



AWS 跨 AZ 部署 FortiGate HA

版本	V1.0
时间	2021 年 9 月
作者	王祥
状态	
反馈	support_cn@fortinet.com

目录

1. 介绍	3
2. 网络拓扑	3
3. 地址规划	4
4. 配置步骤	5
4.1. 创建 VPC、子网和 IGW	5
4.2. 创建 IAM 角色	6
4.3. 创建 FortiGate 实例	7
4.4. 安全组	10
4.5. 创建网卡	12
4.6. 弹性 IP	14
4.7. 配置 VPC 路由表	15
4.8. 禁用源/目标检查	17
4.9. 访问 FortiGate	18
4.10. 配置 FortiGate	20
4.11. FortiGate 配置源 NAT	25
4.12. FortiGate 配置目的 NAT	25
5. 业务测试	28
6. HA 切换测试	29

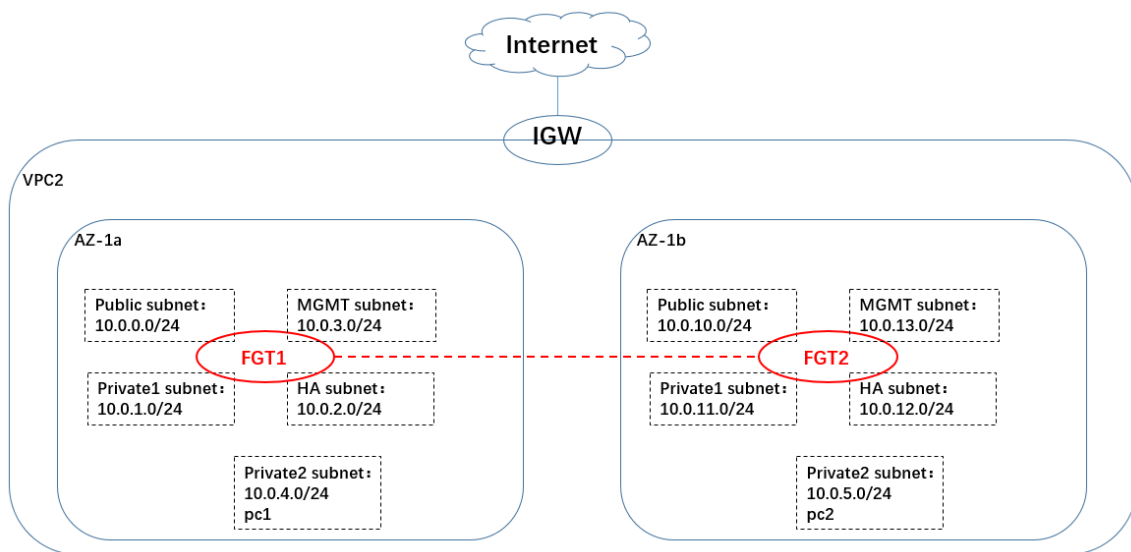
1. 介绍

本文档介绍如何在 AWS 跨 AZ 部署 FortiGate HA，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

FGT1 和 FGT2 部署在不同的 AZ 中，FGT1 和 FGT2 的实例分别需要 4 块网卡。AWS 每种实例类型的最大接口数及每个网络接口的 IP 地址数的查询链接如下：

https://docs.aws.amazon.com/zh_cn/AWSEC2/latest/UserGuide/using-eni.html



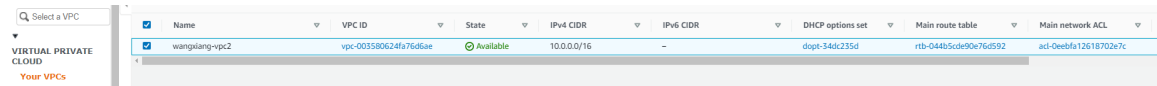
3. 地址规划

FGT1 地址规划 (AZ-1a)	
Port	AWS primary address
Port1	10.0.0.11
Port2	10.0.1.11
Port3	10.0.2.11
Port4	10.0.3.11
FGT2 地址规划 (AZ-1b)	
Port	AWS primary address
Port1	10.0.10.11
Port2	10.0.11.11
Port3	10.0.12.11
Port4	10.0.13.11
测试 PC	
PC 名称	测试地址
PC2	10.0.4.20
PC3	10.0.5.20

4. 配置步骤

4.1. 创建 VPC、子网和 IGW

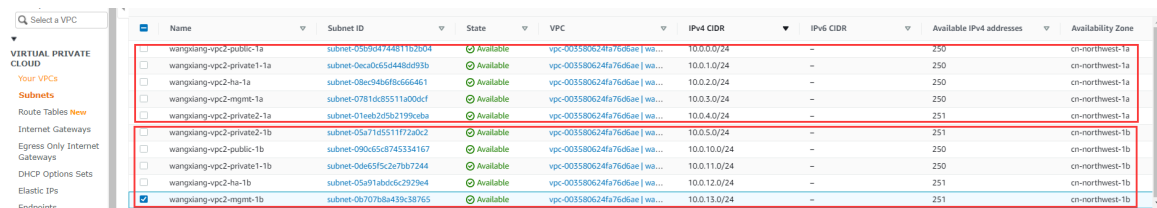
创建 VPC。



The screenshot shows the AWS VPC console with a table of VPCs. The table has columns: Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, Main route table, and Main network ACL. The row for 'wangxiang-vpc2' is highlighted.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main route table	Main network ACL
wangxiang-vpc2	vpc-003580624fa76d6ae	Available	10.0.0.0/16	-	dopt-34dc235d	rtb-04405cde90e76d592	acl-0eebfa12618702e7c

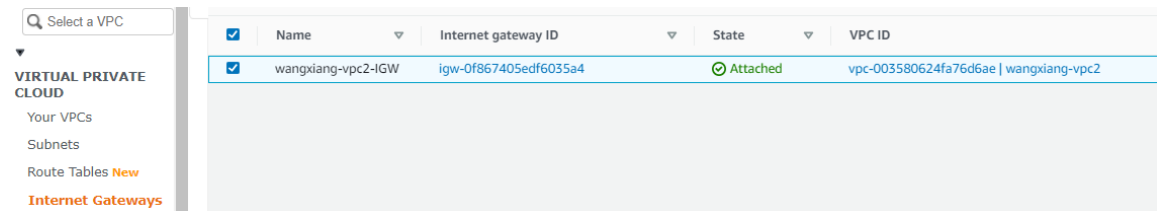
创建子网。



The screenshot shows the AWS VPC console with a table of subnets. The table has columns: Name, Subnet ID, State, VPC, IPv4 CIDR, IPv6 CIDR, Available IPv4 addresses, and Availability Zone. The subnets are listed in a table with a red border.

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone
wangxiang-vpc2-public-1a	subnet-050904744811b2604	Available	vpc-003580624fa76d6ae wa...	10.0.0.0/24	-	250	cn-northwest-1a
wangxiang-vpc2-private1-1a	subnet-0eca0c65d448d993b	Available	vpc-003580624fa76d6ae wa...	10.0.1.0/24	-	250	cn-northwest-1a
wangxiang-vpc2-1a-1a	subnet-08ec94b6f8c666461	Available	vpc-003580624fa76d6ae wa...	10.0.2.0/24	-	250	cn-northwest-1a
wangxiang-vpc2-mgmt-1a	subnet-0781dc85511a00dcf	Available	vpc-003580624fa76d6ae wa...	10.0.3.0/24	-	250	cn-northwest-1a
wangxiang-vpc2-private2-1a	subnet-01eeb2d5b2199caba	Available	vpc-003580624fa76d6ae wa...	10.0.4.0/24	-	251	cn-northwest-1a
wangxiang-vpc2-private2-1b	subnet-05a71d5511f72a0c2	Available	vpc-003580624fa76d6ae wa...	10.0.5.0/24	-	251	cn-northwest-1b
wangxiang-vpc2-public-1b	subnet-090c65c8745334167	Available	vpc-003580624fa76d6ae wa...	10.0.10.0/24	-	250	cn-northwest-1b
wangxiang-vpc2-private1-1b	subnet-0de695fc2678b7244	Available	vpc-003580624fa76d6ae wa...	10.0.11.0/24	-	250	cn-northwest-1b
wangxiang-vpc2-1a-1b	subnet-05a91abd5c2929e4	Available	vpc-003580624fa76d6ae wa...	10.0.12.0/24	-	251	cn-northwest-1b
wangxiang-vpc2-mgmt-1b	subnet-0b707bba459c38765	Available	vpc-003580624fa76d6ae wa...	10.0.13.0/24	-	251	cn-northwest-1b

创建 IGW 并关联此 VPC。



The screenshot shows the AWS VPC console with a table of Internet Gateways. The table has columns: Name, Internet gateway ID, State, and VPC ID. The row for 'wangxiang-vpc2-IGW' is highlighted.

