



## AWS 部署 FortiGate

|    |                                                                      |
|----|----------------------------------------------------------------------|
| 版本 | V1.0                                                                 |
| 时间 | 2021 年 9 月                                                           |
| 作者 | 王祥                                                                   |
| 状态 |                                                                      |
| 反馈 | <a href="mailto:support_cn@fortinet.com">support_cn@fortinet.com</a> |

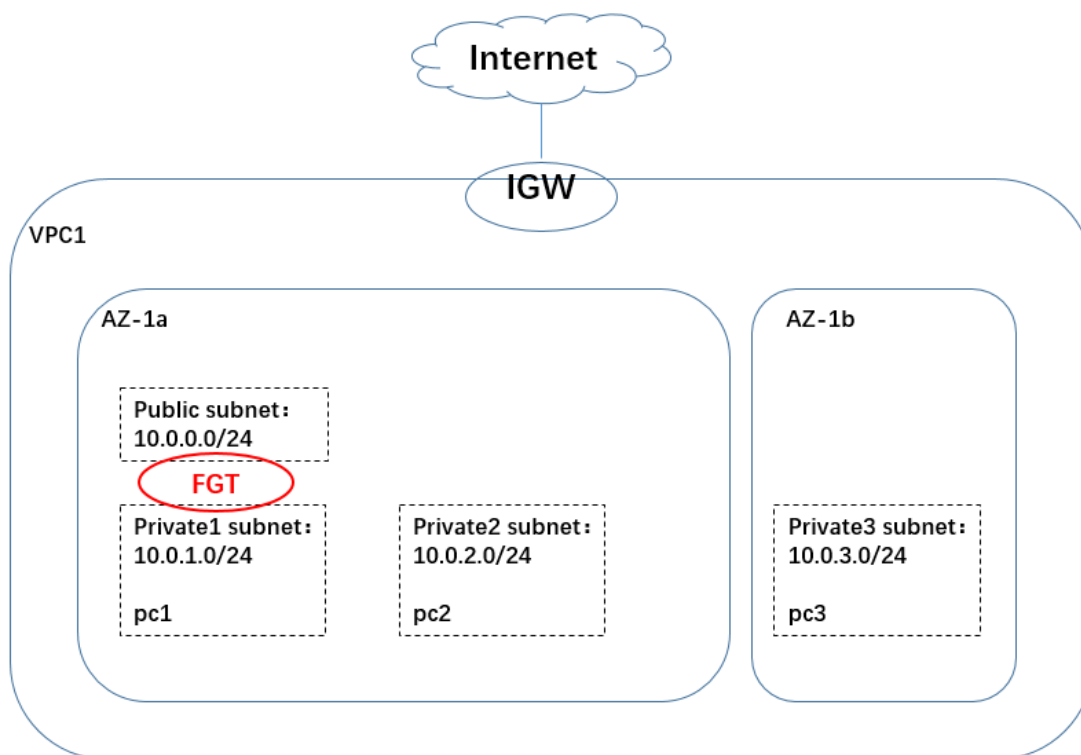
# 目录

|                                |    |
|--------------------------------|----|
| 1. 介绍 .....                    | 3  |
| 2. 网络拓扑 .....                  | 3  |
| 3. 配置步骤 .....                  | 4  |
| 3.1. 创建 VPC 和子网 .....          | 4  |
| 3.2. 创建 IGW .....              | 6  |
| 3.3. 部署 FortiGate .....        | 7  |
| 3.4. 安全组 .....                 | 10 |
| 3.5. 弹性 IP .....               | 12 |
| 3.6. AWS 路由表 .....             | 13 |
| 3.7. 访问 FortiGate .....        | 15 |
| 3.8. 禁用源/目标检查 .....            | 17 |
| 3.9. FortiGate 配置源 NAT .....   | 18 |
| 3.10. FortiGate 配置目的 NAT ..... | 19 |
| 4. 业务测试 .....                  | 22 |

## 1. 介绍

本文档介绍如何在 AWS 上安装和配置单实例 FortiGate-VM，以提供统一的威胁管理安全解决方案，保护您在 AWS 中的工作负载。

## 2. 网络拓扑



### 3. 配置步骤

#### 3.1. 创建 VPC 和子网

VPC，即一个虚拟子网。

选择 Services → VIRTUAL PRIVATE CLOUD → Your VPCs，点击 Create VPC。

VPC > Your VPCs > Create VPC

### Create VPC [Info](#)

A VPC is an isolated portion of the Amazon Web Services cloud populated by Amazon Web Services objects, such as Amazon EC2 instances.

#### VPC settings

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.

**IPv4 CIDR block** [Info](#)

**IPv6 CIDR block** [Info](#)

☒ No IPv6 CIDR block  
☐ Amazon-provided IPv6 CIDR block

**Tenancy** [Info](#)

创建完成。

| Select a VPC                        | Name           | VPC ID               | State     | IPv4 CIDR   | IPv6 CIDR | DHCP options set | Main route table      | Main  |
|-------------------------------------|----------------|----------------------|-----------|-------------|-----------|------------------|-----------------------|-------|
| <input checked="" type="checkbox"/> | wangxiang-vpc1 | vpc-0e010793150f2ee0 | Available | 10.0.0.0/16 | --        | dopt-34dc235d    | rtb-0f814bbf6d39a75ee | acl-0 |

选择 Services → VIRTUAL PRIVATE CLOUD → Subnets，点击 Create Subnet。

VPC > Subnets > Create subnet

## Create subnet [Info](#)

### VPC

VPC ID  
Create subnets in this VPC.

vpc-0e010793150f2eef0 (wangxiang-vpc1) ▼

### Associated VPC CIDRs

IPv4 CIDRs  
10.0.0.0/16

### Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

#### Subnet 1 of 1

Subnet name  
Create a tag with a key of 'Name' and a value that you specify.

wangxiang-vpc1-public-1a

The name can be up to 256 characters long.

Availability Zone [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

China (Ningxia) / cn-northwest-1a ▼

IPv4 CIDR block [Info](#)

10.0.0.0/24 ✕

同理，创建其他三个 private 子网。

创建完成。

|                          | Name                       | Subnet ID                | State     | VPC                           | IPv4 CIDR   | IPv6 CIDR | Available IPv4 addr... | Availability Zone |
|--------------------------|----------------------------|--------------------------|-----------|-------------------------------|-------------|-----------|------------------------|-------------------|
| <input type="checkbox"/> | wangxiang-vpc1-private1-1a | subnet-0d5d49db032849211 | Available | vpc-0e010793150f2eef0   wa... | 10.0.1.0/24 | -         | 251                    | cn-northwest-1a   |
| <input type="checkbox"/> | wangxiang-vpc1-private2-1a | subnet-00110cd9df0af65b1 | Available | vpc-0e010793150f2eef0   wa... | 10.0.2.0/24 | -         | 251                    | cn-northwest-1a   |
| <input type="checkbox"/> | wangxiang-vpc1-private3-1b | subnet-09f37bb13d4a815fc | Available | vpc-0e010793150f2eef0   wa... | 10.0.3.0/24 | -         | 251                    | cn-northwest-1b   |
| <input type="checkbox"/> | wangxiang-vpc1-public1-1a  | subnet-094152dbfaef6ed0  | Available | vpc-0e010793150f2eef0   wa... | 10.0.0.0/24 | -         | 251                    | cn-northwest-1a   |

### 3.2. 创建 IGW

VPC 中的子网通过 IGW 才能访问 Internet。

选择 Services → VIRTUAL PRIVATE CLOUD → Internet gateways，点击 Create Internet gateways。

VPC > Internet gateways > Create internet gateway

## Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

**Internet gateway settings**

**Name tag**  
Creates a tag with a key of 'Name' and a value that you specify.

关联刚创建的 VPC1。

Internet gateways (1/1) [Info](#)

search: wangxiang-vpc1 X Clear filters

| <input checked="" type="checkbox"/> | Name               | Internet gateway ID   | State    | VPC ID |
|-------------------------------------|--------------------|-----------------------|----------|--------|
| <input checked="" type="checkbox"/> | wangxiang-vpc1-IGW | igw-0f1532ffed07fbfa0 | Detached | -      |

Actions: View details, **Attach to VPC**, Detach from VPC, Manage tags, Delete internet gateway

VPC > Internet gateways > Attach to VPC (igw-0f1532ffed07fbfa0)

## Attach to VPC (igw-0f1532ffed07fbfa0) [Info](#)

**VPC**  
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

**Available VPCs**  
Attach the internet gateway to this VPC.

► Amazon Web Services Command Line Interface command

Cancel **Attach internet gateway**

创建完成。

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables [New](#)

