



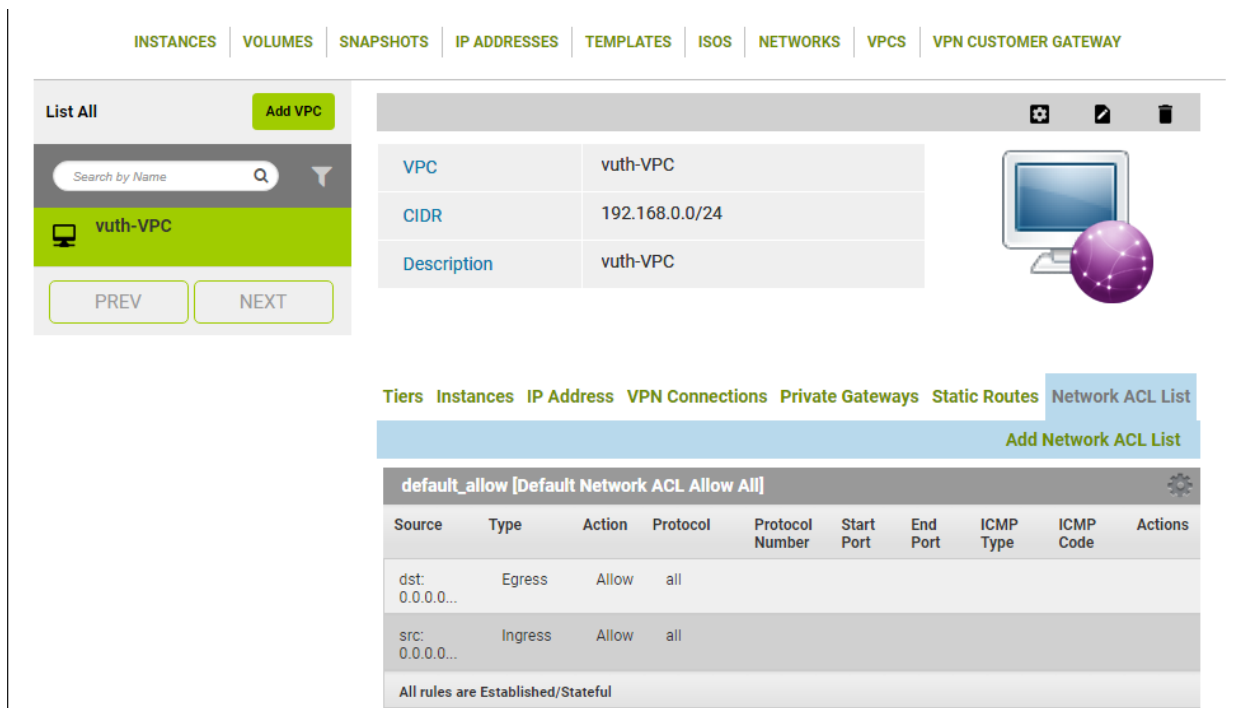
Network Access Control List

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**



The screenshot shows the FPT HI GIO CLOUD console interface. At the top, there are navigation tabs: INSTANCES, VOLUMES, SNAPSHOTS, IP ADDRESSES, TEMPLATES, ISOS, NETWORKS, VPCS, and VPN CUSTOMER GATEWAY. The 'VPCS' tab is selected.

On the left side, there is a sidebar with a search bar labeled 'Search by Name' and a dropdown menu showing 'vuth-VPC'. Below the search bar are 'PREV' and 'NEXT' buttons.

The main content area displays the details for the 'vuth-VPC' VPC:

VPC	vuth-VPC
CIDR	192.168.0.0/24
Description	vuth-VPC

Below the VPC details, there is a navigation bar with tabs: Tiers, Instances, IP Address, VPN Connections, Private Gateways, Static Routes, and Network ACL List. The 'Network ACL List' tab is selected.

Under the 'Network ACL List' tab, there is a button 'Add Network ACL List' and a table showing the default network ACL rules:


default_allow [Default Network ACL Allow All]									
Source	Type	Action	Protocol	Protocol Number	Start Port	End Port	ICMP Type	ICMP Code	Actions
dst: 0.0.0.0...	Egress	Allow	all						
src: 0.0.0.0...	Ingress	Allow	all						


At the bottom of the table, it states: 'All rules are Established/Stateful'.