Name	Internet gateway ID	State	VPC ID
wangxiang-vpc2-IGW	igw-0f867405edf6035a4	Attached	vpc-003580624fa76d6ae wangxiang-vpc2

4.2. 创建 IAM 角色

EC2 实例赋予角色后，才能根据权限使用 API 操作和资源。

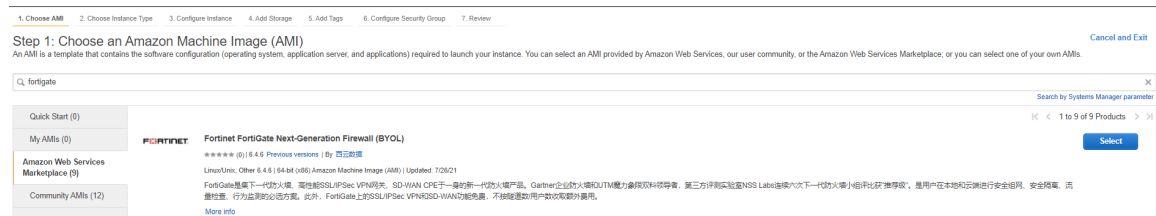
The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Roles' highlighted. The main content area shows the 'Summary' page for the 'FGT-HA-Failover' role. The role's ARN is 'arn:aws-cn:iam::321536109689:role/FGT-HA-Failover', and its description is 'Allows EC2 instances to call AWS services on your behalf.' The role is associated with the 'Instance Profile ARNs' 'arn:aws-cn:iam::321536109689:instance-profile/FGT-HA-Failover'. The creation time is '2021-09-19 13:55 UTC+0800', and the maximum session duration is '1 hour'. Below the summary, the 'Permissions' tab is selected, showing 'Permissions policies (1 policy applied)'. The 'Attach policies' button is visible, and the 'AmazonEC2FullAccess' policy is listed. The 'Policy summary' tab is active, displaying the following JSON policy document:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": "ec2:*",
6       "Effect": "Allow",
7       "Resource": "*"
8     },
9     {
10      "Effect": "Allow",
11      "Action": "elasticloadbalancing:*",
12      "Resource": "*"
13    },
14    {
15      "Effect": "Allow",
```

4.3. 创建 FortiGate 实例

部署实例时请提前准备好两台 FGT 的 license。

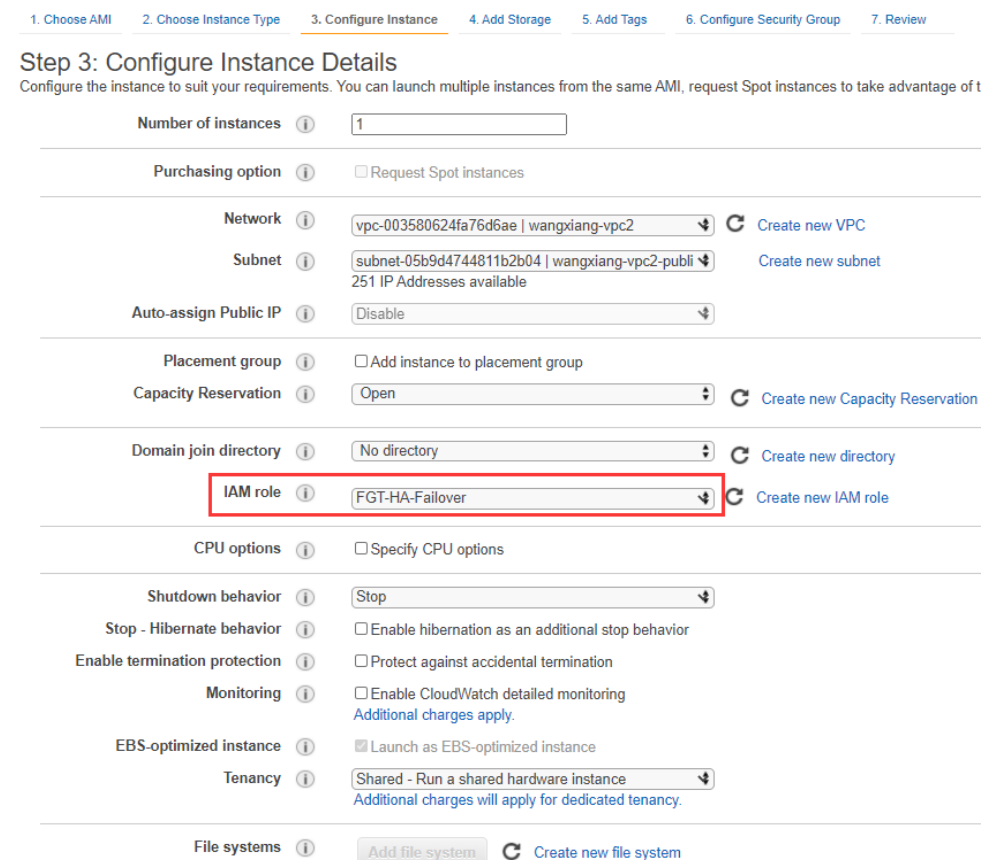
创建 FGT1，选择 FortiGate 镜像。



实例类型请选择计算优化型，这里使用 c5.xlarge。

☐	c4	c4.4xlarge	16	30	EBS only	Yes	High	Yes
☐	c4	c4.8xlarge	36	60	EBS only	Yes	10 Gigabit	Yes
☐	c5	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
☒	c5	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
☐	c5	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes

部署实例时关联 IAM 角色。



GUI 创建实例时，最多只能创建两块网卡，另外两块需要单独创建。

▼ Network interfaces ⓘ

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0 对应port1	New network interface▼	subnet-05b9d47c▼ public-1a	10.0.0.11	Add IP	The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.
eth1 对应port2	New network interface▼	subnet-0eca0c6f▼ private1-1a	10.0.1.11	Add IP	The selected subnet does not support IPv6 because it does not have an IPv6 CIDR. ❌

ⓘ We can no longer assign a public IP address to your instance

- The auto-assign public IP address feature for this instance is disabled because you specified multiple network interfaces. Public IPs can only be assigned to instances with one network interface. To re-enable the auto-assign public IP address feature, please specify only the eth0 network interface.

Add Device

▼ Advanced Details

Metadata accessible ⓘ Enabled▼

Metadata version ⓘ V1 and V2 (token optional)▼

Metadata token response hop limit ⓘ 1▼

User data ⓘ ☒ As text ☐ As file ☐ Input is already base64 encoded

(Optional)

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

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-0dbcd1bc1e44a185b	2	General Purpose SSD (gp2)▼	100 / 3000	N/A	☒	Not Encrypted▼
EBS▼	/dev/sdb▼	Search (case-insensit)▼	30	General Purpose SSD (gp2)▼	100 / 3000	N/A	☒	Not Encrypted▼

Add New Volume

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-vpc2-FGT1	☒	☒	☒

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，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 for 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: fgt-external-secgroup

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



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

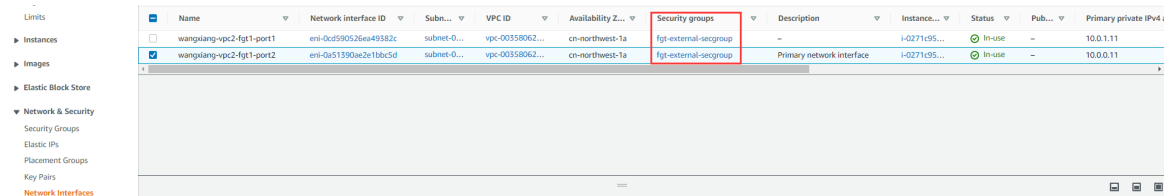
创建完成。FGT2 同理。

Tags	Name	Instance ID	Instance state	Instance t...	Status check	A...	Availability Zone	Public IP...	Publi...	Elastic IP	IPv6...	Securi...	Key n...
Limits	wangxiang-vgc2-FGT1	i-0271c9569a86244e	Running	c5.xlarge	2/2 checks passed	+	cn-northwest-1a	-	-	-	-	fgt-exte...	wangxia...
Instances	wangxiang-vgc2-FGT2	i-0fa40a879f5291993	Running	c5.xlarge	2/2 checks passed	+	cn-northwest-1b	-	-	-	-	fgt-exte...	wangxia...

4. 4. 安全组

点击网络接口可以查看到 FGT 实例创建的接口，建议给每个接口命名以便查询。

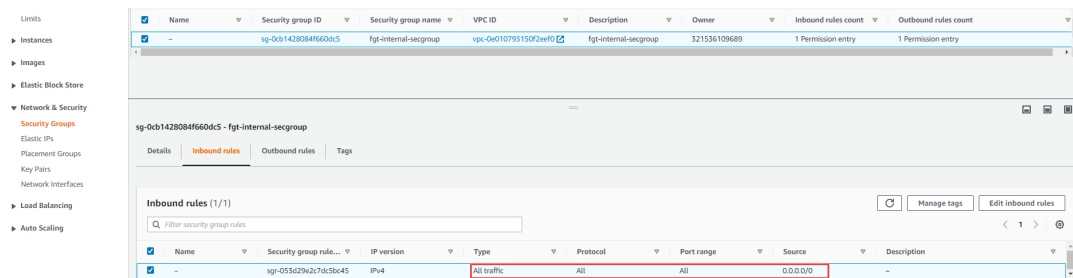
FortiGate 实例给其两个接口使用的安全组都是刚新建的 fgt-external-secgroup。



Name	Network interface ID	Subnet	VPC ID	Availability Zone	Security groups	Description	Instance	Status	Public	Primary private IP
wangliang-vc2-fgt1-port1	eni-0cd590526ea49382c	subnet-0...	vpc-00358062...	cn-northwest-1a	fgt-external-secgroup	-	i-0271c95...	In-use	-	10.0.1.11
wangliang-vc2-fgt1-port2	eni-0a51390ae2e1bbc5d	subnet-0...	vpc-00358062...	cn-northwest-1a	fgt-external-secgroup	Primary network interface	i-0271c95...	In-use	-	10.0.0.11

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。

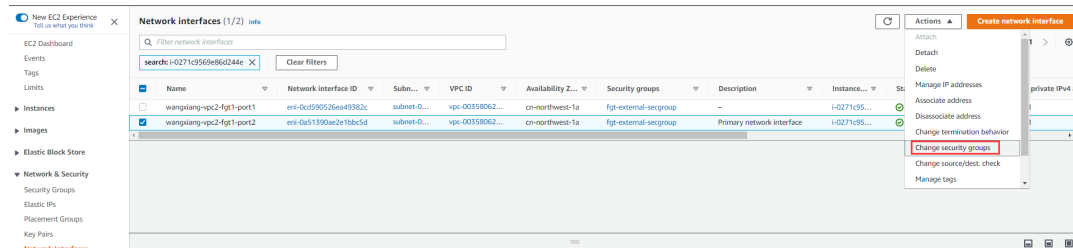
新建安全组 fgt-internal-secgroup。



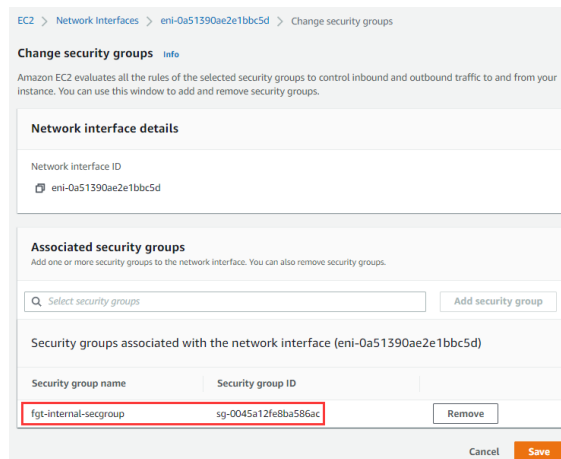
Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
sg-0cb1428084f660dc5	sg-0cb1428084f660dc5	fgt-internal-secgroup	vpc-0e010793150f2ee0f	fgt-internal-secgroup	321536109689	1 Permission entry	1 Permission entry

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgp-053a229a2c7d53bc45	IPv4	All traffic	All	All	0.0.0.0/0	-

修改 port2 接口的安全组为 fgt-internal-secgroup。



Name	Network interface ID	Subnet	VPC ID	Availability Zone	Security groups	Description	Instance	Status
wangliang-vc2-fgt1-port1	eni-0cd590526ea49382c	subnet-0...	vpc-00358062...	cn-northwest-1a	fgt-external-secgroup	-	i-0271c95...	In-use
wangliang-vc2-fgt1-port2	eni-0a51390ae2e1bbc5d	subnet-0...	vpc-00358062...	cn-northwest-1a	fgt-external-secgroup	Primary network interface	i-0271c95...	In-use



Change security groups

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-0a51390ae2e1bbc5d

Associated security groups

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

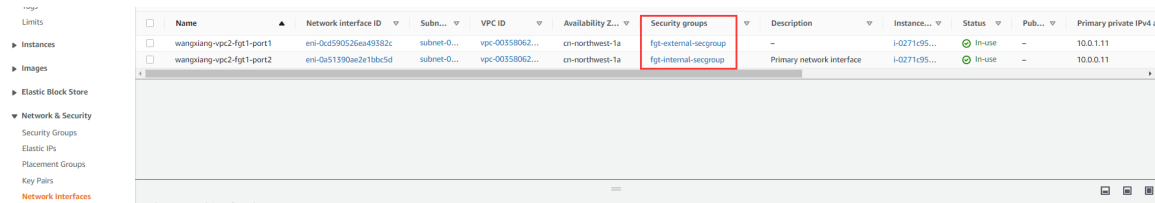
