**

Info Count: 5, Warning Count: 2, Error Count: 3

Overall Score History

Severity	Last Seen	Title	Status	Component	# Affected	# New	# Closed	# Suppressed
Error	2013-10-23 15:01:03	Policy Violation: swlog-svr	Current	Configurations	2	1	1	0
Error	2013-10-23 13:51:03	Policy Violation: PCLDSS 1.2 IOS	Current	Configurations	1	0	0	0
Error	2013-10-23 13:51:03	Policy Violation: PCLDSS 2.0 IOS	Current	Configurations	1	0	0	0
Warning	2013-10-23 00:17:57	CDP Neighbor Changed	Current	Devices	1	1	0	0
Warning	2013-10-23 00:17:17	Device Routing Table Changed	Current	Routing	2	2	0	0
Info	2013-10-23 14:46:27	Device Recently Restarted	Current	Devices	1	0	0	0
Info	2013-10-23 13:45:28	Config Difference	Current	Configurations	1	0	0	0
Info	2013-10-23 12:47:55	Device DNS and SNMP sysName Mism...	Current	Devices	1	0	0	0
Info	2013-10-23 12:18:19	Downstream Hub or Switch	Current	Interfaces	1	1	0	0

To test the policy, connect to the device and modify the configuration by adding another logging statement or modify the existing logging statement. Within 15 minutes, you should see an entry appear on the Network Analysis -> Issues screen like the first entry in the list above.



Configuration Policy Analysis
2013-10-23 15:01:03

Policy swlog-svr
ensure compliance for logging 128.1.1.1 syslog command on switch

Error
Last Check: 2013-10-23 14:58:57

Policy Summary:

Pass	0 (0.00%)
Fail	1 (100.00%)
Error	1 (100.00%)
Warning	0 (0.00%)
Info	0 (0.00%)
Skip	0 (0.00%)
Unknown	0 (0.00%)
Checked	1 (100.00%)

Rules Summary:

log-svr:log-svr	Error
-----------------	-------

Device sw2
IP: 10.80.16.5
Model: catalyst3560v248ps
Version: 12.2(50)SE5
Last Check: 2013-10-23 15:01:30

Rule log-svr
compliance on the syslog server setting for cisco switch

Error

Message:
Line 150 matches expression ``logging (?!(128\.1\.1\.1\$))``.

Remediation:
Alert to network administrator to fix the syslog misconfiguration

Logic:
(
 Config file contains one block:
 "logging 128.1.1.1"
 Config file does not contain any:
 "logging (?!(128\.1\.1\.1\$))"
)

You can then drill down and see the details of the error. In the screen shot above, the line number is given stating where the error occurred, the remediation to be taken, and the logic of the policy. Based upon this information, you can connect to that device, look at that line number in the configuration file, see the misconfiguration, and then correct the misconfiguration.

Below are some additional examples of rules and policies to deploy on a Cisco switch

Access control to the device

Access control to a device is done with access lists. For example, you may want to control which IP address(es) are authorized to access a device. You define which IP addresses are allowed to access this device. In this example, the following access lists are entered into the configuration file:

```
access-list 10 permit 10.76.4.1
access-list 10 permit 10.76.4.2
access-list 10 permit 10.76.4.3
access-list 10 permit 10.76.4.4
```

When assigned to the vty section, only IP addresses 10.76.4.1-4 will have access to this switch.



The screenshot shows the Infoblox Policy Design Center interface. The 'Rules' tab is active, displaying a list of rules on the left and the configuration details for the selected 'acl' rule on the right. The rule configuration includes a 'Simple Rule' section with 'Config File Must Contain' and 'Config File May Not Contain' fields. The 'Must Contain' field contains four lines of ACL permit commands for IP ranges 10.76.4.1 through 10.76.4.4. The 'May Not Contain' field contains a single line of a deny command for the same IP ranges. The interface also shows fields for Rule Name, Short Name, Author, Severity, Description, Remediation, and Device Filter.

© 2013 Infoblox, Inc. All rights reserved.