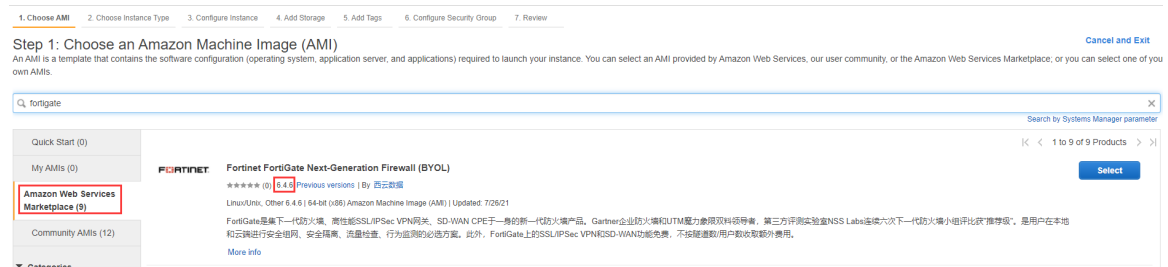
[Internet Gateways](#)

| <input checked="" type="checkbox"/> | Name               | Internet gateway ID   | State    | VPC ID                                 |
|-------------------------------------|--------------------|-----------------------|----------|----------------------------------------|
| <input checked="" type="checkbox"/> | wangxiang-vpc1-IGW | igw-0f1532ffed07fbfa0 | Attached | vpc-0e010793150f2eef0   wangxiang-vpc1 |

### 3.3. 部署 FortiGate

选择 Services→EC2→Instances，点击 Create Instance。

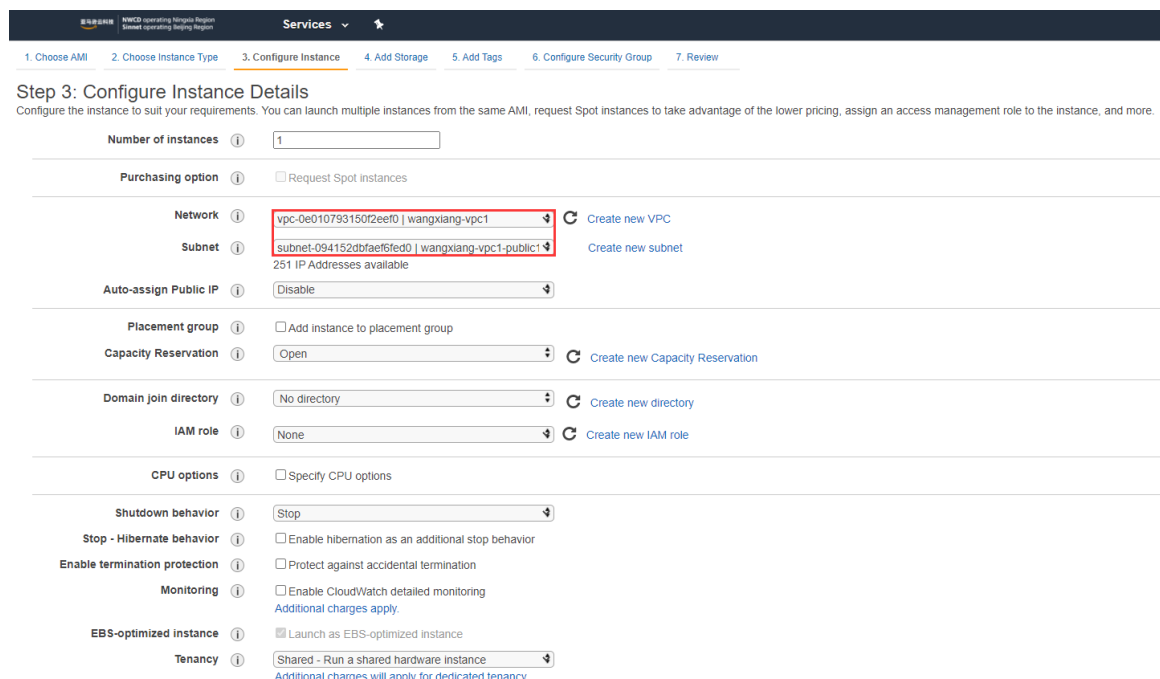
这里选择 FortiGate v6.4.6 的版本。



实例类型请选择计算优化型，这里使用 c5.xlarge。

|                          |    |            |    |    |          |     |                  |     |
|--------------------------|----|------------|----|----|----------|-----|------------------|-----|
| <input type="checkbox"/> | c5 | c5 large   | 2  | 4  | EBS only | Yes | Up to 10 Gigabit | Yes |
| <input type="checkbox"/> | c5 | c5 xlarge  | 4  | 8  | EBS only | Yes | Up to 10 Gigabit | Yes |
| <input type="checkbox"/> | c5 | c5 2xlarge | 8  | 16 | EBS only | Yes | Up to 10 Gigabit | Yes |
| <input type="checkbox"/> | c5 | c5 4xlarge | 16 | 32 | EBS only | Yes | Up to 10 Gigabit | Yes |
| <input type="checkbox"/> | c5 | c5 9xlarge | 36 | 72 | EBS only | Yes | 10 Gigabit       | Yes |

实例配置，选择 VPC1 和子网 public1-1a。



默认实例只有一块网卡 `eth0`，对应 FortiGate `port1` 接口，`eth0` 会自动分配地址，也可以手动指定，这里指定 `10.0.0.10`。

▼ Network interfaces ⓘ

| Device | Network Interface       | Subnet            | Primary IP | Secondary IP addresses | IPv6 IPs                                                                         |
|--------|-------------------------|-------------------|------------|------------------------|----------------------------------------------------------------------------------|
| eth0   | New network interface ▼ | subnet-094152dt ▼ | 10.0.0.10  | <a href="#">Add IP</a> | The selected subnet does not support IPv6 because it does not have an IPv6 CIDR. |

[Add Device](#)

也可以通过 `Add Device` 再添加一块网卡 `eth1`，对应 FortiGate `port2` 接口。

▼ Network interfaces ⓘ

| Device | Network Interface       | Subnet            | Primary IP | Secondary IP addresses | IPv6 IPs                                                                           |
|--------|-------------------------|-------------------|------------|------------------------|------------------------------------------------------------------------------------|
| eth0   | New network interface ▼ | subnet-094152dt ▼ | 10.0.0.10  | <a href="#">Add IP</a> | The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.   |
| eth1   | New network interface ▼ | subnet-0d5d49dt ▼ | 10.0.1.10  | <a href="#">Add IP</a> | The selected subnet does not support IPv6 because it does not have an IPv6 CIDR. ❌ |

添加存储，第二块磁盘用于记录日志，如果 FortiGate 需要开启流量日志，建议发送到 FAZ 或者 syslog 服务器。

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Step 4: Add Storage**

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

| Volume Type ⓘ | Device ⓘ   | Snapshot ⓘ             | Size (GiB) ⓘ | Volume Type ⓘ               | IOPS ⓘ     | Throughput (MB/s) ⓘ | Delete on Termination ⓘ             | Encryption ⓘ      |
|---------------|------------|------------------------|--------------|-----------------------------|------------|---------------------|-------------------------------------|-------------------|
| Root          | /dev/sda1  | snap-0dbc1b1c1e44a185b | 2            | General Purpose SSD (gp2)   | 100 / 3000 | N/A                 | <input checked="" type="checkbox"/> | Not Encrypted ▼   |
| EBS ▼         | /dev/sdb ▼ | Search (case-insensit) | 30           | General Purpose SSD (gp2) ▼ | 100 / 3000 | N/A                 | <input checked="" type="checkbox"/> | Not Encrypted ▼ ❌ |

添加标签用于标识一个实例。

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Step 5: Add Tags**

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

| Key (128 characters maximum) | Value (256 characters maximum) | Instances ⓘ                         | Volumes ⓘ                           | Network Interfaces ⓘ                |
|------------------------------|--------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Name                         | wangxiang-vpc1-FGT             | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

[Add another tag](#) (Up to 50 tags maximum)

创建安全组 `fgt-external-secgroup`，对于管理 FortiGate 需要放行 22、443 端口及 ICMP，其他端口根据业务需求放行。

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic to your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: [Create a new security group](#)

☐ Select an existing security group

Security group name:

Description: (This security group was generated by AWS Marketplace and is based on recommendations)

| Type ⓘ            | Protocol ⓘ | Port Range ⓘ | Source ⓘ                            | Description ⓘ                |
|-------------------|------------|--------------|-------------------------------------|------------------------------|
| SSH ▼             | TCP        | 22           | Custom ▼ 0.0.0.0/0                  | e.g. SSH for Admin Desktop ❌ |
| HTTPS ▼           | TCP        | 443          | Custom ▼ 0.0.0.0/0                  | e.g. SSH for Admin Desktop ❌ |
| All ICMP - IPv4 ▼ | ICMP       | 0 - 65535    | Custom ▼ CIDR, IP or Security Group | e.g. SSH for Admin Desktop ❌ |

[Add Rule](#)

创建 key，或者选择自己已经存在的 key，并启动实例。

Select an existing key pair or create a new key pair

X

A key pair consists of a **public key** that Amazon Web Services stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

wangxiang-ninxia | RSA

☒ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

创建完成，实例 ID 是 i-0faa2e4bc8eb44e84。

**Instances**

| Name               | Instance ID         | Instance state | Instance type | Status check      | Alarm status | Availability Zone | Public IPv4 DNS | Public IP v4 ... | Elastic IP |
|--------------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|-----------------|------------------|------------|
| wangxiang-vpc1-FGT | i-Ofaa2e4bc8eb44e84 | Running        | c5.xlarge     | 2/2 checks passed | No alarms    | cn-northwest-1a   | -               | -                | -          |

### Instance: i-Ofaa2e4bc8eb44e84 (wangxiang-vpc1-FGT)

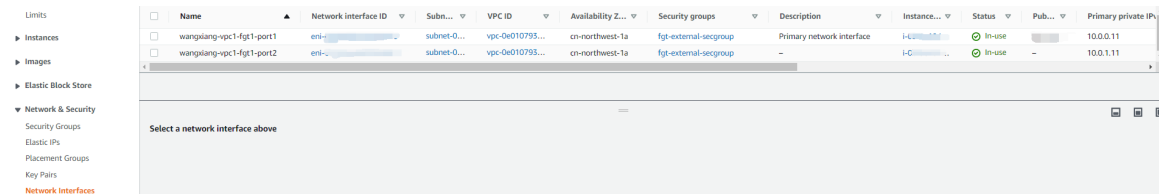
- Details** | Security | Networking | Storage | Status checks | Monitoring | Tags

**▼ Instance summary**

|                                                                |                                 |                                                         |
|----------------------------------------------------------------|---------------------------------|---------------------------------------------------------|
| <b>Instance ID</b><br>i-Ofaa2e4bc8eb44e84 (wangxiang-vpc1-FGT) | <b>Public IPv4 address</b><br>- | <b>Private IPv4 addresses</b><br>10.0.0.10<br>10.0.1.10 |
|----------------------------------------------------------------|---------------------------------|---------------------------------------------------------|

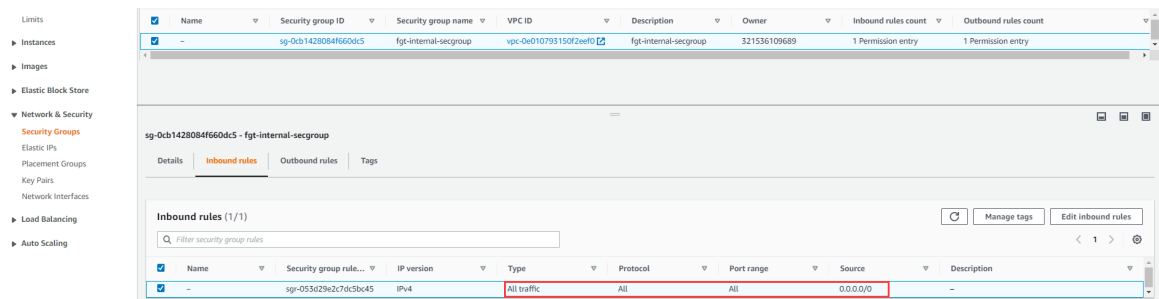
### 3. 4. 安全组

点击网络接口可以，可以查看到实例创建的两个接口。输入 Name 的名称，便于管理。FortiGate 实例的两个接口的安全组都是刚新建的 fgt-external-secgroup。

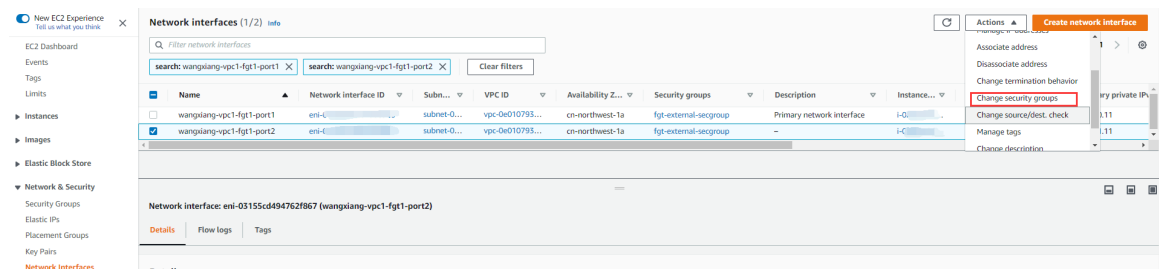


AWS 安全组是基于接口的，对于 FortiGate port2 而言，port2 对应的是由内向外的数据，因此 port2 的安全组要全放通。

新建安全组 fgt-internal-secgroup。



修改 port2 接口的安全组。



Change security groups [Info](#)

Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic to and from your instance. You can use this window to add and remove security groups.

## Network interface details

Network interface ID

eni-...

## Associated security groups

Add one or more security groups to the network interface. You can also remove security groups.

[Add security group](#)

Security groups associated with the network interface (eni-058bbef3c524af52e)

| Security group name   | Security group ID    |                        |
|-----------------------|----------------------|------------------------|
| fgt-internal-secgroup | sg-0cb1428084f660dc5 | <a href="#">Remove</a> |

修改完成。

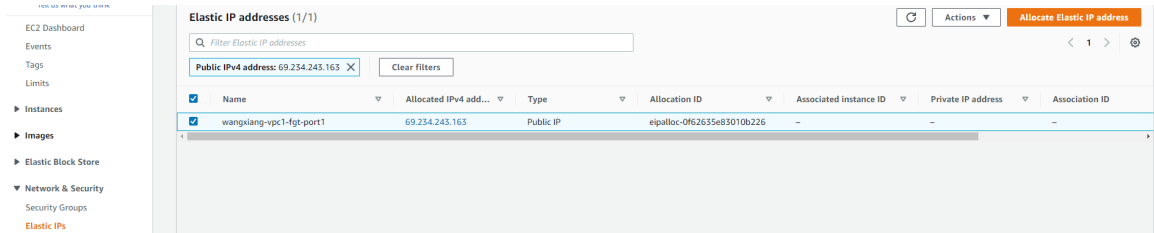
| Name                      | Network interface ID | Subnet...   | VPC ID          | Availability Z... | Security groups       | Description               | Instance... | Status | Pub... | Primary private IP |
|---------------------------|----------------------|-------------|-----------------|-------------------|-----------------------|---------------------------|-------------|--------|--------|--------------------|
| wangliang-vpc1-fgt1-port1 | eni-0...             | subnet-0... | vpc-0e010793... | cn-northwest-1a   | fgt-external-secgroup | Primary network interface | i-4...      | in-use |        | 10.0.0.11          |
| wangliang-vpc1-fgt1-port2 | eni-0...             | subnet-0... | vpc-0e010793... | cn-northwest-1a   | fgt-internal-secgroup | -                         | i-4...      | in-use |        | 10.0.1.11          |