Select security groups: [Add security group]

Security groups associated with the network interface (eni-0a51390ae2e1bbc5d)

Security group name	Security group ID	Remove
fgt-internal-secgroup	sg-0045a12fe8ba586ac	Remove

Cancel Save

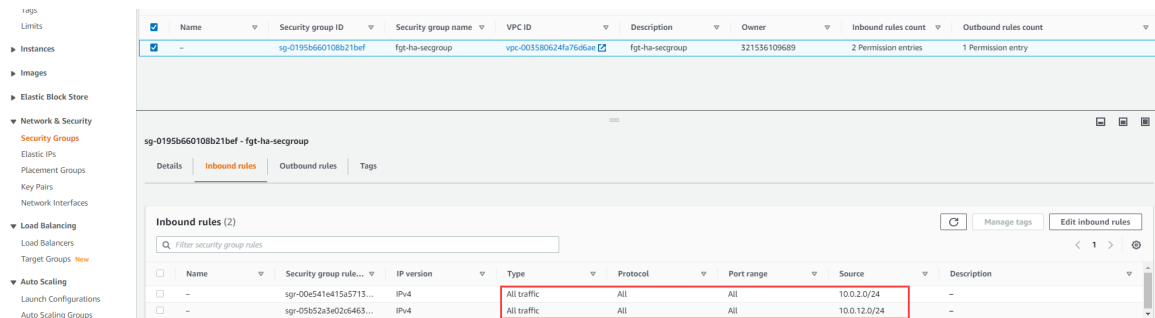
修改完成。



The screenshot shows the AWS Management Console interface. On the left, the 'Network & Security' menu is expanded, with 'Network Interfaces' selected. The main pane displays a table of network interfaces. Two interfaces are listed: 'wangxiang-vpc2-fgt1-port1' and 'wangxiang-vpc2-fgt1-port2'. Both are associated with the 'ftg-external-secgroup' and 'ftg-internal-secgroup' security groups. The 'ftg-external-secgroup' is highlighted with a red box.

Name	Network interface ID	Subnet	VPC ID	Availability Zone	Security groups	Description	Instance	Status	Public	Primary private IPv4
wangxiang-vpc2-fgt1-port1	eni-0cd59026ea49382c	subnet-0...	vpc-00358062...	cn-northwest-1a	ftg-external-secgroup ftg-internal-secgroup	Primary network interface	i-0271c95...	In-use	-	10.0.1.11
wangxiang-vpc2-fgt1-port2	eni-0a51390a2e1bb5d	subnet-0...	vpc-00358062...	cn-northwest-1a	ftg-external-secgroup ftg-internal-secgroup		i-0271c95...	In-use	-	10.0.0.11

FortiGate 还需要新建两个端口，一个 HA 接口 port3，新建对应的安全组 fgt-ha-secgroup，放通 port3 接口网段（FGT1: 10.0.2.0/24, FGT2: 10.0.12.0/24）的所有流量。

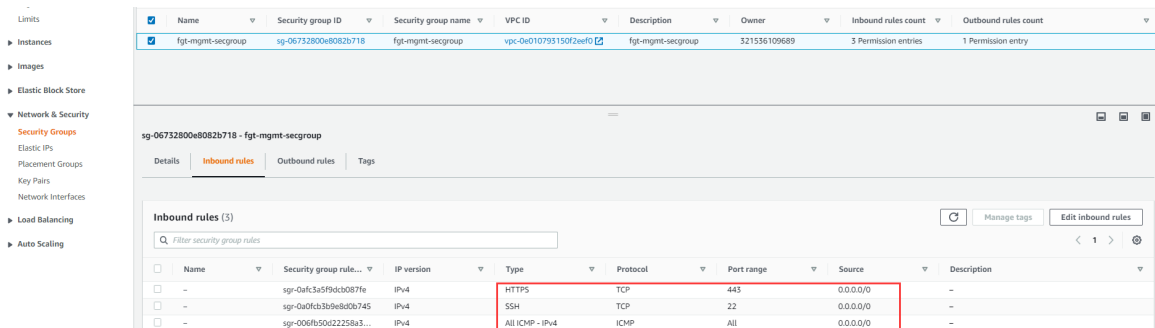


The screenshot shows the AWS Management Console interface. On the left, the 'Network & Security' menu is expanded, with 'Security Groups' selected. The main pane displays the details for the 'sg-0195b660108b21bef' security group. The 'Inbound rules' tab is active, showing a table of inbound rules. Two rules are listed: 'All traffic' from '10.0.2.0/24' and 'All traffic' from '10.0.12.0/24'. Both rules are highlighted with a red box.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
-	sg-0195b660108b21bef	fgt-ha-secgroup	vpc-003580624fa76d6ae	fgt-ha-secgroup	321536109689	2 Permission entries	1 Permission entry

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sg-00e541e415a5713...	IPv4	All traffic	All	All	10.0.2.0/24	-
-	sg-05852a3e02c463...	IPv4	All traffic	All	All	10.0.12.0/24	-

一个MGMT管理口port4,新建对应的安全组 fgt-mgmt-secgroup,放通 SSH,HTTPS 和 ICMP。



The screenshot shows the AWS Management Console interface. On the left, the 'Network & Security' menu is expanded, with 'Security Groups' selected. The main pane displays the details for the 'sg-06732800e8082b718' security group. The 'Inbound rules' tab is active, showing a table of inbound rules. Three rules are listed: 'HTTPS' from '0.0.0.0/0', 'SSH' from '0.0.0.0/0', and 'All ICMP - IPv4' from '0.0.0.0/0'. All three rules are highlighted with a red box.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
fgt-mgmt-secgroup	sg-06732800e8082b718	fgt-mgmt-secgroup	vpc-0a010795150f2ee0d	fgt-mgmt-secgroup	321536109689	3 Permission entries	1 Permission entry

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sg-0af33e5f9dc087fe	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
-	sg-0a9fcb39e8e80b745	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sg-006fb50022258a3...	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	-

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。

4.5. 创建网卡

选择 Services → Network & Security → Network interfaces, 点击 Create Network interface, 创建 FGT1 的 port3 接口, 安全组选择 fgt-ha-secgroup, 如果是 port4, 则选择 fgt-mgmt-secgroup。

Create network interface

An elastic network interface is a logical networking component in a VPC that represents a virtual network card.

Details Info

Description - optional
A descriptive name for the network interface.

wangxiang-vpc2-fgt1-port3

Subnet
The subnet in which to create the network interface.

subnet-08ec94b6f8c666461

Private IPv4 address
The private IPv4 address to assign to the network interface.

☐ Auto-assign
☒ Custom
IPv4 address

10.0.2.11

Elastic Fabric Adapter
☐ Enable

Security groups (1/5) Info

Find resources

	Group ID	Group name	Description
☐	sg-0900fbf91236b5fff	fgt-mgmt-secgroup	fgt-mgmt-secgroup
☐	sg-0045a12fe8ba586ac	fgt-internal-secgroup	fgt-internal-secgroup
☒	sg-0195b660108b21bef	fgt-ha-secgroup	fgt-ha-secgroup
☐	sg-06699f0a1bb4b4885	fgt-external-secgroup	This security group was generate...

关联网卡到 FGT 实例。请先关联 port3, port3 关联成功后, 再关联 port4。

Tags

Limits

Instances

Instances New

Instance Types

Launch Templates

Spot Requests

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Snapshots

Name	Instance ID	Instance state	Instance t...
wangxiang-vpc2-FGT1	i-0271c9569e86d244e	Running	c5.xlarge
wangxiang-vpc2-FGT2		Running	c5.xlarge

Instance: i-0271c9569e86d244e

Details Security Netwo

Instance summary Info

Instance ID

i-0271c9569e86d244e (wangxi)

IPv6 address

-

Public IPv4 address

Attach network interface

Detach network interface

Change source/destination check

Disassociate Elastic IP address

Manage IP addresses

EC2 > Instances > i-0271c9569e86d244e > Attach network interface

Attach network interface Info

You can create and configure network interfaces in your account and then attach them to instances in your VPC.

Instance ID
i-0271c9569e86d244e (wangxiang-vpc2-FGT1)

Network interface
Select a network interface to attach to the instance.

eni-0467deef52c171442 (wangxiang-vpc2-figt1-port3)

⚠ If you attach another network interface to your instance, your current public IP address is released when you restart your instance. Learn more about [public IP addresses](#)

Cancel Attach

关联完成。

	Name	Network interface ID	Subnet ID	VPC ID	Availability Z...	Security groups	Description	Inst...	Status	Pub...	Primary privat
