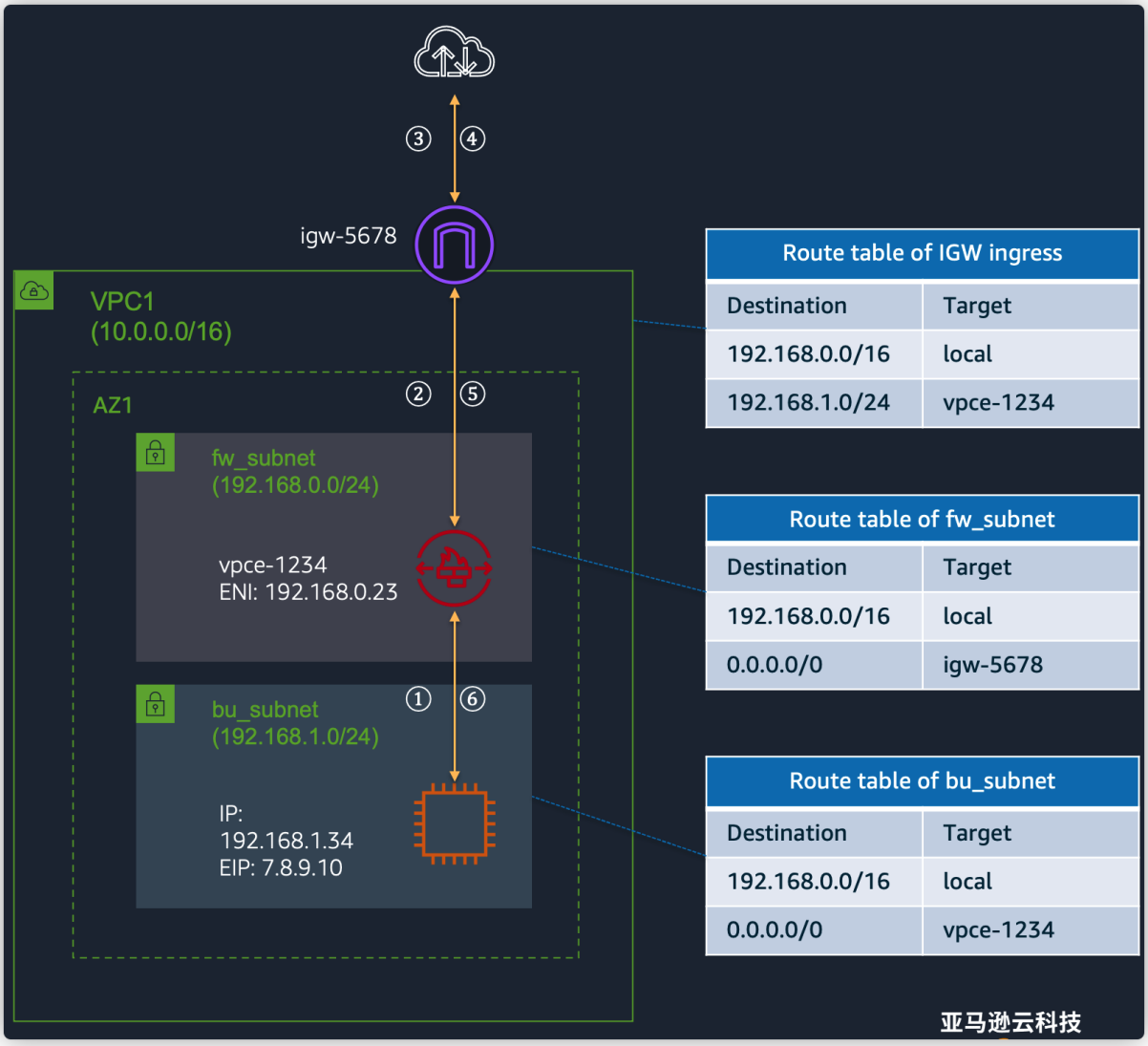
Security Day 构建增强云端环境指导手册（一）

2021 年 3 月 12 日

Table of Contents

一、实验拓扑

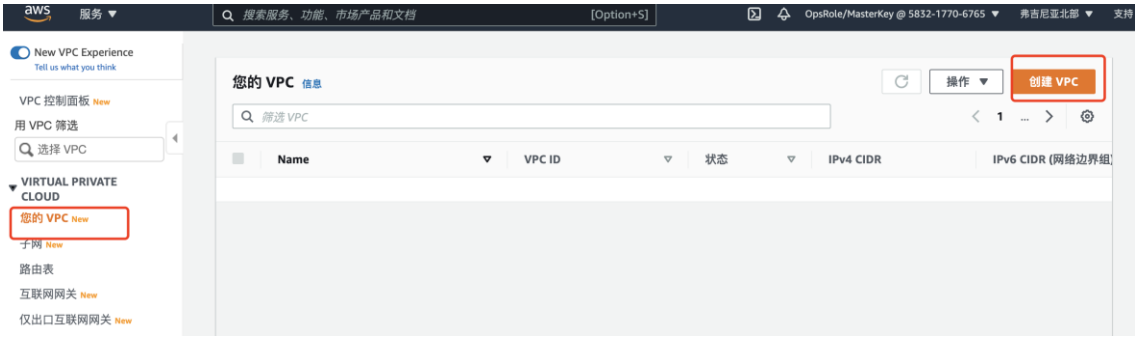
实验采用单 AZ 分布式部署模式



二、实验准备

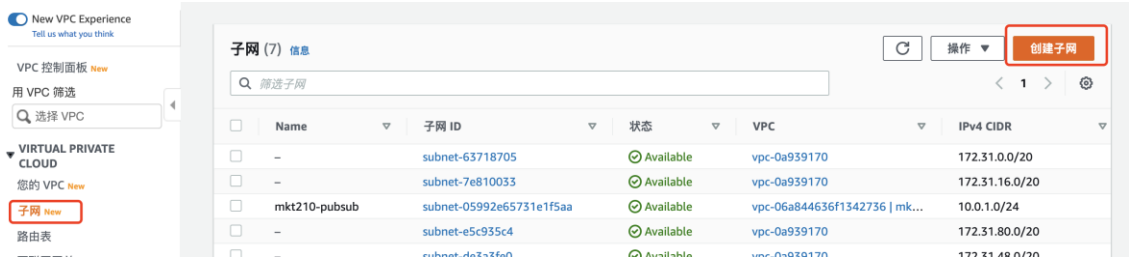
1、创建实验 VPC

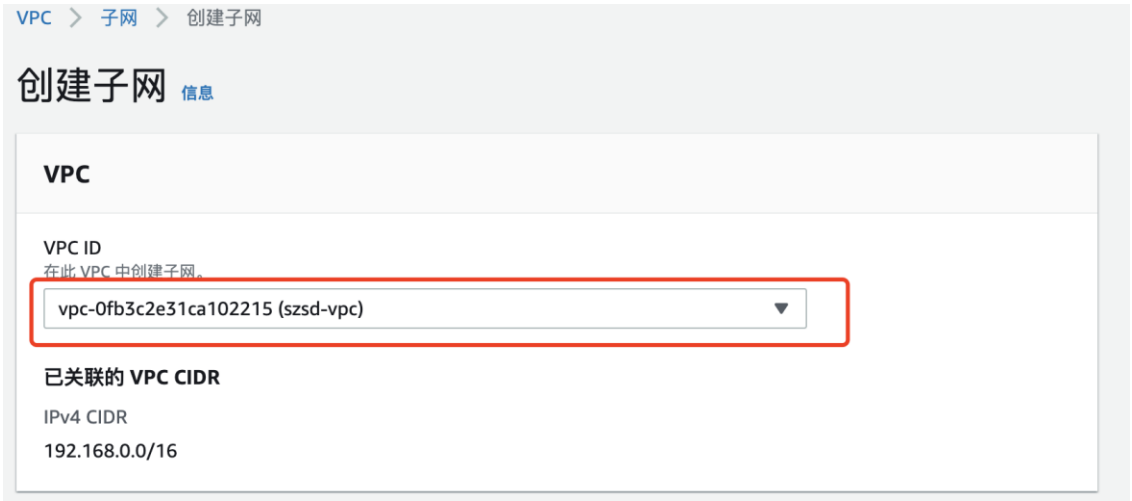
1.1、创建 VPC



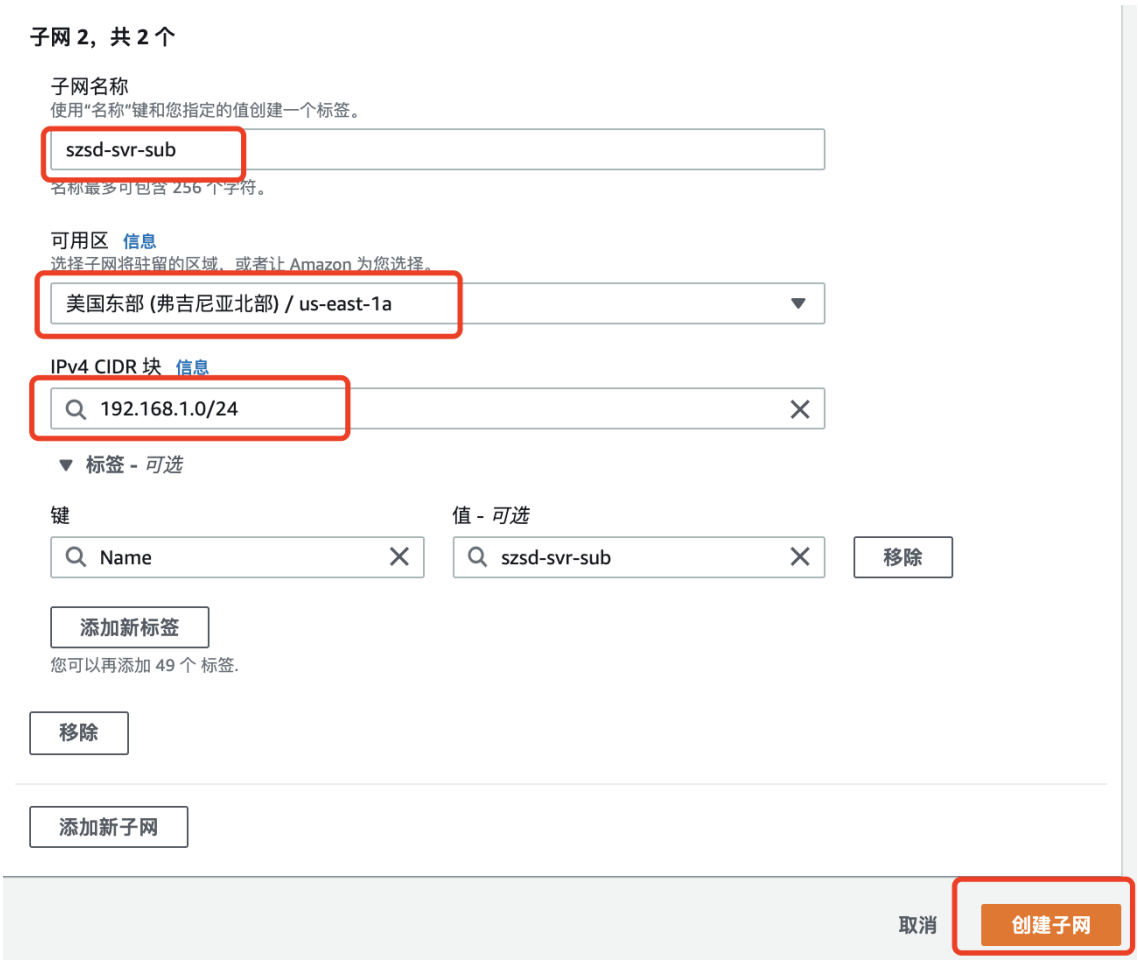
其余保留为默认，点击创建 VPC。