Select a network interface above

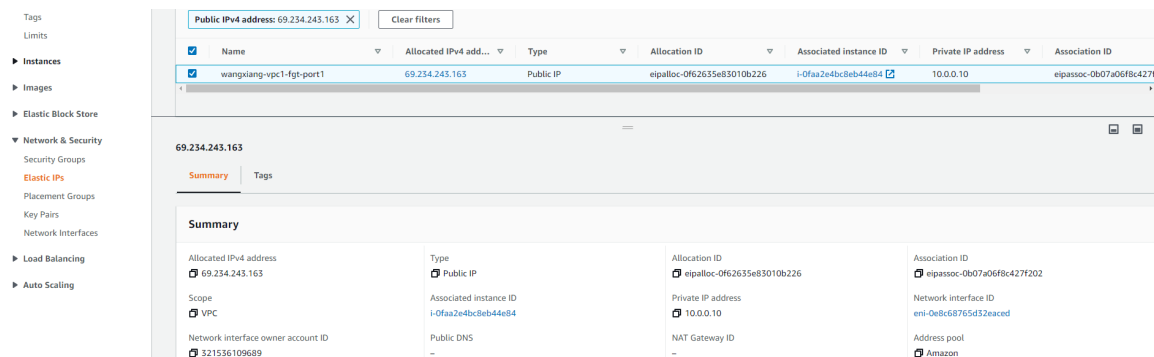
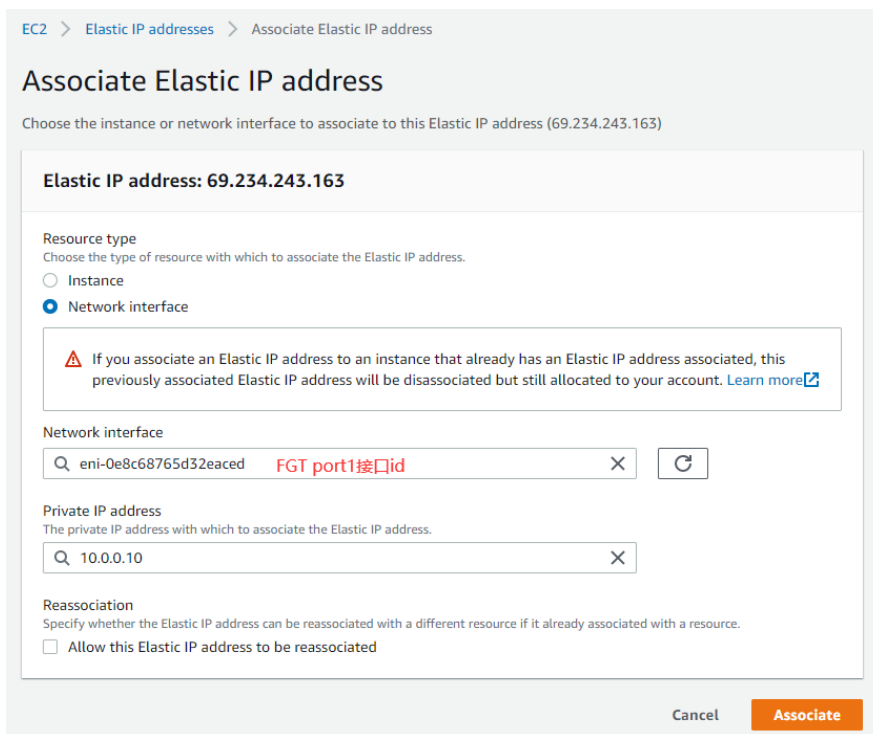
备注：FortiGate 本身就有防火墙策略对流量进行控制，如果嫌安全组控制太麻烦，可以将 FortiGate 的所有端口都应用允许所有的安全组。

### 3.5. 弹性 IP

选择 Services → Network & Security → Elastic IPs, 点击 Allocate Elastic IP address。

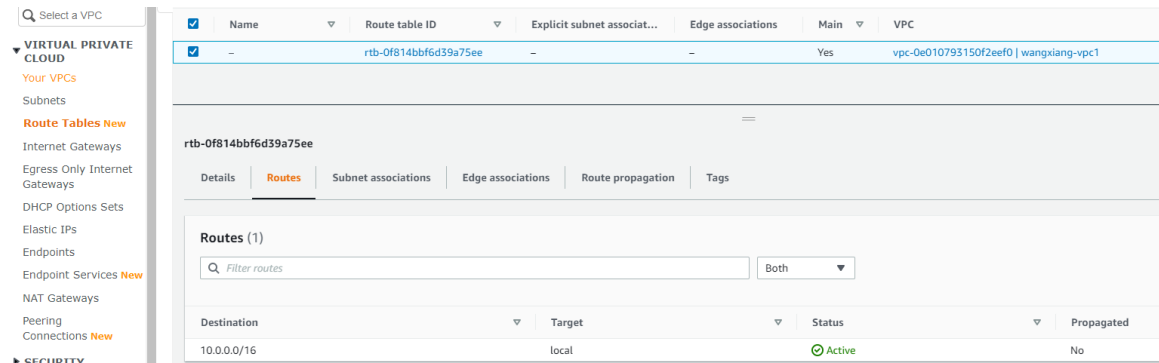


关联弹性 IP 到 FortiGate port1 接口，即 FortiGate 连接 Internet 的公网地址就是该 IP，选中该弹性 IP，点击 Action → Associate Elastic IP address。



### 3. 6. AWS 路由表

创建 VPC 后，默认会为该 VPC 创建一张主路由表，默认关联了该 VPC 的所有子网。



这里创建 public 路由表和 private 路由表用于 AWS 网络的路由。

选择 Services → VIRTUAL PRIVATE CLOUD → Route tables，点击 Create Route table。

VPC > Route tables > Create route table

### Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

#### Route table settings

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.

**VPC**  
The VPC to use for this route table.

#### Tags

A tag is a label that you assign to an Amazon Web Services resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your Amazon Web Services costs.

| Key  | Value - optional          |        |
|------|---------------------------|--------|
| Name | wangxiang-vpc1-public-rtb | Remove |

[Add new tag](#)

You can add 49 more tags.

[Cancel](#) [Create route table](#)

## 创建 public 路由表关联 public 子网，默认路由指向 IGW:

Q Select a VPC

**VIRTUAL PRIVATE CLOUD**

- Your VPCs
- Subnets
- Route Tables New**
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services New
- NAT Gateways
- Peering Connections New

**SECURITY**

**VIRTUAL PRIVATE CLOUD**

| Name                      | Route table ID        | Explicit subnet associat... | Edge associations | Main | VPC                                    |
|---------------------------|-----------------------|-----------------------------|-------------------|------|----------------------------------------|
| wangxiang-vpc1-public-rtb | rtb-026f58e5a0076293d | subnet-094152dbfaef6f...    | -                 | No   | vpc-0e010793150f2eef0   wangxiang-vpc1 |

rtb-026f58e5a0076293d / wangxiang-vpc1-public-rtb

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Filter routes Both

| Destination | Target               | Status | Propagated |
|-------------|----------------------|--------|------------|
| 10.0.0.0/16 | local                | Active | No         |
| 0.0.0.0/0   | igw-0f1532fde07bfda0 | Active | No         |

rtb-026f58e5a0076293d / wangxiang-vpc1-public-rtb

Details Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (1)

Find subnet association

| Subnet ID                                            | IPv4 CIDR   |
|------------------------------------------------------|-------------|
| subnet-094152dbfaef6fed0 / wangxiang-vpc1-public1-1a | 10.0.0.0/24 |

## 创建 private 路由表关联 private 子网，默认路由指向 FortiGate port2 接口:

**VIRTUAL PRIVATE CLOUD**

- Your VPCs
- Subnets
- Route Tables New**
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services New
- NAT Gateways
- Peering Connections New

**SECURITY**

**VIRTUAL PRIVATE NETWORK (VPN)**

**TRANSIT GATEWAYS**

| Name                       | Route table ID        | Explicit subnet associat... | Edge associations | Main | VPC                                    |
|----------------------------|-----------------------|-----------------------------|-------------------|------|----------------------------------------|
| wangxiang-vpc1-private-rtb | rtb-0e0b19014c9999715 | 3 subnets                   | -                 | No   | vpc-0e010793150f2eef0   wangxiang-vpc1 |

rtb-0e0b19014c9999715 / wangxiang-vpc1-private-rtb

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Filter routes Both

| Destination | Target                             | Status | Propagated |
|-------------|------------------------------------|--------|------------|
| 10.0.0.0/16 | local                              | Active | No         |
| 0.0.0.0/0   | eni-0b343e8899682354 FGT port2接口ID | Active | No         |

rtb-0e0b19014c9999715 / wangxiang-vpc1-private-rtb

Details Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (3)

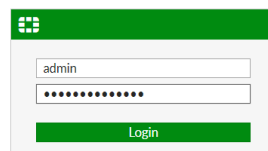
Find subnet association

| Subnet ID                                             | IPv4 CIDR   |
|-------------------------------------------------------|-------------|
| subnet-0d5d49db032849211 / wangxiang-vpc1-private1-1a | 10.0.1.0/24 |
| subnet-00110cb9df0af65b1 / wangxiang-vpc1-private2-1a | 10.0.2.0/24 |
| subnet-09f37bb13d4a815fc / wangxiang-vpc1-private3-1b | 10.0.3.0/24 |