	wangxiang-vpc2-figt1-port1	eni-0a51390ae261bdc5d	subnet-05890474...	vpc-003580624fa76d...	cn-northwest-1a	fgt-external-secgroup	Primary network interface	i-0271c...	in-use	10.0.0.11	
	wangxiang-vpc2-figt1-port2	eni-0cd590526ea49382c	subnet-0eca0c65d...	vpc-003580624fa76d...	cn-northwest-1a	fgt-internal-secgroup	-	i-0271c...	in-use	10.0.1.11	
	wangxiang-vpc2-figt1-port3	eni-0467deef52c171442	subnet-08ec94b6f...	vpc-003580624fa76d...	cn-northwest-1a	fgt-ha-secgroup	wangxiang-vpc2-figt1-port3	i-0271c...	in-use	10.0.2.11	
	wangxiang-vpc2-figt1-port4	eni-08f4361097b1f59a1	subnet-0781dc85...	vpc-003580624fa76d...	cn-northwest-1a	fgt-mgmt-secgroup	wangxiang-vpc2-figt1-port4	i-0271c...	in-use	10.0.3.11	
	wangxiang-vpc2-figt2-port1	eni-01338913334708282	subnet-19900c0c8f...	vpc-003580624fa76d...	cn-northwest-1b	fgt-external-secgroup	Primary network interface	i-0fa40...	in-use	10.0.10.11	
	wangxiang-vpc2-figt2-port2	eni-083fe1ed3da12d98b	subnet-0d66f5c2...	vpc-003580624fa76d...	cn-northwest-1b	fgt-internal-secgroup	-	i-0fa40...	in-use	10.0.11.11	
	wangxiang-vpc2-figt2-port3	eni-03f72fb7545398b1	subnet-05a91abdc...	vpc-003580624fa76d...	cn-northwest-1b	fgt-ha-secgroup	wangxiang-vpc2-figt2-port3	i-0fa40...	in-use	10.0.12.11	
	wangxiang-vpc2-figt2-port4	eni-02496a37094af09ae	subnet-06707b8a...	vpc-003580624fa76d...	cn-northwest-1b	fgt-mgmt-secgroup	wangxiang-vpc2-figt2-port4	i-0fa40...	in-use	10.0.13.11	

4.6. 弹性 IP

创建 4 个弹性 IP，最终使用 3 个，另外 1 个是临时的，HA 形成后可以释放。

最终使用的 3 个弹性 IP：

一个弹性 IP 关联 FGT1 实例 NIC4 10.0.3.11，即 FGT1 HA 的独立管理口 port4。

一个弹性 IP 关联 FGT2 实例 NIC4 10.0.13.11，即 FGT2 HA 的独立管理口 port4。

下面临时配置的弹性 IP 保留一个，关联 FGT HA 的 Master 实例（当前 FGT1）NIC1 的地址 10.0.0.11。

临时配置 FGT2 的弹性 IP：

一个弹性 IP 关联 FGT1 实例 NIC1 10.0.0.11，即 FGT1 port1 接口。

一个弹性 IP 关联 FGT2 实例 NIC1 10.0.10.11，即 FGT2 port1 接口。

Instances	Name	Allocated IPv4 address	Type	Allocation ID	Associated instance ID	Private IP address	Network interface ID
Images	wangxiang-vpc2-fgt1-port1	161.189.120.39	Public IP	eipalloc-092c8f1c3cc34b49b	i-0271c9569e86d244e	10.0.0.11	eni-0a51390a2e1b8c5d
Elastic Block Store	wangxiang-vpc2-fgt2-port1	161.189.15.250	Public IP	eipalloc-03e6afde5a7114cba	i-0fa40e879f5291993	10.0.10.11	eni-01358913334708282
Network & Security	wangxiang-vpc2-fgt2-mgmt	161.189.82.107	Public IP	eipalloc-08afa487f18ed4b0c	i-0fa40e879f5291993	10.0.13.11	eni-02496a37094af09ae
Security Groups	wangxiang-vpc2-fgt1-mgmt	52.83.63.81	Public IP	eipalloc-09c9736600a16f4ac	i-0271c9569e86d244e	10.0.3.11	eni-08fd361097b1f59a1
Elastic IPs							

4. 7. 配置 VPC 路由表

Public 路由表默认路由指向 IGW，关联 public（10.0.0.0/24，10.0.10.0/24），ha（10.0.2.0/24，10.0.12.0/24），mgmt（10.0.3.0/24，10.0.13.0/24）6 个子网。

rtb-045cee56a1ee72a5b / wangxiang-vpc2-public-rtb

Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (6)

Subnet ID	IPv4 CIDR
subnet-08ec94b6f8c666461 / wangxiang-vpc2-ha-1a	10.0.2.0/24
subnet-05a91abdc6c2929e4 / wangxiang-vpc2-ha-1b	10.0.12.0/24
subnet-05b9d4744811b2b04 / wangxiang-vpc2-public-1a	10.0.0.0/24
subnet-090c65c8745334167 / wangxiang-vpc2-public-1b	10.0.10.0/24
subnet-0781dc85511a00dcf / wangxiang-vpc2-mgmt-1a	10.0.3.0/24
subnet-0b707b8a439c38765 / wangxiang-vpc2-mgmt-1b	10.0.13.0/24

Private 路由表默认路由指向 FGT HA Master(当前 FGT1)实例的 NIC2 的接口 ID, 关联 private 子网 (10.0.1.0/24, 10.0.11.0/24, 10.0.4.0/24, 10.0.5.0/24)

The screenshot displays the AWS Management Console interface for configuring a route table. The left sidebar shows the navigation menu with categories like VIRTUAL PRIVATE CLOUD and SECURITY. The main content area shows the 'Routes' tab for the route table 'rtb-0a1623244f20b063c / wangxiang-vpc2-private-rtb'. Below the 'Routes' tab, the 'Subnet associations' tab is selected, showing 'Explicit subnet associations (4)'. The table lists four subnets and their associated IPv4 CIDR blocks.

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
☒ wangxiang-vpc2-private-rtb	rtb-0a1623244f20b063c	4 subnets	-	No	vpc-003580624fa76d6ae wangxiang-vpc2
☐ wangxiang-vpc2-public-rtb	rtb-045cee56a7ee72a5b	6 subnets	-	No	vpc-003580624fa76d6ae wangxiang-vpc2
☐ -	rtb-044b5cde90e76d592	-	-	Yes	vpc-003580624fa76d6ae wangxiang-vpc2

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	eni-0cd590526ea49382c [fgt1 nic2]	Active	No

Subnet ID	IPv4 CIDR
subnet-0eca0c65d448dd93b / wangxiang-vpc2-private1-1a	10.0.1.0/24
subnet-01eeb2d5b2199ceba / wangxiang-vpc2-private2-1a	10.0.4.0/24
subnet-0de65f5c2e7bb7244 / wangxiang-vpc2-private1-1b	10.0.11.0/24
subnet-05a71d5511f72a0c2 / wangxiang-vpc2-private2-1b	10.0.5.0/24

4.8. 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，FGT 实例必须禁用源/目标检查。

The screenshot shows the AWS Management Console interface. On the left, the navigation pane is open, showing 'Instances' under 'EC2'. The main content area displays a list of instances. The instance 'wangxiang-vpc-FGT1' with ID 'i-0271c9569e86d244e' is selected. A context menu is open over this instance, showing options like 'Launch instances', 'Connect', 'Stop instance', etc. The 'Instance settings' option is highlighted, and a sub-menu is shown with 'Networking' selected. In the 'Networking' sub-menu, the 'Change source/destination check' option is highlighted with a red box.

EC2 > Instances > i-0271c9569e86d244e > 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-0271c9569e86d244e (wangxiang-vpc-FGT1)

Network interface [Info](#)

- eni-0a51390ae2e1bbc5d (wangxiang-vpc-fgt1-port2)
- eni-0467deef52c171442 (wangxiang-vpc-fgt1-port3)
- eni-0cd590526ea49382c (wangxiang-vpc-fgt1-port1)
- eni-08fd361097b1f59a1 (wangxiang-vpc-fgt1-port4)

Source / destination checking [Info](#)

☒ Stop

ⓘ 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-0271c9569e86d244e --no-source-dest-check
```

