Security Day 构建增强云端环境指导手册（二）

2021 年 3 月 12 日

目录

实验介绍及准备......3

实验架构......4

环境部署......5

确认部署结果......7

网络配置......8

VPC 路由配置......8

配置 Central VPC 中转网关路由......9

配置 Central VPC 公共子网路由......9

配置 Inspect VPC 中转网关子网路由......9

配置 Inspect VPC 防火墙子网路由......10

配置 Business VPC 中转网关子网路由......10

配置 Business VPC 私有子网路由......10

TGW 路由配置......11

配置 Spoke 路由......11

配置 NFW 路由......11

测试验证......12

南北向防护......13

实验有状态规则......14

东西向防护......18

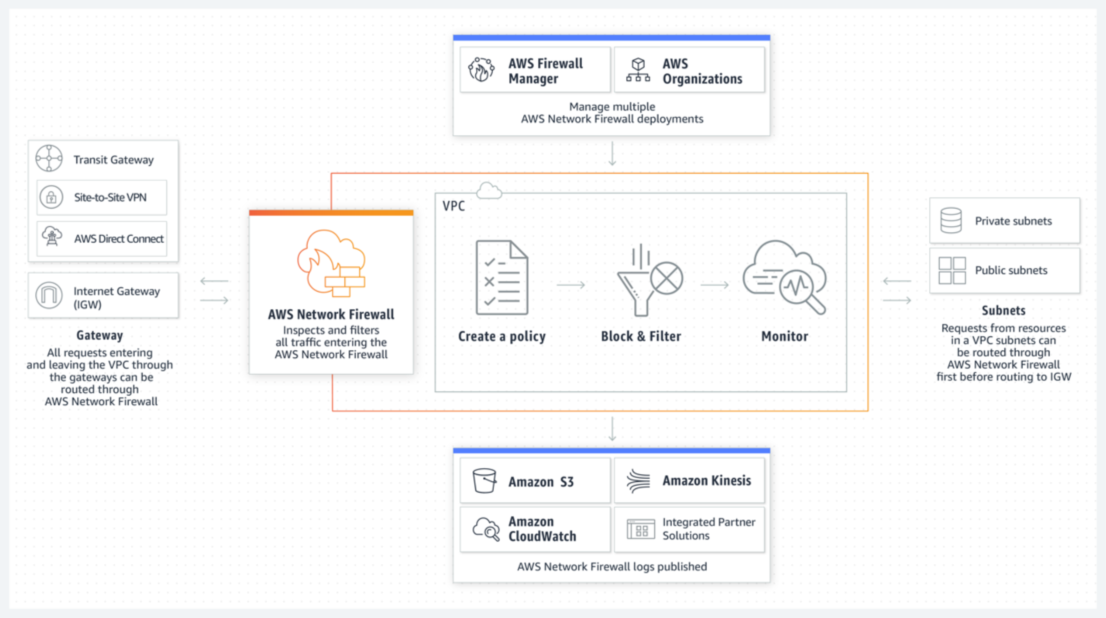
实验无状态规则......19

参考资料......20

实验介绍及准备

AWS 在 2020 年底的 Re:Invent 大会上发布了新的安全产品的管理服务 Network Firewall（网络防火墙），客户可以通过使用它来对外网进行隔离（也叫南北向），也可以用于内网之间进行隔离（也叫东西向，如同一个区域的不同 VPC 之间，不同区域的不同 VPC 之间，云和 IDC 之间等），实现基于规则的检测和防护。它支持有状态的规则，也支持无状态的规则，可以灵活的配置。

AWS Network Firewall（网络防火墙）提供常见的网络威胁保护的能力，它可以合并流量的上下文，如跟踪连接和协议识别，匹配对应策略进行处理，防止未经授权的访问。


AWS Firewall Manager
AWS Organizations
Manage multiple AWS Network Firewall deployments
Transit Gateway
Site-to-Site VPN
AWS Direct Connect
Internet Gateway (IGW)
Gateway
All requests entering and leaving the VPC through the gateways can be routed through AWS Network Firewall
AWS Network Firewall
Inspects and filters all traffic entering the AWS Network Firewall
VPC
Create a policy
Block & Filter
Monitor
Private subnets
Public subnets
Subnets
Requests from resources in a VPC subnets can be routed through AWS Network Firewall first before routing to IGW
Amazon S3
Amazon Kinesis
Amazon CloudWatch
Integrated Partner Solutions
AWS Network Firewall logs published

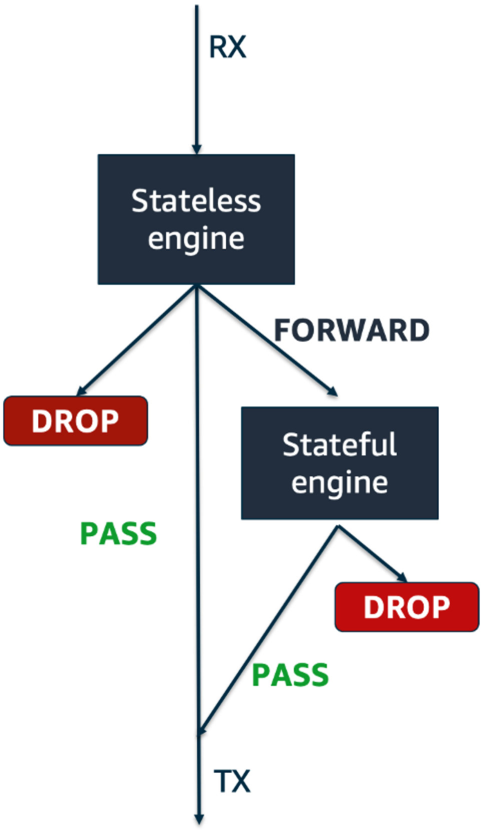
图例：Network Firewall 工作原理

AWS Network Firewall 支持有状态的规则（最大规则组容量 30,000），也支持无状态的规则（最大规则组容量 10,000）。

无状态规则优先于有状态规则执行，且按配置的顺序执行，支持 pass，drop 和 forward 到有状态的规则三种处理方式。

假如无状态规则配置有冲突，按优先级匹配执行；有状态的规则如果有冲突（例如某个规则设置了允许 ssh，另外一个规则设置了禁止 ssh），它是合并后再统一匹配执行，优先级为 pass > drop > alert，所以只要有一个 pass 的设置，其他的非 pass 设置全部会失效，所以我们在设置规则时要明确具体。

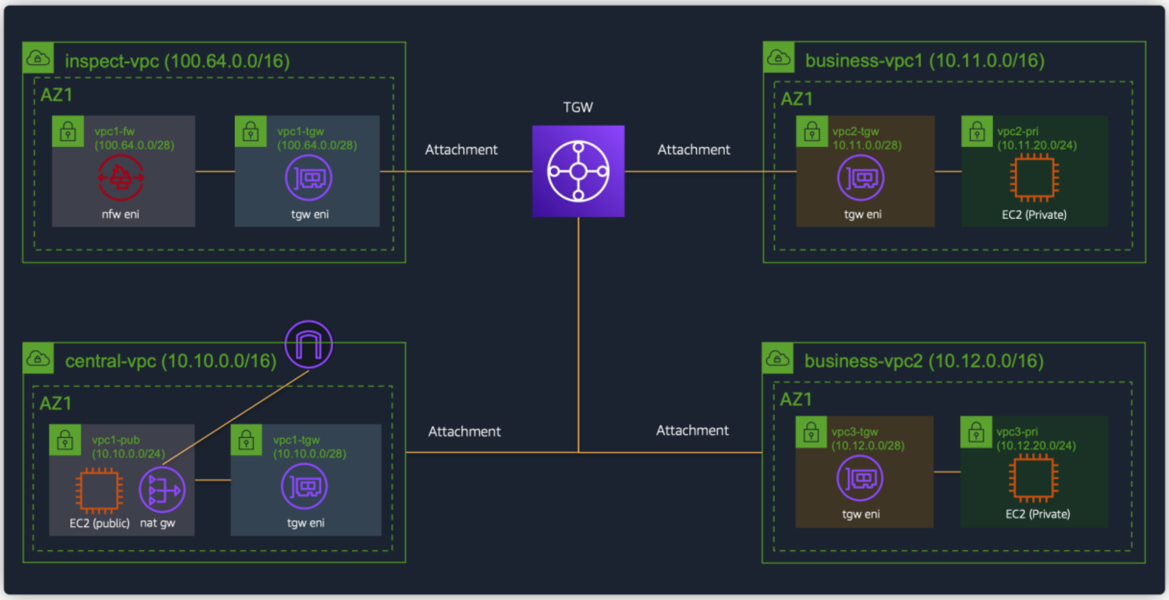
其执行流程如下图所示：



图例：Network Firewall 规则处理顺序

实验架构

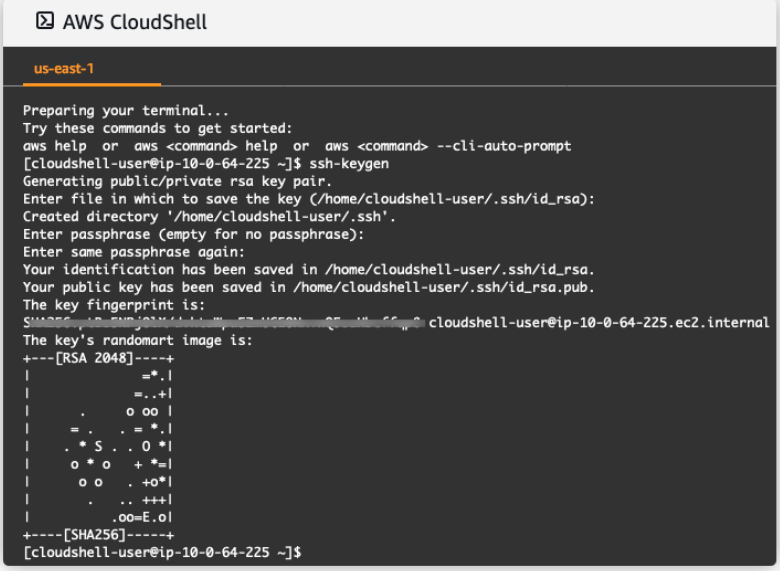
这是我们设计的中心部署网络架构图，云上环境 VPC 之间通过中转网关（Transit Gateway TGW）连通，云上环境的内网（东西向）和外网（南北向）有网络防火墙隔离。所有外网流量经 Central VPC 统一控制。



环境部署

首先通过 CloudShell 创建用于 SSH 登陆的密钥（点击这里）

输入 ssh-keygen 命令后， 按三次回车键



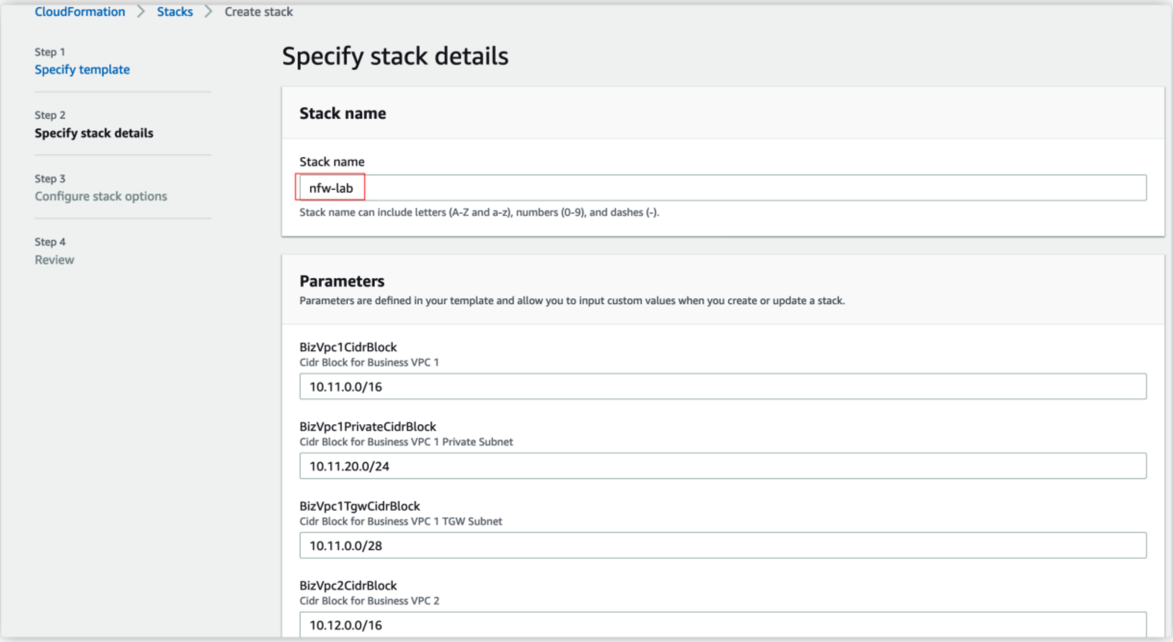
```
Preparing your terminal...
Try these commands to get started:
aws help  or  aws <command> help  or  aws <command> --cli-auto-prompt
[cloudshell-user@ip-10-0-64-225 ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cloudshell-user/.ssh/id_rsa):
Created directory '/home/cloudshell-user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/cloudshell-user/.ssh/id_rsa.
Your public key has been saved in /home/cloudshell-user/.ssh/id_rsa.pub.
The key fingerprint is:
[redacted] cloudshell-user@ip-10-0-64-225.ec2.internal
The key's randomart image is:
+---[RSA 2048]----+
|              =*.|
|             =..+|
|      .     o oo |
|     = .   . = *.|
|    . * S . . O *|
|     o * o   + *=|
|      o o   . +o*|
|       .    .. +++|
|           .oo=E.o|
+----[SHA256]-----+
[cloudshell-user@ip-10-0-64-225 ~]$
```