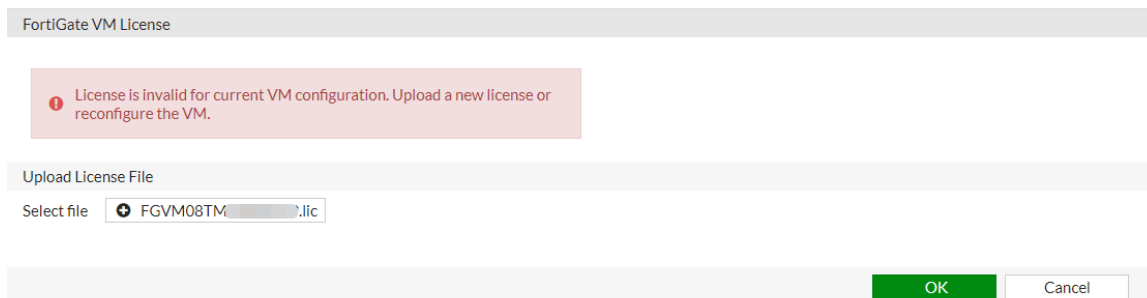
### 3.7. 访问 FortiGate

#### Https 访问 FortiGate:

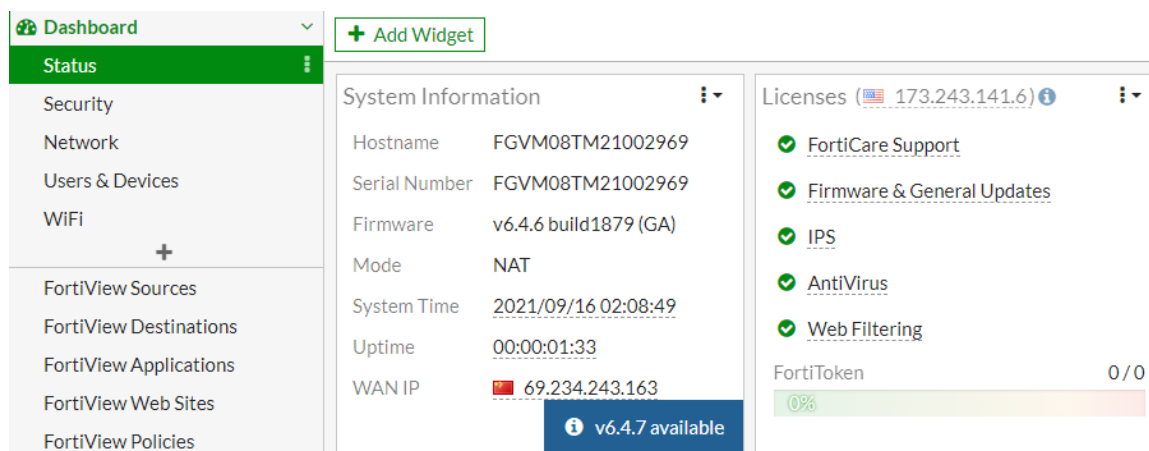
使用 <https://69.234.243.163>（弹性 IP）访问 FortiGate，账号是 admin，密码默认是实例 ID。首次登录后，请按照提示修改密码。



登录后，请先上传购买好的 license，导入 license 会重启 FortiGate。

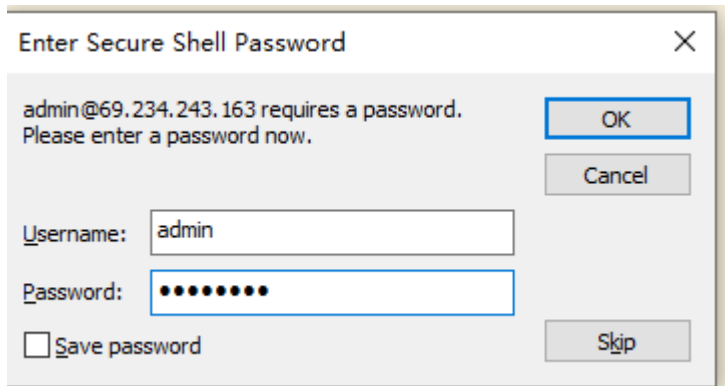


FortiGate 登录成功。

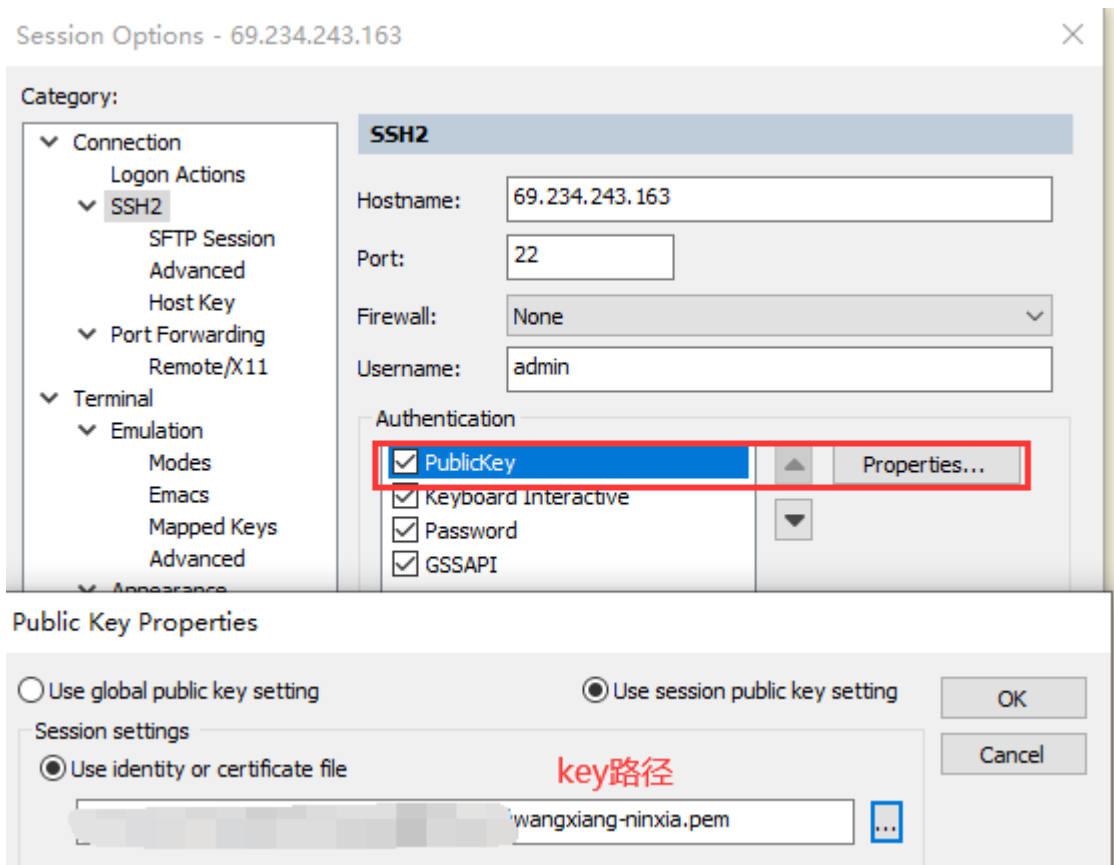


SSH 访问 FortiGate 有两种方式，一下是 CRT 软件的访问截图：

一种是通过账号密码的方式：

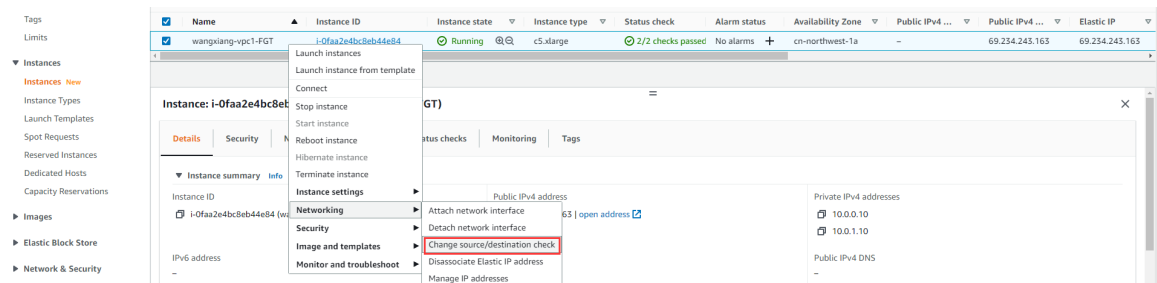


一种是通过 key 的方式：



### 3.8. 禁用源/目标检查

每个 EC2 实例都会默认执行源/目标检查。这意味着实例必须为其发送或接收的数据流的源头或目标。但是，NAT 实例必须能够在源或目标并非其本身时发送和接收数据流。因此，FortiGate 实例必须禁用源/目标检查。



EC2 > Instances > i-0faa2e4bc8eb44e84 > Change source / destination check

### Source / destination check [Info](#)

Each EC2 instance performs source and destination checks by default. The instance must be the source or destination of all the traffic it sends and receives.