[Copy](#)

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

4.9. 访问 FortiGate

Https 访问 FortiGate:

使用 <https://161.189.15.230/>（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。



Username
Password
Login

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

FortiGate VM License

License is invalid for current VM configuration. Upload a new license or reconfigure the VM.

Upload License File

Select file

OK Cancel

FortiGate 登录成功。

Dashboard

System Information

Hostname	FGVM08TM21002971
Serial Number	FGVM08TM21002971
Firmware	v6.4.6 build1879 (GA)
Mode	NAT
System Time	2021/09/22 19:35:28
Uptime	00:00:03:08
WAN IP	161.189.15.230

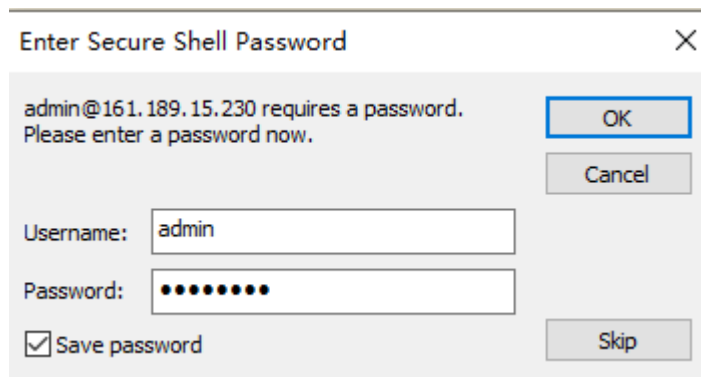
Licenses (173.243.141.6)

- FortiCare Support
- Firmware & General Updates
- IPS
- AntiVirus
- Web Filtering

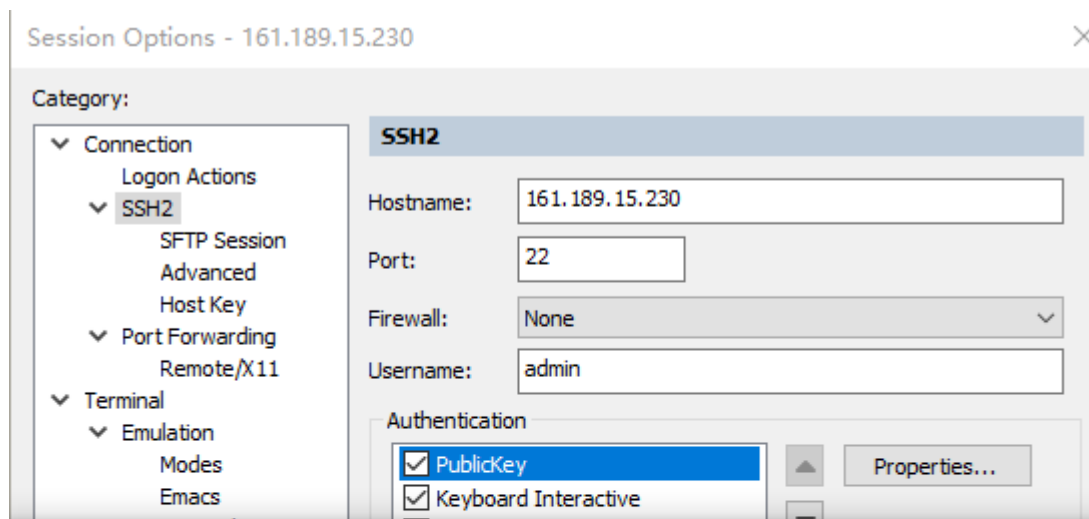
FortiToken 0/0

SSH 访问 FortiGate 有两种方式，下图是 CRT 软件的访问截图：

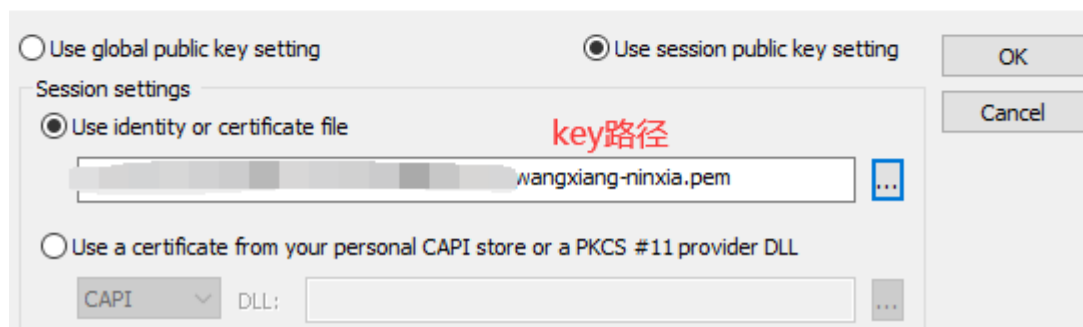
一种是通过账号密码的方式：



一种是通过 key 的方式：



Public Key Properties



4. 10. 配置 FortiGate

FGT1 基本配置，先配置路由，再修改地址，否则 FGT1 将无法访问。

```
config router static
    edit 1
        set gateway 10.0.0.1
        set device "port1"
    next
    edit 2
        set dst 10.0.0.0 255.255.0.0
        set gateway 10.0.1.1
        set device "port2"
    next
end
config system interface
    edit "port1"
        set mode static
        set ip 10.0.0.11 255.255.255.0
        set allowaccess ping https ssh
    next
    edit "port2"
        set mode static
        set ip 10.0.1.11 255.255.255.0
        set allowaccess ping
    next
    edit "port3"
        set mode static
        set ip 10.0.2.11 255.255.255.0
        set allowaccess ping
    next
    edit "port4"
        set mode static
        set ip 10.0.3.11 255.255.255.0
        set allowaccess ping https ssh
    next
end
config system global
    set admintimeout 50
    set hostname "FGT1"
    set timezone 55
```

```
end
```

#因为不同 AZ 的地址段是不一样的，因此下面的配置不需要同步

```
config system vdom-exception
    edit 1
        set object system.interface
    next
    edit 2
        set object router.static
    next
    edit 3
        set object firewall.vip
    next
end
```

FGT2 基本配置，先配置路由，再修改地址，否则 FGT2 将无法访问。

```
config router static
    edit 1
        set gateway 10.0.10.1
        set device "port1"
    next
    edit 2
        set dst 10.0.0.0 255.255.0.0
        set gateway 10.0.11.1
        set device "port2"
    next
end

config system interface
    edit "port1"
        set mode static
        set ip 10.0.10.11 255.255.255.0
        set allowaccess ping https ssh
    next
    edit "port2"
        set mode static
        set ip 10.0.11.11 255.255.255.0
        set allowaccess ping
    next
    edit "port3"
        set mode static
        set ip 10.0.12.11 255.255.255.0
        set allowaccess ping
    next
end
```

```
edit "port4"
    set mode static
    set ip 10.0.13.11 255.255.255.0
    set allowaccess ping https ssh
next
end
config system global
    set admintimeout 50
    set hostname "FGT2"
    set timezone 55
end
#因为不同 AZ 的地址段是不一样的，因此下面的配置不需要同步
config system vdom-exception
    edit 1
        set object system.interface
    next
    edit 2
        set object router.static
    next
    edit 3
        set object firewall.vip
    next
end
```

