`

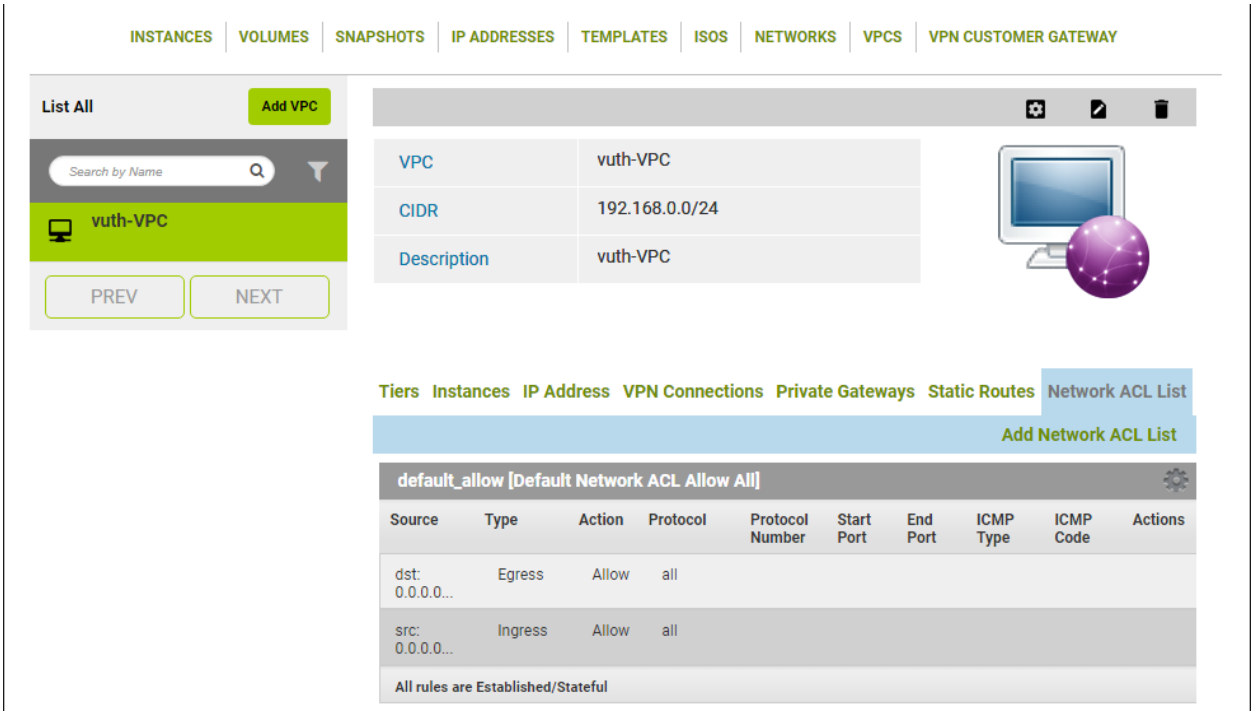
Network Access Control List

Giới thiệu :