将生成的密钥导入实验区域并修改执行权限

```
aws ec2 import-key-pair --key-name "nfwlab" --public-key-material fileb://~/.ssh/id_rsa.pub
chmod 400 ~/.ssh/id_rsa
```

通过 CloudFormation 模版，创建实验环境。实验区域为弗吉尼亚(us-east-1)。

stack”开始创建堆栈。模版执行完成大概需要 5 分钟。



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name
nfw-lab
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

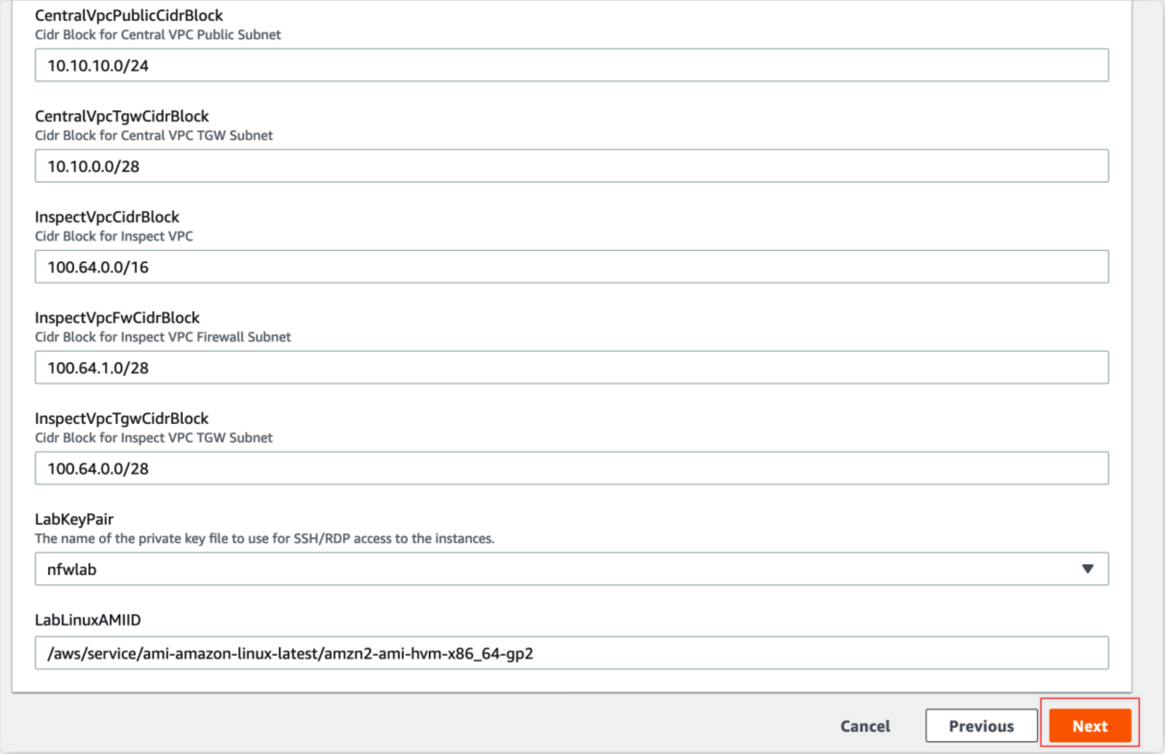
BizVpc1CidrBlock
Cidr Block for Business VPC 1
10.11.0.0/16

BizVpc1PrivateCidrBlock
Cidr Block for Business VPC 1 Private Subnet
10.11.20.0/24

BizVpc1TgwCidrBlock
Cidr Block for Business VPC 1 TGW Subnet
10.11.0.0/28

BizVpc2CidrBlock
Cidr Block for Business VPC 2
10.12.0.0/16

可以根据需要，调整参数，如果修改默认网段参数，请确保同一个 VPC 的不同子网包含在 VPC 的网段定义里。确定参数后，拉到页面底部，点击“Next”进入下一步。



CentralVpcPublicCidrBlock
Cidr Block for Central VPC Public Subnet
10.10.10.0/24

CentralVpcTgwCidrBlock
Cidr Block for Central VPC TGW Subnet
10.10.0.0/28

InspectVpcCidrBlock
Cidr Block for Inspect VPC
100.64.0.0/16

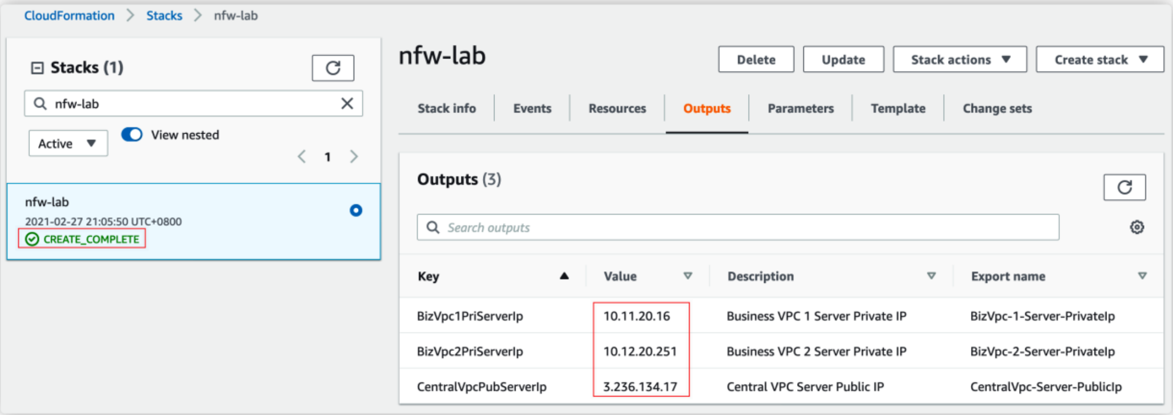
InspectVpcFwCidrBlock
Cidr Block for Inspect VPC Firewall Subnet
100.64.1.0/28

InspectVpcTgwCidrBlock
Cidr Block for Inspect VPC TGW Subnet
100.64.0.0/28

LabKeyPair
The name of the private key file to use for SSH/RDP access to the instances.
nfwlab ▼

LabLinuxAMIID
/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2

实验文档步骤中未截图，或未特别说明的地方，取默认值。连续点击“Next”,“Create stack”开始创建堆栈。模版执行完成大概需要 5 分钟。



nfw-lab

2021-02-27 21:05:50 UTC+0800

✓ CREATE_COMPLETE

Outputs (3)

Key	Value	Description	Export name
BizVpc1PriServerIp	10.11.20.16	Business VPC 1 Server Private IP	BizVpc-1-Server-PrivateIp
BizVpc2PriServerIp	10.12.20.251	Business VPC 2 Server Private IP	BizVpc-2-Server-PrivateIp
CentralVpcPubServerIp	3.236.134.17	Central VPC Server Public IP	CentralVpc-Server-PublicIp

部署完成后（请确保没有任何错误输出），点击 Outputs，可以看到三台测试服务器的 IP 地址，之后的实验会用到。

确认部署结果

主要部署的资源和环境包括：

A.四个 VPC，八个子网，每个子网都有自己单独的路由表（点击这里）

一个专门用于检测流量的 VPC（Inspect VPC），配置两个子网：

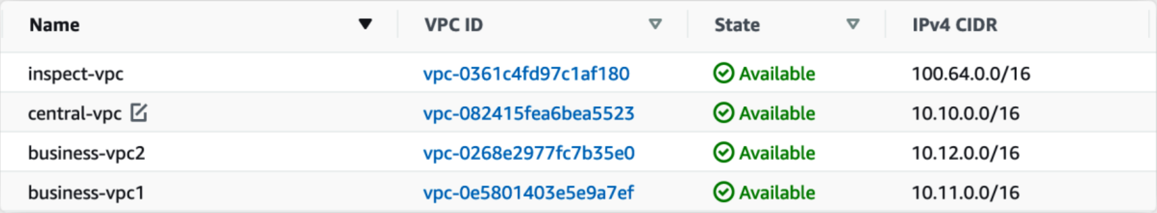
- 一个防火墙所在子网
- 一个中转网关所在子网

一个用作中心路由控制的 VPC （Central VPC），配置两个子网：

- 一个公共子网（部署 NAT 网关，以及需要面向公网的服务，如 EC2）
- 一个中转网关所在子网

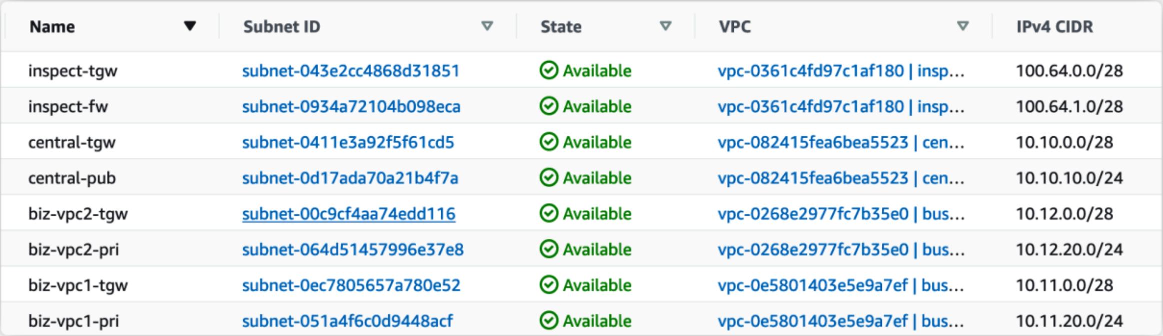
两个业务 VPC（Business VPC 1 和 Business VPC 2），每个 VPC 配置两个子网：

- 一个私有子网（纯内网环境）
- 一个中转网关所在子网



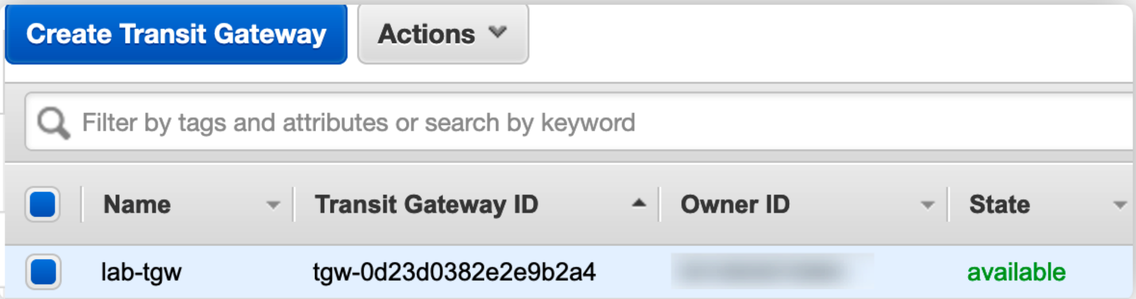
Name	VPC ID	State	IPv4 CIDR
inspect-vpc	vpc-0361c4fd97c1af180	✓ Available	100.64.0.0/16
central-vpc	vpc-082415fea6bea5523	✓ Available	10.10.0.0/16
business-vpc2	vpc-0268e2977fc7b35e0	✓ Available	10.12.0.0/16
business-vpc1	vpc-0e5801403e5e9a7ef	✓ Available	10.11.0.0/16