1.2、创建防火墙子网和公共服务器子网

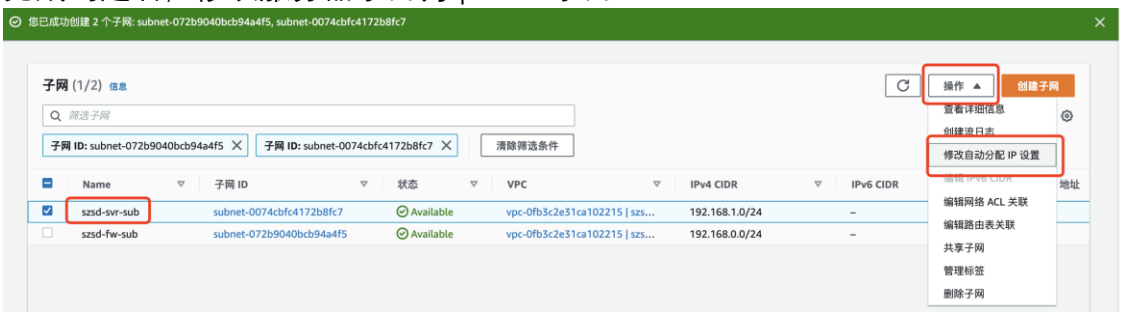




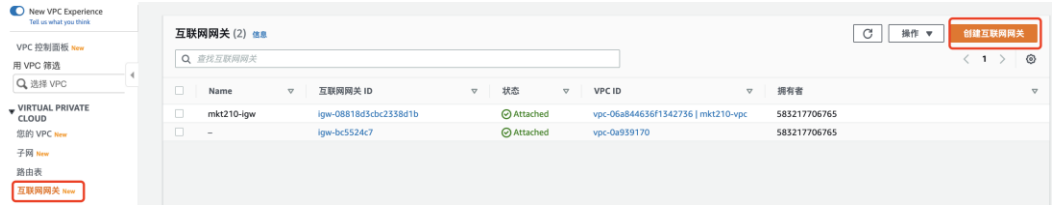

子网 1，共 1 个
子网名称
使用"名称"键和您指定的值创建一个标签。
szsd-fw-sub
名称最多可包含 256 个字符。
可用区 信息
选择子网将驻留的区域，或者让 Amazon 为您选择
美国东部 (弗吉尼亚北部) / us-east-1a
IPv4 CIDR 块 信息
192.168.0.0/24
标签 - 可选
键
值 - 可选
Name
szsd-fw-sub
移除
添加新标签
您可以再添加 49 个 标签.
移除
添加新子网