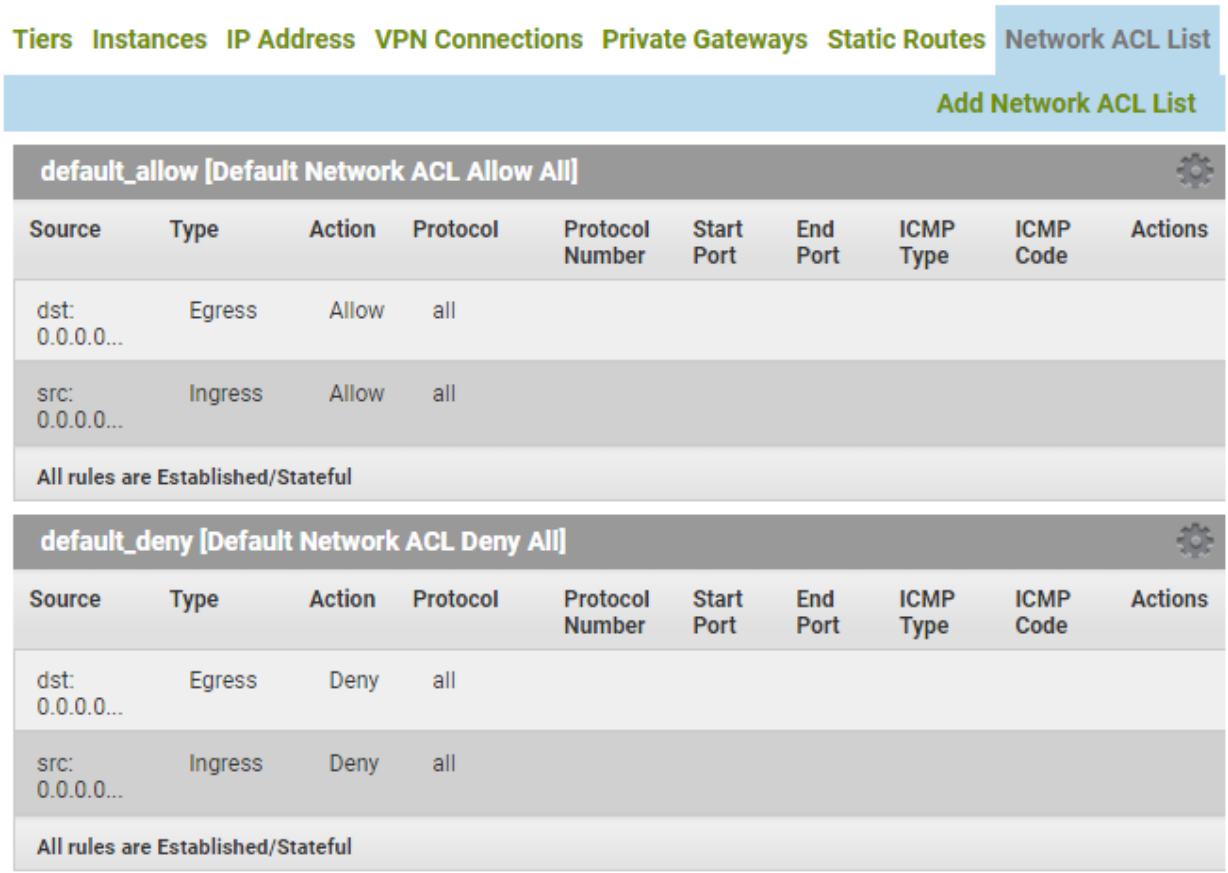
Network ACL- Network Access Control List: cung cấp khả năng xây dựng các chính sách bảo vệ network trong một VPC. Tài liệu này sẽ hướng dẫn các bạn cấu hình ACL

Network Access Control List (ACL):