查看子网列表（点击这里）



Name	Subnet ID	State	VPC	IPv4 CIDR
inspect-tgw	subnet-043e2cc4868d31851	✓ Available	vpc-0361c4fd97c1af180 | insp…	100.64.0.0/28
inspect-fw	subnet-0934a72104b098eca	✓ Available	vpc-0361c4fd97c1af180 | insp…	100.64.1.0/28
central-tgw	subnet-0411e3a92f5f61cd5	✓ Available	vpc-082415fea6bea5523 | cen…	10.10.0.0/28
central-pub	subnet-0d17ada70a21b4f7a	✓ Available	vpc-082415fea6bea5523 | cen…	10.10.10.0/24
biz-vpc2-tgw	subnet-00c9cf4aa74edd116	✓ Available	vpc-0268e2977fc7b35e0 | bus…	10.12.0.0/28
biz-vpc2-pri	subnet-064d51457996e37e8	✓ Available	vpc-0268e2977fc7b35e0 | bus…	10.12.20.0/24
biz-vpc1-tgw	subnet-0ec7805657a780e52	✓ Available	vpc-0e5801403e5e9a7ef | bus…	10.11.0.0/28
biz-vpc1-pri	subnet-051a4f6c0d9448acf	✓ Available	vpc-0e5801403e5e9a7ef | bus…	10.11.20.0/24

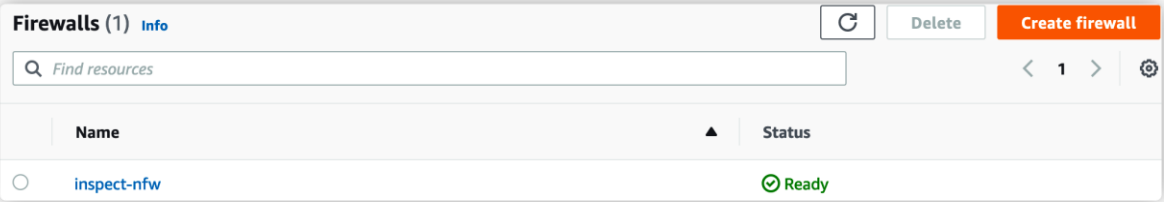
B.一个中转网关（点击这里）



■	Name	Transit Gateway ID	Owner ID	State
■	lab-tgw	tgw-0d23d0382e2e9b2a4	[redacted]	available

C.一个 Network Firewall（点击这里）

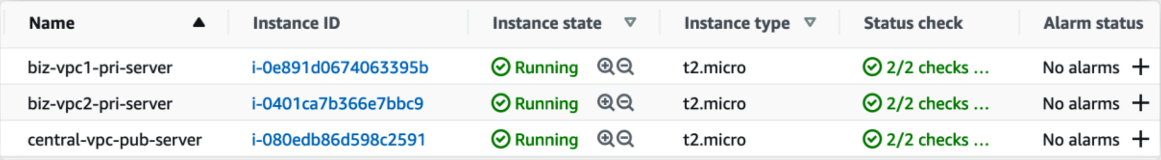
一个网络防火墙已关联配置了无状态和有状态规则组。



	Name	Status
○	inspect-nfw	✓ Ready

D.三台测试 EC2 服务器（点击这里）

一台面向公网的服务器，两台私有服务器。



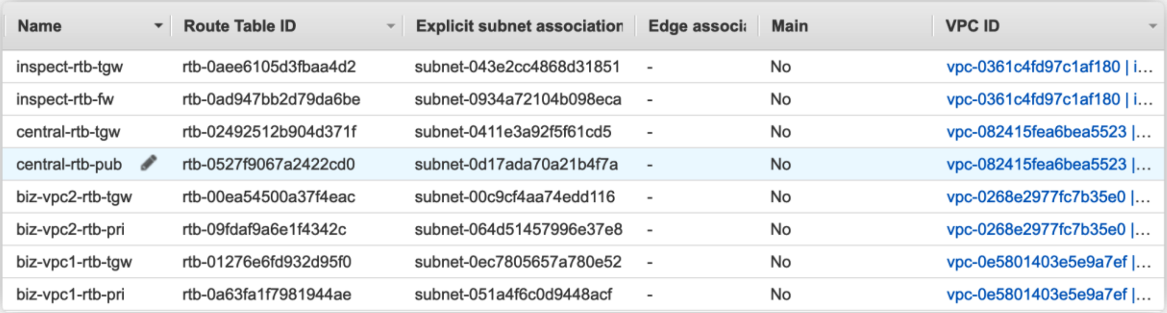
Name	Instance ID	Instance state	Instance type	Status check	Alarm status
biz-vpc1-pri-server	i-0e891d0674063395b	✓ Running	t2.micro	✓ 2/2 checks …	No alarms +
biz-vpc2-pri-server	i-0401ca7b366e7bbc9	✓ Running	t2.micro	✓ 2/2 checks …	No alarms +
central-vpc-pub-server	i-080edb86d598c2591	✓ Running	t2.micro	✓ 2/2 checks …	No alarms +

网络配置

通过模版生成基础架构需要的各个组件，但路由链路尚未配置，接下来将对每个子网的路由表（已关联未配置条目）添加相应的路由条目，并借助 TGW 连通各个 VPC。

VPC 路由配置

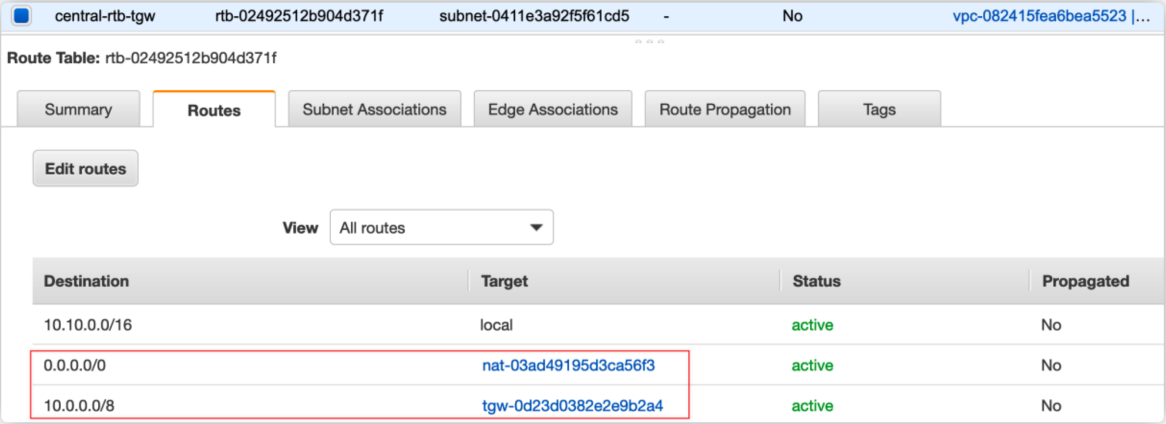
打开 VPC 路由表控制台（点击此处），找到相应路由表，依次进行配置。



Name	Route Table ID	Explicit subnet association	Edge associ:	Main	VPC ID
inspect-rtb-tgw	rtb-0aee6105d3fbaa4d2	subnet-043e2cc4868d31851	-	No	vpc-0361c4fd97c1af180 | i...
inspect-rtb-fw	rtb-0ad947bb2d79da6be	subnet-0934a72104b098eca	-	No	vpc-0361c4fd97c1af180 | i...
central-rtb-tgw	rtb-02492512b904d371f	subnet-0411e3a92f5f61cd5	-	No	vpc-082415fea6bea5523 |...
central-rtb-pub	rtb-0527f9067a2422cd0	subnet-0d17ada70a21b4f7a	-	No	vpc-082415fea6bea5523 |...
biz-vpc2-rtb-tgw	rtb-00ea54500a37f4eac	subnet-00c9cf4aa74edd116	-	No	vpc-0268e2977fc7b35e0 |...
biz-vpc2-rtb-pri	rtb-09fdaf9a6e1f4342c	subnet-064d51457996e37e8	-	No	vpc-0268e2977fc7b35e0 |...
biz-vpc1-rtb-tgw	rtb-01276e6fd932d95f0	subnet-0ec7805657a780e52	-	No	vpc-0e5801403e5e9a7ef |...
biz-vpc1-rtb-pri	rtb-0a63fa1f7981944ae	subnet-051a4f6c0d9448acf	-	No	vpc-0e5801403e5e9a7ef |...

配置 Central VPC 中转网关路由

选中 central-rtb-tgw 路由表，配置如下路由



central-rtb-tgw rtb-02492512b904d371f subnet-0411e3a92f5f61cd5 - No vpc-082415fea6bea5523 |...

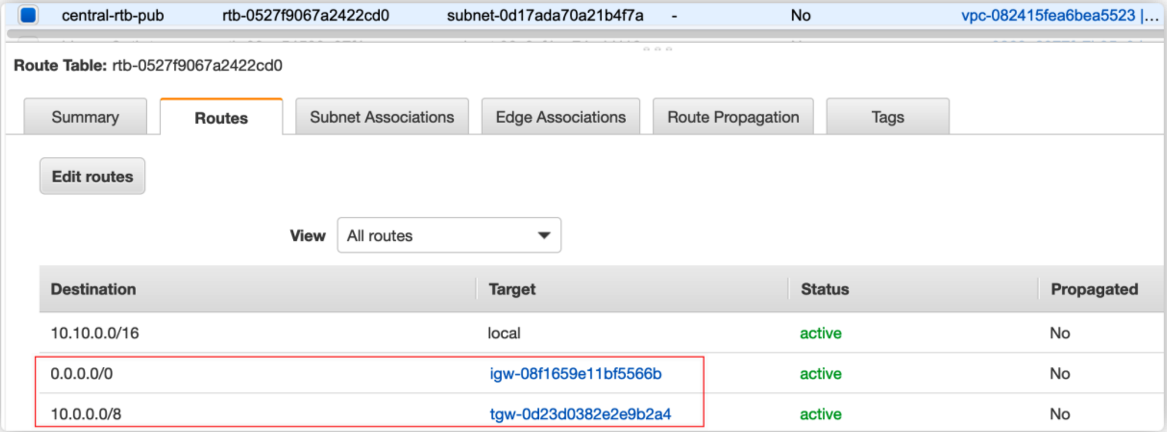
Route Table: rtb-02492512b904d371f

View All routes

Destination	Target	Status	Propagated
10.10.0.0/16	local	active	No
0.0.0.0/0	nat-03ad49195d3ca56f3	active	No
10.0.0.0/8	tgw-0d23d0382e2e9b2a4	active	No

配置 Central VPC 公共子网路由

选中 central-rtb-pub 路由表，配置如下路由



central-rtb-pub rtb-0527f9067a2422cd0 subnet-0d17ada70a21b4f7a - No vpc-082415fea6bea5523 |...

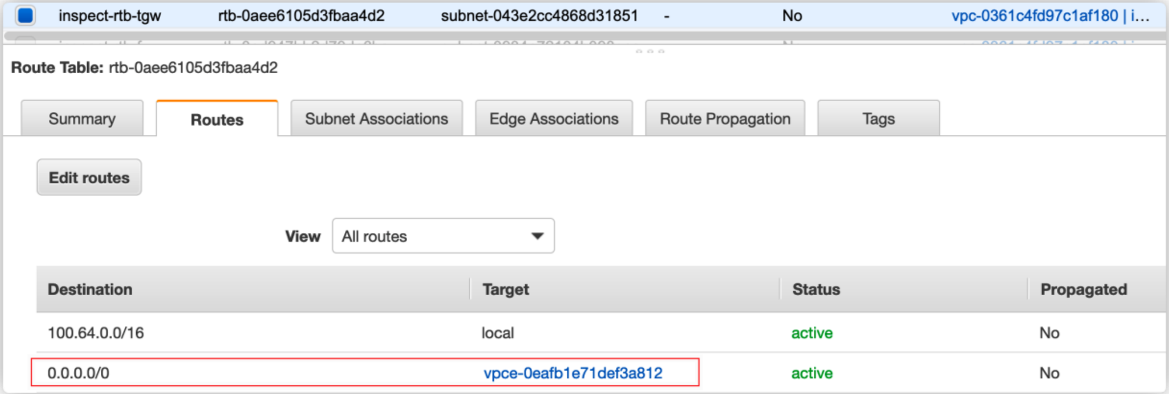
Route Table: rtb-0527f9067a2422cd0

View All routes

Destination	Target	Status	Propagated
10.10.0.0/16	local	active	No
0.0.0.0/0	igw-08f1659e11bf5566b	active	No
10.0.0.0/8	tgw-0d23d0382e2e9b2a4	active	No

配置 Inspect VPC 中转网关子网路由

选中 inspect-rtb-tgw 路由表，配置如下路由



inspect-rtb-tgw	rtb-0aee6105d3fbaa4d2	subnet-043e2cc4868d31851	-	No	vpc-0361c4fd97c1af180 | i...