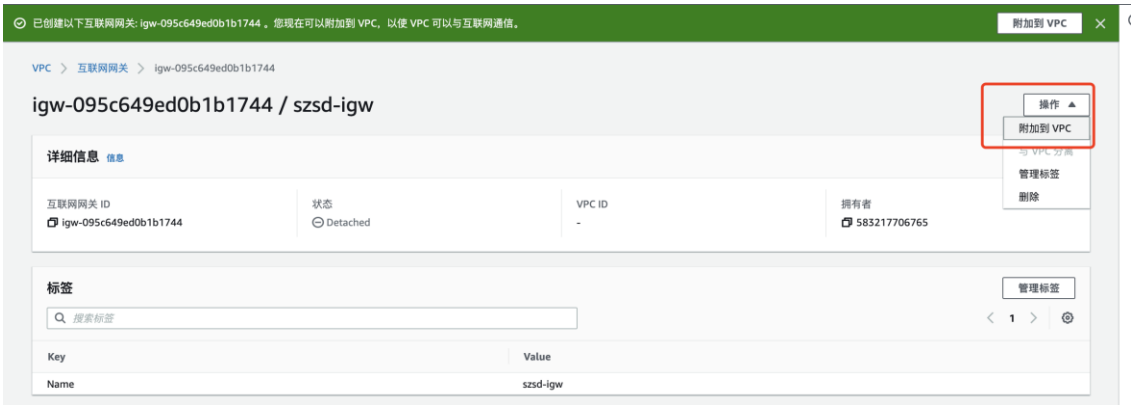
完成创建后，修改服务器子网为 public 子网



1.3、创建 Internet Gateway 并关联到 VPC



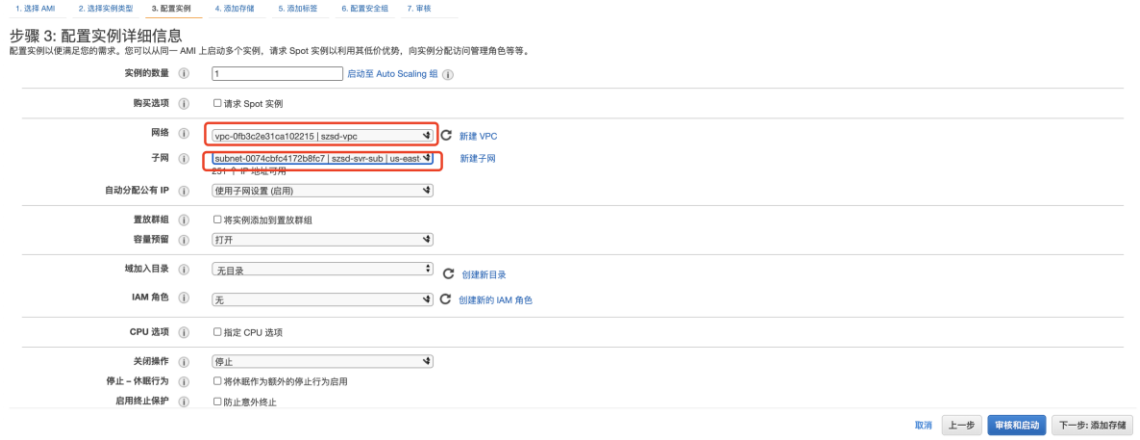
完成创建后，附加到 VPC



2、创建应用服务器

2.1、创建 Amazon Linux 2 EC2 服务器

选择 szsd-vpc 和 svr 子网，其他保持默认



存储保持默认，点击下一步。
增加标签，方便后续使用和管理。点击下一步。

点击启动，进入密钥对选择或创建界面，此处选择新建，下载保存后，启动实例。

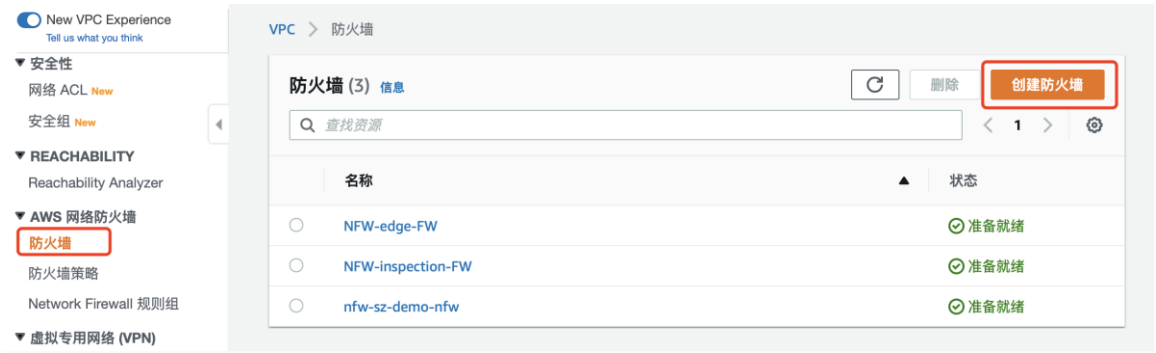
预计一分钟后，实例会完成创建并完成 2 阶段的健康检查后，进入可使用状态。可继续进行下面的实验。

2.2、修改 Key Pair 权限（Mac 或 Linux 系统）

chmod 400 szsd-key.pem

3、创建网络防火墙

回到 VPC 控制台，创建 Network Firewall



防火墙创建预计需要 1-2 分钟完成。完成后，记录防火墙的 endpoint。

4、设置路由

4.1、创建 ingress route table

添加路由 192.168.1.0/24 vpce-id#(上一步记录的防火墙 endpoint)

Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No
192.168.1.0/24	vpce-0f3c11a58c6962e45	active	No

4.2、创建网络防火墙路由表

关联防火墙子网

添加路由 0.0.0.0/0 internet gateway

Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No
0.0.0.0/0	igw-0e0e35875c0766427	active	No

4.3、创建服务器子网路由表

关联服务器子网

添加路由 0.0.0.0/0 vpce-id#（同 5.1）

Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No
