

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BTL: TRIỂN KHAI NSM CHO OPENSTACK
HỌC PHẦN: KỸ THUẬT THEO DÕI VÀ GIÁM SÁT AN TOÀN
MẠNG
MÃ HỌC PHẦN: INT1429M**

NHÓM LỚP: D21CQAT01 - B

Sinh viên thực hiện:

B21DCAT193 Mai Đức Trung

Giảng viên: Ninh Thị Thu Trang

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
CHƯƠNG 1. Triển khai hệ thống OpenStack.....	5
1.1 Demo hệ thống sử dụng mạng ảo trên OpenStack	5
1.1.1 Mô hình hệ thống	5
1.1.2 Quá trình cài đặt	5
1.1.3 Triển khai hệ thống	11

DANH MỤC CÁC HÌNH VẼ

Hình 1 Sơ đồ mạng hệ thống.....	5
Hình 2 Cấu hình floating IP trên Pfsense	5
Hình 3 Cấu hình NAT forwarding trên Pfsense	6
Hình 4 Cấu hình rule WAN trong Pfsense	6
Hình 5 Rule Snort trên WAN Interface.....	6
Hình 6 Rule Snort trên LAN interface	7
Hình 7 Lấy mật khẩu admin OpenStack	7
Hình 8 Giao diện đăng nhập OpenStack	8
Hình 9 Các dải mạng được cấu hình	8
Hình 10 Các security group.....	8
Hình 11 Cấu hình rule trong security group.....	9
Hình 12 Cấu hình router OpenStack	9
Hình 13 Cấu hình interface cho các router để kết nối mạng internal với external.....	9
Hình 14 Các instance trong hệ thống	10
Hình 15 Cấu hình Port Forwarding trên máy chủ OpenStack.....	10
Hình 16 SSH từ WAN vào instance trên dải 192.168.222.0/24.....	11
Hình 17 SSH từ WAN vào instance trên dải 20.20.0.0/24.....	11
Hình 18 Alert trên Snort theo dõi các cố gắng SSH đến instance từ WAN.....	12
Hình 19 SSH từ LAN vào instance trên dải 20.20.0.0/24	12
Hình 20 SSH từ LAN vào instance trên dải 192.168.222.0/24	12
Hình 21 Alert trên Snort theo dõi các cố gắng SSH đến instance từ LAN	13
Hình 22 Tiến hành tấn công DOS và quét cổng trên máy chủ OpenStack	13
Hình 23 Alert trên Snort theo dõi các cố gắng tấn công đến máy chủ OpenStack	13
Hình 24 Kết nối giữa 2 instance khác security group	14

DANH MỤC CÁC TỪ VIẾT TẮT

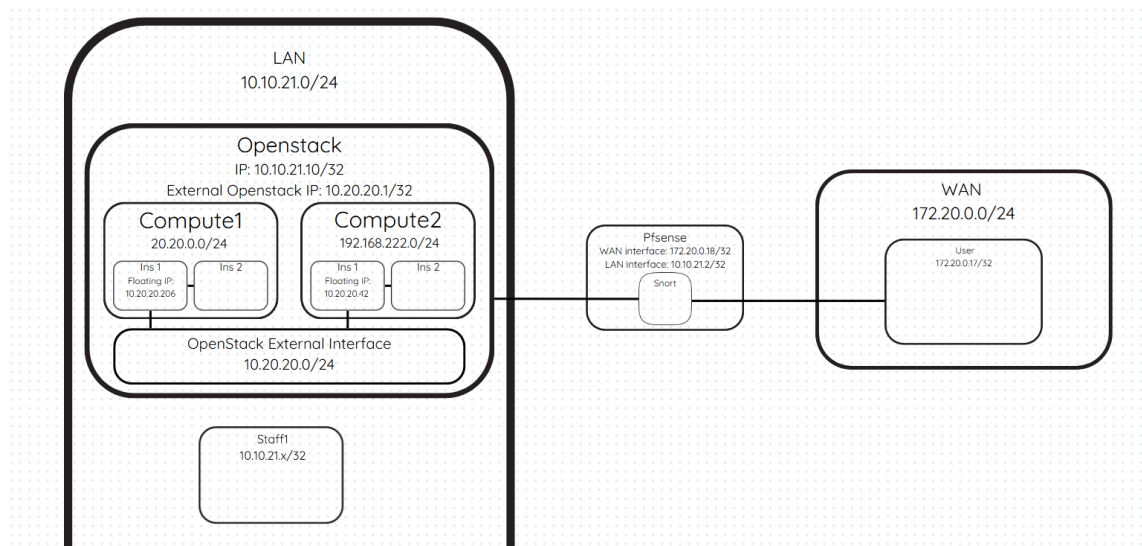
Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
IP	Internet Protocol	Giao thức định địa chỉ và định tuyến cho các thiết bị trong mạng.
TCP	Transmission Control Protocol	Giao thức truyền tin cậy, đảm bảo dữ liệu được gửi đến đúng thứ tự và không bị mất mát.
WAN	Wide Area Network	Mạng diện rộng, kết nối nhiều mạng LAN ở các khu vực địa lý khác nhau.
LAN	Local Area Network	Mạng cục bộ, kết nối các thiết bị trong phạm vi nhỏ như nhà, văn phòng.
NAT	Network Address Translation	Cơ chế chuyển đổi địa chỉ IP riêng thành IP công cộng và ngược lại.
SSH	Secure Shell	Giao thức truy cập từ xa an toàn qua mạng, thường dùng để quản lý máy chủ.
DOS	Denial of Service	Tấn công từ chối dịch vụ nhằm làm hệ thống không thể phục vụ người dùng hợp lệ.

CHƯƠNG 1. TRIỂN KHAI HỆ THỐNG OPENSTACK

1.1 Demo hệ thống sử dụng mạng ảo trên OpenStack

1.1.1 Mô hình hệ thống

Hệ thống xây dựng giả định sẽ cung cấp 2 cụm máy ảo cho 2 khách hàng riêng biệt. Máy chủ chạy OpenStack sẽ được đặt sau tường lửa chạy công cụ Snort để theo dõi các gói tin đi vào các instance.