FGT1 HA 配置：

```
config system ha
    set group-name "FGTHA"
    set mode a-p
    set password fortinet
    set hbdev "port3" 50
    set session-pickup enable
    set session-pickup-connectionless enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.3.1
        next
    end
    set override disable
    set priority 200
    set unicast-hb enable
```

```

set unicast-hb-peerip 10.0.12.11
end

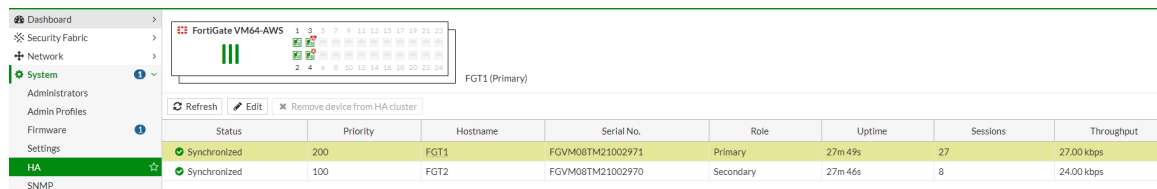
FGT2 HA 配置:

config system ha
    set group-name "FGTHA"
    set mode a-p
    set password fortinet
    set hbdev "port3" 50
    set session-pickup enable
    set session-pickup-connectionless enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.0.13.1
        next
    end
    set override disable
    set priority 100
    set unicast-hb enable
    set unicast-hb-peerip 10.0.2.11
end

```

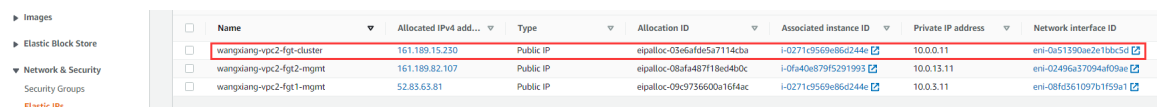
配置完成后，即可使用 FGT 实例 NIC4 关联的弹性 IP 进行访问。

注意：如果删除 HA 的配置，port3 和 port4 的接口地址也会移除。



Status	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
Synchronized	200	FGT1	FGVM08TM21002971	Primary	27m 49s	27	27.00 kbps
Synchronized	100	FGT2	FGVM08TM21002970	Secondary	27m 46s	8	24.00 kbps

形成 HA 后，即可删除临时配置一个弹性 IP。



Name	Allocated IPv4 address	Type	Allocation ID	Associated Instance ID	Private IP address	Network interface ID
wangxiang-vpc2-fgt-cluster	161.189.15.230	Public IP	eipalloc-03e6afde5a7114c9a	i-0271c9569e86cd244e	10.0.0.11	eni-0a51390ae3e1bbcd5d
wangxiang-vpc2-fgt2-mgmt	161.189.82.107	Public IP	eipalloc-08af4487f18ed4b0c	i-0fa40e879f5291993	10.0.13.11	eni-02496a37094af09ae
wangxiang-vpc2-fgt1-mgmt	52.83.63.81	Public IP	eipalloc-09c9736600a16f4ac	i-0271c9569e86cd244e	10.0.3.11	eni-08fd361097b1f59a1

FGT1 接口及路由：

Dashboard > Security Fabric > Network > Interfaces

FortiGate VM64-AWS

+ Create New Edit Delete Search

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
Physical Interface 4				
port1	Physical Interface		10.0.0.11/255.255.255.0	PING HTTPS SSH
port2	Physical Interface		10.0.1.11/255.255.255.0	PING
port3	Physical Interface		10.0.2.11/255.255.255.0	PING
port4	Physical Interface		10.0.3.11/255.255.255.0	PING HTTPS SSH

System 1

Dashboard > Security Fabric > Network > Static Routes

+ Create New Edit Clone Delete Search

Destination	Gateway IP	Interface	Status
IPv4 2			
0.0.0.0/0	10.0.0.1	port1	Enabled
10.0.0.0/16	10.0.1.1	port2	Enabled

FGT2 接口及路由：

Dashboard > Security Fabric > Network > Interfaces

FortiGate VM64-AWS

+ Create New Edit Clone Delete Search

Name	Type	Members	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
Physical Interface 4				
port1	Physical Interface		10.0.10.11/255.255.255.0	PING HTTPS SSH
port2	Physical Interface		10.0.11.11/255.255.255.0	PING
port3	Physical Interface		10.0.12.11/255.255.255.0	PING
port4	Physical Interface		10.0.13.11/255.255.255.0	PING HTTPS SSH

System 1

Dashboard > Security Fabric > Network > Static Routes

+ Create New Edit Clone Delete Search

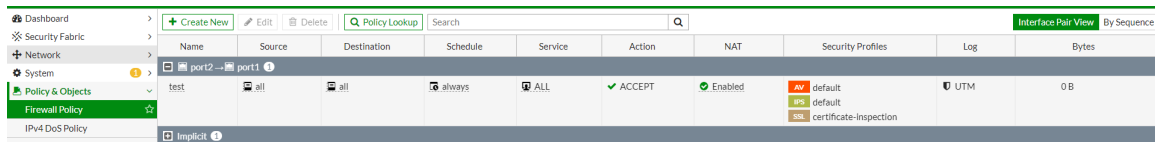
Destination	Gateway IP	Interface	Status
IPv4 2			
0.0.0.0/0	10.0.10.1	port1	Enabled
10.0.0.0/16	10.0.11.1	port2	Enabled

4.11. FortiGate 配置源 NAT

使用接口地址做源 NAT:

FGT1 配置防火墙策略, 会自动同步给 FGT2:

注意: 因为 FGT1 和 FGT2 的接口 ip 地址或者 pool 地址池是不一样的, 因此 snat 的会话同步没有意义, HA 切换时, 原有的 snat 连接会断开。



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
test	port12	port1	always	ALL	ACCEPT	Enabled	default, default, certificate-inspection	UTM	0 B

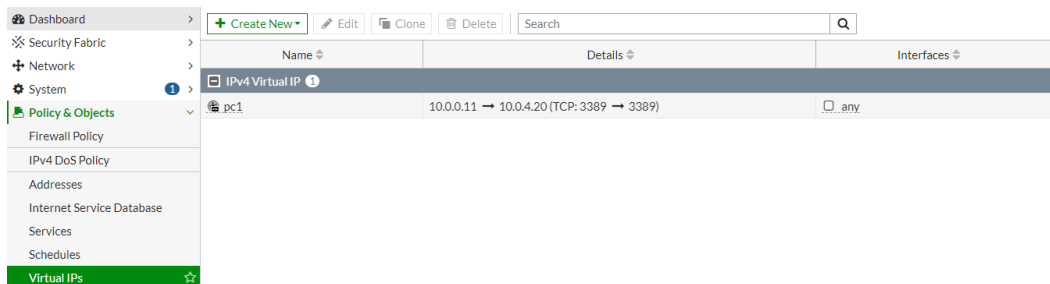
4.12. FortiGate 配置目的 NAT

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。

注意: 因为 FGT1 和 FGT2 的 vip 地址是不一样的, 因此目的 nat 的会话同步没有意义, HA 切换时, 原有的目的 nat 连接会断开。

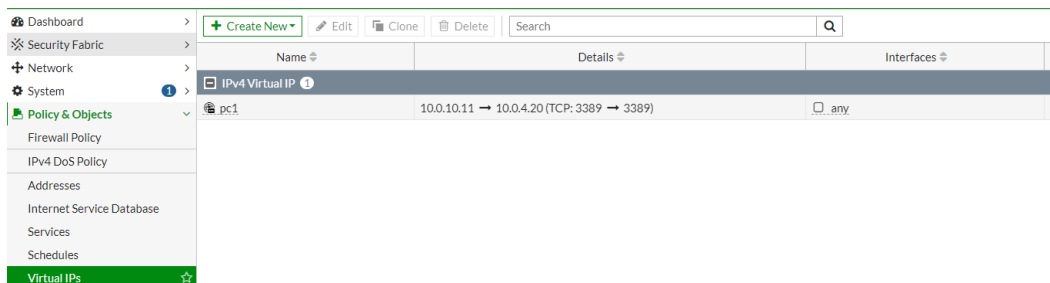
用 port1 接口的地址做目的 NAT:

FGT1 配置 VIP, 名称 pc1:



Name	Details	Interfaces
pc1	10.0.0.11 → 10.0.4.20 (TCP: 3389 → 3389)	.any

FGT2 配置 VIP, 名称 pc1, 要和 FGT1 的 VIP 名称一样, 这样防火墙策略才能够同步:



Name	Details	Interfaces
pc1	10.0.10.11 → 10.0.4.20 (TCP: 3389 → 3389)	.any

FGT1 配置防火墙策略调用此 VIP，会同步给 FGT2:

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
test2	all	pc1	always	ALL	ACCEPT	Disabled	av default ips default ssl certificate-inspection	UTM	0 B

分配单独的 IP 来做目的 NAT:

因为 FGT1 和 FGT2 的地址段不一样，因此 FGT1 和 FGT2 给 NIC1 都需要单独分配一个地址。

EC2 > Instances > i-0271c9569e86d244e > Manage IP addresses
fgt1实例

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.

▶ eth1: eni-0cd590526ea49382c - 10.0.1.0/24
▼ eth0: eni-0a51390ae2e1bbc5d - Primary network interface - 10.0.0.0/24

IPv4 addresses

Private IP addressPublic IP address

10.0.0.11161.189.15.230Unassign

10.0.0.100Undo

Assign new IP address

▶ eth2: eni-0467deef52c171442 - wangxiang-vpc2-figt1-port3 - 10.0.2.0/24
▶ eth3: eni-08fd361097b1f59a1 - wangxiang-vpc2-figt1-port4 - 10.0.3.0/24

☐ 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.