0.0.0.0/0	vpce-0f3c11a58c6962e45	active	No

三、实验步骤

实验内容：

1. 实验一、无状态规则验证，拒绝 ssh 到目标服务器
2. 实验二、有状态规则验证，允许远端 ssh 到目标服务器
3. 实验三、域名过滤验证，过滤目标服务器主动访问 amazon.com 流量

3.1、验证连通性

开始之前通过本地电脑，ssh 访问应用服务器

ssh -i szsd.pem ec2-user@public-ip

Linux/Mac 参考如下链接 ssh 访问 EC2

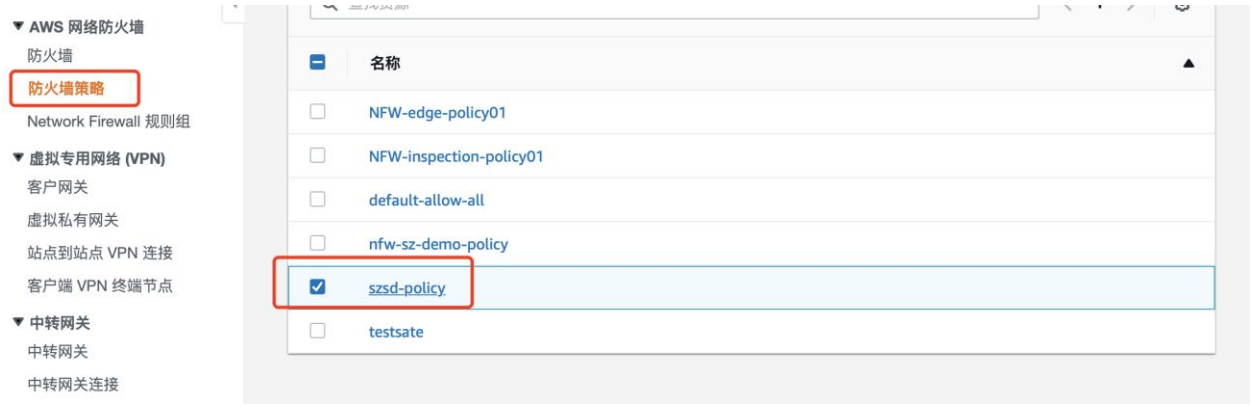
https://aws.amazon.com/cn/premiumsupport/knowledge-center/new-user-accounts-linux-instance/

Windows 参考如下链接 ssh 访问 EC2

https://docs.aws.amazon.com/zh_cn/AWSEC2/latest/UserGuide/putty.html

3.2、实验一、无状态规则组，拒绝 ssh 访问目标服务器。

进入防火墙策略控制台，双击进入 szsd-policy




szsd-policy 信息
删除
Network Firewall 规则组
详细信息
无状态规则组 (0)
编辑优先级
删除
添加规则组
创建并添加新的无状态规则组
将无状态规则组添加到防火墙策略
优先级
名称
容量
没有无状态规则组
选择"添加规则组"以将无状态规则组添加到策略中。
无状态默认操作
要对不匹配任何无状态规则的数据包执行的操作。
编辑
对完整数据包的操作
转发至有状态规则组
对分段数据包的操作
传递


无状态规则组
名称
为在您的有状态规则组中唯一的规则组输入名称。
szsd-stateless-rg
该名称必须具有 1-128 个字符。有效字符: a-z、A-Z、0-9 和 - (连字符)。名称不能以连字符开头或结尾，并且不能包含两个连续的连字符。
描述 – 可选
描述可以包含 0-256 个字符。
容量 信息
该规则组允许的最大处理容量。按照您希望添加的规则容量需求之和来估计无状态规则组的容量需求。更新规则组时不能更改或超过出设置。
1000
此容量必须大于或等于 1 且小于 10000。