Instance ID  
[i-0faa2e4bc8eb44e84](#) (wangxiang-vpc1-FGT)

Network interface [Info](#)  
[eni-0b343e88899682354](#) (wangxiang-vpc1-fgt-port2)  
[eni-0e8c68765d32eaced](#) (wangxiang-vpc1-fgt-port1)

Source / destination checking [Info](#)  
☒ Stop

[Info](#) If this is a NAT instance, you must stop source / destination checking. A NAT instance must be able to send and receive traffic when the source or destination is not itself.

[Amazon Web Services CLI Command](#)

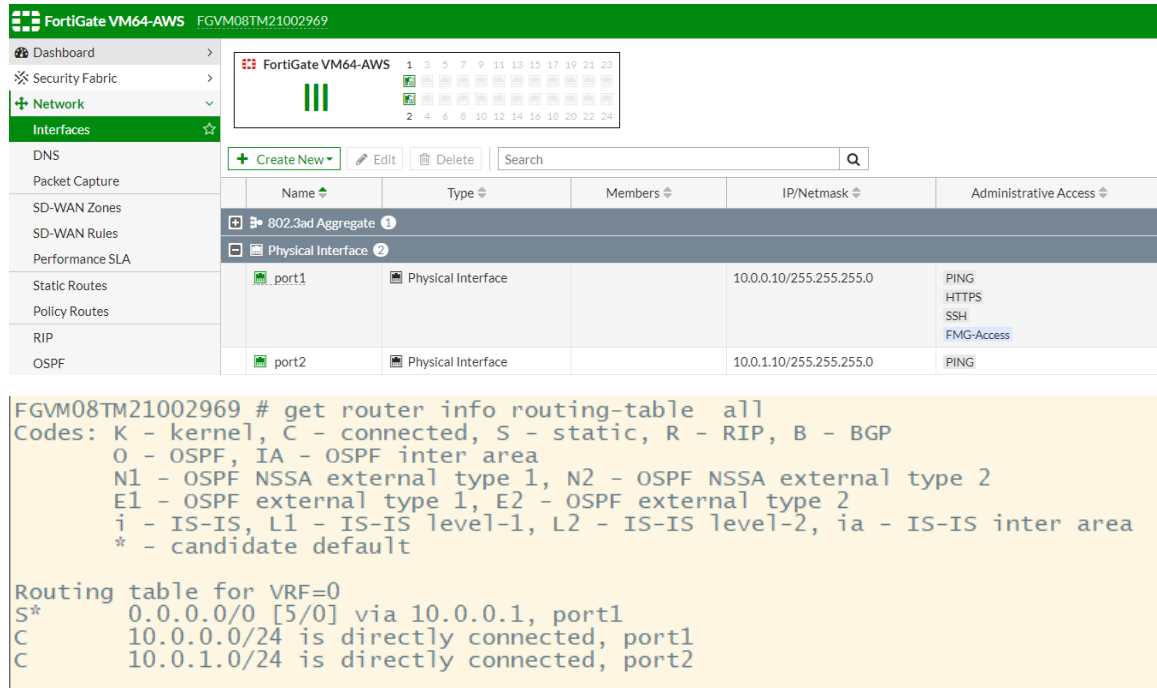
```
aws ec2 modify-instance-attribute --instance-id=i-0faa2e4bc8eb44e84 --no-source-dest-check
```

[Copy](#)

[Cancel](#) [Save](#)

### 3.9. FortiGate 配置源 NAT

FortiGate 默认会 DHCP 获取 AWS 分配的地址及路由表如下：



The screenshot shows the FortiGate VM64-AWS configuration interface. The left sidebar lists various configuration sections, with 'Network' and 'Interfaces' expanded. The main area displays a table of interfaces:

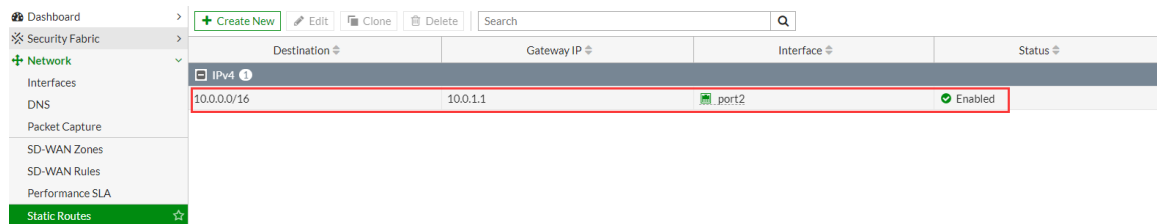
| Name                        | Type               | Members | IP/Netmask              | Administrative Access              |
|-----------------------------|--------------------|---------|-------------------------|------------------------------------|
| <b>802.3ad Aggregate 1</b>  |                    |         |                         |                                    |
| <b>Physical Interface 2</b> |                    |         |                         |                                    |
| port1                       | Physical Interface |         | 10.0.0.10/255.255.255.0 | PING<br>HTTPS<br>SSH<br>FMG-Access |
| port2                       | Physical Interface |         | 10.0.1.10/255.255.255.0 | PING                               |

Below the table, a terminal window shows the output of the command `get router info routing-table all`:

```
FGVM08TM21002969 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

Routing table for VRF=0
S* 0.0.0.0/0 [5/0] via 10.0.0.1, port1
C 10.0.0.0/24 is directly connected, port1
C 10.0.1.0/24 is directly connected, port2
```

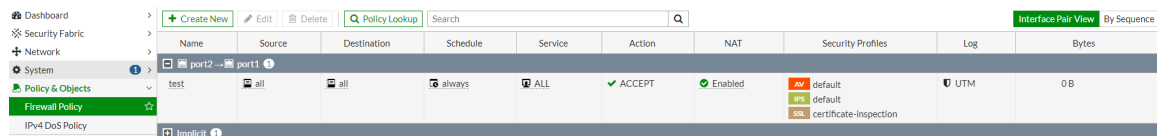
配置 10.0.0.0/16 的内部路由指向 10.0.1.1。AWS 虚拟路由的器的地址为每个子网的第一个地址，port2 接口的子网是 10.0.1.0/24，因此虚拟路由器的地址是 10.0.1.1。



The screenshot shows the FortiGate VM64-AWS configuration interface with the 'Static Routes' section selected. A table displays the configured static route:

| Destination | Gateway IP | Interface | Status  |
|-------------|------------|-----------|---------|
| 10.0.0.0/16 | 10.0.1.1   | port2     | Enabled |

配置防火墙策略。



The screenshot shows the FortiGate VM64-AWS configuration interface with the 'Firewall Policy' section selected. A table displays the configured firewall policy:

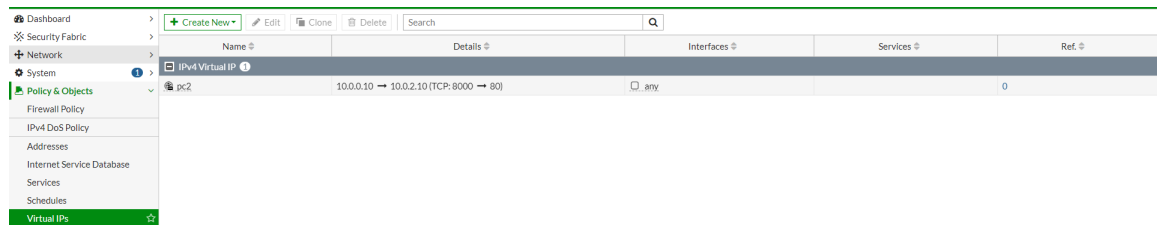
| Name | Source | Destination | Schedule | Service | Action | NAT     | Security Profiles                                       | Log | Bytes |
|------|--------|-------------|----------|---------|--------|---------|---------------------------------------------------------|-----|-------|
| test | all    | all         | always   | ALL     | ACCEPT | Enabled | AV default<br>IPS default<br>SRA certificate-inspection | UTM | 0B    |