Hình 1 Sơ đồ mạng hệ thống

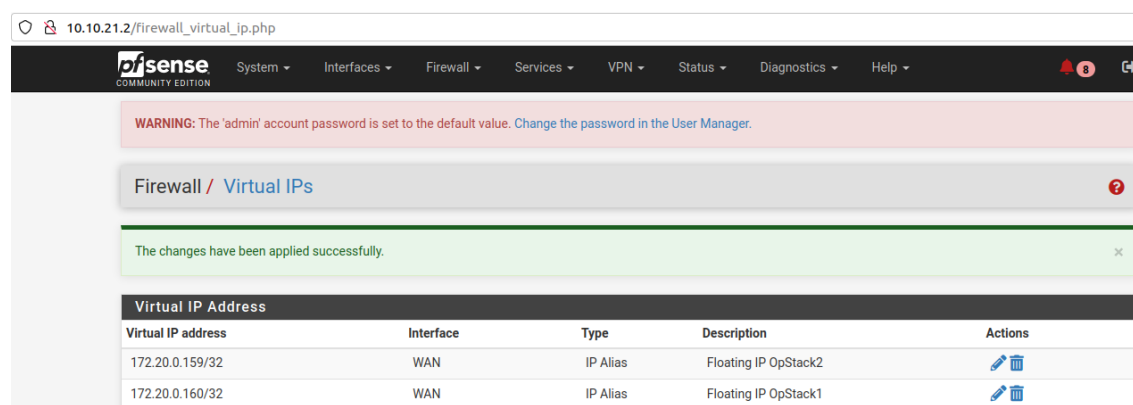
Các máy user từ ngoài mạng WAN muốn truy cập vào các Instance trong OpenStack sẽ đi qua route như sau:

- Gói tin TCP gửi đến PfSense qua floating IP tạo bởi tường lửa
- Tường lửa chuyển tiếp gói tin TCP qua máy chủ OpenStack.
- Máy chủ OpenStack chuyển tiếp gói tin TCP đến Instance.

1.1.2 Quá trình cài đặt

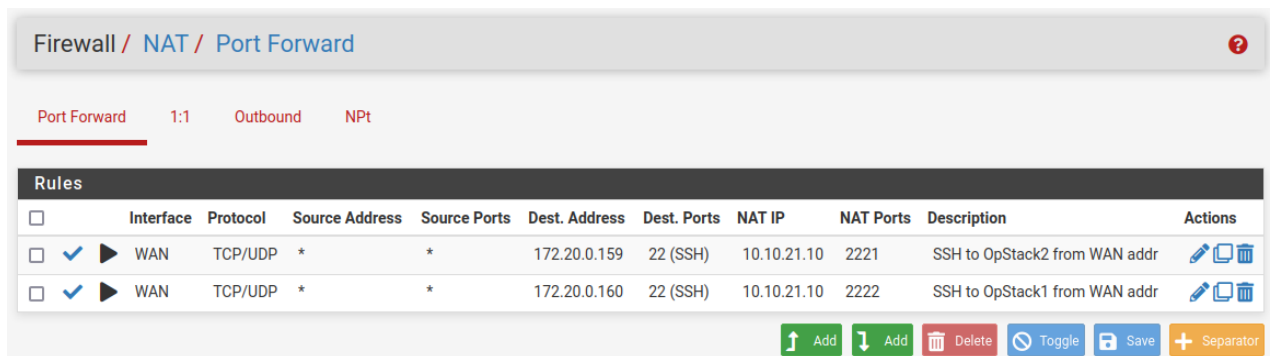
1.1.2.1 Cài đặt tường lửa PfSense.

- Ta cần tạo các floating IP trên PfSense để kết nối instance với WAN interface



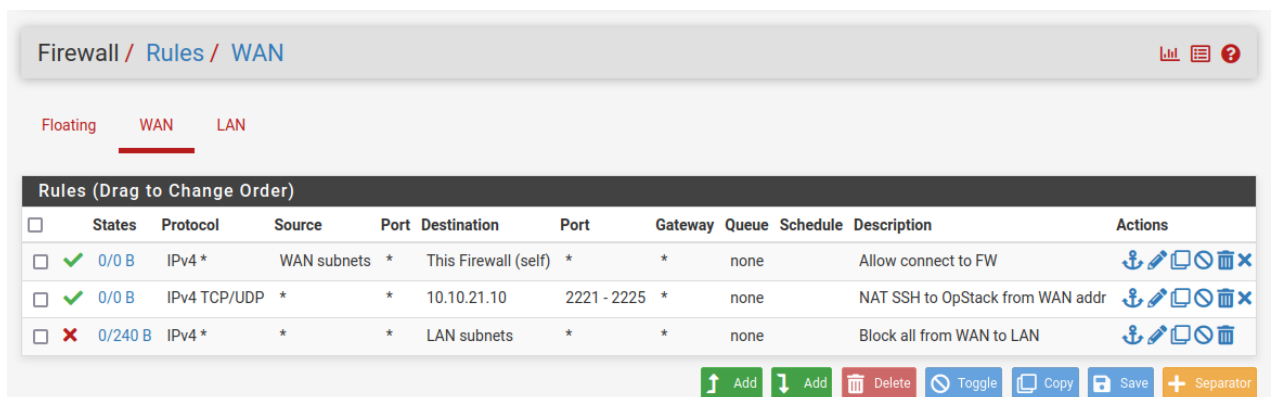
Hình 2 Cấu hình floating IP trên PfSense

- Tiếp theo ta cấu hình NAT forwarding để chuyển tiếp gói tin đến máy chủ OpenStack trên LAN interface, gửi gói tin cụ thể đến port cố định cấu hình riêng cho từng instance.