2013-11-05 14:50

You would follow the same steps in the section for rules creation. The only difference would be the commands. For example, enter the strings below into the respective rules creation screen:

[Config File Must Contain]

```
^access-list 10 permit 10.76.4.1$
^access-list 10 permit 10.76.4.2$
^access-list 10 permit 10.76.4.3$
^access-list 10 permit 10.76.4.4$
```

[Config File May Not Contain]

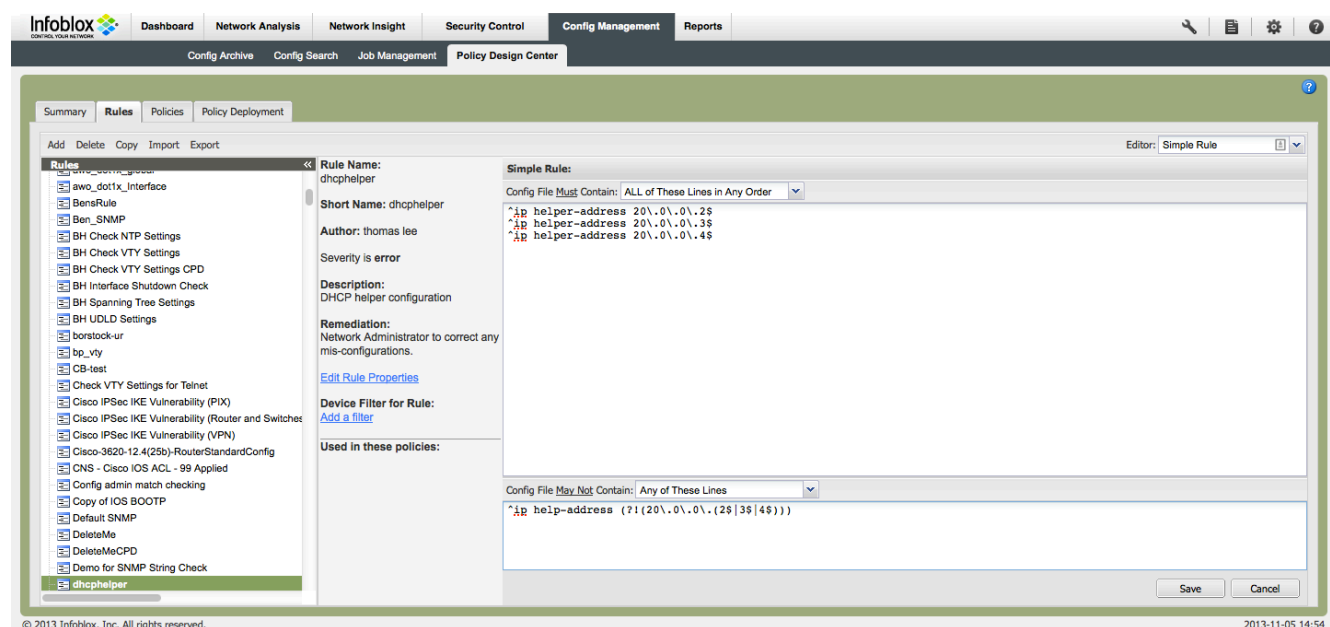
```
^access-list 10 permit (!(10.76.4.(1$|2$|3$|4$)))
```

The screenshot shows the 'Configuration Rule Test Results' page. At the top, the Infoblox logo and the title 'Configuration Rule Test Results' are displayed, along with the timestamp '2013-11-14 17:11:10'. Below this, the rule name 'Rule accesslist' is shown with the description 'access to control access to switch'. A green checkmark indicates the test result is 'Pass'. The 'Device sw2' section provides details: IP: 10.60.16.5, Model: catalyst3560v248ps, Version: 12.2(50)SE5, and Last Check: 2013-11-14 17:09:24. The 'Remediation' section contains the text 'network administrator to correct any misconfigurations on the access list'. The 'Logic' section shows a code block with the same ACL commands as seen in the previous screenshot.



DHCP helper configuration pointing to a specific DHCP server on a Cisco switch

Configuring the right DHCP helper address(es) ensures the users in their assigned VLANs are given the correct IP subnets. If a computer gets the wrong address from the DHCP server, the computer will not be able to communicate.