再次通过本地机器 ssh 到远端服务器进行验证。

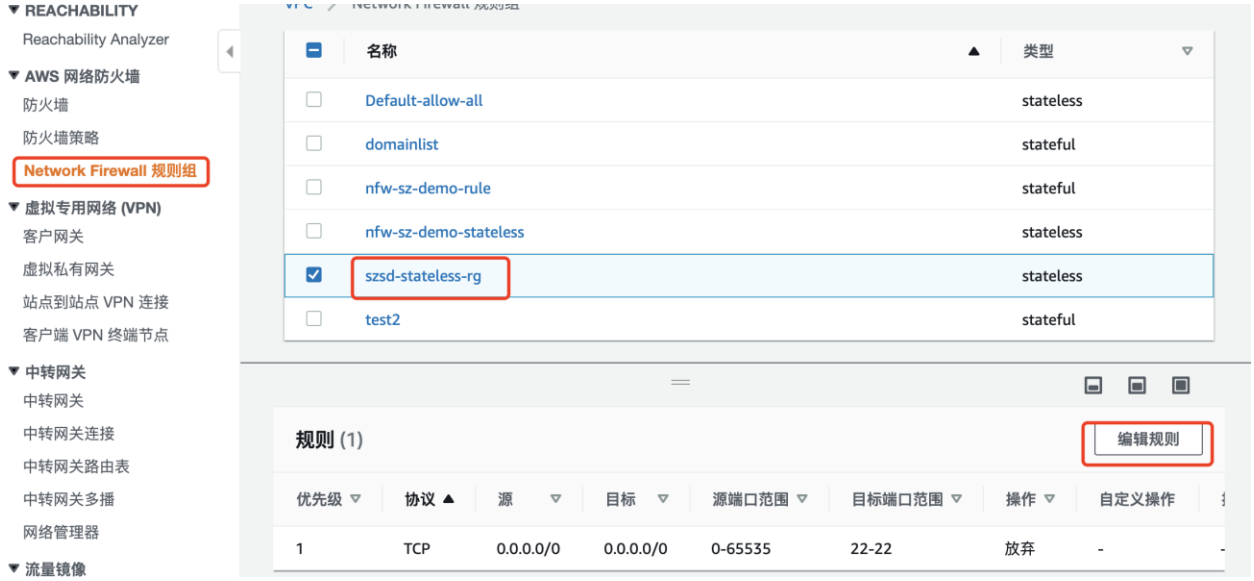
ssh -i szsd.pem ec2-user@public-ip

无法访问。

3.3、实验二、有状态规则验证，允许远端 ssh 到目标服务器

修改无状态规则组，针对 22 端口规则的动作为转发到有状态规则组。

由于窗口大小，可能无法直接查看到编辑规则按钮，向下浏览页面即可找到。



操作

操作
选择您希望防火墙处理与规则条件匹配的数据包的方式。

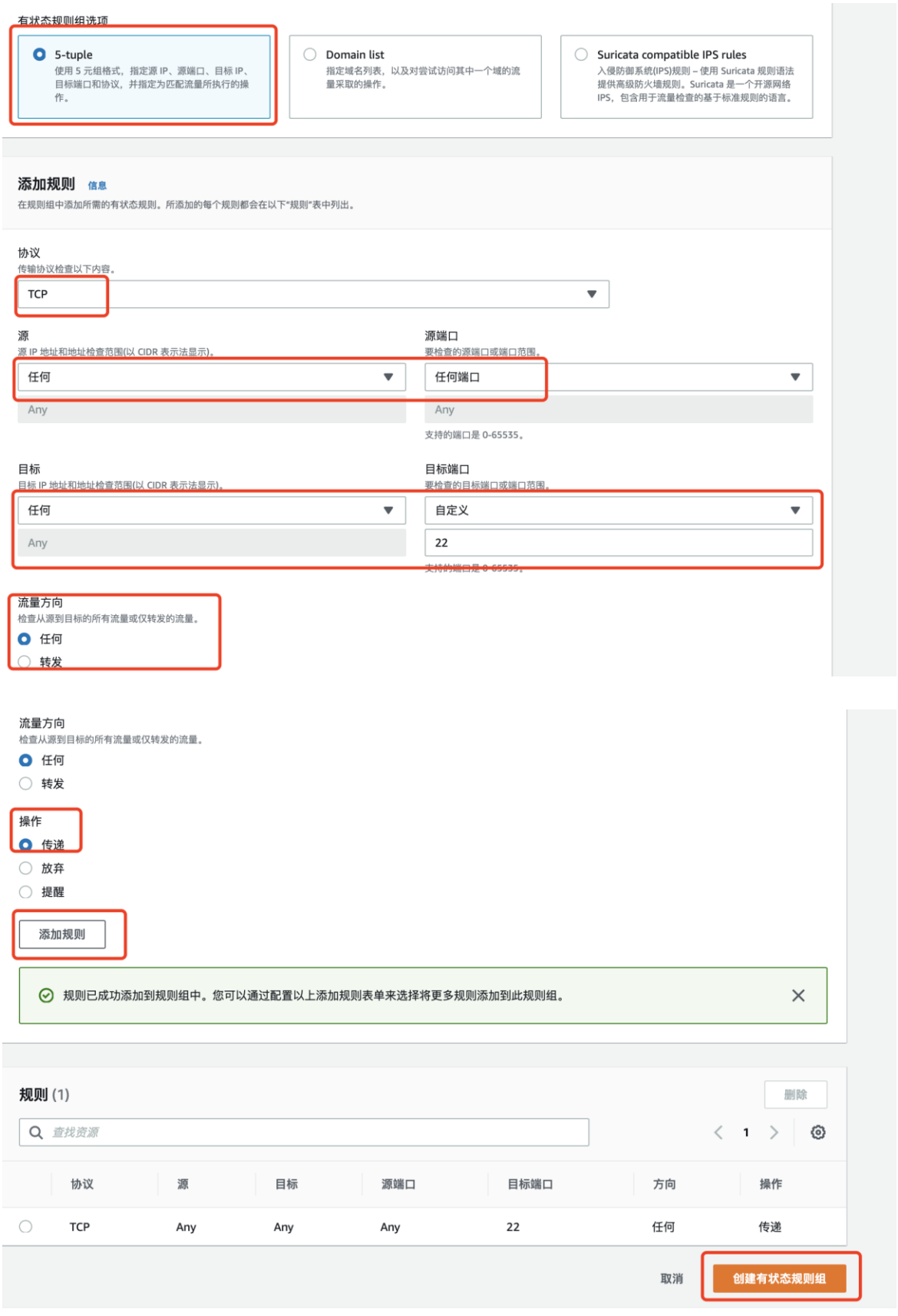
- ○ 传递
- ○ 放弃
- ◉ 转发至有状态规则组

自定义操作 – *可选*
除了标准规则操作之外，添加自定义操作以发布 CloudWatch 指标。您在此处定义的自定义操作可供此规则组中的其他规则使用。

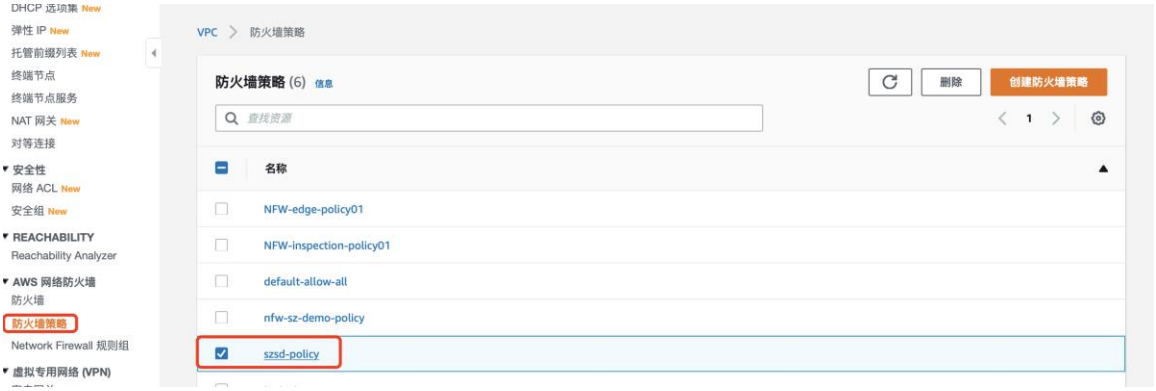
–

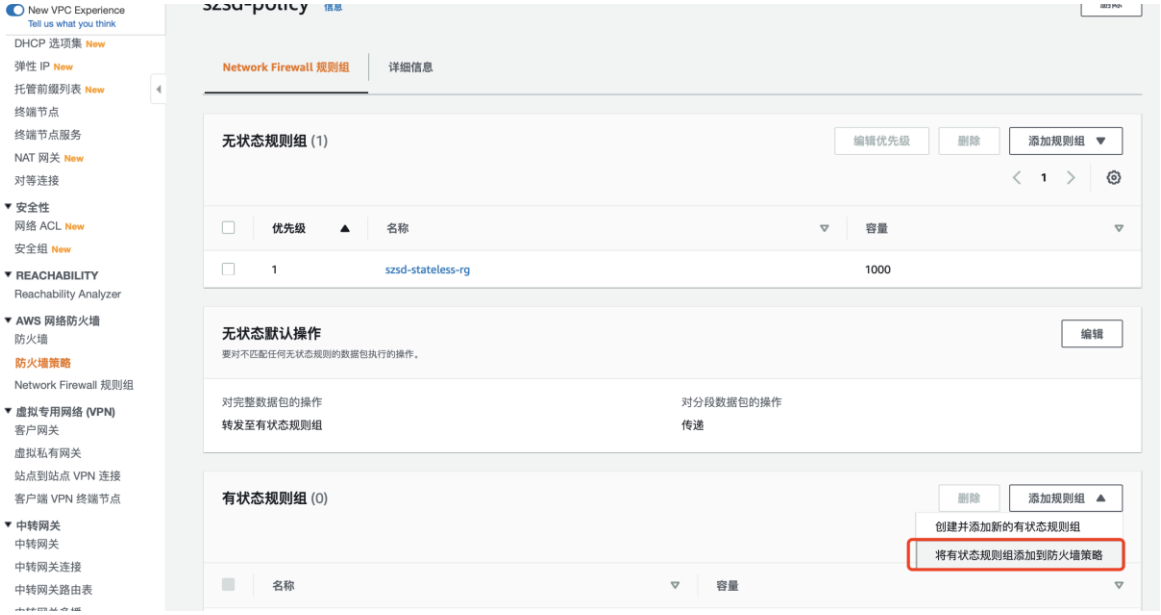
取消　保存

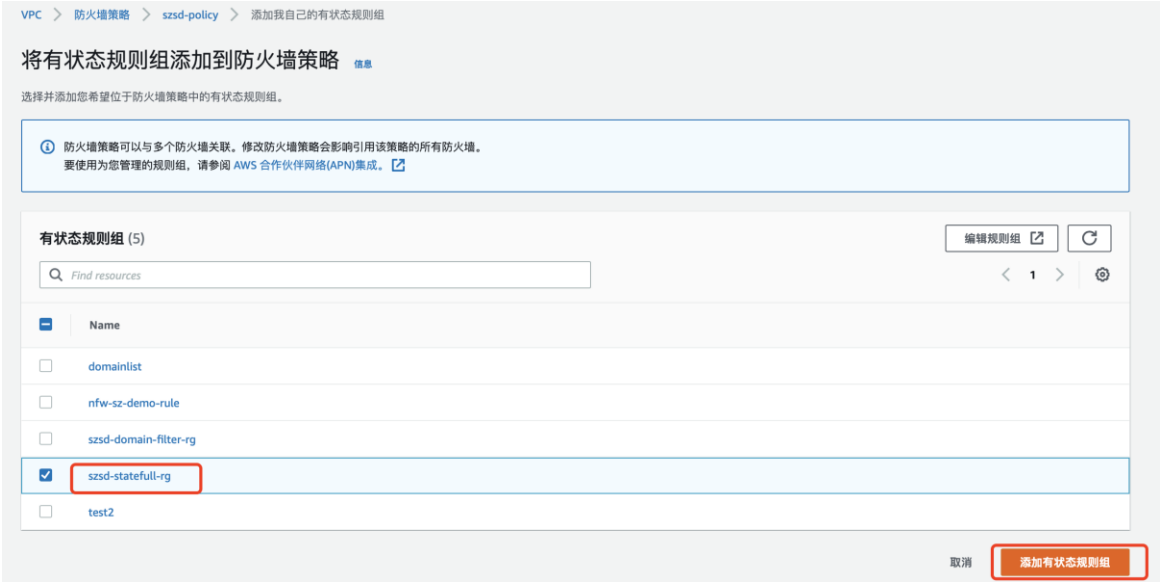
创建有状态规则组


有状态规则组选项
5-tuple
使用 5 元组格式，指定源 IP、源端口、目标 IP、目标端口和协议，并指定为匹配流量所执行的操作。