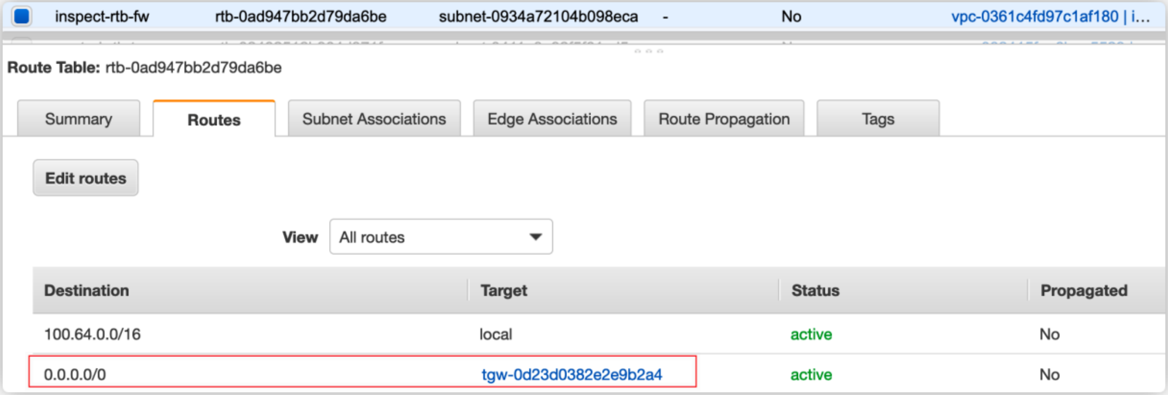
Route Table: rtb-0aee6105d3fbaa4d2

View All routes

Destination	Target	Status	Propagated
100.64.0.0/16	local	active	No
0.0.0.0/0	vpce-0eafb1e71def3a812	active	No

配置 Inspect VPC 防火墙子网路由

选中 inspect-rtb-fw 路由表，配置如下路由



inspect-rtb-fw	rtb-0ad947bb2d79da6be	subnet-0934a72104b098eca	-	No	vpc-0361c4fd97c1af180 | i...

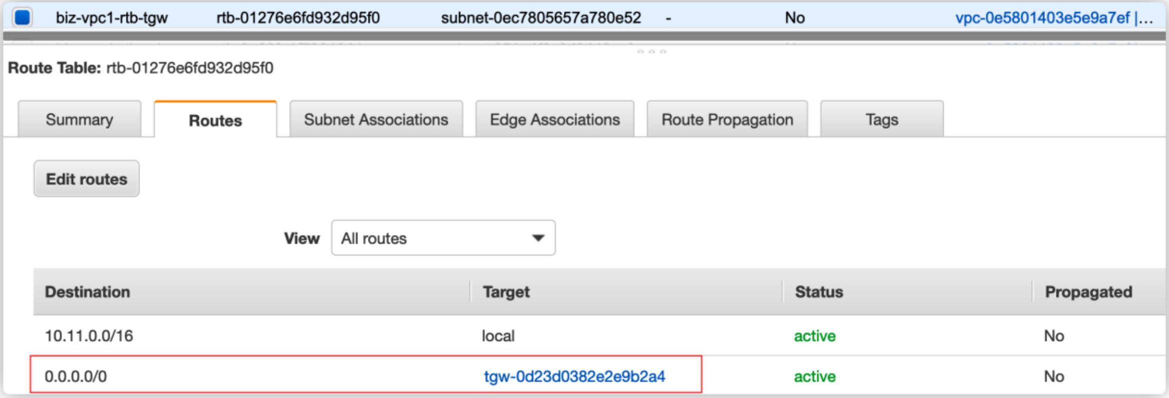
Route Table: rtb-0ad947bb2d79da6be

View All routes

Destination	Target	Status	Propagated
100.64.0.0/16	local	active	No
0.0.0.0/0	tgw-0d23d0382e2e9b2a4	active	No

配置 Business VPC 中转网关子网路由

以 Business VPC 1 为例，选中 biz-vpc1-rtb-tgw 路由表，配置如下路由



biz-vpc1-rtb-tgw	rtb-01276e6fd932d95f0	subnet-0ec7805657a780e52	-	No	vpc-0e5801403e5e9a7ef |...

Route Table: rtb-01276e6fd932d95f0

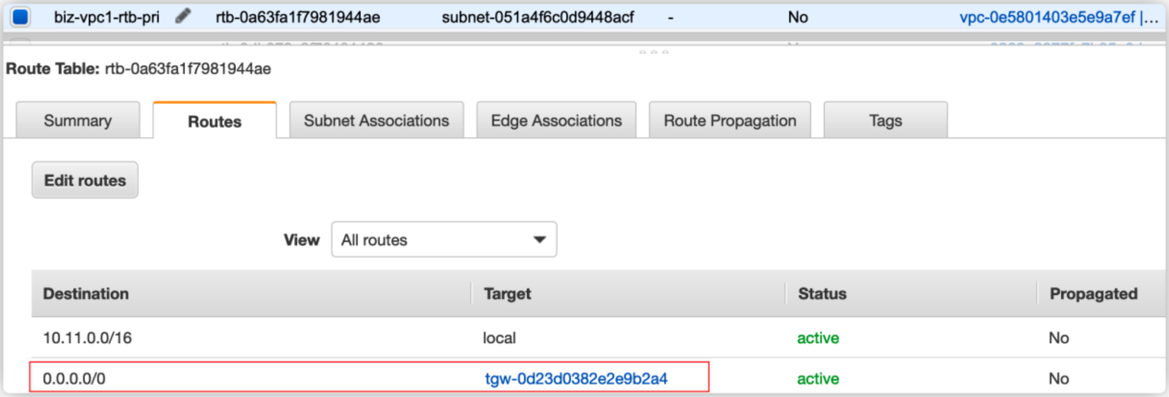
View All routes

Destination	Target	Status	Propagated
10.11.0.0/16	local	active	No
0.0.0.0/0	tgw-0d23d0382e2e9b2a4	active	No

类似的配置 Business VPC 2 中转网关子网路由。

配置 Business VPC 私有子网路由

以 Business VPC 1 为例，选中 biz-vpc1-rtb-pri 路由表，配置如下路由



biz-vpc1-rtb-pri	rtb-0a63fa1f7981944ae	subnet-051a4f6c0d9448acf	-	No	vpc-0e5801403e5e9a7ef |...

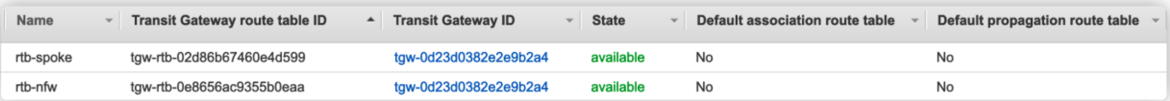
Route Table: rtb-0a63fa1f7981944ae

Destination	Target	Status	Propagated
10.11.0.0/16	local	active	No
0.0.0.0/0	tgw-0d23d0382e2e9b2a4	active	No

类似的配置 Business VPC 2 私有子网路由。

TGW 路由配置

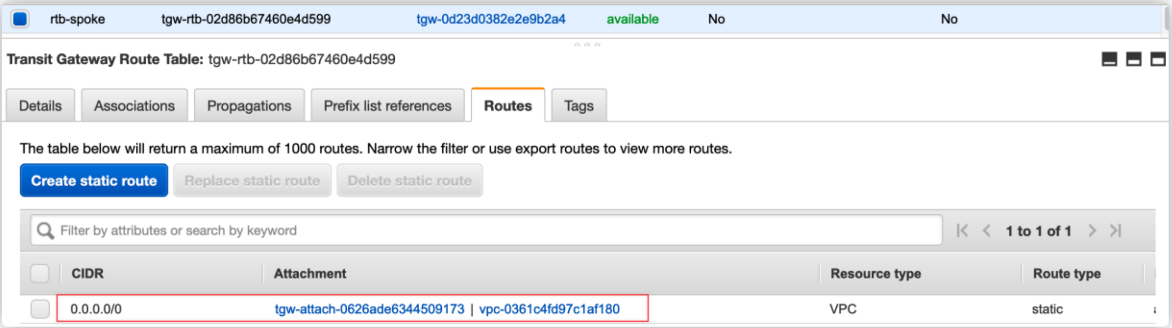
前面已经完成 4 个 VPC，8 个子网的路由配置，下面通过配置 TGW 路由表来实现跨 VPC 连通并进行流量控制。打开 TGW 路由表控制台（点击此处），找到相应路由表，依次进行配置。



Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
rtb-spoke	tgw-rtb-02d86b67460e4d599	tgw-0d23d0382e2e9b2a4	available	No	No
rtb-nfw	tgw-rtb-0e8656ac9355b0eaa	tgw-0d23d0382e2e9b2a4	available	No	No

配置 Spoke 路由

选中 rtb-spoke 路由表，添加 0.0.0.0/0 指向 inspect-vpc



rtb-spoke	tgw-rtb-02d86b67460e4d599	tgw-0d23d0382e2e9b2a4	available	No	No

Transit Gateway Route Table: tgw-rtb-02d86b67460e4d599

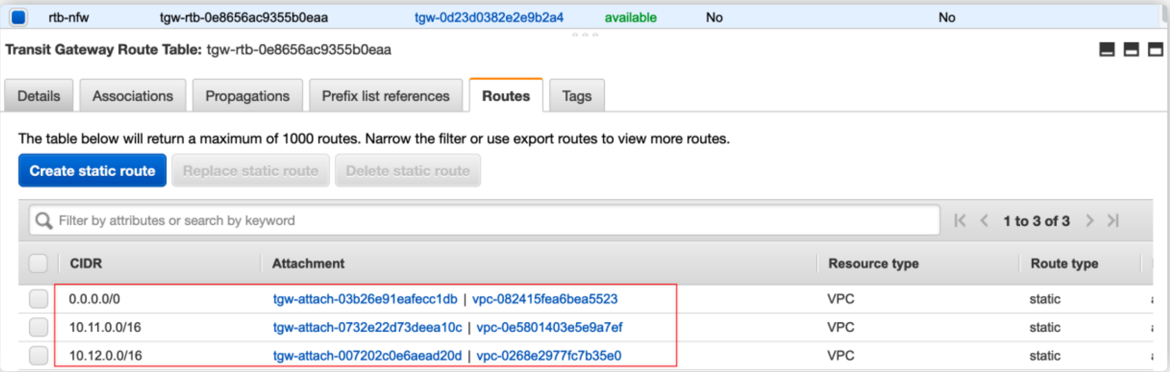
The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

CIDR	Attachment	Resource type	Route type
0.0.0.0/0	tgw-attach-0626ade6344509173 | vpc-0361c4fd97c1af180	VPC	static

配置 NFW 路由

选中 rtb-spoke 路由表，添加如下规则：

- 0.0.0.0/0 指向 central-vpc
- 10.11.0.0/16 指向 biz-vpc1
- 10.12.0.0/16 指向 biz-vpc2



rtb-nfw tgw-rtb-0e8656ac9355b0eaa tgw-0d23d0382e2e9b2a4 available No No

Transit Gateway Route Table: tgw-rtb-0e8656ac9355b0eaa

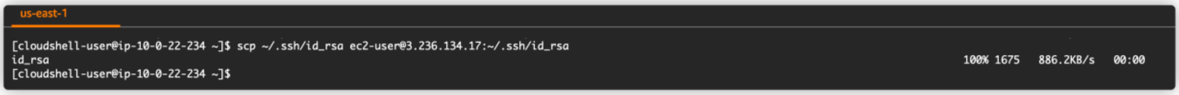
The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

CIDR	Attachment	Resource type	Route type
0.0.0.0/0	tgw-attach-03b26e91eafecc1db | vpc-082415fea6bea5523	VPC	static
10.11.0.0/16	tgw-attach-0732e22d73deea10c | vpc-0e5801403e5e9a7ef	VPC	static
10.12.0.0/16	tgw-attach-007202c0e6aead20d | vpc-0268e2977fc7b35e0	VPC	static