You would follow the same steps in the section for rules creation. The only difference would be the commands. For example, enter the strings below into the respective rules creation screen:

[Config File Must Contain]

```
^ip helper-address 20\.\.0\.\.2$
^ip helper-address 20\.\.0\.\.3$
^ip helper-address 20\.\.0\.\.4$
```

[Config File May Not Contain]

```
^ip help-address (?!(20\.\.0\.\.0\.\.(2$|3$|4$)))
```

In the configuration file segment, the IP helper addresses are configured correctly:

```
interface Vlan1
ip address 10.60.16.5 255.255.255.0
ip helper-address 20.0.0.2
ip helper-address 20.0.0.3
ip helper-address 20.0.0.4
```

When the rule is tested, the following result is displayed:



Configuration Rule Test Results
2013-11-11 15:40:12

Rule dhcphelper
dhcp helper configuration

Pass

Device sw2
IP: 10.60.16.5
Model: catalyst3560v248ps
Version: 12.2(50)SE5
Last Check: 2013-11-11 15:38:09

Remediation:
network administrator to restore configuration if misconfigured

Logic:

```
(
  Config file contains all:
  ^ ip helper-address 20\.0\.0\.2$
  ^ ip helper-address 20\.0\.0\.3$
  ^ ip helper-address 20\.0\.0\.4$
  Config file does not contain any:
  ^ ip help-address (?!(20\.0\.0\.)(2$|3$|4$))
)
```

This test passed as indicated in the upper left corner.

Telnet disabled on a Cisco switch

Disabling telnet access on devices is good security practice. In telnet, all characters typed and responses are sent in the clear. In SSH, all characters typed and responses are encrypted before transmission.

MyNetwork **INFOBLOX** FindIT User: admin Logout

Dashboard Network Analysis Network Insight Security Control Config Management Reports

Config Archive Config Search Job Management Policy Design Center

Summary **Rules** Policies Policy Deployment

Add Delete Copy Import Export Editor: Rule Logic Builder

Rules

- IOS Telnet Source
- IOS TFTP Source
- IOS Timestamps Debug
- IOS Timestamps Logging
- IOS Two Factor Authentication
- IOS UDP Small-Servers (11.2)
- IOS UDP Small-Servers (11.3)
- IOS Unicast helper address
- IOS User Encrypted Passwords
- IOS User Passwords
- IOS User Secrets
- IOS UTC Timezone
- IOS VTY AAA Login
- IOS VTY Access Class Inbound
- IOS VTY Exec 15 Minute Timeout
- IOS VTY Exec Timeout
- IOS VTY Login
- IOS VTY Password
- IOS VTY Transport Input Limit
- IOS VTY Transport Input SSH
- IOS VTY Transport Output None
- routerconfig
- sshenable
- telnet disable/ssh enable
- test**

Rule Name: test
Short Name: test
Author: test
Severity: is error
Description: test
Remediation:
[Edit Rule Properties](#)
Device Filter for Rule:
[Add a filter](#)
Used in these policies:

Rule Logic Builder

Enforce This Rule: 1 and 2 and 3 and 4

#	Type	Note
1	Device Attribute	Sys Description contains IOS
2	Config File Match	Must Contain ALL of These Lines in Any Order ^ transport input ssh\$
3	Config File Match	May Not Contain Any of These Lines ^ transport input none\$
4	Config File Match	May Not Contain Any of These Lines ^ transport input all\$

Add Config File Match Add Device Attribute

Test Rule Edit

© 2013 Infoblox, Inc. All rights reserved. 2013-11-11 16:35

You would follow the same steps in the section for rules creation. The only difference would be the commands. For example, enter the strings below into the respective rules creation screen using the rule logic builder:



Internal Compliance Use Cases

Use Case | November, 2013

[Config File Must Contain]
^ transport input ssh\$

[May Not Contain Any of These Lines]
^ transport input all\$

[May Not Contain Any of These Lines]
^ transport input none\$

Line 216 below contains a misconfiguration based upon the rule above which is to ensure 'transport input ssh' is the only acceptable command

```
207 line vty 0 4
208 session-timeout 15
209 password infoblox
210 login local
211 transport input ssh
212 line vty 5 15
213 session-timeout 15
214 password infoblox
215 login local
216 transport input all
```

When the rule is tested against this configuration, the following screen will appear:

Configuration Rule Test Results
2013-11-11 16:28:38

Rule test
test

Error

Device am2
IP: 10.80.16.5
Model: catalyst3560v248ps
Version: 12.2(50)SE5
Last Check: 2013-11-11 16:27:24