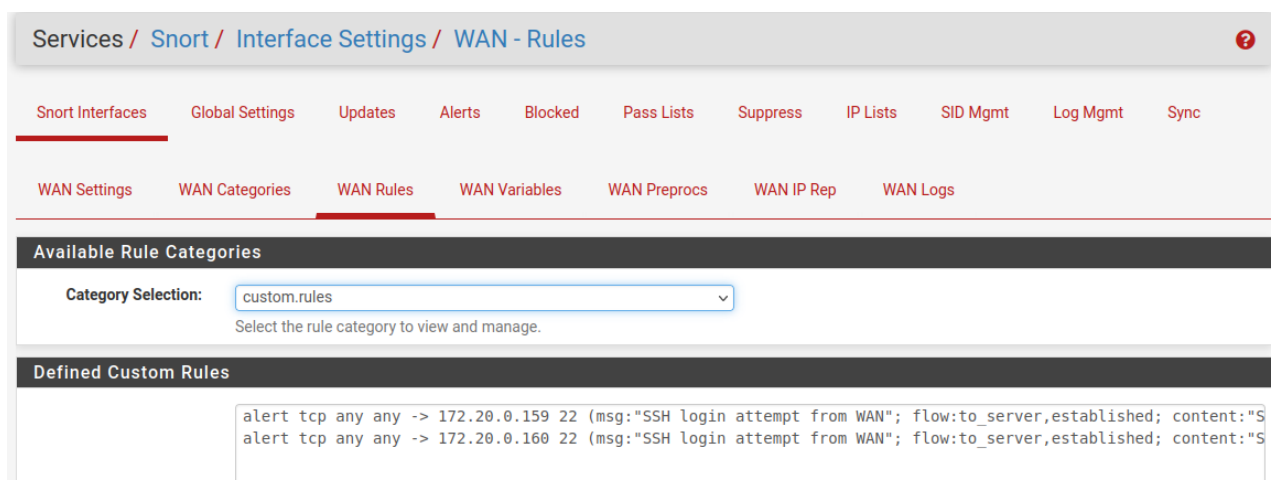
Hình 3 Cấu hình NAT forwarding trên PfSense

- Tiếp theo ta cần cấu hình rule để cho phép máy từ ngoài WAN có thể truy cập được và chặn các truy cập khác.

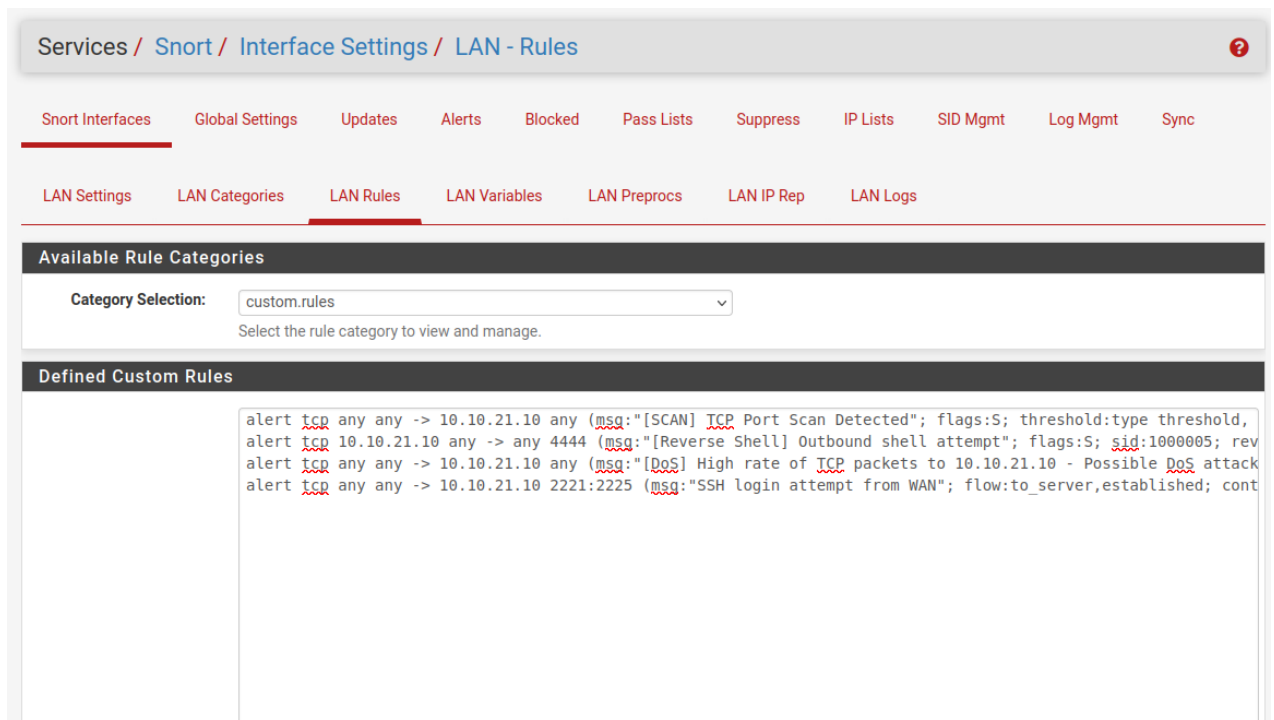


Hình 4 Cấu hình rule WAN trong PfSense

- Cấu hình các rule Snort trên tường lửa để bắt các gói tin truy cập đến các instance OpenStack.



Hình 5 Rule Snort trên WAN Interface



Hình 6 Rule Snort trên LAN interface

1.1.2.2 Cài đặt máy chủ OpenStack

Hệ thống này sẽ sử dụng phiên bản OpenStack đơn giản và nhẹ hơn được cung cấp bởi Canonical (hãng phát triển Ubuntu) và được phân phối qua Snap.

- Để cài đặt hệ thống, ta chạy lệnh:

```
sudo snap install microstack --beta --devmode
```

- Tiếp theo, ta cài đặt openstack tự động theo mặc định bằng lệnh

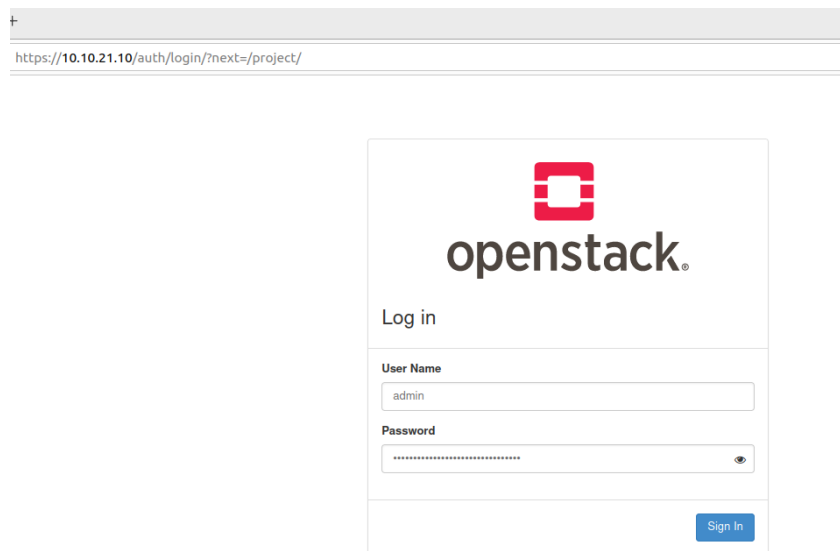
```
sudo microstack init --auto --control
```