测试验证

回到 CloudShell 界面，将之前生成 SSH 密钥上传到 Public Server。

```
scp ~/.ssh/id_rsa ec2-user@3.236.134.17:~/.ssh/id_rsa
```



```
[cloudshell-user@ip-10-0-22-234 ~]$ scp ~/.ssh/id_rsa ec2-user@3.236.134.17:~/.ssh/id_rsa
id_rsa                                                                100% 1675   886.2KB/s   00:00
[cloudshell-user@ip-10-0-22-234 ~]$
```

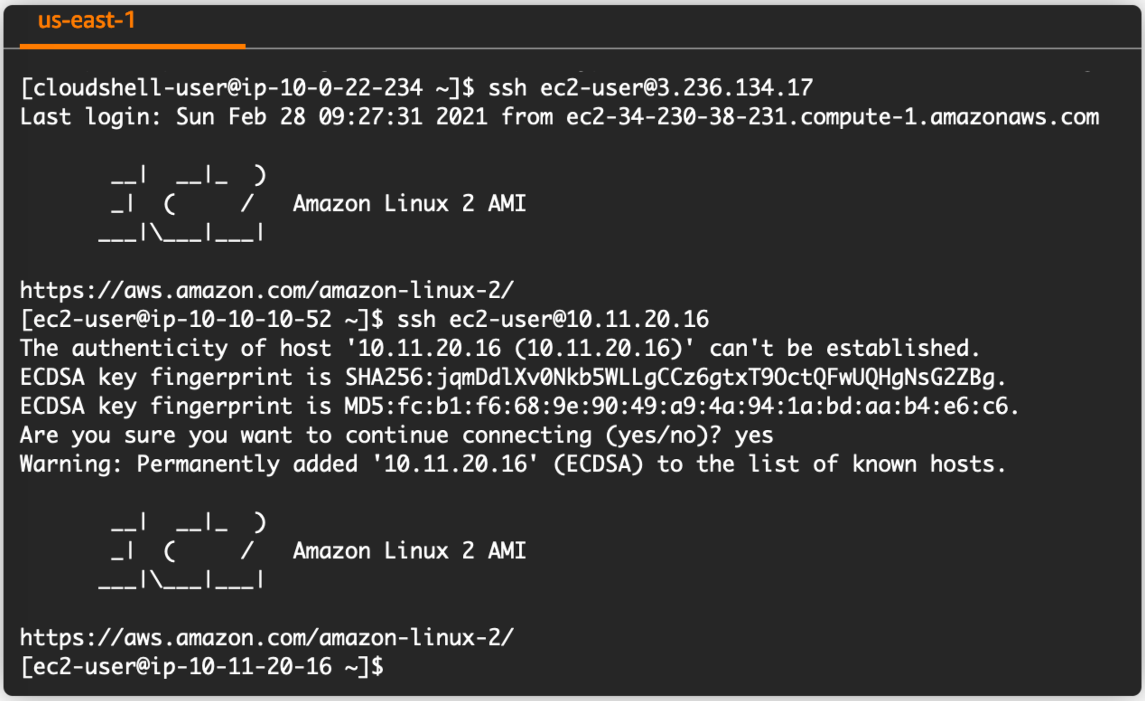
登录到公共测试机后，可以通过它再跳转到位于业务子网的私有服务器。

先登录到 public server:

```
ssh ec2-user@3.236.134.17
```

再跳转到 private server:

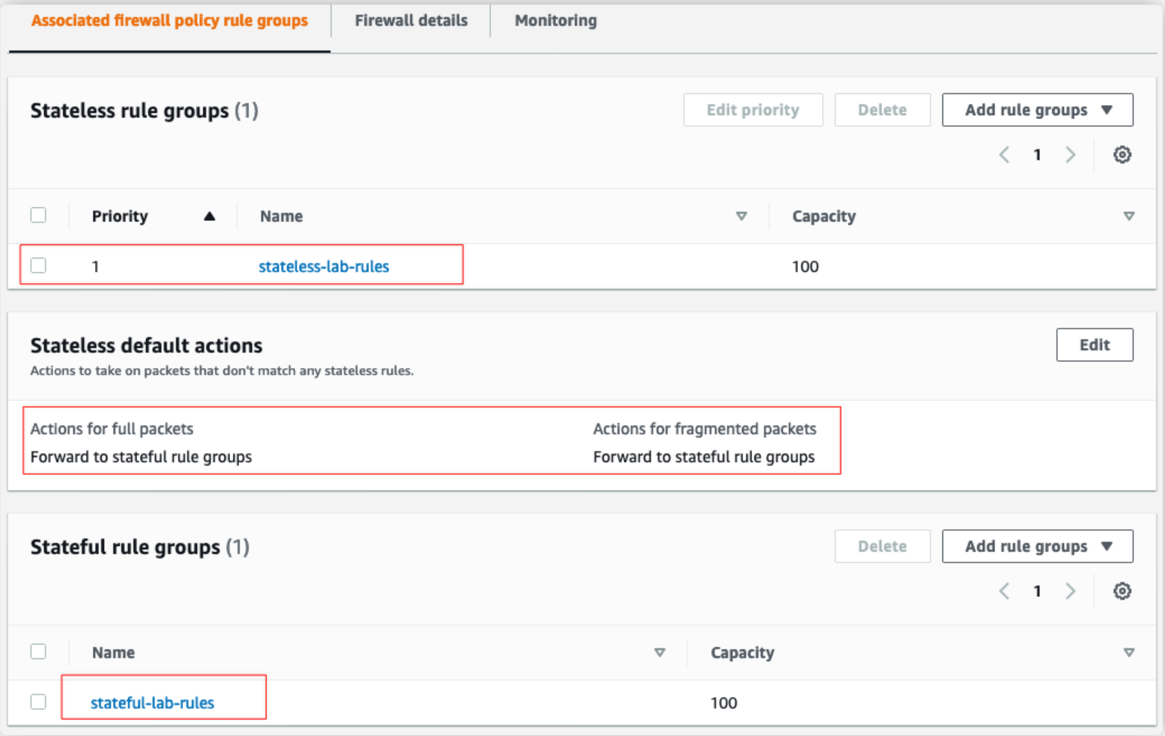
```
ssh ec2-user@10.11.20.16
```



```
[cloudshell-user@ip-10-0-22-234 ~]$ ssh ec2-user@3.236.134.17
Last login: Sun Feb 28 09:27:31 2021 from ec2-34-230-38-231.compute-1.amazonaws.com

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-10-10-52 ~]$ ssh ec2-user@10.11.20.16
The authenticity of host '10.11.20.16 (10.11.20.16)' can't be established.
ECDSA key fingerprint is SHA256:jqmDdlXv0Nkb5WLLgCCz6gtxT9OctQFwUQHgNsG2ZBg.
ECDSA key fingerprint is MD5:fc:b1:f6:68:9e:90:49:a9:4a:94:1a:bd:aa:b4:e6:c6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.11.20.16' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-11-20-16 ~]$
```

南北向防护

找到 **inspect-nfw**（点击这里）防火墙，点击查看防火墙明细。



Stateless rule groups (1)

□	Priority ▲	Name	Capacity
□	1	stateless-lab-rules	100

Stateless default actions

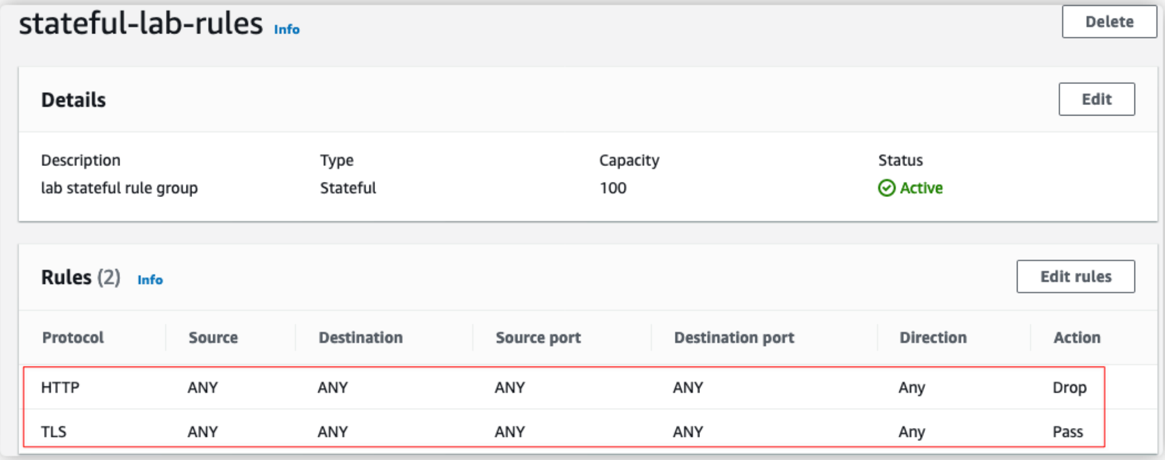
Actions to take on packets that don't match any stateless rules.

Actions for full packets	Actions for fragmented packets
Forward to stateful rule groups	Forward to stateful rule groups

Stateful rule groups (1)

□	Name	Capacity
□	stateful-lab-rules	100

可以看到关联了一个无状态规则组 stateless-lab-rules，如果关联的无状态规则组没有匹配到，默认是转发到有状态规则组。这里实验配置的南北向规则放在有状态规则组 stateful-lab-rules。点击查看规则明细如下：



stateful-lab-rules Info

Details

Description	Type	Capacity	Status
lab stateful rule group	Stateful	100	✓ Active

Rules (2) Info

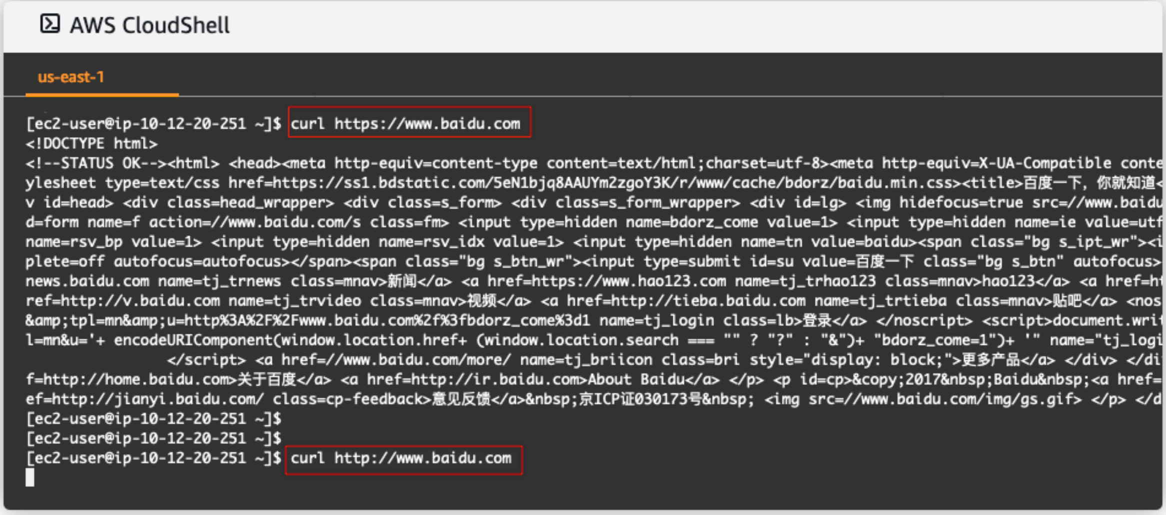
Protocol	Source	Destination	Source port	Destination port	Direction	Action
HTTP	ANY	ANY	ANY	ANY	Any	Drop
TLS	ANY	ANY	ANY	ANY	Any	Pass

我们配置的南北向防火墙策略是允许访问 https，但是不允许 http。

登录到任意一台 Private server，如 BizVpc2PriServer（注意先登录公共测试机）：

```
ssh ec2-user@10.12.20.251
curl https://www.baidu.com
curl http://www.baidu.com
```

