* + 3.6 Ensure That SSH Access Is Restricted from the Internet.
  + ***Sentinel Policy Name:***

* + 3.6 Ensure That SSH Access Is Restricted from the Internet.

* + ***Category :***

* + Networking

* + ***Description of Policy:***

* + In this policy, we are creating a rule in firewall to ensure 2 things:
    - The Port number in a firewall rule is not equal to 22 (SSH) and Action is not set to Allow
    - The IP Ranges is not equal to 0.0.0.0/0 (or other public CIDR range) under Source filters.
  + ***Sentinel Policy Restriction:***

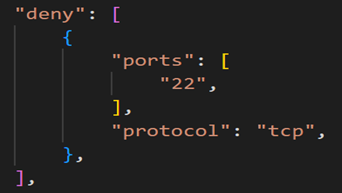
* + - If port 22 (SSH) is mentioned in the “allowed” then the source range CAN NOT be from the public (“0.0.0.0/0”, “::0”, “/0”, “0.0.0.0”).
  + ***Terraform attributes:***

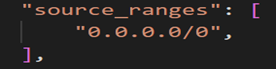
* + Provider Ref: <https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/compute_firewall>
  + Filter: 1. source\_ranges 2. Ports

* + ***Test cases:***

**Pass cases**

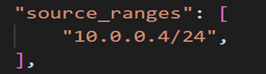
1. SSH Port 22 is denied, when the traffic is coming from the public internet (0.0.0.0/0)





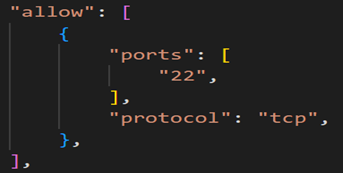
2. When the inbound traffic is not coming from the public internet, port 22 is allowed.

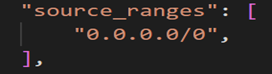




**Fail case:**

1. Allowing the port 22, when the inbound traffic is coming from the public internet





**Testcases Output:**