- Sau khi cài đặt xong hệ thống OpenStack, chạy lệnh sau để lấy mật khẩu người dùng OpenStack


```
trung@trung-virtual-machine:~$ sudo snap get microstack config.credentials.keystone-password
[sudo] password for trung:
j49YR03nXotu48b9596mSNDXaVBFRKzd
trung@trung-virtual-machine:~$
```

Hình 7 Lấy mật khẩu admin OpenStack

- Sau đó, trên trình duyệt truy cập vào ip của máy triển khai OpenStack, tài khoản mặc định là admin với mật khẩu là dãy kí tự lấy được ở trên.



https://10.10.21.10/auth/login/?next=/project/



openstack.

Log in

User Name

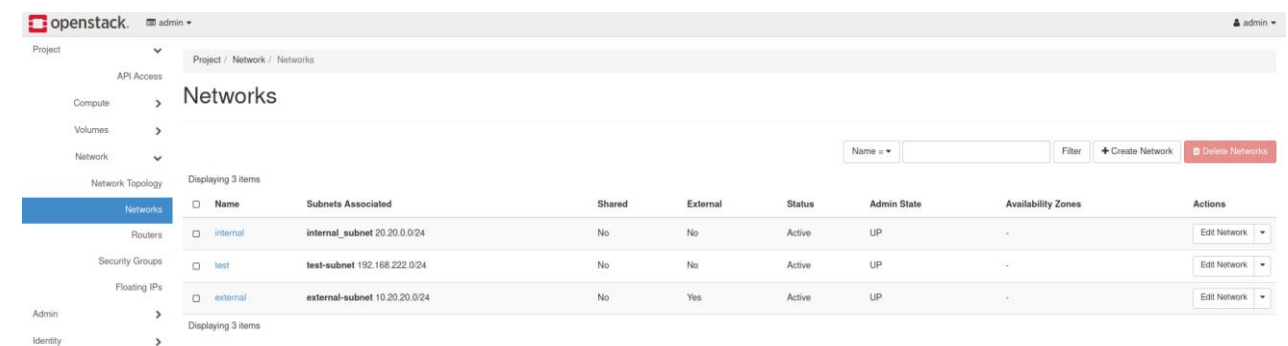
admin

Password

Sign In

Hình 8 Giao diện đăng nhập OpenStack

- Sau khi đăng nhập vào giao diện quản lý OpenStack, ta tiến hành cấu hình mạng cho hệ thống OpenStack



Project / Network / Networks

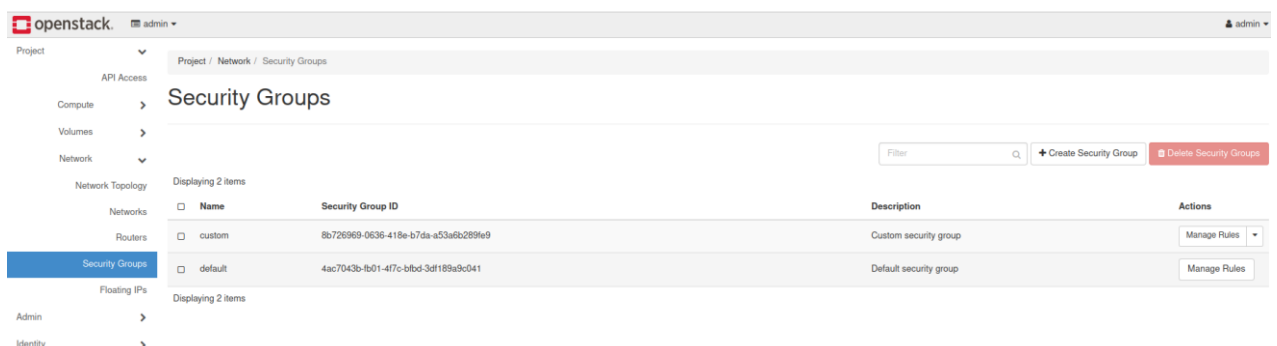
Networks

Displaying 3 items

Name	Subnets Associated	Shared	External	Status	Admin State	Availability Zones	Actions
internal	internal_subnet 20.20.0.0/24	No	No	Active	UP	-	Edit Network
test	test_subnet 192.168.222.0/24	No	No	Active	UP	-	Edit Network
external	external_subnet 10.20.20.0/24	No	Yes	Active	UP	-	Edit Network

Hình 9 Các dải mạng được cấu hình

- Vì có 2 người dùng tách biệt nên ta cũng cần tạo 2 security group riêng biệt cho từng cụm instance để tách biệt chúng.



Project / Network / Security Groups

Security Groups

Displaying 2 items

Name	Security Group ID	Description	Actions
custom	8b726969-0636-418e-b7da-a53a6b289fe9	Custom security group	Manage Rules
default	4ac7043b-b011-4f7c-bfb3-df189a9c0411	Default security group	Manage Rules

Hình 10 Các security group

- Cấu hình các rule trong security group. Ở đây ta cho phép tất cả gói tin đi ra (Egress) và cho phép tất cả các gói tin đi vào (Ingress) với các instance cùng security group (Các instance cùng cụm). Ngoài ra ta cho phép gói tin TCP đến cổng 22 từ 10.20.20.1/32 (IP của máy chủ OpenStack trên External Network của hệ thống mạng OpenStack)

Displaying 6 items

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
<input type="checkbox"/>	Egress	IPv6	Any	Any	:::0	-	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	Any	Any	-	custom	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	10.20.20.1/32	-	-	Delete Rule
<input type="checkbox"/>	Ingress	IPv6	Any	Any	-	custom	-	Delete Rule

Displaying 6 items

Hình 11 Cấu hình rule trong security group

- Cấu hình router để kết nối mạng internal của cụm instance ra ngoài mạng external

openstack admin

Project / Network / Routers

Routers

Router Name: Filter [+ Create Router](#) [Delete Routers](#)