CancelSave

EC2 > Instances > i-0fa40e679f5291993 > Manage IP addresses
fgt2实例

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-01338913334708282 - Primary network interface - 10.0.10.0/24

IPv4 addresses

Private IP addressPublic IP address

10.0.10.11Undo

10.0.10.100Undo

Assign new IP address

▶ eth1: eni-083fe1ed3da12d9b9 - 10.0.11.0/24
▶ eth3: eni-02496a37094af09ae - wangxiang-vpc2-figt2-port4 - 10.0.13.0/24
▶ eth2: eni-03f27fb75345398b1 - wangxiang-vpc2-figt2-port5 - 10.0.12.0/24

☐ 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.

CancelSave

分配弹性 IP 关联 FGT1 实例的 NIC1 10.0.0.100。FGT2 不用关联。

Instances	Name	Allocated IPv4 add...	Type	Allocation ID	Associated Instance ID	Private IP address	Network interface ID
wangxiang-vpc2-figt-cluster2		69.234.245.221	Public IP	eipalloc-0a0b5404ac469ee15	i-0271c9569e86d244e	10.0.0.100	eni-0a51390ae2e1bbc5d

FGT1 配置 VIP，名称 pc2:

Name	Details	Interfaces
IPv4 Virtual IP 2		
pc1	10.0.0.11 → 10.0.4.20 (TCP: 3389 → 3389)	any
pc2	10.0.0.100 → 10.0.5.20 (TCP: 2222 → 22)	any

FGT2 配置 VIP，名称 pc2，要和 FGT1 的 VIP 名称一样，这样防火墙策略才能够同步：

The screenshot shows the Palo Alto Networks GUI. On the left, the 'Virtual IPs' menu item is selected. The main panel displays the 'IPv4 Virtual IP' configuration page. A table lists the configured virtual IP addresses:

Name	Details	Interfaces
pc1	10.0.10.11 → 10.0.4.20 (TCP: 3389 → 3389)	any
pc2	10.0.10.100 → 10.0.5.20 (TCP: 2222 → 22)	any

The 'pc2' row is highlighted, and its IP address and details are enclosed in a red box.

FGT1 配置防火墙策略调用此 VIP，会同步给 FGT2:

Dashboard											+ Create New		Edit	Delete	Q Policy Lookup		Search			Interface Pair View		By Sequence
Security Fabric		Network		System		Policy & Objects		Firewall Policy		IP4 DoS Policy		Addresses		Internet Service Database								
Name		Source		Destination		Schedule		Service		Action		NAT		Security Profiles		Log		Bytes				
test2		port1 → port2		pc1		always		ALL		ACCEPT		Disabled		default		UTM		0B				
test3		all		pc2		always		ALL		ACCEPT		Disabled		default		UTM		0B				

FGT 实例 NIC1，即 port1 安全组 fgt-external-secgroup 放通 3389，2222 这 2 个对外的端口。

Limits

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
-	sg-06699fa1bb4b4885	fgt-external-secgroup	vpc-003580624fa76dcae	This security group wa...	321E36109689	5 Permission entries	1 Permission entry

Instances

Images

Elastic Block Store

Network & Security

Security Groups

sg-06699fa1bb4b4885 - fgt-external-secgroup

Details | **Inbound rules** | Outbound rules | Tags

Inbound rules (5)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sg-006e498da262467f	IPv4	RDP	TCP	3389	0.0.0.0/0	-
-	sg-000da7ef9226455...	IPv4	Custom TCP	TCP	2222	0.0.0.0/0	-
-	sg-032c7f8f0a516a483	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
-	sg-0dadce8b8e2d2a195	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sg-0ab748552df690fa	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	-

5. 业务测试

测试的 PC 如下：

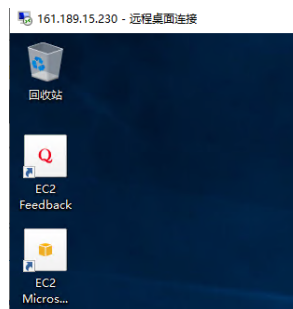
Tags	Name	Instance ID	Instance state	Instance t...	Status check	A...	Availability Zone	Public IP...	Publi...	Elastic IP	IPv6...	Secur...	Key n...
Limits	wangliang-ipc2-pc1	i-01a8f1c50e10e2af2	Running	t2.medium	2/2 checks passed	+	cn-northwest-1a	-	-	-	-	permit-all	wanglia...
Instances	wangliang-ipc2-pc2	i-0dfe3d76b7c01846	Running	t2.medium	2/2 checks passed	+	cn-northwest-1b	-	-	-	-	permit-all	wanglia...

目的 NAT 测试：

ssh 69.234.249.221 2222 访问正常。

```
ec2-user@ip-10-0-5-20:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.0.5.20 netmask 255.255.255.0 broadcast 10.0.5.255
    inet6 fe80::4f0:39ff:fedd:2168 prefixlen 64 scopeid 0x20<link>
    ether 06:f0:39:dd:21:68 txqueuelen 1000 (Ethernet)
    RX packets 458 bytes 51002 (49.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 703 bytes 70624 (68.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

远程桌面访问正常。



源 NAT 测试：

PC2 10.0.5.20 ping 114.114.114.114 正常

```
[ec2-user@ip-10-0-5-20 ~]$ 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=83 time=40.5 ms
64 bytes from 114.114.114.114: icmp_seq=2 ttl=66 time=40.5 ms
64 bytes from 114.114.114.114: icmp_seq=3 ttl=57 time=40.4 ms
64 bytes from 114.114.114.114: icmp_seq=4 ttl=71 time=40.4 ms
^C
--- 114.114.114.114 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 40.398/40.453/40.518/0.148 ms
```

PC1 10.0.4.20 访问 baidu 正常。



6. HA 切换测试

HA 测试目的：FGT 支持跨 AZ 的 HA，但不同 AZ 的地址段不一样，因此 SNAT 和 DNAT 的会话同步无意义，HA 切换后 SNAT 和 DNAT 的连接会断开，需要重新连接。

从外网 ssh 到 pc2。

```
ec2-user@ip-10-0-5-20:~ x
Last login: Thu Sep 23 06:44:31 2021 from 61.149.143.226
[ec2-user@ip-10-0-5-20 ~]$
[ec2-user@ip-10-0-5-20 ~]$
[ec2-user@ip-10-0-5-20 ~]$
[ec2-user@ip-10-0-5-20 ~]$
```

从外网 RDP 连接到 pc1，从 pc1 ping 114。

```
161.189.15.230 - 远程桌面连接
管理员: 命令提示符 - ping 114.114.114.114 -t
Microsoft Windows [版本 10.0.17763.2183]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping 114.114.114.114 -t

正在 Ping 114.114.114.114 具有 32 字节的数据:
来自 114.114.114.114 的回复: 字节=32 时间=39ms TTL=83
来自 114.114.114.114 的回复: 字节=32 时间=39ms TTL=72
来自 114.114.114.114 的回复: 字节=32 时间=39ms TTL=60
来自 114.114.114.114 的回复: 字节=32 时间=39ms TTL=75
```

HA 切换前，FGT 是主，FGT2 是备：

业务口的弹性 IP 关联到 FGT1 NIC1 网卡，即 port1。

Name	Allocated IPv4 add...	Type	Allocation ID	Associated Instance ID	Private IP address	Network interface ID
wangxiang-vpc2-igt-cluster	161.189.15.230	Public IP	eipalloc-03e6a4de5a7114cba	i-0271c9569e86d244e	10.0.0.11	eni-oa51390ae2e1bb5d
wangxiang-vpc2-igt-cluster2	69.234.249.221	Public IP	eipalloc-0a0b5404ac469ee15	i-0271c9569e86d244e	10.0.0.100	eni-oa51390ae2e1bb5d

Private 路由表默认路由指向 FGT1 NIC2 网卡，即 port2

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
wangxiang-vpc2-private-rtb	rtb-0a1623244f20b063c	4 subnets	-	No	vpc-003580624fa76d6ae wangxiang-vpc2
wangxiang-vpc2-public-rtb	rtb-045cee56a1ee72a5b	6 subnets	-	No	vpc-003580624fa76d6ae wangxiang-vpc2
-	rtb-044b5cde90e76d592	-	-	Yes	vpc-003580624fa76d6ae wangxiang-vpc2

rtb-0a1623244f20b063c / wangxiang-vpc2-private-rtb			
Routes (2)			
Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	eni-0cd590526ea49582c fgt1 nic2	Active	No

FGT1 的 SNAT 和 DNAT 会话同步到 FGT2，但是 FGT2 是利用不了的：

RDP 会话：

```
52.63.63.81 x 161.189.82.107 x
FGT1 # diagnose sys session filter dport 3389
FGT1 # diagnose sys session list
session info: proto=6 proto_state=11 duration=774 expire=3599 timeout=3600 flags=00
000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced
statistic(bytes/packets/allow_err): org=478913/5859/1 reply=2057406/6156/1 tuples=3
tx speed(Bps/kbps): 618/4 rx speed(Bps/kbps): 2656/21
origin->sink: org pre->post_reply pre->post dev=3->4/4->3 mvs=10.0.1.1/10.0.0.1
hook-pre dir=org act=dnat 61.149.143.226:20616->10.0.0.11:3389(10.0.4.20:3389)
hook-post dir=reply act=snat 10.0.4.20:3389->61.149.143.226:20616(10.0.0.11:3389)
hook-post dir=org act=noop 61.149.143.226:20616->10.0.4.20:3389(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00002bd9 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdbs_link_id=00000000 rpdbs_svc_id=0 ngfwid=n/a
npu_state=0x041008
total session 1