Domain list
指定域名列表，以及对尝试访问其中一个域的流量采取的操作。
Suricata compatible IPS rules
入侵防御系统(IPS)规则 – 使用 Suricata 规则语法提供高级防火墙规则。Suricata 是一个开源网络 IPS，包含用于流量检查的基于标准规则的语言。
添加规则 信息
在规则组中添加所需的有状态规则。所添加的每个规则都会在以下"规则"表中列出。
协议
传输协议检查以下内容。
TCP
源
源 IP 地址和地址检查范围(以 CIDR 表示法显示)。
任何
Any
源端口
要检查的源端口或端口范围。
任何端口
Any
支持的端口是 0-65535。
目标
目标 IP 地址和地址检查范围(以 CIDR 表示法显示)。
任何
Any
目标端口
要检查的目标端口或端口范围。
自定义
22
支持的端口是 0-65535。
流量方向
检查从源到目标的所有流量或仅转发的流量。
任何
转发
流量方向
检查从源到目标的所有流量或仅转发的流量。
任何
转发
操作
传递
放弃
提醒
添加规则
规则已成功添加到规则组中。您可以通过配置以上添加规则表单来选择将更多规则添加到此规则组。
规则 (1)
删除
查找资源
1
协议
源
目标
源端口
目标端口
方向
操作
TCP
Any
Any
Any
22
任何
传递
取消
创建有状态规则组