### 3.10. FortiGate 配置目的 NAT

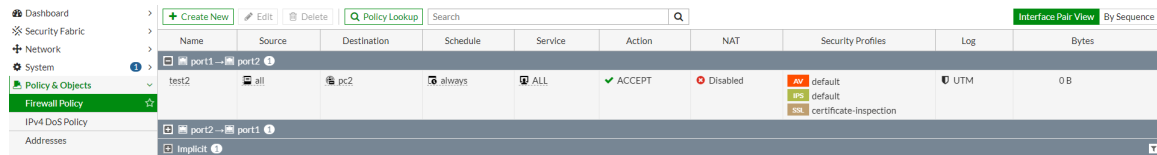
可以使用 port1 接口的地址做目的 NAT,也可以分配一个单独的 IP 来做目的 NAT。

用 port1 接口的地址做目的 NAT:

配置 VIP, external 地址是 10.0.0.10, internal 地址是 10.0.2.10:

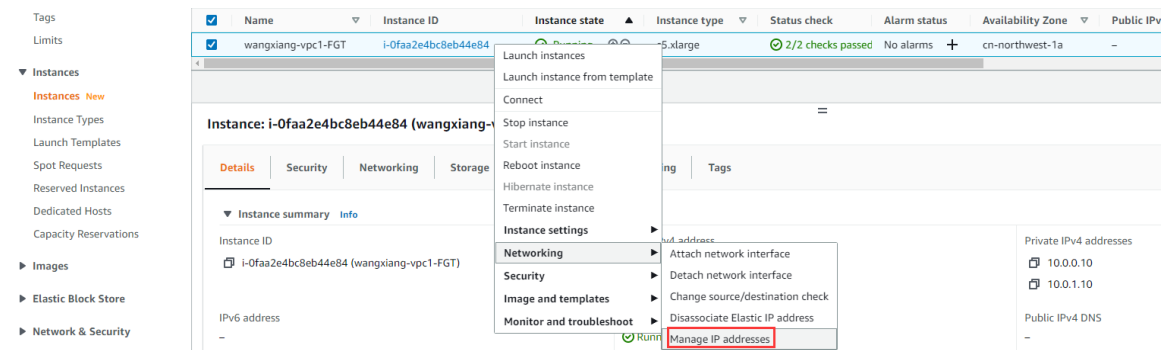


配置防火墙策略调用 VIP:



分配单独的 IP 来做目的 NAT:

如下图, 右击实例, 选择 Networking→Manage IP addresses



EC2 > Instances > i-0faa2e4bc8eb44e84 > Manage IP addresses

### Manage IP addresses Info

Assign or unassign IPv4 and IPv6 addresses to or from an instance's network interfaces.

**To assign additional public IPv4 addresses to this instance, you must allocate Elastic IP addresses and associate them with the instance or its network interfaces.**

▼ eth0: eni-0e8c68765d32eaced - Primary network interface - 10.0.0.0/24

#### IPv4 addresses

| Private IP address | Public IP address |                           |
|--------------------|-------------------|---------------------------|
| 10.0.0.10          | 69.234.243.163    | <button>Unassign</button> |
| 10.0.0.11          |                   | <button>Undo</button>     |

Assign new IP address

► eth1: eni-0b343e88899682354 - 10.0.1.0/24

☐ Allow secondary private IPv4 addresses to be reassigned  
Allows you to reassign a private IPv4 address that is assigned to this instance to another instance or network interface.

Cancel Save

10.0.0.11 是没有关联弹性 IP 的，因此给此 IP 关联弹性 IP 才可以连接 Internet。分配弹性 IP 并关联 10.0.0.11。

EC2 > Elastic IP addresses > Associate Elastic IP address

### Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (52.83.138.72)

**Elastic IP address: 52.83.138.72**

**Resource type**  
Choose the type of resource with which to associate the Elastic IP address.

☐ Instance

☒ Network interface

**Network interface**  
eni-0e8c68765d32eaced port1接口的ID

**Private IP address**  
The private IP address with which to associate the Elastic IP address.  
10.0.0.11

**Reassociation**  
Specify whether the Elastic IP address can be reassigned with a different resource if it already associated with a resource.  
☐ Allow this Elastic IP address to be reassigned

Cancel Associate

EC2 Dashboard

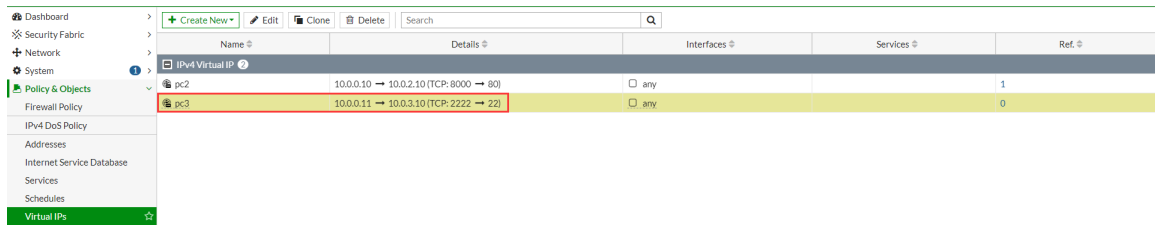
- Events
- Tags
- Limits
- Instances
- Images
- Elastic Block Store
- Network & Security
  - Security Groups
  - Elastic IPs**

#### Elastic IP addresses (1/2)

Filter Elastic IP addresses

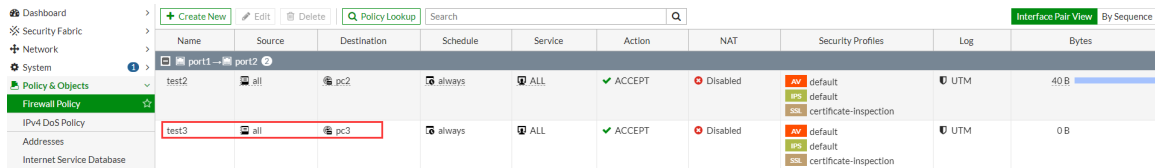
|                                     | Name                        | Allocated IPv4 address | Type      | Allocation ID              | Associated instance ID | Private IP address | Association ID          |
|-------------------------------------|-----------------------------|------------------------|-----------|----------------------------|------------------------|--------------------|-------------------------|
| <input checked="" type="checkbox"/> | wangxiang-vpc1-fgt-port1-11 | 52.83.138.72           | Public IP | eipalloc-0f6ac05e3e0c64aa  | i-0faa2e4bc8eb44e84    | 10.0.0.11          | eipassoc-0e42bc19631f5f |
| <input type="checkbox"/>            | wangxiang-vpc1-fgt-port1    | 69.234.243.163         | Public IP | eipalloc-0f62655e83010b226 | i-0faa2e4bc8eb44e84    | 10.0.0.10          | eipassoc-0b07a06f8c427f |

配置 VIP，external 地址是 10.0.0.11，internal 地址是 10.0.3.10:



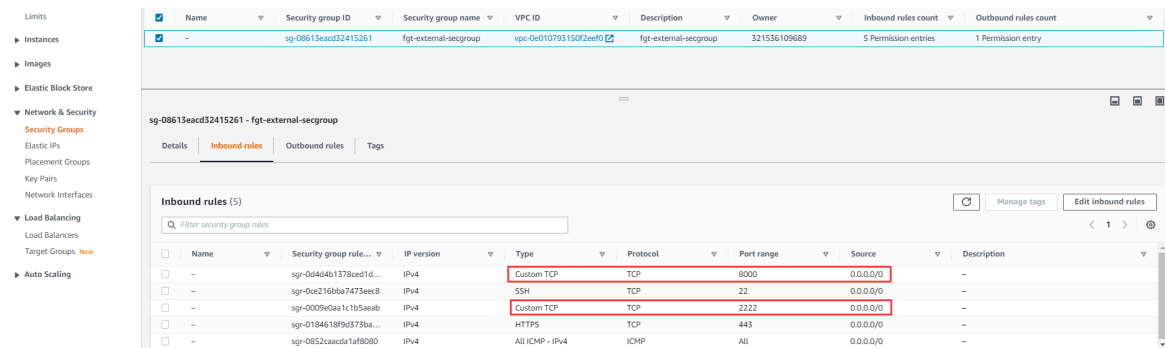
| Name            | Details                                 | Interfaces | Services | Ref. |
|-----------------|-----------------------------------------|------------|----------|------|
| IPv4 Virtual IP |                                         |            |          |      |
| pc2             | 10.0.0.10 -> 10.0.2.10 (TCP:8000 -> 80) | any        |          | 1    |
| pc3             | 10.0.0.11 -> 10.0.3.10 (TCP:2222 -> 22) | any        |          | 0    |

