Table of Contents

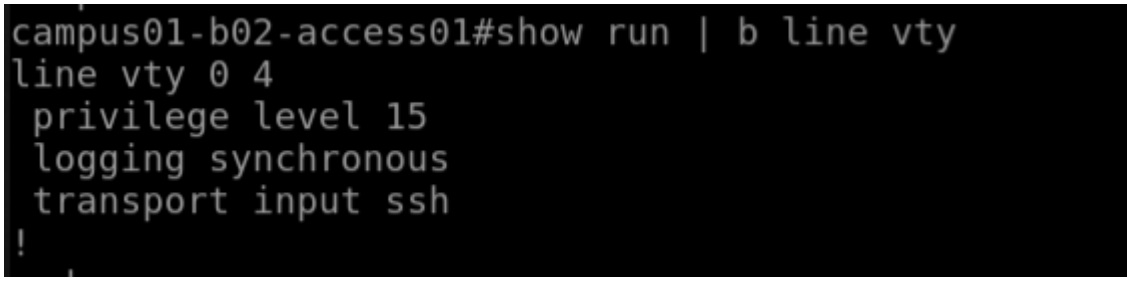
Verify telnet is disabled

Disabling Telnet and enabling SSH is one of the best practices suggested by the official Cisco Hardening Guide for IOS devices to secure the management plane. Below example helps in validating telnet configuration disabled using NetYCE Compliance module

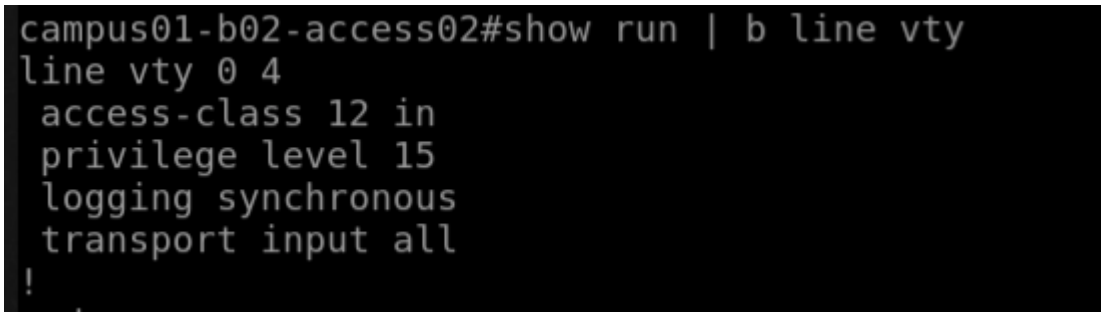
campus01-b02-access01 and campus01-b02-access02 are the two reference devices which we are using for this example. One has telnet configuration enabled and other does not.