将创建的有状态规则组与 szsd-policy 关联。双击进入 szsd-policy。





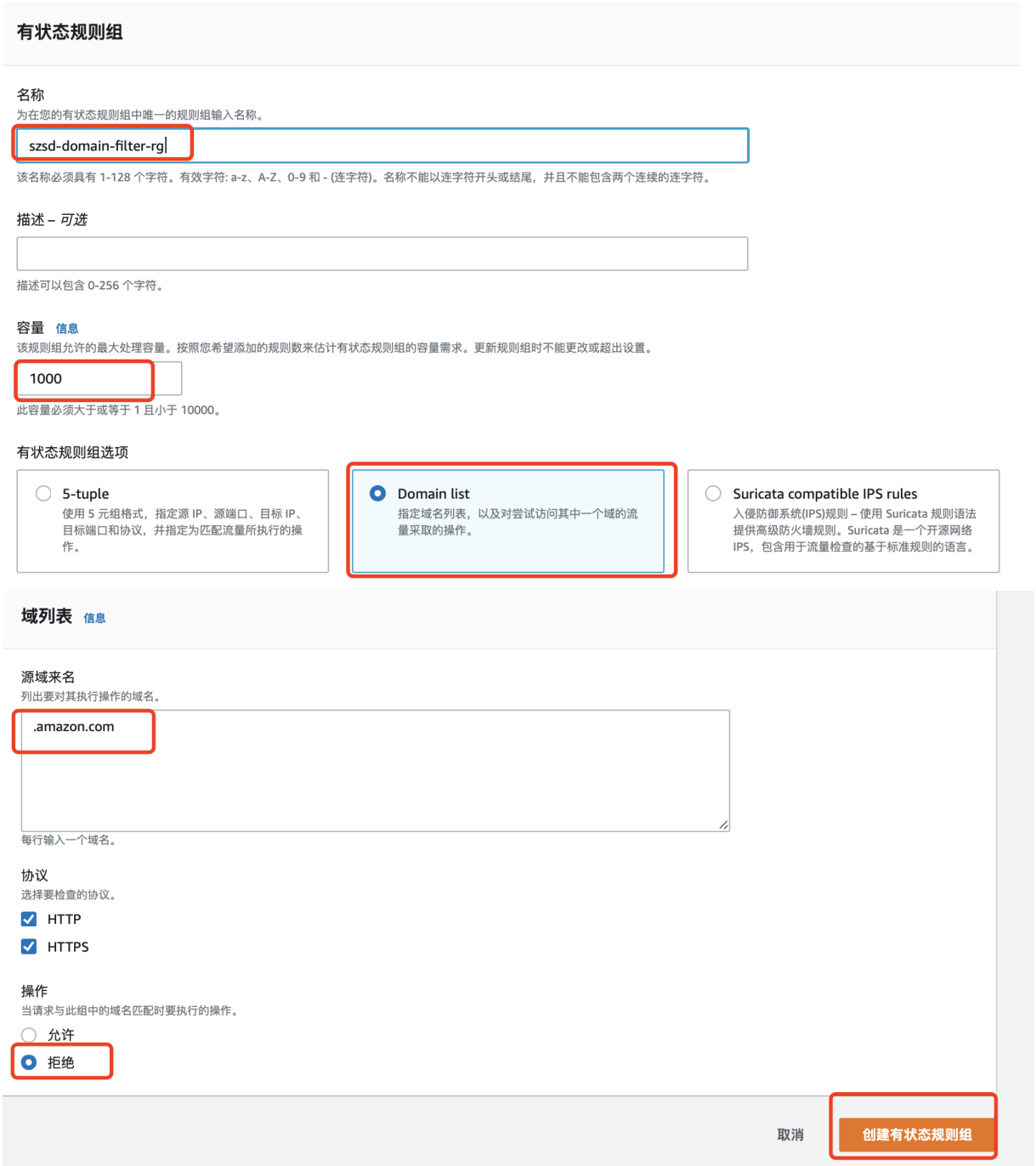


再次在本地客户段进行验证测试: ssh -i szsd.pem ec2-user@public-ip

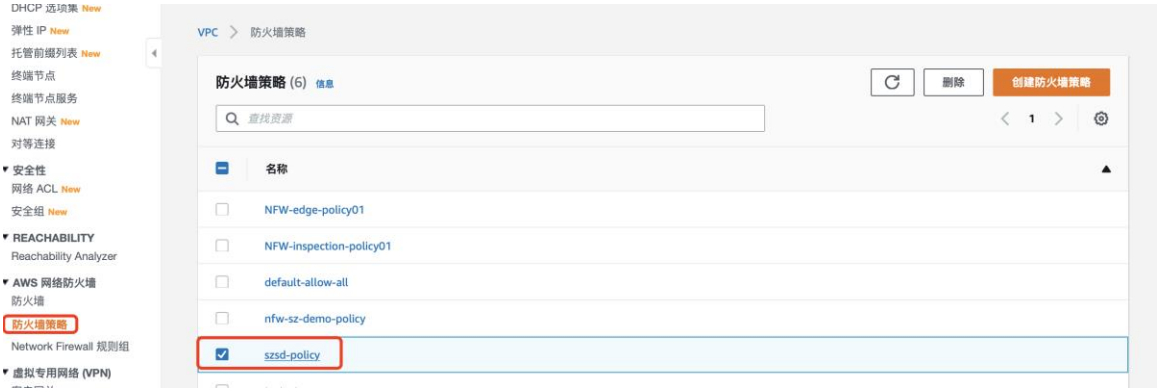
结果可以正常访问目标服务器。为了下一个实验，此处多进行一步操作，在目标服务器上输入 wget https://www.amazon.com 或 curl https://www.amazon.com
有正常返回结果。