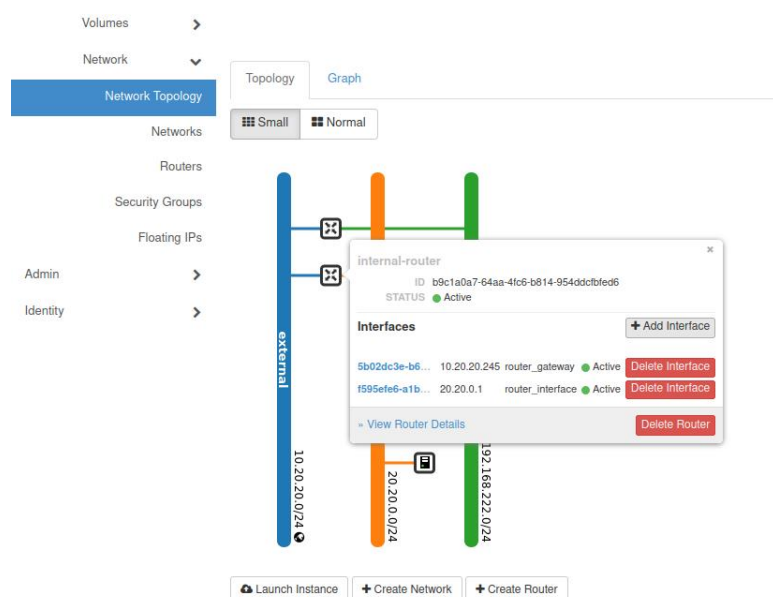
Displaying 2 items

<input type="checkbox"/>	Name	Status	External Network	Admin State	Availability Zones	Actions
<input type="checkbox"/>	test-router	Active	external	UP	-	Clear Gateway
<input type="checkbox"/>	internal-router	Active	external	UP	-	Clear Gateway

Displaying 2 items

Hình 12 Cấu hình router OpenStack

- Cấu hình interface tương ứng cho các router



Hình 13 Cấu hình interface cho các router để kết nối mạng internal với external

- Tiến hành tạo các instance trên OpenStack, lưu ý cần xác định rõ dải mạng và security group của các instance. Ở đây có 2 cụm instance, mỗi cụm có 2 instance và chỉ có một instance mỗi cụm được cấp floating IP để kết nối với bên ngoài.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
test-2	cirros	192.168.222.87, 10.20.20.42	m1.tiny	-	Shutoff	nova	None	Shut Down	1 week, 3 days	Start Instance
test-1	cirros	192.168.222.220	m1.tiny	-	Shutoff	nova	None	Shut Down	1 week, 3 days	Start Instance
internal-2	cirros	20.20.0.155, 10.20.20.206	m1.tiny	-	Shutoff	nova	None	Shut Down	1 week, 3 days	Start Instance
internal-1	cirros	20.20.0.131	m1.tiny	-	Shutoff	nova	None	Shut Down	1 week, 3 days	Start Instance

Hình 14 Các instance trong hệ thống

- Tiến hành cấu hình Port Forwarding trên máy chủ OpenStack, cấu hình đường vào qua port cố định đến floating IP của instance cổng 22 để cho phép SSH và đường ra cấu hình đi từ floating IP của instance ra đến IP của máy chủ OpenStack trên External Network (10.20.20.1), ở đây ta sử dụng các lệnh:

sudo iptables -t nat -A PREROUTING -i ens33 -p tcp --dport <port forward> -j DNAT --to-destination <Instance floating IP>:22

sudo iptables -t nat -A POSTROUTING -d <Instance floating IP> -p tcp --dport 22 -j SNAT --to-source 10.20.20.1

```

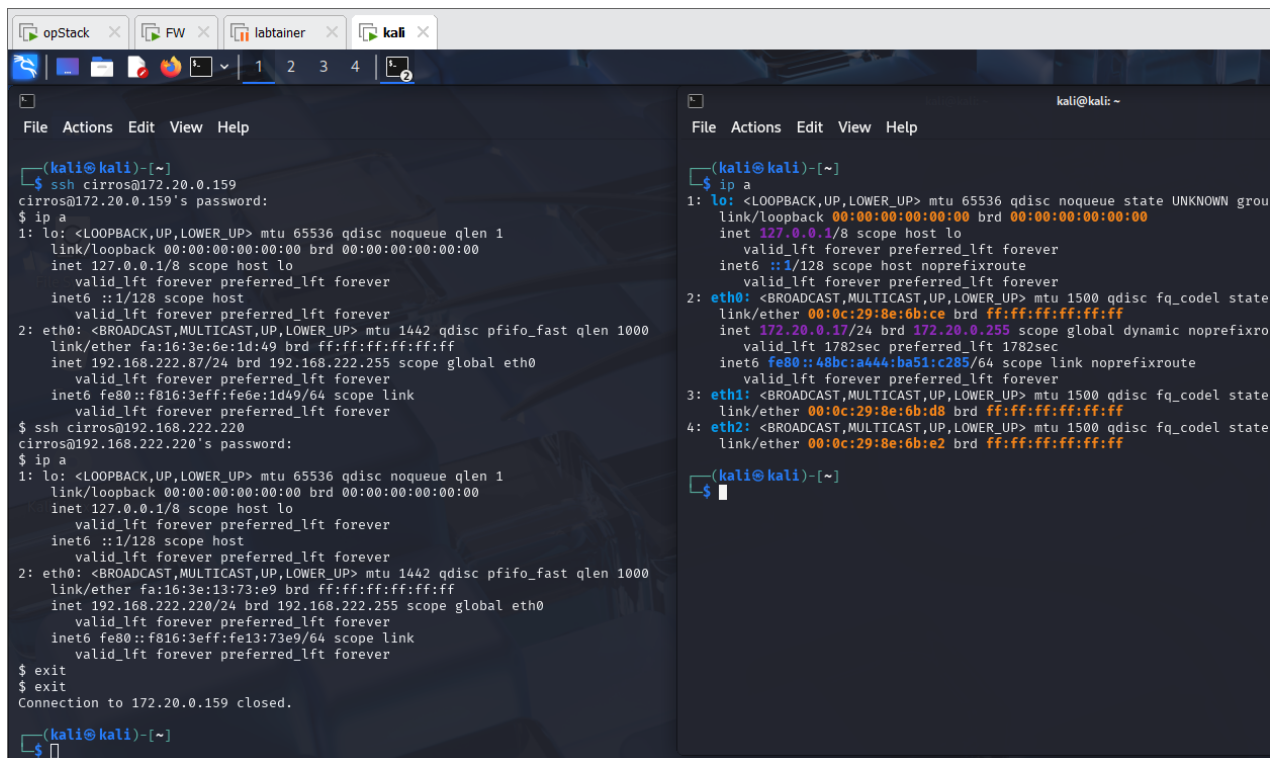
trung@trung-virtual-machine:~$ sudo iptables -t nat -L -n -v
[sudo] password for trung:
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain PREROUTING (policy ACCEPT 6 packets, 1172 bytes)
 pkts bytes target    prot opt in     out     source    destination
    4   240 DNAT      tcp  --  ens33  *      0.0.0.0/0      0.0.0.0/0      tcp dpt:2222 to:10.20.20.206:22
    2   120 DNAT      tcp  --  ens33  *      0.0.0.0/0      0.0.0.0/0      tcp dpt:2221 to:10.20.20.42:22
Chain INPUT (policy ACCEPT 6 packets, 1172 bytes)
 pkts bytes target    prot opt in     out     source    destination
Chain OUTPUT (policy ACCEPT 21664 packets, 1491K bytes)
 pkts bytes target    prot opt in     out     source    destination
Chain POSTROUTING (policy ACCEPT 21653 packets, 1490K bytes)
 pkts bytes target    prot opt in     out     source    destination
    4   240 SNAT      tcp  --  *      *      0.0.0.0/0      10.20.20.206      tcp dpt:22 to:10.20.20.1
    2   120 SNAT      tcp  --  *      *      0.0.0.0/0      10.20.20.42      tcp dpt:22 to:10.20.20.1
trung@trung-virtual-machine:~$