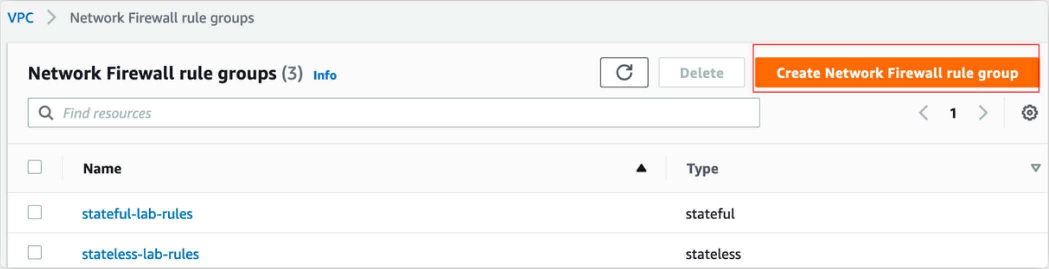
测试如下图所示（curl http 会一直卡在这里）



```
[ec2-user@ip-10-12-20-251 ~]$ curl https://www.baidu.com
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html;charset=utf-8><meta http-equiv=X-UA-Compatible conte
ylesheet type=text/css href=https://ss1.bdstatic.com/5eN1bjq8AAUYm2zgoY3K/r/www/cache/bdorz/baidu.min.css><title>百度一下，你就知道<
v id=head> <div class=head_wrapper> <div class=s_form> <div class=s_form_wrapper> <div id=lg> <img hidefocus=true src=//www.baidu
d=form name=f action=//www.baidu.com/s class=fm> <input type=hidden name=bdorz_come value=1> <input type=hidden name=ie value=utf
name=rsv_bp value=1> <input type=hidden name=rsv_idx value=1> <input type=hidden name=tn value=baidu><span class="bg s_ipt_wr"><i
plete=off autofocus=autofocus></span><span class="bg s_btn_wr"><input type=submit id=su value=百度一下 class="bg s_btn" autofocus>
news.baidu.com name=tj_trnews class=mnav>新闻</a> <a href=https://www.hao123.com name=tj_trhao123 class=mnav>hao123</a> <a href=ht
ref=http://v.baidu.com name=tj_trvideo class=mnav>视频</a> <a href=http://tieba.baidu.com name=tj_trtieba class=mnav>贴吧</a> <nos
&amp;tpl=mn&amp;u=http%3A%2F%2Fwww.baidu.com%2f%3fbdorz_come%3d1 name=tj_login class=lb>登录</a> </noscript> <script>document.writ
l=mn&u='+ encodeURIComponent(window.location.href+ (window.location.search === "" ? "?" : "&")+ "bdorz_come=1")+ '" name="tj_logi
                </script> <a href=//www.baidu.com/more/ name=tj_briicon class=bri style="display: block;">更多产品</a> </div> </di
f=http://home.baidu.com>关于百度</a> <a href=http://ir.baidu.com>About Baidu</a> </p> <p id=cp>&copy;2017&nbsp;Baidu&nbsp;<a href=
ef=http://jianyi.baidu.com/ class=cp-feedback>意见反馈</a>&nbsp;京ICP证030173号&nbsp; <img src=//www.baidu.com/img/gs.gif> </p> </d
[ec2-user@ip-10-12-20-251 ~]$
[ec2-user@ip-10-12-20-251 ~]$
[ec2-user@ip-10-12-20-251 ~]$ curl http://www.baidu.com
█
```

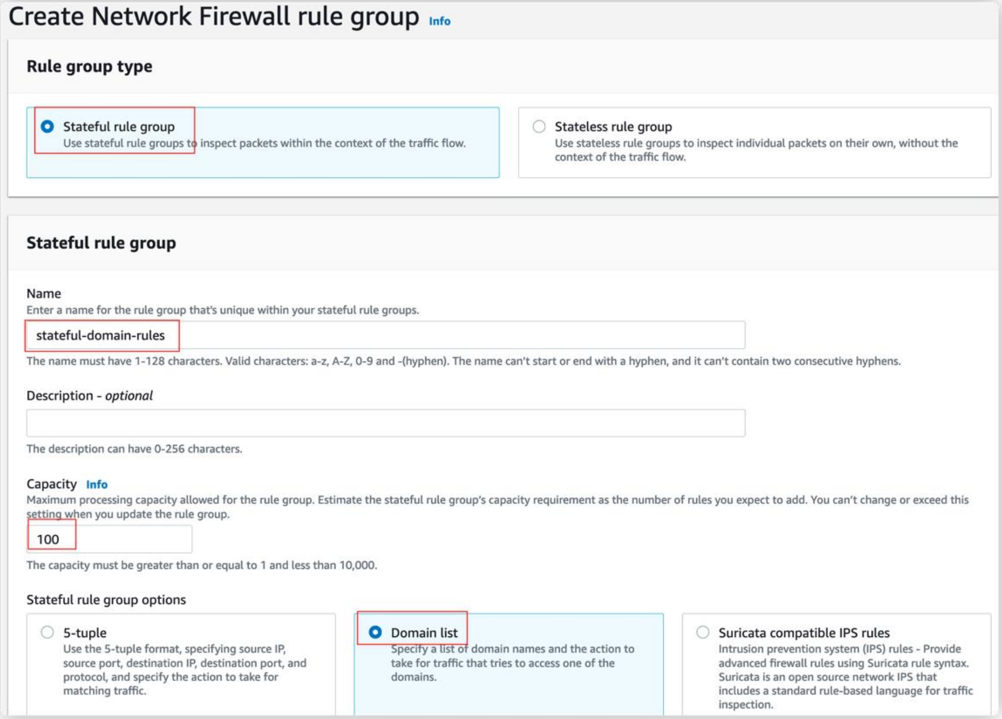
实验有状态规则

首先创建一个新的有状态规则组（点击这里）



VPC > Network Firewall rule groups
Network Firewall rule groups (3) Info
Delete
Create Network Firewall rule group
Find resources
1

□	Name ▲	Type
□	stateful-lab-rules	stateful
□	stateless-lab-rules	stateless



Create Network Firewall rule group Info

Rule group type

● Stateful rule group
Use stateful rule groups to inspect packets within the context of the traffic flow.

○ Stateless rule group
Use stateless rule groups to inspect individual packets on their own, without the context of the traffic flow.

Stateful rule group

Name
Enter a name for the rule group that's unique within your stateful rule groups.
stateful-domain-rules
The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9 and -(hyphen). The name can't start or end with a hyphen, and it can't contain two consecutive hyphens.

Description - *optional*

The description can have 0-256 characters.

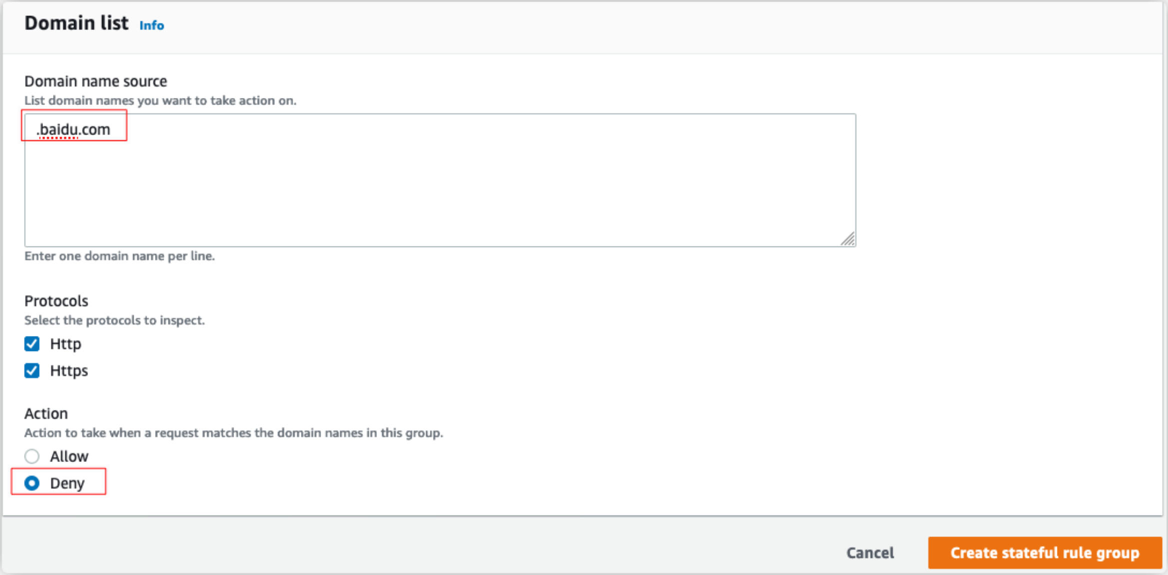
Capacity Info
Maximum processing capacity allowed for the rule group. Estimate the stateful rule group's capacity requirement as the number of rules you expect to add. You can't change or exceed this setting when you update the rule group.
100
The capacity must be greater than or equal to 1 and less than 10,000.

Stateful rule group options

○ 5-tuple
Use the 5-tuple format, specifying source IP, source port, destination IP, destination port, and protocol, and specify the action to take for matching traffic.

● Domain list
Specify a list of domain names and the action to take for traffic that tries to access one of the domains.

○ Suricata compatible IPS rules
Intrusion prevention system (IPS) rules - Provide advanced firewall rules using Suricata rule syntax. Suricata is an open source network IPS that includes a standard rule-based language for traffic inspection.



Domain list Info

Domain name source
List domain names you want to take action on.

```
.baidu.com
```

Enter one domain name per line.

Protocols
Select the protocols to inspect.

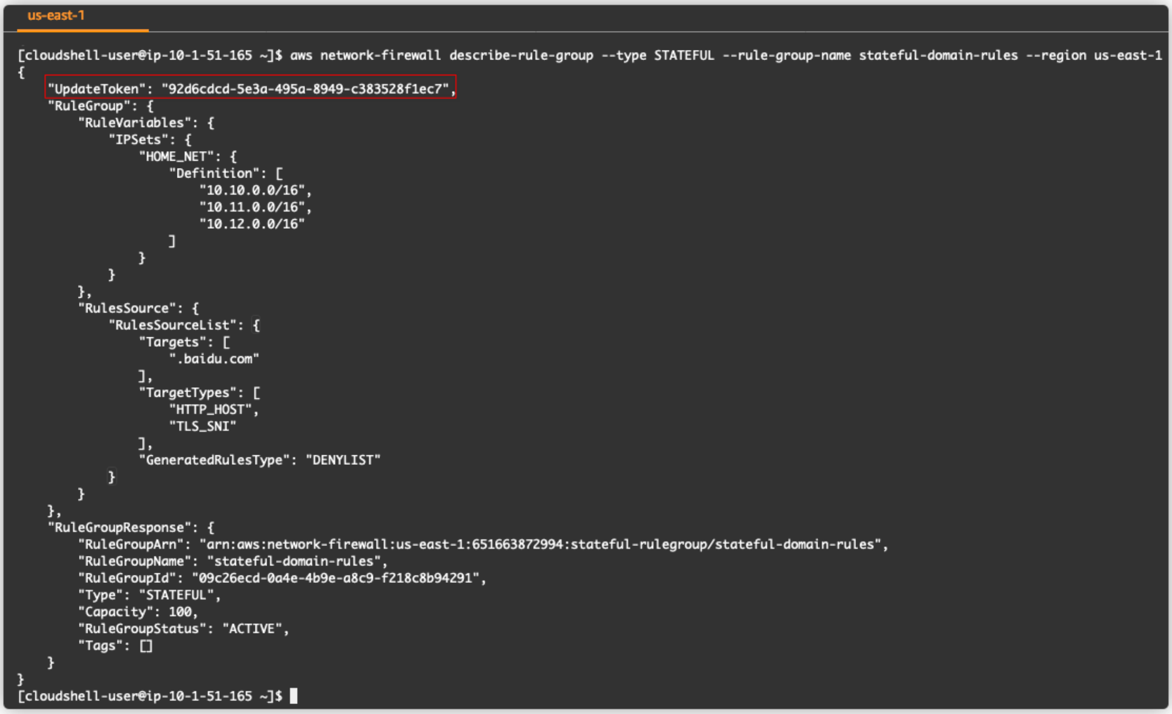
☑ Http
☑ Https

Action
Action to take when a request matches the domain names in this group.