Message:
Line 216 matches expression '^ transport input all\$'

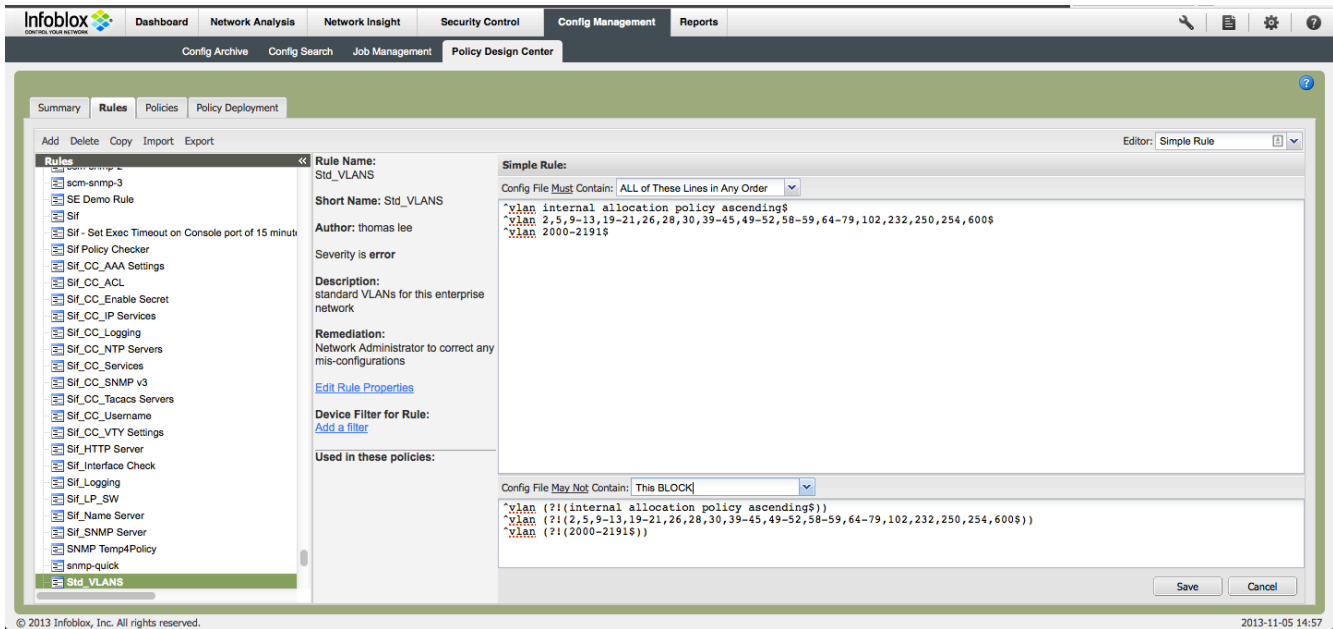
Logic:
Rule: 1 and 2 and 3 and 4
1: { sysname? contains 'IOS' }
2: Config file contains all:
^ transport input ssh\$
3: Config file does not contain any:
^ transport input none\$
4: Config file does not contain any:
^ transport input all\$

An error is indicated in the upper left portion of the screen and the message indicates an error on line 216.



Standard VLAN numbers

Standardizing VLAN numbers within your network is good network practice. This is to ensure configuration consistency.



You would follow the same steps in the section for rules creation. The only difference would be the commands. For example, enter the strings below into the respective rules creation screen:

[Config File Must Contain]

```
^vlan internal allocation policy ascending$
^vlan 2,5,9-13,19-21,26,28,30,39-45,49-52,58-59,64-79,102,232,250,254,600$
^vlan 2000-2191$
```

[Config File May Not Contain]

```
^vlan (?!(internal allocation policy ascending$))
^vlan (?!(2,5,9-13,19-21,26,28,30,39-45,49-52,58-59,64-79,102,232,250,254,600$))
^vlan (?!(2000-2191$))
```

Note: Set the 'Config File May Not Contain' pull down menu to 'This Block.'