```

Hình 15 Cấu hình Port Forwarding trên máy chủ OpenStack

1.1.3 Triển khai hệ thống

- Trước tiên, ta vào vị trí client truy cập từ ngoài WAN vào OpenStack, client có thể SSH vào instance qua các floating IP 172.20.0.159 và 172.20.0.160. Từ máy instance có floating IP SSH đến các instance còn lại trong cụm máy ảo.

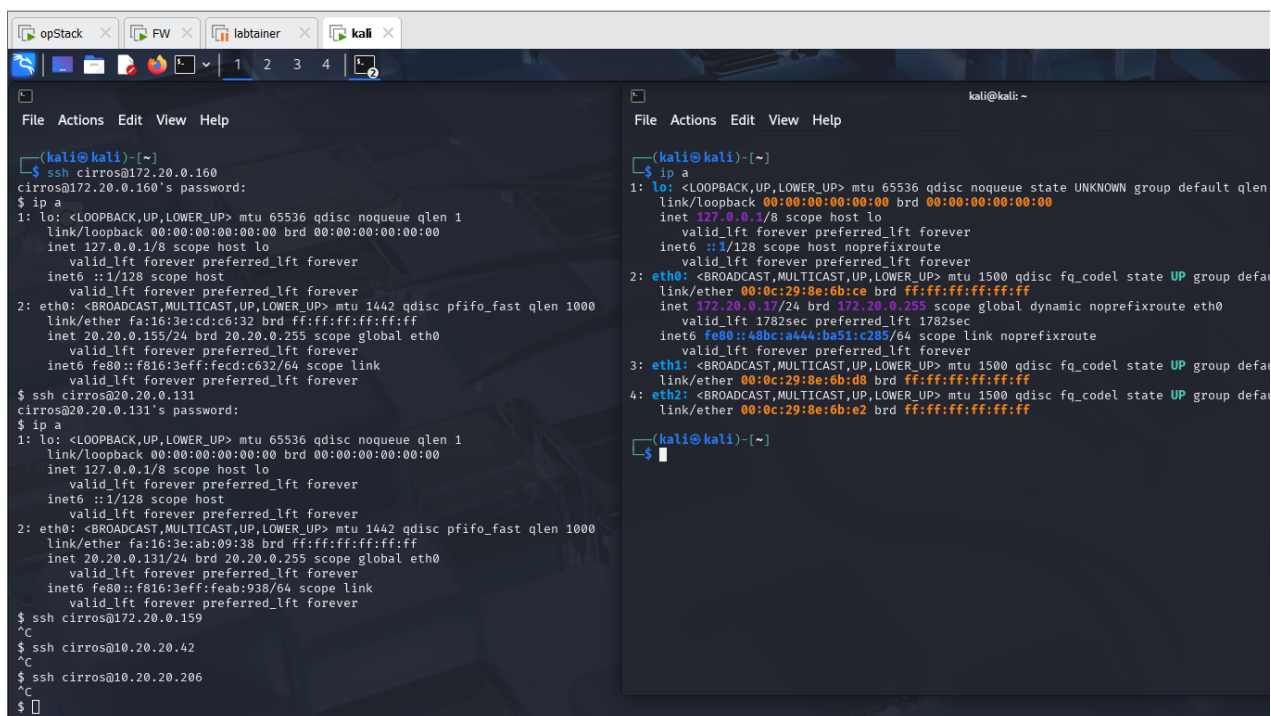


The image shows two terminal windows side-by-side. The left window is a Kali terminal with tabs for 'opStack', 'FW', 'labtainer', and 'kali'. It shows a sequence of SSH connections from a Kali machine to three OpenStack instances: 172.20.0.159, 192.168.222.220, and 192.168.222.220. The right window is another Kali terminal showing the output of the 'ip a' command on the first instance, displaying network interfaces 'lo', 'eth0', 'eth1', and 'eth2' with their respective IP addresses and MAC addresses.

```
(kali@kali)-[~]
$ ssh cirros@172.20.0.159
cirros@172.20.0.159's password:
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen 1000
    link/ether fa:16:3e:6e:1d:49 brd ff:ff:ff:ff:ff:ff
    inet 192.168.222.87/24 brd 192.168.222.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe6e:1d49/64 scope link
        valid_lft forever preferred_lft forever
$ ssh cirros@192.168.222.220
cirros@192.168.222.220's password:
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen 1000
    link/ether fa:16:3e:13:73:e9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.222.220/24 brd 192.168.222.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe13:73e9/64 scope link
        valid_lft forever preferred_lft forever
$ exit
$ exit
Connection to 172.20.0.159 closed.

(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 00:0c:29:8e:6b:ce brd ff:ff:ff:ff:ff:ff
    inet 172.20.0.17/24 brd 172.20.0.255 scope global dynamic noprefixroute eth0
        valid_lft 1782sec preferred_lft 1782sec
    inet6 fe80::48bc:a444:ba51:c285/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 00:0c:29:8e:6b:d8 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 00:0c:29:8e:6b:e2 brd ff:ff:ff:ff:ff:ff
```