FGT2 # diagnose sys session filter dport 3389
FGT2 # diagnose sys session list
session info: proto=6 proto_state=11 duration=785 expire=2814 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty ndr syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0 fgt2 dnat的地址是10.0.10.11
origin->sink: org pre->post_reply pre->post dev=3->4/4->3 mvs=0.0.0.0/0.0.0.0
hook-pre dir=org act=dnat 61.149.143.226:20616->10.0.0.11:3389(10.0.4.20:3389)
hook-post dir=reply act=snat 10.0.4.20:3389->61.149.143.226:20616(10.0.0.11:3389)
hook-post dir=org act=noop 61.149.143.226:20616->10.0.4.20:3389(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00002bd9 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdbs_link_id=00000000 rpdbs_svc_id=0 ngfwid=n/a
npu_state=0x041000
total session 1
```

SSH 会话：

```
FGT1 # FGT1 # diagnose sys session filter dport 2222
FGT1 # diagnose sys session list
session info: proto=6 proto_state=11 duration=444 expire=3521 timeout=3600 flags=00
000000 socktype=0 sockport=0 av_idx=0 use=4
61.189.41.157 laper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty ndr synced
statistic(bytes/packets/allow_err): org=5110/40/1 reply=6005/29/1 tuples=3
tx speed(Bps/kbps): 11/0 rx speed(Bps/kbps): 13/0
origin->sink: org pre->post_reply pre->post dev=3->4/4->3 mvs=10.0.1.1/10.0.0.1
hook-pre dir=org act=dnat 61.149.143.226:21397->10.0.0.100:2222(10.0.5.20:22)
hook-post dir=reply act=snat 10.0.5.20:22->61.149.143.226:21397(10.0.0.100:2222)
hook-post dir=org act=noop 61.149.143.226:21397->10.0.5.20:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=00002e0e tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdbs_link_id=00000000 rpdbs_svc_id=0 ngfwid=n/a
npu_state=0x041008
total session 1
FGT1 #

FGT2 # FGT2 # diagnose sys session filter dport 2222
FGT2 # diagnose sys session list
session info: proto=6 proto_state=11 duration=449 expire=3150 timeout=3600 flags=00
0000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty ndr syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0 fgt2 dnat的地址是10.0.10.100
origin->sink: org pre->post_reply pre->post dev=3->4/4->3 mvs=0.0.0.0/0.0.0.0
hook-pre dir=org act=dnat 61.149.143.226:21397->10.0.0.100:2222(10.0.5.20:22)
hook-post dir=reply act=snat 10.0.5.20:22->61.149.143.226:21397(10.0.0.100:2222)
hook-post dir=org act=noop 61.149.143.226:21397->10.0.5.20:22(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=00002e0e tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdbs_link_id=00000000 rpdbs_svc_id=0 ngfwid=n/a
npu_state=0x041000
total session 1
```

Ping 会话：

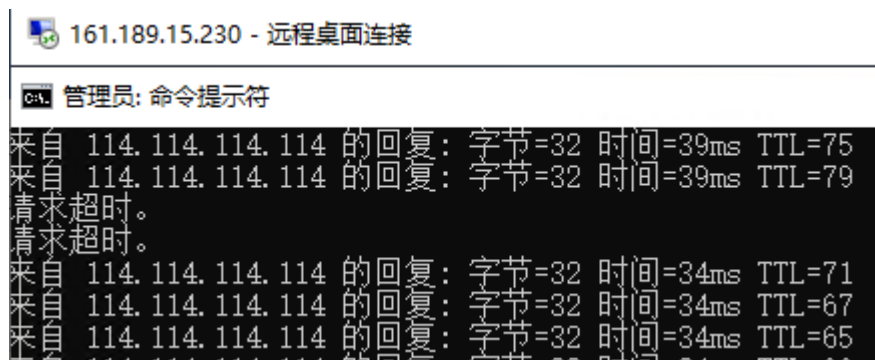
```
FGT1 # diagnose sys session filter proto 1
FGT1 # diagnose sys session list
session info: proto=1 proto_state=00 duration=607 expire=59 timeout=0 flags=00000000
0 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty ndr synced
statistic(bytes/packets/allow_err): org=35880/598/1 reply=35880/598/1 tuples=3
tx speed(Bps/kbps): 59/0 rx speed(Bps/kbps): 59/0
origin->sink: org pre->post_reply pre->post dev=3->4/4->3 mvs=10.0.0.1/10.0.1.1
hook-pre dir=org act=snat 10.0.4.20:1->114.114.114.114:8(10.0.0.11:60417)
hook-post dir=reply act=dnat 114.114.114.114:60417->10.0.0.11:0(10.0.4.20:1)
hook-post dir=org act=noop 114.114.114.114:1->10.0.4.20:0(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00002def tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdbs_link_id=00000000 rpdbs_svc_id=0 ngfwid=n/a
npu_state=0x041008
total session 1

FGT2 # diagnose sys session filter proto 1
FGT2 # diagnose sys session list
session info: proto=1 proto_state=00 duration=590 expire=19 timeout=0 flags=000000000
0 socktype=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty ndr syn_ses
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0 fgt2 snat的地址是10.0.10.11
origin->sink: org pre->post_reply pre->post dev=3->4/4->3 mvs=0.0.0.0/0.0.0.0
hook-pre dir=org act=snat 10.0.4.20:1->114.114.114.114:8(10.0.0.11:60417)
hook-post dir=reply act=dnat 114.114.114.114:60417->10.0.0.11:0(10.0.4.20:1)
hook-post dir=org act=noop 114.114.114.114:1->10.0.4.20:0(0.0.0.0:0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00002def tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdbs_link_id=00000000 rpdbs_svc_id=0 ngfwid=n/a
npu_state=0x041000
total session 1
```

重启 FGT2，HA 切换后，FGT2 是主，FGT1 是备：

原有 RDP 和 SSH 连接断开，重新连接后正常。

Ping 丢 2 个包。



从 FGT2 debug 可以看出，除了 FGT 本身的 HA 切换以外，还需要移动弹性 ip 到 FGT2 实例，更新 AWS private 路由表的默认路由指向 FGT2 NIC2。

```
FGT2 # diagnose debug application awsd -1
Debug messages will be on for 30 minutes.

FGT2 # diagnose debug enable

FGT2 # HA event
HA state: primary
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port2 ip 10.0.11.11
send_vip_arp: vd root primary 1 intf fortalink ip 169.254.1.1
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.100
awsd get instance id i-0fa40e879f5291993
awsd get iam role FGT-HA-Failover
awsd get region cn-northwest-1
awsd get vpc id vpc-003580624fa76d6ae
awsd doing ha failover for vdom root
awsd associate elastic ip for port1
awsd associate elastic ip allocation eipalloc-03e6afde5a7114cba to 10.0.10.11 of eni eni-01338913334708282
awsd associate elastic ip successfully
awsd associate elastic ip allocation eipalloc-0a0b5404ac469ee15 to 10.0.10.100 of eni eni-01338913334708282
awsd associate elastic ip successfully
awsd associate elastic ip for port2
awsd update route table rtb-0a1623244f20b063c, replace route of dst 0.0.0.0/0 to eni-083fe1ed3da12d9b9
awsd update route successfully
HA event
HA state: primary
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port2 ip 10.0.11.11
send_vip_arp: vd root primary 1 intf fortalink ip 169.254.1.1
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.100
awsd get instance id i-0fa40e879f5291993
awsd get iam role FGT-HA-Failover
awsd get region cn-northwest-1
awsd get vpc id vpc-003580624fa76d6ae
awsd doing ha failover for vdom root
awsd associate elastic ip for port1
awsd associate elastic ip for port2
```

弹性 IP 重新在 FGT2 实例绑定。

	Name	Allocated IPv4 add...	Type	Allocation ID	Associated instance ID	Private IP address	Network interface ID
☐	wangxiang-vpc2-fig-cluster	161.189.15.230	Public IP	eipalloc-03e6afde5a7114cba	i-0fa40e879f5291993	10.0.10.11	eni-01338913334708282
☐	wangxiang-vpc2-fig-cluster2	69.234.249.221	Public IP	eipalloc-0a0b5404ac469ee15	i-0fa40e879f5291993	10.0.10.100	eni-01338913334708282

Private 路由表默认路由指向 FGT2 NIC2。

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
☒	wangxiang-vpc2-private-rtb	rtb-0a1623244f20b063c	4 subnets	-	No	vpc-003580624fa76d6ae wangxiang-vpc2
☐	wangxiang-vpc2-public-rtb	rtb-045cee56a1ee72a5b	6 subnets	-	No	vpc-003580624fa76d6ae wangxiang-vpc2

rtb-0a1623244f20b063c / wangxiang-vpc2-private-rtb				
Details Routes Subnet associations Edge associations Route propagation Tags				
Routes (2)				
Filter routes				
Destination	Target	Status	Propagated	
10.0.0.0/16	local	Active	No	
0.0.0.0/0	eni-083fe1ed3da12d9b9 fgt2 nic2	Active	No	