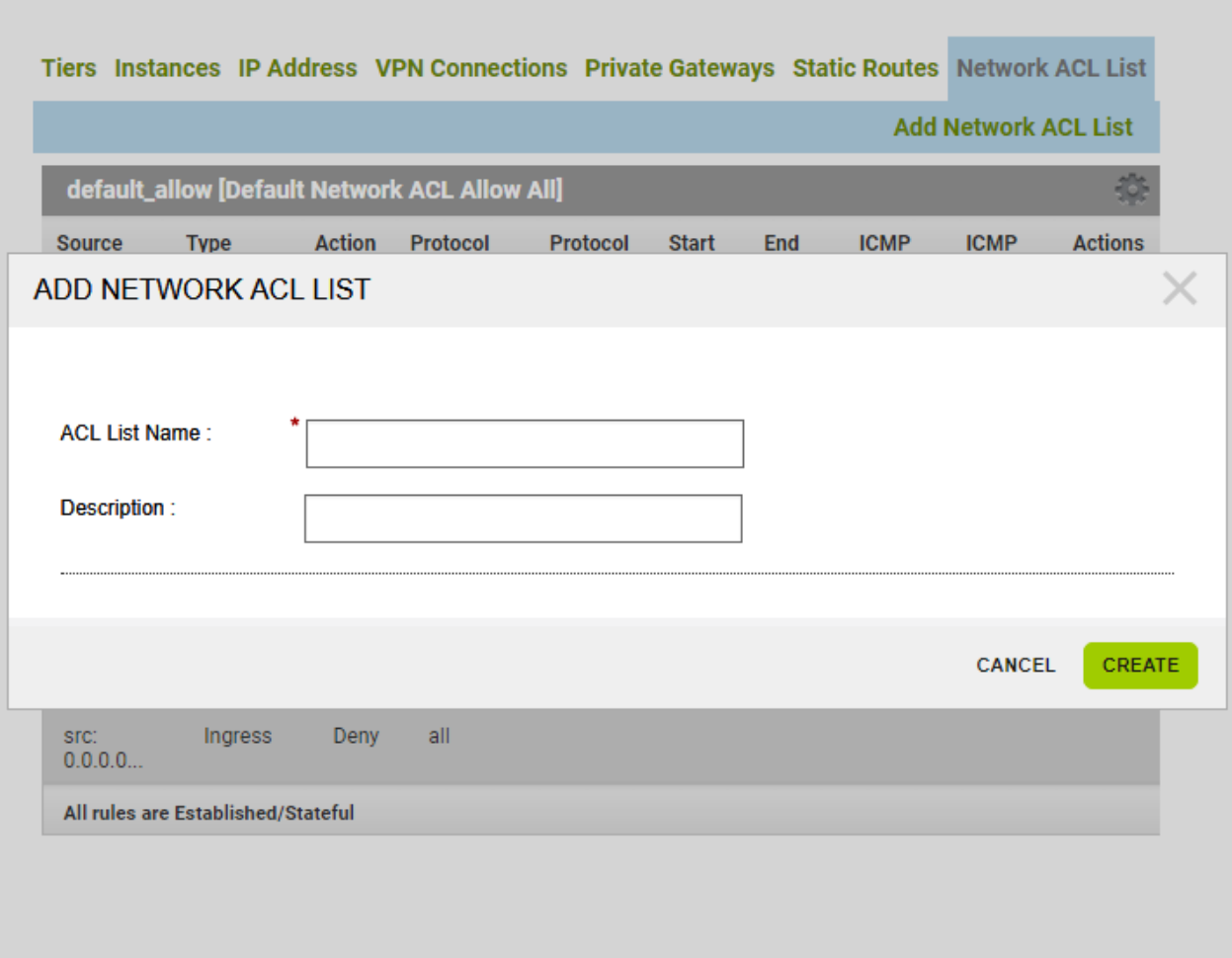
Bước 1 : Ở Tab VPCS chúng ta chọn Network ACL List



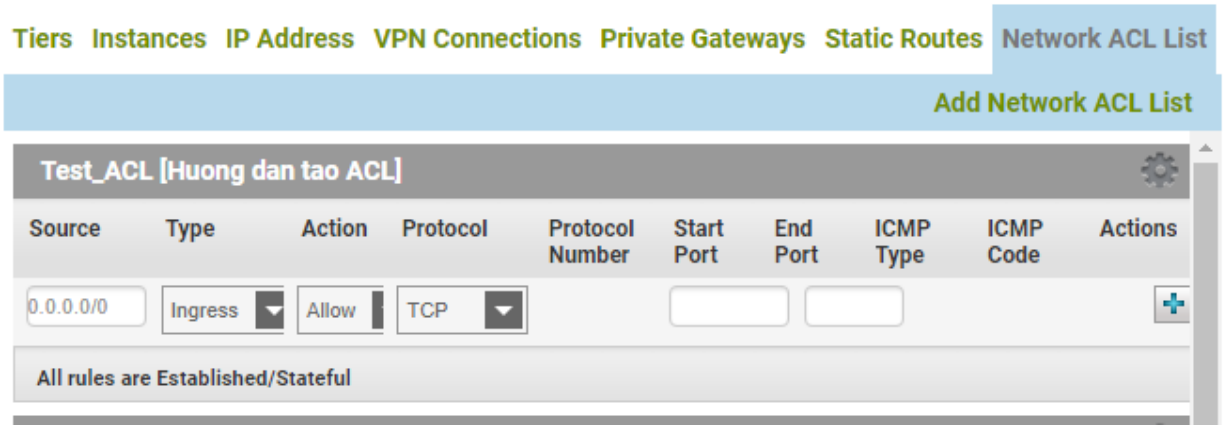
- Mặc định khi khởi tạo một VPC network thì hệ thống sẽ tạo sẵn cho bạn 2 ACL là Default_allow và Default_deny