Hình 16 SSH từ WAN vào instance trên dải 192.168.222.0/24



The image shows two terminal windows side-by-side. The left window is a Kali terminal with tabs for 'opStack', 'FW', 'labtainer', and 'kali'. It shows a sequence of SSH connections from a Kali machine to three OpenStack instances: 172.20.0.160, 20.20.0.131, and 20.20.0.131. The right window is another Kali terminal showing the output of the 'ip a' command on the first instance, displaying network interfaces 'lo', 'eth0', 'eth1', and 'eth2' with their respective IP addresses and MAC addresses.

```
(kali@kali)-[~]
$ ssh cirros@172.20.0.160
cirros@172.20.0.160's password:
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen 1000
    link/ether fa:16:3e:cd:c6:32 brd ff:ff:ff:ff:ff:ff
    inet 20.20.0.155/24 brd 20.20.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fedc:c632/64 scope link
        valid_lft forever preferred_lft forever
$ ssh cirros@20.20.0.131
cirros@20.20.0.131's password:
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen 1000
    link/ether fa:16:3e:ab:09:38 brd ff:ff:ff:ff:ff:ff
    inet 20.20.0.131/24 brd 20.20.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:feab:938/64 scope link
        valid_lft forever preferred_lft forever
$ ssh cirros@172.20.0.159
^C
$ ssh cirros@10.20.20.42
^C
$ ssh cirros@10.20.20.206
^C
$
```

Hình 17 SSH từ WAN vào instance trên dải 20.20.0.0/24

Services / Snort / Alerts

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Alert Log View Settings

Interface to Inspect: WAN (em0) Auto-refresh view: [checked] 250 Alert lines to display. Save

Alert Log Actions: Download Clear

Alert Log View Filter

5 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	UID:SID	Description
2025-05-05 04:57:58	⚠	1	TCP	Attempted User Privilege Gain	172.20.0.17	42994	172.20.0.160	22	1:1000055	SSH login attempt from WAN
2025-05-05 04:57:49	⚠	1	TCP	Attempted User Privilege Gain	172.20.0.17	46784	172.20.0.160	22	1:1000055	SSH login attempt from WAN
2025-05-05 04:51:04	⚠	1	TCP	Attempted User Privilege Gain	172.20.0.17	47254	172.20.0.159	22	1:1000001	SSH login attempt from WAN
2025-05-05 04:50:08	⚠	1	TCP	Attempted User Privilege Gain	172.20.0.17	55268	172.20.0.159	22	1:1000001	SSH login attempt from WAN
2025-05-05 04:50:00	⚠	1	TCP	Attempted User Privilege Gain	172.20.0.17	55262	172.20.0.159	22	1:1000001	SSH login attempt from WAN

Hình 18 Alert trên Snort theo dõi các cố gắng SSH đến instance từ WAN

- Tiếp theo ta vào vai staff nằm trong LAN interface, người dùng này sẽ truy cập vào instance.

```
student@LabtainerVMware: ~
student@LabtainerVMware:~$ ssh cirros@10.10.21.10 -p 2222
cirros@10.10.21.10's password:
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen 1000
    link/ether fa:16:3e:cd:c6:32 brd ff:ff:ff:ff:ff:ff
    inet 20.20.0.155/24 brd 20.20.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fedc:c632/64 scope link
        valid_lft forever preferred_lft forever
$
```

```
student@LabtainerVMware: ~
ether 16:1d:8f:57:86:16 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 46 overruns 0 carrier 0 collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.21.30 netmask 255.255.255.0 broadcast 10.10.21.255
    ether 00:0c:29:04:8c:c5 txqueuelen 1000 (Ethernet)
    RX packets 172 bytes 28140 (28.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 298 bytes 39382 (39.3 KB)
    TX errors 0 dropped 2 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 291 bytes 23767 (23.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 291 bytes 23767 (23.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
student@LabtainerVMware:~$
```

Hình 19 SSH từ LAN vào instance trên dải 20.20.0.0/24

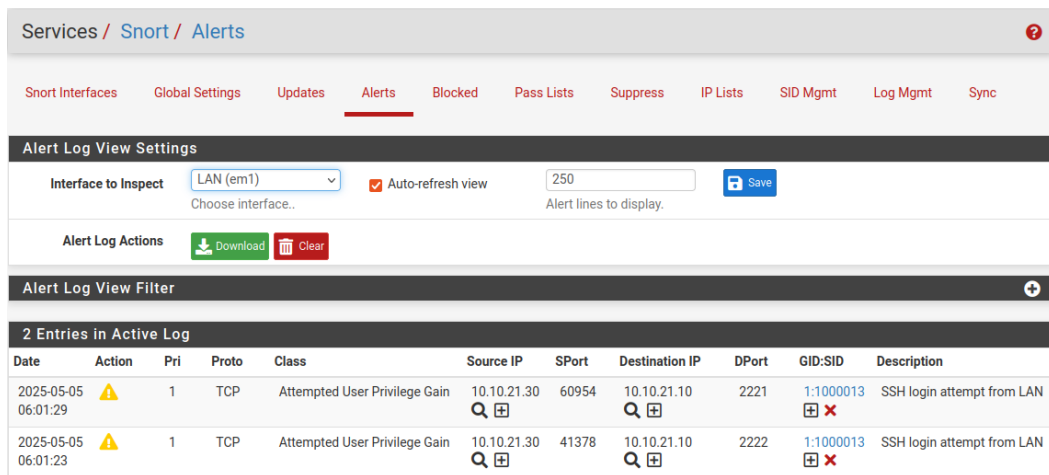
```
student@LabtainerVMware: ~
student@LabtainerVMware:~$ ssh cirros@10.10.21.10 -p 2221
cirros@10.10.21.10's password:
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen 1000
    link/ether fa:16:3e:6e:1d:49 brd ff:ff:ff:ff:ff:ff
    inet 192.168.222.87/24 brd 192.168.222.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe6e:1d49/64 scope link
        valid_lft forever preferred_lft forever
$
```

```
student@LabtainerVMware: ~
ether 16:1d:8f:57:86:16 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 46 overruns 0 carrier 0 collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.21.30 netmask 255.255.255.0 broadcast 10.10.21.255
    ether 00:0c:29:04:8c:c5 txqueuelen 1000 (Ethernet)
    RX packets 172 bytes 28140 (28.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 298 bytes 39382 (39.3 KB)
    TX errors 0 dropped 2 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 291 bytes 23767 (23.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 291 bytes 23767 (23.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
student@LabtainerVMware:~$
```