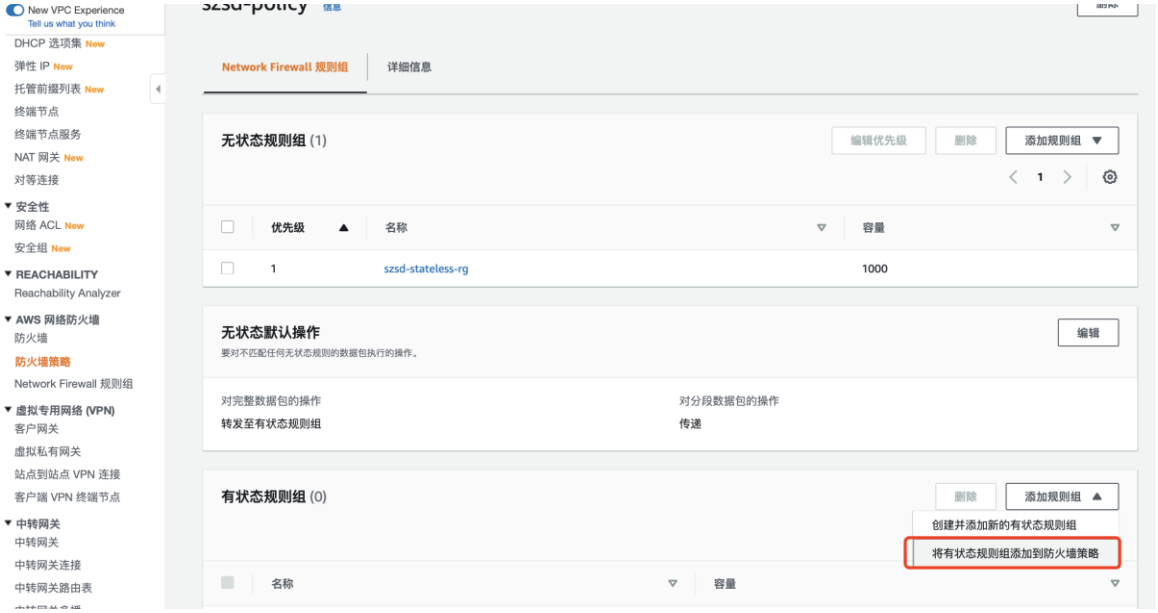
3.4、实验三、域名过滤，禁止目标服务器主动访问 amazon.com 后缀的网站。

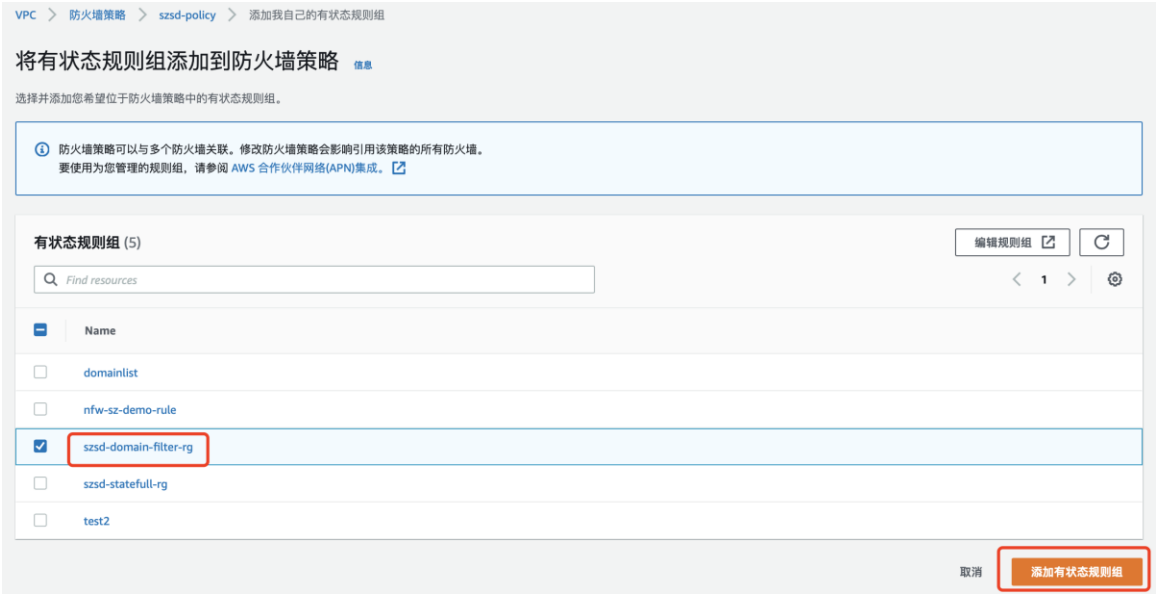
创建一个新的有状态规则组



将有状态规则组，关联到 szsd-policy。







再次在本地客户段进行验证测试，重新 ssh -i szsd.pem ec2-user@public-ip 后，再输入 wget https://www.amazon.com 或 curl https://www.amazon.com 进行验证，发现无法访问。