Bước 2: Click vào Add Network ACL List hộp thoại hiện ra bạn nhập tên của ACL vào ACL List Name và phần mô tả vào Description sau đó click vào Create.



Sau khi tạo xong ta được một ACL mới.

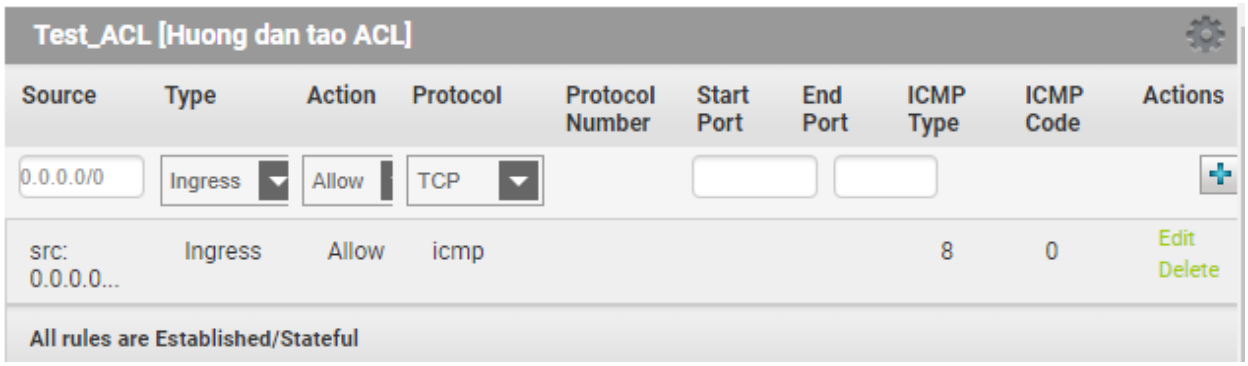


Bước 3: Thêm rule cho ACL.

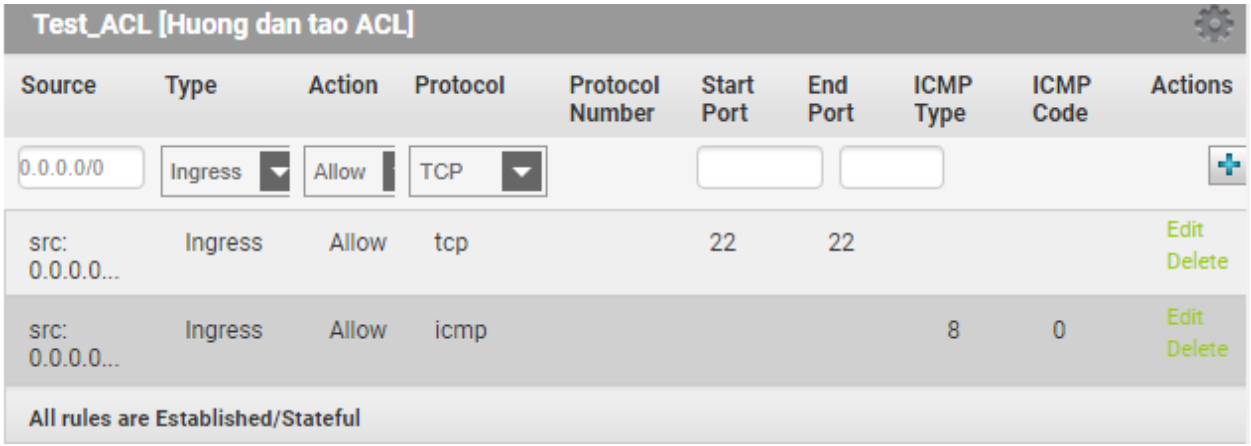
Các thông tin cần lưu ý:

- Source: Nhập địa chỉ IP hoặc dải IP sẽ được tạo rule, giá trị mặc định là 0.0.0.0/0
- Type: Có 2 lựa chọn Ingress (dữ liệu đi vào) và Egress (dữ liệu đi ra)
- Action: Có 2 lựa chọn là Allow(cho phép) và Deny(không cho phép)
- Protocol: Gồm các lựa chọn: TCP, UDP, ICMP, ALL và Protocol Number(Sử dụng cho những tính năng đặc biệt như VRRP, ESP…)

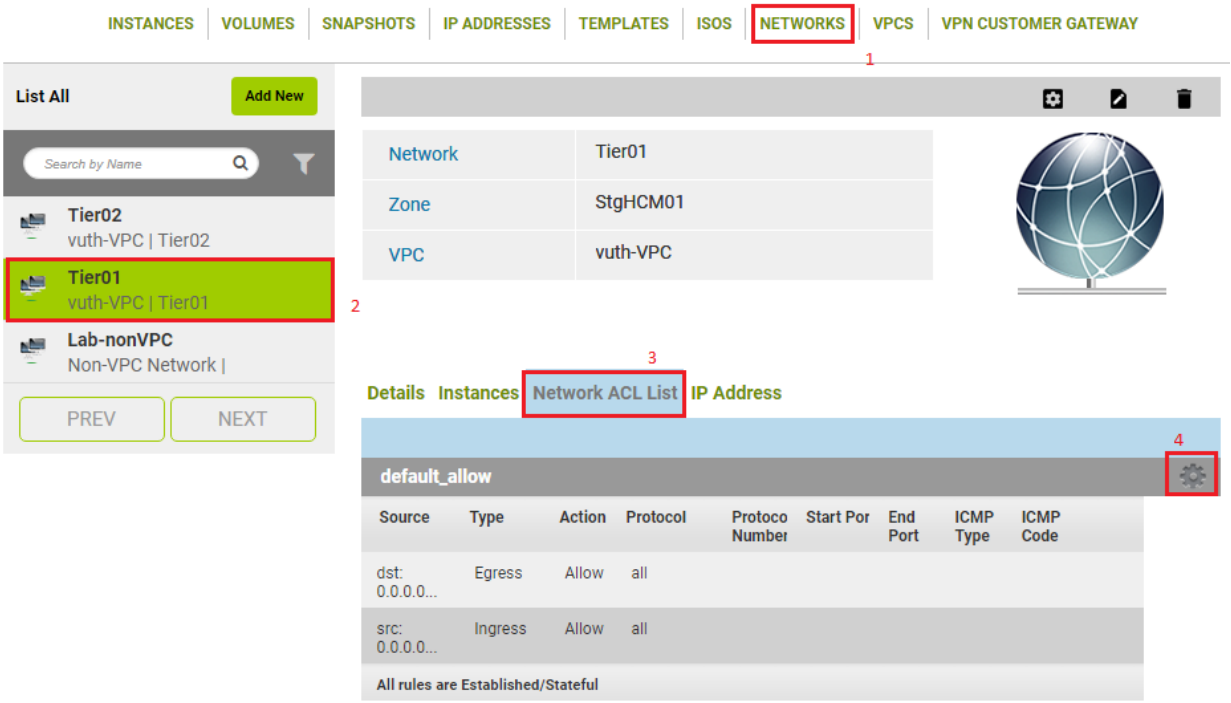
Tiên hành thêm rule cho phep Ping từ bên ngoài vào VPC network, mặc định sẽ sử dụng ICMP type 8 và ICMP code 0:



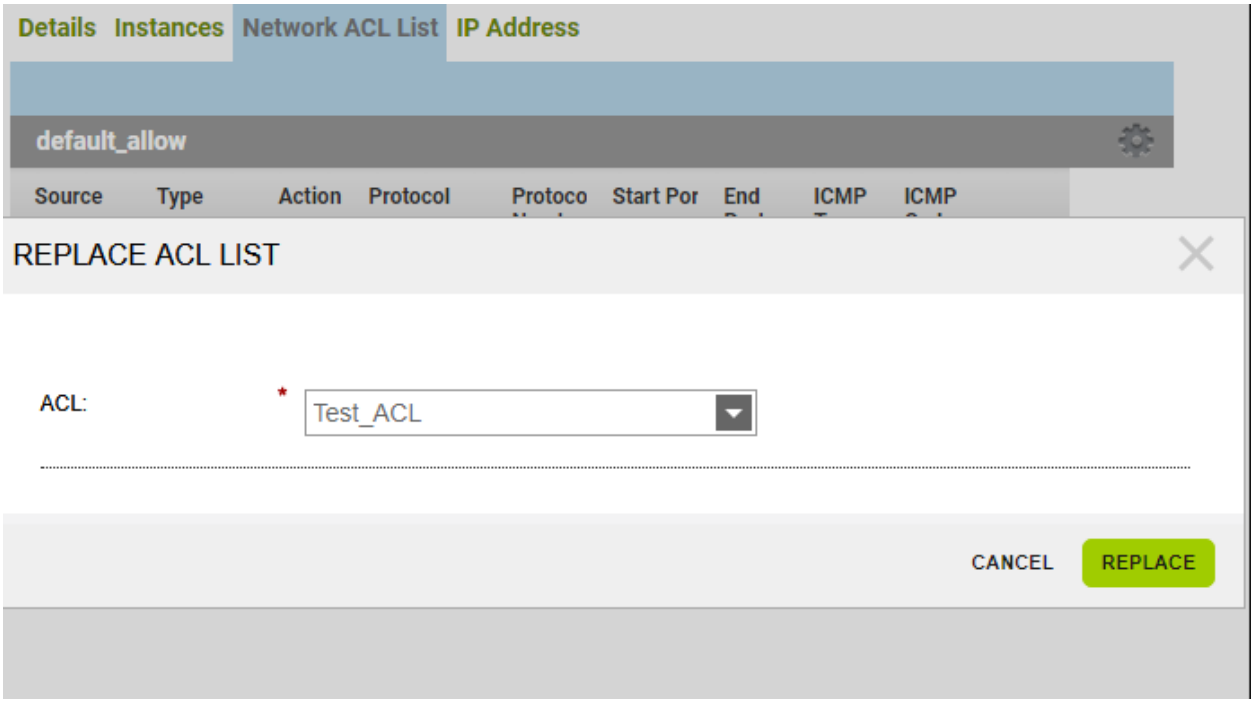
Tiến hành thêm rule cho phép port 22:



Bước 4: Sau khi cấu hình ACL xong ta tiến hành chỉ định ACL cho một Tier. Ở tab NETWORK ta chọn Tier cần được áp dụng ACL mới. Ở đây là Tier1 và mặc định khi khởi tạo đã được áp dụng ACL là default_allow. Ta sẽ tiến hành thay thế bằng Test_ACL



Chọn biểu tượng setting [4] hộp thoại hiện ra.



Chọn ACL mới tạo là Test_ACL sau đó nhấn REPLACE

Bước 5: Đây là kết quả sau khi đã thay đổi ACL.