配置防火墙策略:



| Name  | Source | Destination | Schedule | Service | Action | NAT      | Security Profiles                                   | Log | Bytes |
|-------|--------|-------------|----------|---------|--------|----------|-----------------------------------------------------|-----|-------|
| test2 | all    | pc2         | always   | ALL     | ACCEPT | Disabled | AV default, IPS default, SSL certificate-inspection | UTM | 40 B  |
| test3 | all    | pc3         | always   | ALL     | ACCEPT | Disabled | AV default, IPS default, SSL certificate-inspection | UTM | 0 B   |

FGT 实例 NIC1, 即 port1 安全组 fgt-external-secgroup 放通 8000 和 2222 这两个对外的端口。



| Name | Security group rule... | IP version | Type            | Protocol | Port range | Source    | Description |
|------|------------------------|------------|-----------------|----------|------------|-----------|-------------|
| -    | sg-0d464b1378e4d1d...  | IPv4       | Custom TCP      | TCP      | 8000       | 0.0.0.0/0 | -           |
| -    | sg-0ec216bba7473ee08   | IPv4       | SSH             | TCP      | 22         | 0.0.0.0/0 | -           |
| -    | sg-0009e0aa1c105aeab   | IPv4       | Custom TCP      | TCP      | 2222       | 0.0.0.0/0 | -           |
| -    | sg-0184618f9d373ba...  | IPv4       | HTTPS           | TCP      | 443        | 0.0.0.0/0 | -           |
| -    | sg-0852caac1af8080     | IPv4       | All ICMP - IPv4 | ICMP     | All        | 0.0.0.0/0 | -           |

## 4. 业务测试

测试的 PC 如下

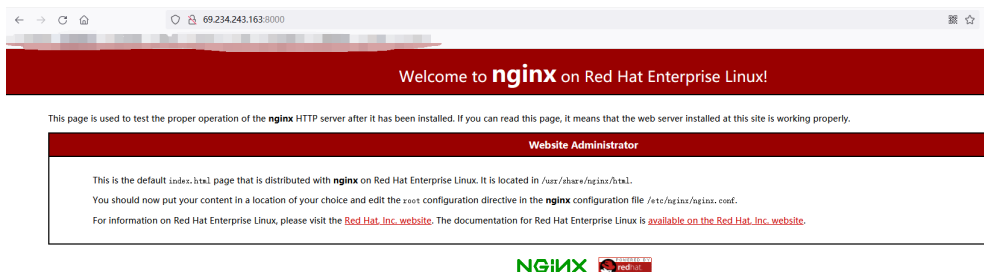
| Tags           | Name                  | Instance ID         | Instance state | Instance type | Status check      | Alarm status | Availability Zone | Public IPv4 ... | Public IPv4 ... |
|----------------|-----------------------|---------------------|----------------|---------------|-------------------|--------------|-------------------|-----------------|-----------------|
| Limits         | wangxiang-vpc1-pc1-1a | i-03964db5654510b02 | Running        | t2.medium     | 2/2 checks passed | No alarms    | cn-northwest-1a   | 10.0.1.20       | -               |
| Instances      | wangxiang-vpc1-pc2-1a | i-07dae93431321f6b7 | Running        | t2.medium     | 2/2 checks passed | No alarms    | cn-northwest-1a   | 10.0.2.10       | -               |
| Instances New  | wangxiang-vpc1-pc3-1b | i-05201a73aa2f4e005 | Running        | t2.medium     | 2/2 checks passed | No alarms    | cn-northwest-1b   | 10.0.3.10       | -               |
| Instance Types |                       |                     |                |               |                   |              |                   |                 |                 |

目的 NAT 测试:

ssh 52.83.138.72 2222 访问正常。

```
ec2-user@ip-10-0-3-10:~  
[ec2-user@ip-10-0-3-10 ~]$ ifconfig eth0  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001  
    inet 10.0.3.10 netmask 255.255.255.0 broadcast 10.0.3.255  
    inet6 fe80::463:24ff:fedf:121c prefixlen 64 scopeid 0x20<link>  
    ether 06:63:24:df:12:1c txqueuelen 1000 (Ethernet)  
    RX packets 55101 bytes 76831166 (73.2 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 12128 bytes 1402480 (1.3 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

http://69.234.243.163:8000 访问正常。



源 NAT 测试:

ping 114.114.114.114 正常

```
[ec2-user@ip-10-0-3-10 ~]$ ping 114.114.114.114  
PING 114.114.114.114 (114.114.114.114) 56(84) bytes of data.  
64 bytes from 114.114.114.114: icmp_seq=1 ttl=80 time=34.7 ms  
64 bytes from 114.114.114.114: icmp_seq=2 ttl=81 time=34.5 ms  
64 bytes from 114.114.114.114: icmp_seq=3 ttl=78 time=34.6 ms  
64 bytes from 114.114.114.114: icmp_seq=4 ttl=79 time=34.6 ms  
^C  
--- 114.114.114.114 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 8ms  
rtt min/avg/max/mdev = 34.510/34.587/34.671/0.059 ms  
[ec2-user@ip-10-0-3-10 ~]$
```

使用 10.0.3.10 作为跳板登录到 10.0.20.10，访问 baidu 正常。

```
sudo ssh -i "wangxiang-ninxia.pem" ec2-user@10.0.2.10
```

```
[ec2-user@ip-10-0-3-10 ~]$ sudo ssh -i "wangxiang-ninxia.pem" ec2-user@10.0.2.10
Last login: Thu Sep 16 12:00:06 2021 from 10.0.3.10
[ec2-user@ip-10-0-2-10 ~]$ curl www.baidu.com
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html;charset=utf-8
me=referrer><link rel=stylesheet type=text/css href=http://s1.bdstatic.com/r/www/cache/bd
0cc> <div id=wrapper> <div id=head> <div class=head_wrapper> <div class=s_form> <div clas
bd_logo1.png width=270 height=129> </div> <form id=form name=f action=/www.baidu.com/s c
me=ie value=utf-8> <input type=hidden name=f value=8> <input type=hidden name=rsv_bp valu
alue=baidu><span class="bg s_ipt_wr"><input id=kw name=wd class=s_ipt value maxlength=255
ubmit id=su value=百度一下 class="bg s_btn"></span> </form> </div> </div> <div id=u1> <a h
://www.hao123.com name=tj_trhao123 class=mnnav>hao123</a> <a href=http://map.baidu.com name
class=mnnav>视频</a> <a href=http://tieba.baidu.com name=tj_trtieba class=mnnav>贴吧</a> <nc
;u=http%3A%2F%2Fwww.baidu.com%2F%3Fbdorz_come%3D1 name=tj_login class=lb>登录</a> </noscr
?login&tpl=mn&u='+ encodeURIComponent(window.location.href+ (window.location.search === ""
</script> <a href=/www.baidu.com/more/ name=tj_briicon class=bri style="display: block;"
> <a href=http://home.baidu.com>关于百度</a> <a href=http://ir.baidu.com>About Baidu</a>
/>使用百度前必读</a>&nbsp; <a href=http://jianshi.baidu.com/ class=cp-feedback>意见反馈</a>
iv> </div> </div> </body> </html>
```

同理 10.0.1.20 访问外网也正常。

```
[ec2-user@ip-10-0-3-10 ~]$ sudo ssh -i "wangxiang-ninxia.pem" ec2-user@10.0.1.20
Last login: Thu Sep 16 12:26:10 2021 from 10.0.3.10
[ec2-user@ip-10-0-1-20 ~]$ curl www.hao123.com
<!DOCTYPE html><html><head><noscript><meta http-equiv="refresh" content="0; URL='/?__no
_blank"><meta charset="utf-8"/><meta http-equiv=X-UA-Compatible content="IE=edge,chrom
dns-prefetch" href="//s1.hao123img.com" /><link rel="dns-prefetch" href="//s0.hao123img
refetch" href="//img1.hao123.com" /><meta name="keywords" content="上网导航,网址大全,网
活动"/><meta name="description"content="hao123是汇集全网优质网址及资源的中文上网导航。上
上网,从hao123开始。"/><script>window.HAO=window.HAO||{};window.HAO.https = false;windo
></style><script>(function (win) {var HAO = win.HAO = win.HAO || {};HAO.domainMap = {"h
com", "https://dgssl.bdstatic.com/5eNldDebRNRTm2_p8IuM_a": "http://s1.hao123img.com"
3img.com", "https://dgssl.bdstatic.com/5hvXsi_n_tVS5dkfNU_Y_D3": "http://s1.hao123i
```