○ Allow
● Deny

创建完成后，回到 CloudShell 界面，查看规则组明细。

```
aws network-firewall describe-rule-group --type STATEFUL --rule-group-name stateful-domain-rules --region us-east-1
```



```
[cloudshell-user@ip-10-1-51-165 ~]$ aws network-firewall describe-rule-group --type STATEFUL --rule-group-name stateful-domain-rules --region us-east-1
{
    "UpdateToken": "92d6cdcd-5e3a-495a-8949-c383528f1ec7",
    "RuleGroup": {
        "RuleVariables": {
            "IPSets": {
                "HOME_NET": {
                    "Definition": [
                        "10.10.0.0/16",
                        "10.11.0.0/16",
                        "10.12.0.0/16"
                    ]
                }
            }
        },
        "RulesSource": {
            "RulesSourceList": {
                "Targets": [
                    ".baidu.com"
                ],
                "TargetTypes": [
                    "HTTP_HOST",
                    "TLS_SNI"
                ],
                "GeneratedRulesType": "DENYLIST"
            }
        }
    },
    "RuleGroupResponse": {
        "RuleGroupArn": "arn:aws:network-firewall:us-east-1:651663872994:stateful-rulegroup/stateful-domain-rules",
        "RuleGroupName": "stateful-domain-rules",
        "RuleGroupId": "09c26ecd-0a4e-4b9e-a8c9-f218c8b94291",
        "Type": "STATEFUL",
        "Capacity": 100,
        "RuleGroupStatus": "ACTIVE",
        "Tags": []
    }
}
[cloudshell-user@ip-10-1-51-165 ~]$
```

记录下来 UpdateToken，后面更新需要用到。

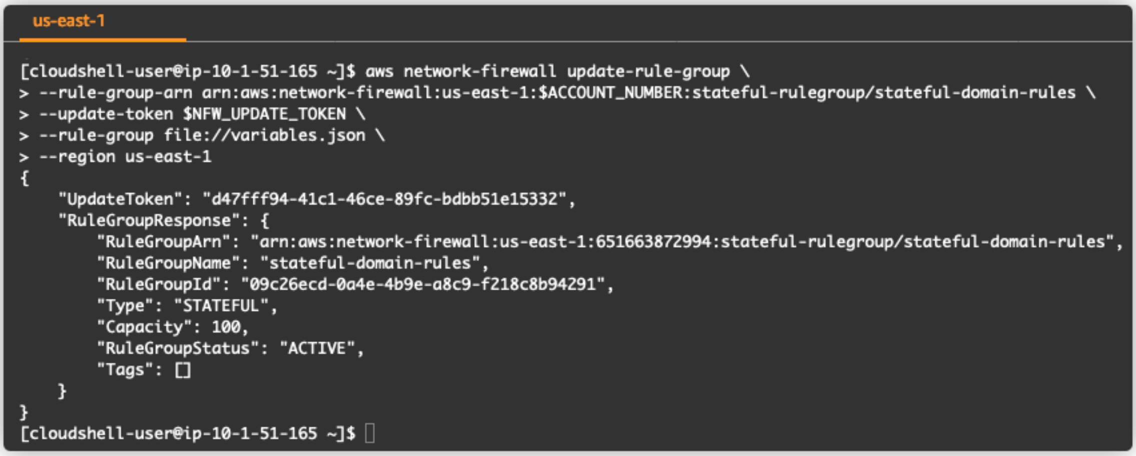
```
export NFW_UPDATE_TOKEN=92d6cdcd-5e3a-495a-8949-c383528f1ec7
export ACCOUNT_NUMBER=`aws sts get-caller-identity --query Account --output text`
```

默认 NFW 在 domain name filtering 规则中只会检查来源于 nfw 所在 vpc cidr 的流量，来源于 nfw 所在 vpc 外部的其它流量均不会进行过滤，需要设置这个 HOME_NET 将需要检查流量的 CIDR 添加进去。创建 variables.json 文件。

```
cat > variables.json <<EOF
{
  "RuleVariables": {
    "IPSets": {
      "HOME_NET": {
        "Definition": [
          "10.10.0.0/16",
          "10.11.0.0/16",
          "10.12.0.0/16"
        ]
      }
    }
  },
  "RulesSource": {
    "RulesSourceList": {
      "Targets": [
        ".baidu.com"
      ],
      "TargetTypes": [
        "HTTP_HOST",
        "TLS_SNI"
      ],
      "GeneratedRulesType": "DENYLIST"
    }
  }
}
EOF
```

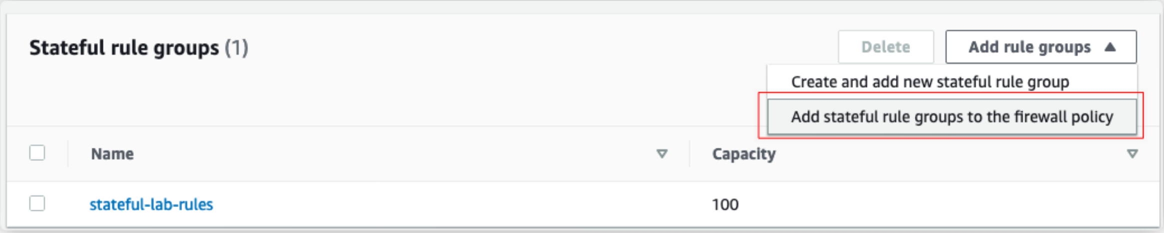
通过 AWS CLI 更新规则组

```
aws network-firewall update-rule-group \
--rule-group-arn arn:aws:network-firewall:us-east-1:$ACCOUNT_NUMBER:stateful-rulegroup/stateful-domain-rules \
--update-token $NFW_UPDATE_TOKEN \
--rule-group file://variables.json \
--region us-east-1
```



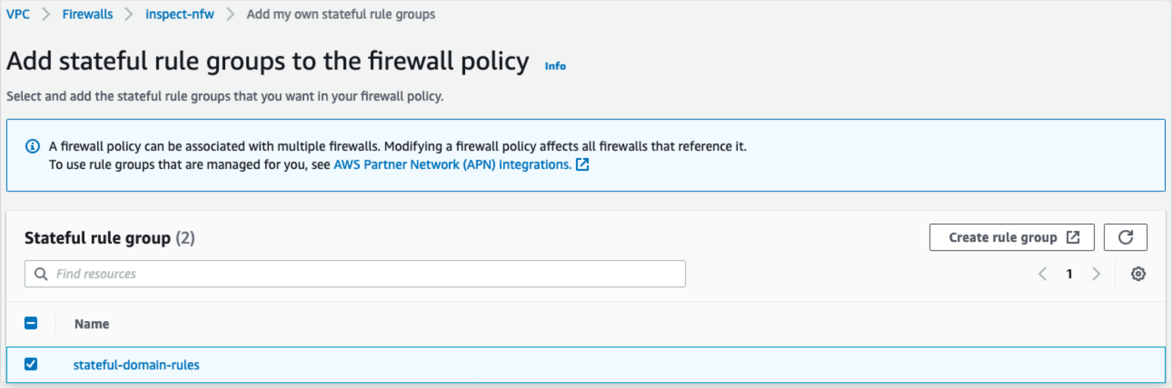
```
[cloudshell-user@ip-10-1-51-165 ~]$ aws network-firewall update-rule-group \
> --rule-group-arn arn:aws:network-firewall:us-east-1:$ACCOUNT_NUMBER:stateful-rulegroup/stateful-domain-rules \
> --update-token $NFW_UPDATE_TOKEN \
> --rule-group file://variables.json \
> --region us-east-1
{
    "UpdateToken": "d47fff94-41c1-46ce-89fc-bdbb51e15332",
    "RuleGroupResponse": {
        "RuleGroupArn": "arn:aws:network-firewall:us-east-1:651663872994:stateful-rulegroup/stateful-domain-rules",
        "RuleGroupName": "stateful-domain-rules",
        "RuleGroupId": "09c26ecd-0a4e-4b9e-a8c9-f218c8b94291",
        "Type": "STATEFUL",
        "Capacity": 100,
        "RuleGroupStatus": "ACTIVE",
        "Tags": []
    }
}
[cloudshell-user@ip-10-1-51-165 ~]$ 
```

将新创建的规则组绑定到防火墙策略，（点击这里），选中防火墙查看明细，并添加有状态规则组。


Delete
Add rule groups ▲
Create and add new stateful rule group
Add stateful rule groups to the firewall policy

Stateful rule groups (1)

□	Name	Capacity
□	stateful-lab-rules	100


VPC > Firewalls > inspect-nfw > Add my own stateful rule groups
Info
Create rule group
Find resources
1

Add stateful rule groups to the firewall policy

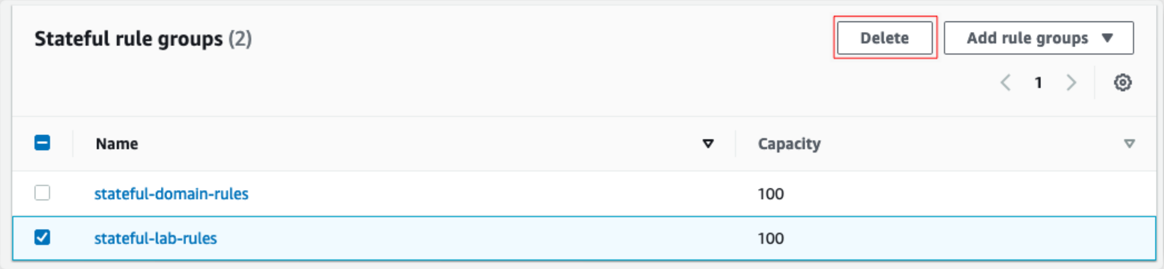
Select and add the stateful rule groups that you want in your firewall policy.

A firewall policy can be associated with multiple firewalls. Modifying a firewall policy affects all firewalls that reference it.
To use rule groups that are managed for you, see AWS Partner Network (APN) integrations.

Stateful rule group (2)

☑	Name
☑	stateful-domain-rules

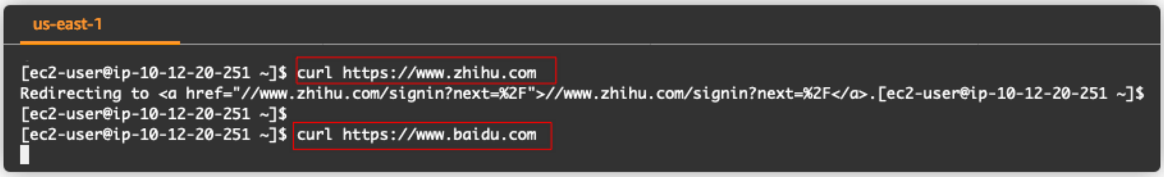
有状态规则校验是合并所有的组，取并集，只要有一条符合条件就放行，故这里校验需要先移除 stateful-lab-rules



Stateful rule groups (2)

☑	Name	Capacity
□	stateful-domain-rules	100
☑	stateful-lab-rules	100

再次验证，首先尝试未被明确禁用的域名，例如 zhihu；然后尝试访问百度。

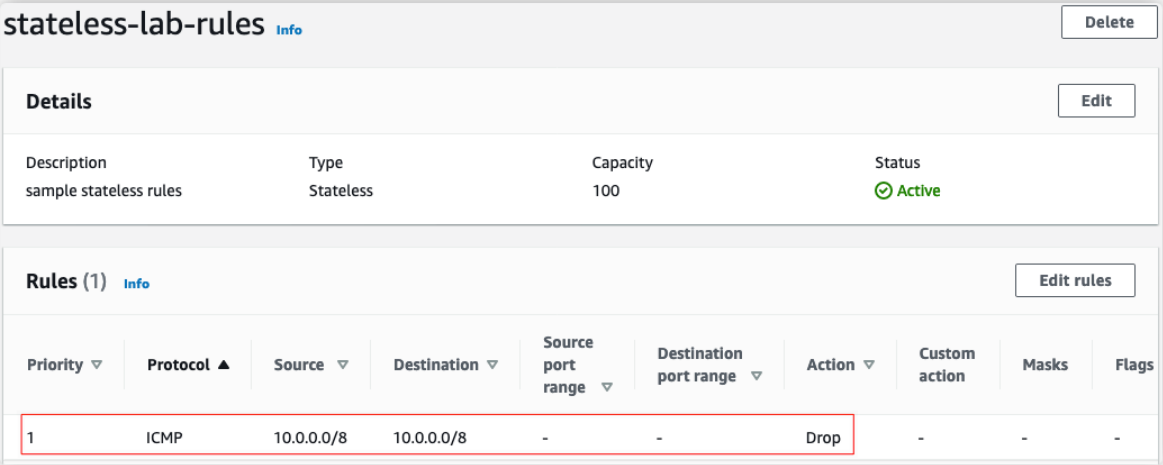


```
[ec2-user@ip-10-12-20-251 ~]$ curl https://www.zhihu.com
Redirecting to <a href="//www.zhihu.com/signin?next=%2F">//www.zhihu.com/signin?next=%2F</a>.[ec2-user@ip-10-12-20-251 ~]$
[ec2-user@ip-10-12-20-251 ~]$
[ec2-user@ip-10-12-20-251 ~]$ curl https://www.baidu.com
▌
```