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

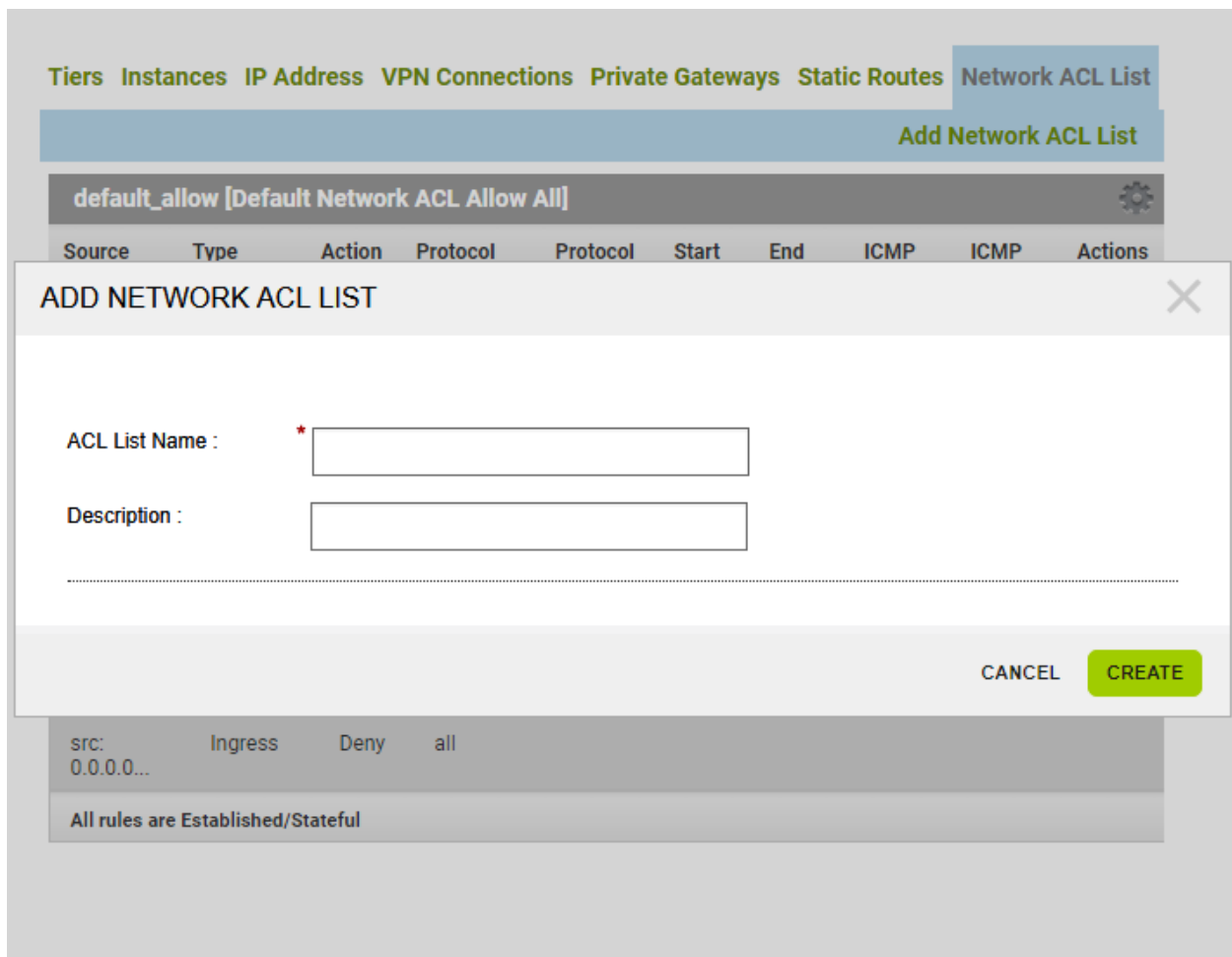
Tiers Instances IP Address VPN Connections Private Gateways Static Routes **Network ACL List**