Example config

campus01-b02-access01#



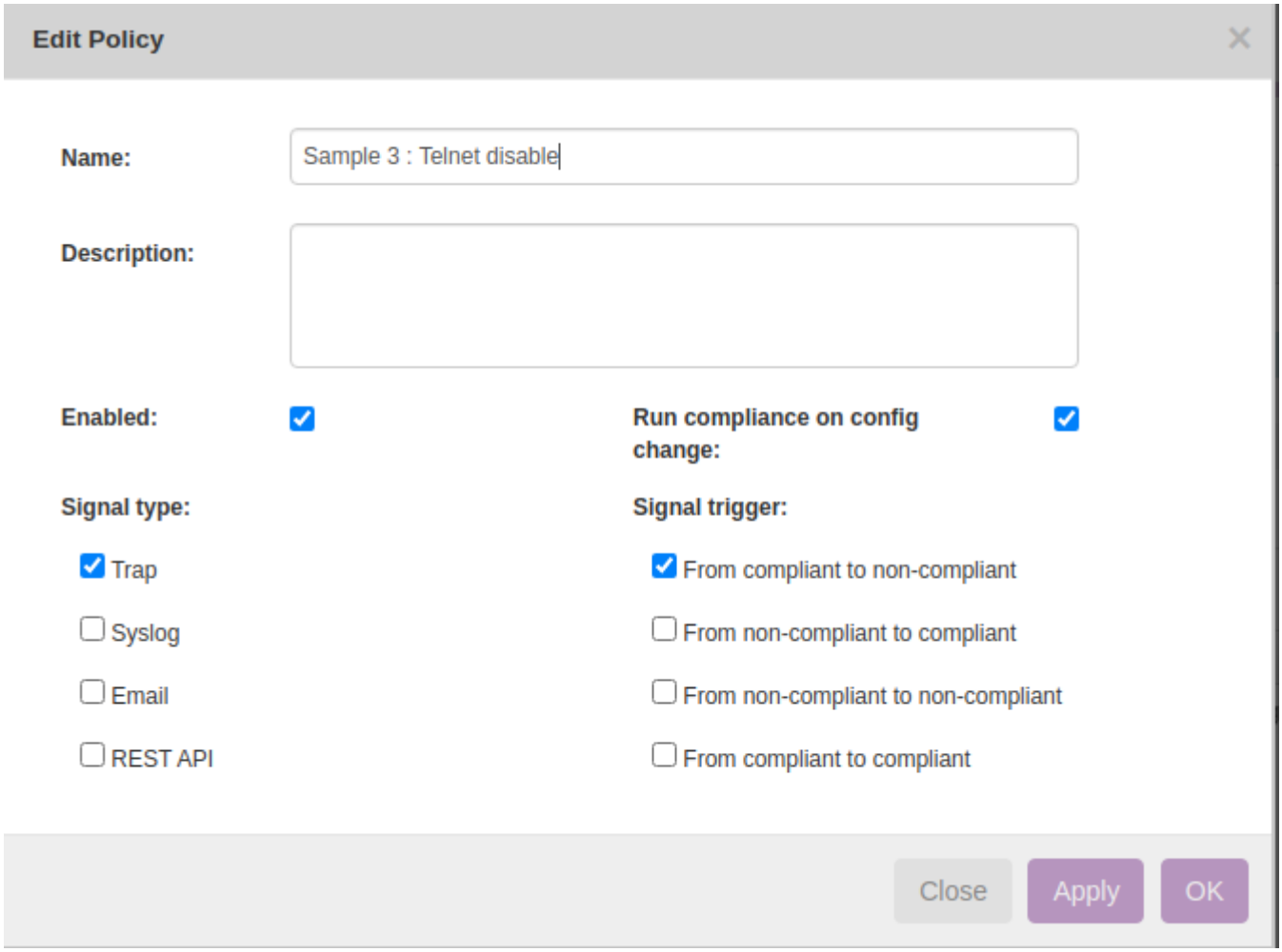
campus01-b02-access02#



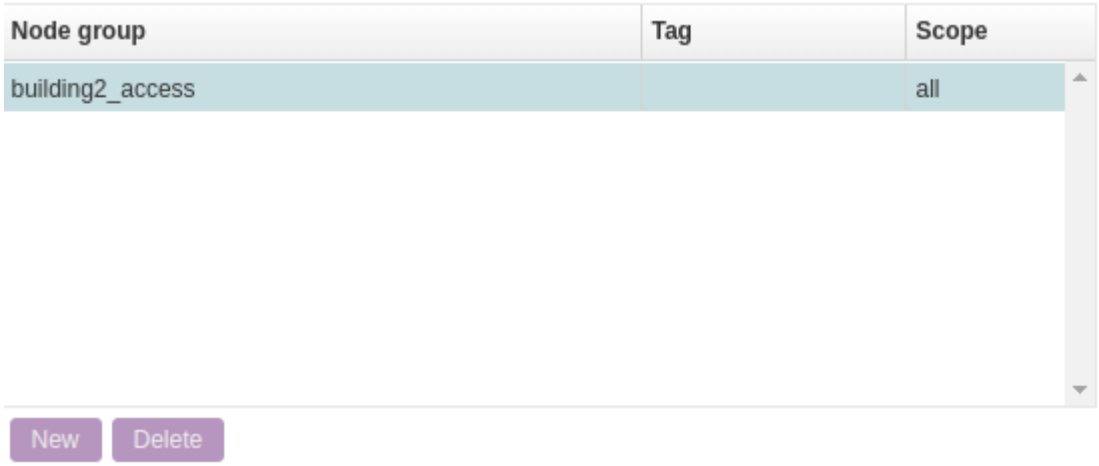
How its done

Below are the steps to create new policy.