可以看到，知乎可以正常访问，但是现在 curl 百度就会卡住不动，达到了实验预期的效果。

东西向防护

实验配置的南北向规则放在无状态规则组 stateless-lab-rules。点击查看规则明细如下：

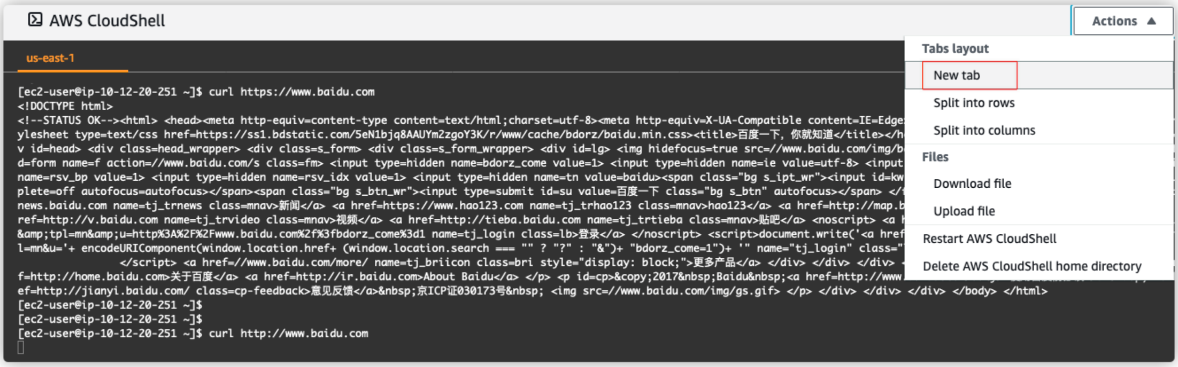


Description	Type	Capacity	Status
sample stateless rules	Stateless	100	✓ Active

Priority	Protocol	Source	Destination	Source port range	Destination port range	Action	Custom action	Masks	Flags
1	ICMP	10.0.0.0/8	10.0.0.0/8	-	-	Drop	-	-	-

我们配置的东西向防火墙策略是不允许访问 ping。

可以在 CloudShell 里新开一个 Tab，点击 Actions->New Tab。



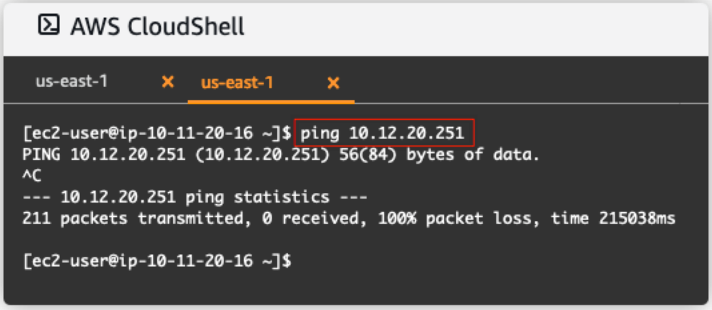
```
[ec2-user@ip-10-12-20-251 ~]$ curl https://www.baidu.com
<!DOCTYPE html>
<!--STATUS OK--><html> <head><meta http-equiv=content-type content=text/html;charset=utf-8><meta http-equiv=X-UA-Compatible content=IE=Edge
ylesheet type=text/css href=https://ss1.bdstatic.com/5eN1bjq8AAUYm2zgoY3K/r/www/cache/bdorz/baidu.min.css><title>百度一下，你就知道</title></h
v id=head> <div class=head_wrapper> <div class=s_form> <div class=s_form_wrapper> <div id=lg> <img hidefocus=true src=//www.baidu.com/img/b
d=form name=f action=//www.baidu.com/s class=fm> <input type=hidden name=bdorz_come value=1> <input type=hidden name=ie value=utf-8> <input
name=rsv_bp value=1> <input type=hidden name=rsv_idx value=1> <input type=hidden name=tn value=baidu><span class="bg s_ipt_wr"><input id=kw
plete=off autofocus=autofocus></span><span class="bg s_btn_wr"><input type=submit id=su value=百度一下 class="bg s_btn" autofocus></span> </
news.baidu.com name=tj_trnews class=mnav>新闻</a> <a href=https://www.hao123.com name=tj_trhao123 class=mnav>hao123</a> <a href=http://map.b
ref=http://v.baidu.com name=tj_trvideo class=mnav>视频</a> <a href=http://tieba.baidu.com name=tj_trtieba class=mnav>贴吧</a> <noscript> <a h
&amp;tpl=mn&amp;u=http%3A%2F%2Fwww.baidu.com%2f%3fbdorz_come%3d1 name=tj_login class=lb>登录</a> </noscript> <script>document.write('<a href
l=mn&u='+ encodeURIComponent(window.location.href+ (window.location.search === "" ? "?" : "&")+ "bdorz_come=1")+ '" name="tj_login" class="
                </script> <a href=//www.baidu.com/more/ name=tj_briicon class=bri style="display: block;">更多产品</a> </div> </div> </div> <
f=http://home.baidu.com>关于百度</a> <a href=http://ir.baidu.com>About Baidu</a> </p> <p id=cp>&copy;2017&nbsp;Baidu&nbsp;<a href=http://www
ef=http://jianyi.baidu.com/ class=cp-feedback>意见反馈</a>&nbsp;京ICP证030173号&nbsp; <img src=//www.baidu.com/img/gs.gif> </p> </div> </div> </div> </body> </html>
[ec2-user@ip-10-12-20-251 ~]$
[ec2-user@ip-10-12-20-251 ~]$
[ec2-user@ip-10-12-20-251 ~]$ curl http://www.baidu.com
▯
```

登录到任意一台 Private server，例如 BizVpc1PriServer：

ssh ec2-user@10.11.20.16 （注意先登录到公共测试机）

尝试 ping 另一个 Business VPC 里的测试机 10.12.20.251

ping 10.12.20.251

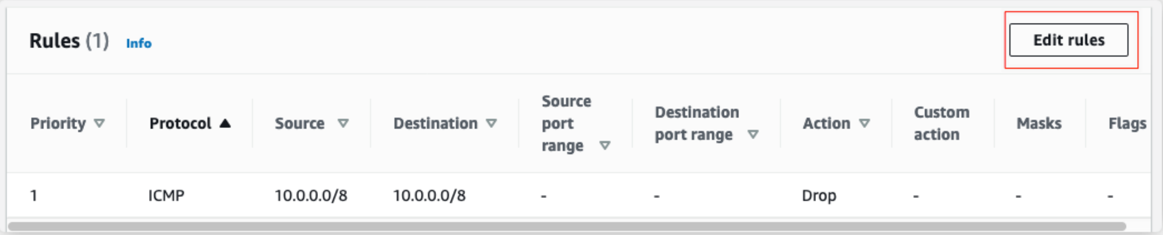


```
[ec2-user@ip-10-11-20-16 ~]$ ping 10.12.20.251
PING 10.12.20.251 (10.12.20.251) 56(84) bytes of data.
^C
--- 10.12.20.251 ping statistics ---
211 packets transmitted, 0 received, 100% packet loss, time 215038ms

[ec2-user@ip-10-11-20-16 ~]$
```

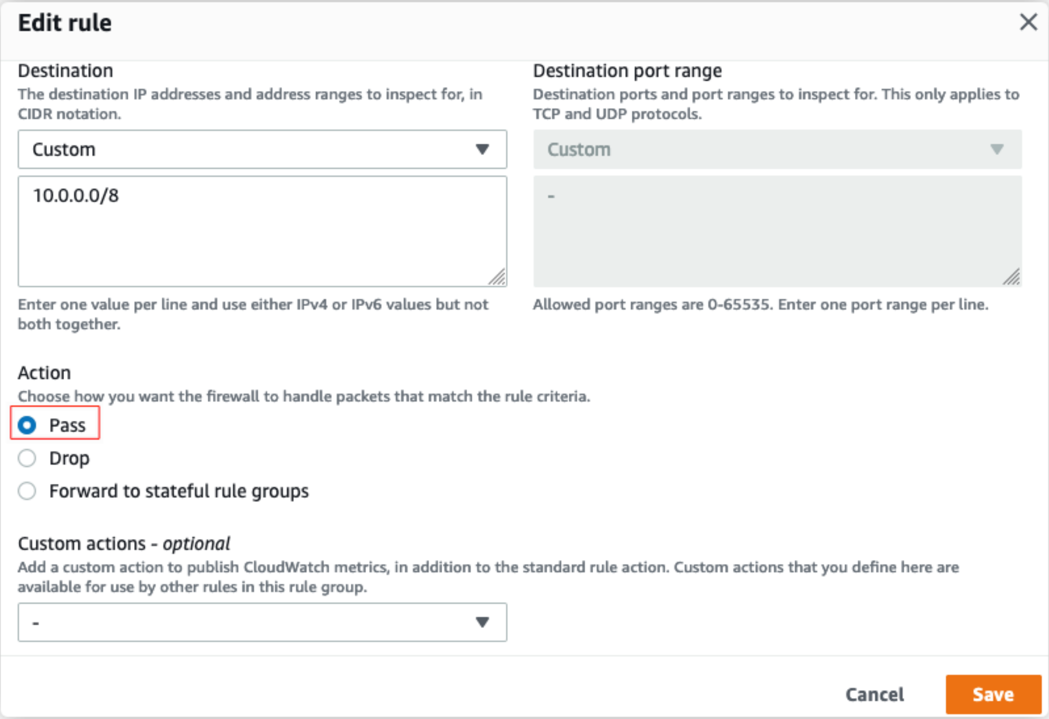
可以看到当前规则下，无法 ping 通。

实验无状态规则

放开 ping（将 Action 由 Drop 改为 Pass），按下图截图操作：



Priority	Protocol	Source	Destination	Source port range	Destination port range	Action	Custom action	Masks	Flags
1	ICMP	10.0.0.0/8	10.0.0.0/8	-	-	Drop	-	-	-



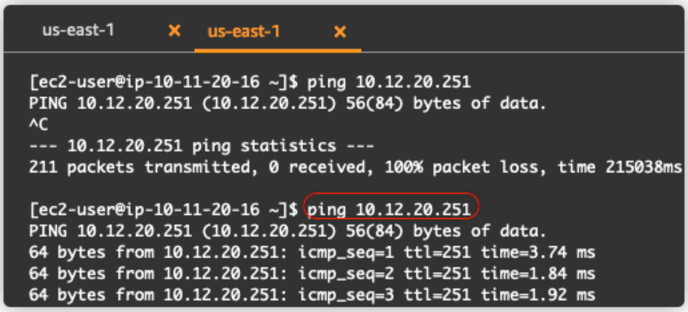
Destination
The destination IP addresses and address ranges to inspect for, in CIDR notation.
Custom
10.0.0.0/8
Enter one value per line and use either IPv4 or IPv6 values but not both together.

Destination port range
Destination ports and port ranges to inspect for. This only applies to TCP and UDP protocols.
Custom
-
Allowed port ranges are 0-65535. Enter one port range per line.

Action
Choose how you want the firewall to handle packets that match the rule criteria.
● Pass
○ Drop
○ Forward to stateful rule groups

Custom actions - *optional*
Add a custom action to publish CloudWatch metrics, in addition to the standard rule action. Custom actions that you define here are available for use by other rules in this rule group.
-

重新测试 ping，可以看到现在可以 ping 通了：



```
[ec2-user@ip-10-11-20-16 ~]$ ping 10.12.20.251
PING 10.12.20.251 (10.12.20.251) 56(84) bytes of data.
^C
--- 10.12.20.251 ping statistics ---
211 packets transmitted, 0 received, 100% packet loss, time 215038ms

[ec2-user@ip-10-11-20-16 ~]$ ping 10.12.20.251
PING 10.12.20.251 (10.12.20.251) 56(84) bytes of data.
64 bytes from 10.12.20.251: icmp_seq=1 ttl=251 time=3.74 ms
64 bytes from 10.12.20.251: icmp_seq=2 ttl=251 time=1.84 ms
64 bytes from 10.12.20.251: icmp_seq=3 ttl=251 time=1.92 ms
```

参考资料

Deployment models for AWS Network Firewall

通过 AWS Network Firewall 实现南北向资源和服务的有效防护

通过 AWS Network Firewall 实现东西向资源和服务的有效防护

通过 AWS Network Firewall 实现混合云环境下资源和服务的有效防护