Add Network ACL List

default_allow [Default Network ACL Allow All] 									
Source	Type	Action	Protocol	Protocol Number	Start Port	End Port	ICMP Type	ICMP Code	Actions
dst: 0.0.0.0...	Egress	Allow	all						
src: 0.0.0.0...	Ingress	Allow	all						
All rules are Established/Stateful									

default_deny [Default Network ACL Deny All] 									
Source	Type	Action	Protocol	Protocol Number	Start Port	End Port	ICMP Type	ICMP Code	Actions
dst: 0.0.0.0...	Egress	Deny	all						
src: 0.0.0.0...	Ingress	Deny	all						
All rules are Established/Stateful									

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**.



The screenshot shows a web interface for managing Network ACL Lists. A modal dialog titled "ADD NETWORK ACL LIST" is open, featuring two input fields: "ACL List Name" (marked with a red asterisk) and "Description". Below the fields are "CANCEL" and "CREATE" buttons. The background interface includes a navigation menu with "Network ACL List" selected, a table with columns for "Source", "Type", "Action", "Protocol", "Start", "End", "ICMP", and "Actions", and a row for "default_allow [Default Network ACL Allow All]".

Sau khi tạo xong ta được một ACL mới.

Tiers Instances IP Address VPN Connections Private Gateways Static Routes **Network ACL List**

Add Network ACL List

Test_ACL [Huong dan tao ACL] ⚙️

Source	Type	Action	Protocol	Protocol Number	Start Port	End Port	ICMP Type	ICMP Code	Actions
<input type="text" value="0.0.0.0/0"/>	Ingress ▼	Allow	TCP ▼		<input type="text"/>	<input type="text"/>			+

All rules are Established/Stateful

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...)

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

Test_ACL [Huong dan tao ACL] ⚙️

Source	Type	Action	Protocol	Protocol Number	Start Port	End Port	ICMP Type	ICMP Code	Actions
<input type="text" value="0.0.0.0/0"/>	Ingress ▼	Allow	TCP ▼		<input type="text"/>	<input type="text"/>			+
src: 0.0.0.0...	Ingress	Allow	icmp				8	0	Edit Delete

All rules are Established/Stateful

Tiến hành thêm rule cho phép port 22:

Test_ACL [Huong dan tao ACL]									
Source	Type	Action	Protocol	Protocol Number	Start Port	End Port	ICMP Type	ICMP Code	Actions
0.0.0.0/0	Ingress	Allow	TCP						+
src: 0.0.0.0...	Ingress	Allow	tcp		22	22			Edit Delete
src: 0.0.0.0...	Ingress	Allow	icmp				8	0	Edit Delete
All rules are Established/Stateful									

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

INSTANCES | VOLUMES | SNAPSHOTS | IP ADDRESSES | TEMPLATES | ISOS | **NETWORKS** | VPCS | VPN CUSTOMER GATEWAY

1

Network	Tier01
Zone	StgHCM01
VPC	vuth-VPC

2

3

Details Instances **Network ACL List** IP Address

default_allow									
Source	Type	Action	Protocol	Protocol Number	Start Port	End Port	ICMP Type	ICMP Code	
dst: 0.0.0.0...	Egress	Allow	all						
src: 0.0.0.0...	Ingress	Allow	all						
All rules are Established/Stateful									

4

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

Details Instances **Network ACL List** IP Address

default_allow


Source	Type	Action	Protocol	Protoco	Start Por	End	ICMP	ICMP
REPLACE ACL LIST								
ACL:	* Test_ACL							
							CANCEL	REPLACE

Chọn ACL mới tạo là Test_ACL sau đó nhấn REPLACE

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

Replace ACL List Succeeded

Network	Tier01
Zone	StgHCM01
VPC	vuth-VPC



Details Instances **Network ACL List** IP Address

Test_ACL

Source	Type	Action	Protocol	Protoco Number	Start Por	End Port	ICMP Type	ICMP Code
src: 0.0.0.0...	Ingress	Allow	tcp		22	22		
src: 0.0.0.0...	Ingress	Allow	icmp				8	0
All rules are Established/Stateful								