In the configuration segment, the VLAN configuration is correct:

```
vlan internal allocation policy ascending
vlan 2,5,9-13,19-21,26,28,30,39-45,49-52,58-59,64-79,102,232,250,254,600
vlan 2000-2191
```

When the rule is test, the following result is displayed:



Configuration Rule Test Results
2013-11-11 15:42:24

Rule vian-config
ensure the vian statement is correct

Pass

Device sw2
IP: 10.60.16.5
Model: catalyst3560v248ps
Version: 12.2(50)SE5
Last Check: 2013-11-11 15:42:01

Remediation:
network administrator to go in and restore back to original configuration

Logic:

```
(
  Config file contains all:
  ^vlan internal allocation policy ascending$
  ^vlan 2,5,9-13,19-21,26,28,30,39-45,49-52,58-59,64-79,102,232,250,254,600$
  ^vlan 2000-2191$

  Config file does not contain block:
  ^vlan (?!(internal allocation policy ascending$))
  ^vlan (?!(2,5,9-13,19-21,26,28,30,39-45,49-52,58-59,64-79,102,232,250,254,600$))
  ^vlan (?!(2000-2191$))
)
```

The rule passed as indicated in the upper left corner.

Standard routing protocol on a Cisco switch

Ensuring your routing protocol standards are correct is good network operations practice. This is to ensure memory and CPU cycles are not utilized for unauthorized purposes.

Infoblox Dashboard Network Analysis Network Insight Security Control **Config Management** Reports

Config Archive Config Search Job Management Policy Design Center

Summary Rules Policies Policy Deployment

Add Delete Copy Import Export

Rules

- DISA v8, r11 NET1645 - SSH session timeout is no
- DISA v8, r11 NET1645 - SSH session timeout is no
- DISA v8, r11 NET1646 - SSH login attempts value i
- DISA v8, r11 NET1646 - SSH login attempts value i
- DISA v8, r11 NET1647 - The network element must
- DISA v8, r11 NET1660 - An insecure version of SN
- DISA v8, r11 NET1665 - Using default SNMP conn
- DISA v8, r11 NET1665 - Using default SNMP conn
- DISA v8, r11 NET1675 - SNMP privileged and non-p
- DISA v8, r11 NET1710 - NMS security alarms not d
- DISA v8, r11 NET1720 - NMS security alarms not d
- DISA v8, r11 NET1731 - The SNMP manager is not
- DISA v8, r11 NET1732 - A HIDS hasn't been impler
- DISA v8, r11 NET1733 - The SNMP manager conn
- DISA v8, r11 NET1734 - SNMP messages are stor
- DISA v8, r11 NET1750 - Logons and transactions a
- DISA v8, r11 NET1760 - Logon access to the NMS
- DISA v8, r11 NET1762 - In-band access to the NMS
- DISA v8, r11 NET1780 - Least Privilege not IAW po
- DISA v8, r11 NET1800 - IPSec VPN is not configu
- DISA v8, r11 NET1807 - Management traffic is not i
- DISA v8, r11 NET1807 - Management traffic is not i
- DISA v8, r11 NET1808 - Remote VPN end-point no
- DISA v8, r11 NET1970 - PAT is vulnerable to DNS c

Rule Name: eigrp 100

Short Name: eigrp 100

Author: thomas lee

Severity: is error

Description: ensure eigrp 100 is the only eigrp router configuration

Remediation: Network Administrator to correct any mis-configurations

[Edit Rule Properties](#)

Device Filter for Rule: [Add a filter](#)

Used in these policies:

Simple Rule:

Config File **Must** Contain: ALL of These Lines in Any Order

```
^router eigrp 100$
```

Config File **May Not** Contain: Any of These Lines

```
^router (?!(eigrp 100$))
```

Save Cancel

You would follow the same steps in the section for rules creation. The only difference would be the commands. For example, enter the strings below into the respective rules creation screen:

[Config File Must Contain]
^router eigrp 100\$



[Config File May Not Contain]

```
^router (?!(eigrp 100$))
```

In the configuration segment below, you will see a misconfiguration:

```
180 router eigrp 100
181 eigrp stub connected summary
182 !
183 !
184 router eigrp 200
185 eigrp stub connected summary
186 !
```

Line 184 is the misconfiguration. When the rule above is tested, Network Automation returns the following result:

An error is indicated in the upper left corner. In the message section, line 184 is noted as the line in which the error was detected. You can now go to that line in the configuration file to resolve the error.