Hình 20 SSH từ LAN vào instance trên dải 192.168.222.0/24

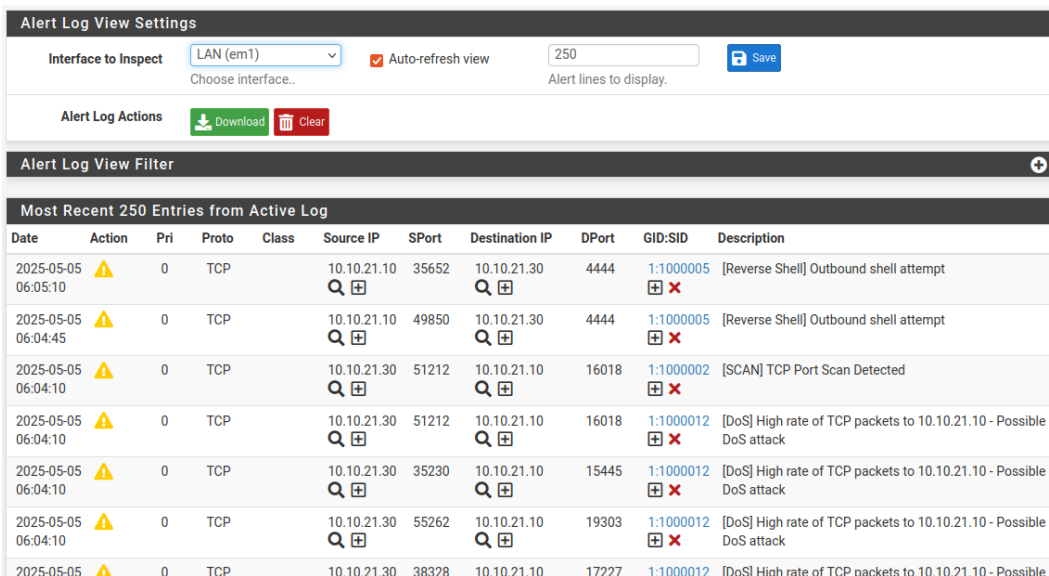


Hình 21 Alert trên Snort theo dõi các cố gắng SSH đến instance từ LAN

- Tiếp theo, ta tiến hành kiểm thử từ máy staff vào máy chủ OpenStack

```
student@LabtainerVMware:~$ sudo hping3 -S -p 80 --flood 10.10.21.10
[sudo] password for student:
HPING 10.10.21.10 (ens33 10.10.21.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.21.10 hping statistic ---
1578309 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
student@LabtainerVMware:~$ nmap -p- -T4 -Pn 10.10.21.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-05 07:27 PDT
Nmap scan report for 10.10.21.10
Host is up (0.00097s latency).
Not shown: 65508 closed tcp ports (conn-refused)
PORT      STATE SERVICE
443/tcp   open  https
2221/tcp  open  rockwell-csp1
2222/tcp  open  EthernetIP-1
3306/tcp  open  mysql
4369/tcp  open  epmd
5000/tcp  open  upnp
5672/tcp  open  amqp
5900/tcp  open  vnc
5981/tcp  open  vnc-1
```

Hình 22 Tiến hành tấn công DOS và quét cổng trên máy chủ OpenStack



Hình 23 Alert trên Snort theo dõi các cố gắng tấn công đến máy chủ OpenStack

- Ta tiến hành thử SSH giữa 2 instance được cấp floating IP, từ đó ta nhận thấy các cụm instance đã được tách biệt. Ở đây ta thấy, theo rule của sec rule thì ta chỉ có thể ping giữa các instance để kiểm tra xem nó có thực sự kết nối được với nhau không. Ngoài ra các instance khác sec group không thể SSH được vào nhau mà chỉ cho phép SSH qua máy chủ OpenStack

The screenshot displays the OpenStack dashboard on the left and two terminal windows on the right. The dashboard shows a list of instances with columns for Instance Name, Image Name, IP Address, Flavor, Key Pair, and Status. The instances listed are test-2, test-1, internal-2, and internal-1, all using the cirros image and m1.tiny flavor.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status
test-2	cirros	192.168.222.87, 10.20.20.42	m1.tiny	-	Active
test-1	cirros	192.168.222.220	m1.tiny	-	Active
internal-2	cirros	20.20.0.155, 10.20.20.206	m1.tiny	-	Active
internal-1	cirros	20.20.0.131	m1.tiny	-	Active

The terminal windows show the following commands and outputs:

```

$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1442 qdisc pfifo_fast qlen 1000
    link/ether fa:16:3e:cd:c0:32 brd ff:ff:ff:ff:ff:ff
    inet 20.20.0.155/24 brd 20.20.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fedc:c032/64 scope link
        valid_lft forever preferred_lft forever
$ ssh cirros@10.20.20.42
ssh: Exited: Error connecting: Connection timed out
$ ping 10.20.20.42 -c 2
PING 10.20.20.42 (10.20.20.42): 56 data bytes
64 bytes from 10.20.20.42: seq=0 ttl=62 time=18.986 ms
64 bytes from 10.20.20.42: seq=1 ttl=62 time=3.716 ms

$ ifconfig
br-ex: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.20.20.1 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::44cc:29ff:fe97:b34f prefixlen 64 scopeid 0x20<link>
    ether 46:cc:29:97:b3:4f txqueuelen 1000 (Ethernet)
    RX packets 1151 bytes 154574 (154.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1787 bytes 211537 (211.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.21.10 netmask 255.255.255.0 broadcast 10.10.21.255
    inet6 fe80::d38f:534c:6acb:2dd4 prefixlen 64 scopeid 0x20<link>
  
```

Hình 24 Kết nối giữa 2 instance khác security group