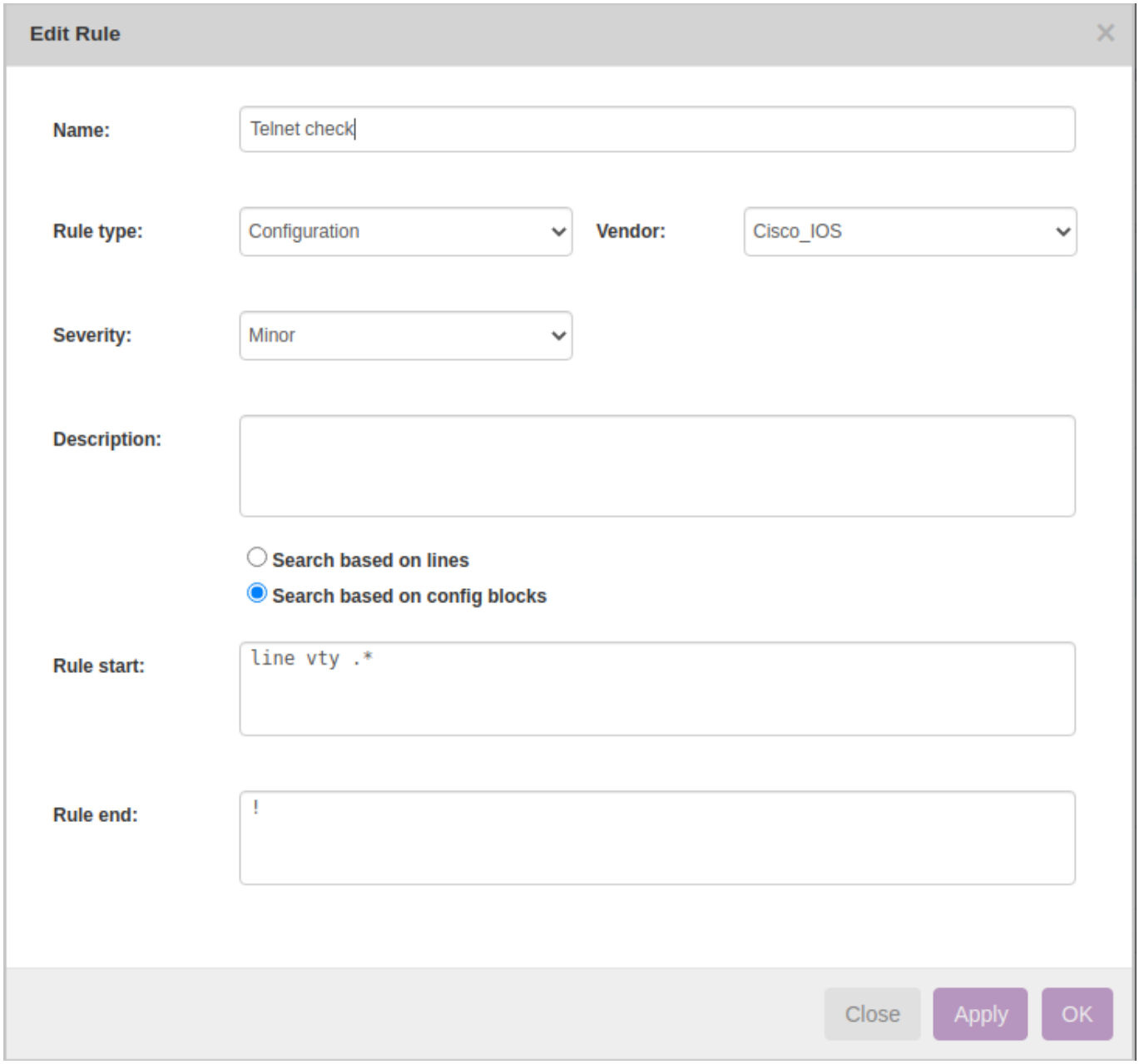
Operate → Compliance → Policies → New→

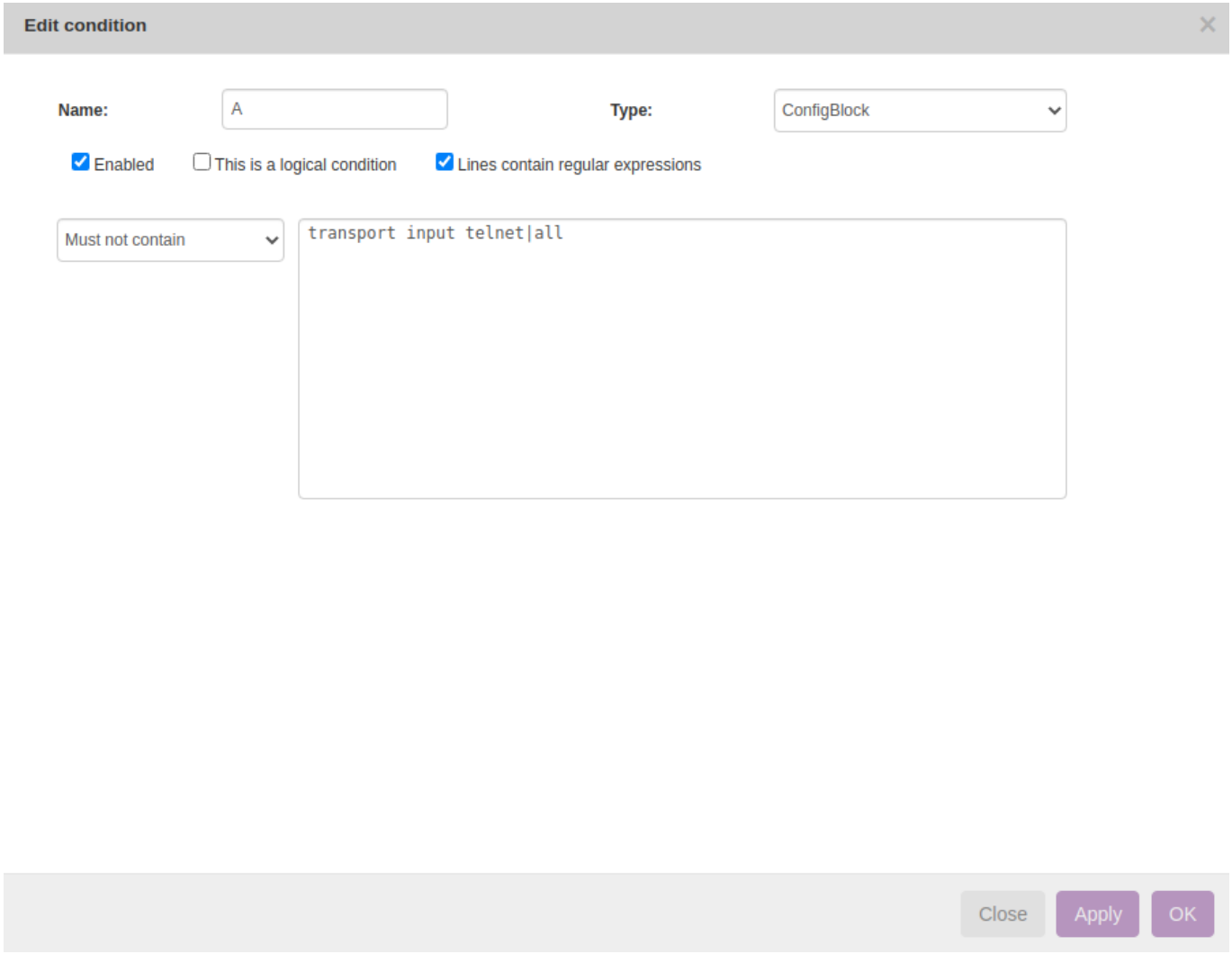


Click on the Node Group to select the relevant group of devices to add. Node group named “building2_access” holds the nodes of both the nodes:



Rule → New

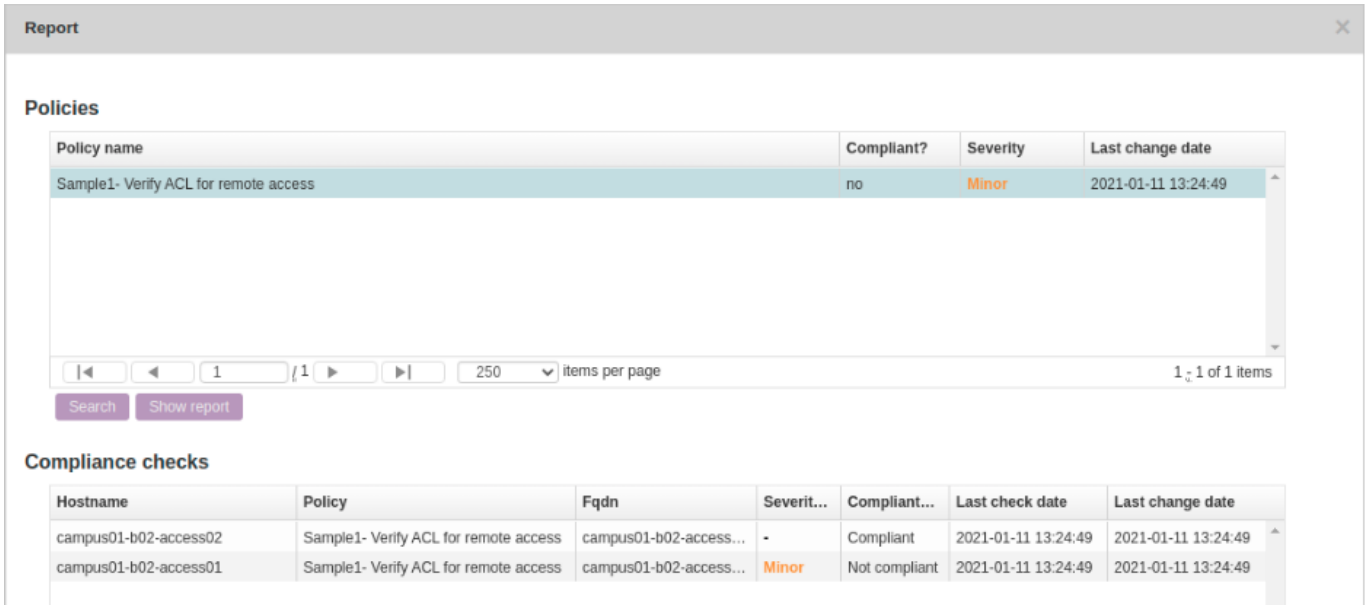

Edit Rule
Name:
Telnet check
Rule type:
Configuration
Vendor:
Cisco_IOS
Severity:
Minor
Description:
Search based on lines
Search based on config blocks
Rule start:
line vty .*
Rule end:
!
Close
Apply
OK



Report/test results:

Below is how to create reports to see the results of the compliance policies.

Operate → Compliance → Reports → New → Report Name “test” → Report type “Policies” → Policy Name “Sample 2 : Login banner” → Show Report



This was a simple example to understand how to implement compliance policy to verify if telnet access is disabled or enabled on the network devices.