

# 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.....3

二、实验准备.....4

1、创建实验 VPC.....4

1.1、创建 VPC.....4

1.2、创建防火墙子网和公共服务器子网.....5

1.3、创建 Internet Gateway 并关联到 VPC.....8

2、创建应用服务器.....9

2.1、创建 Amazon Linux 2 EC2 服务器.....9

2.2、修改 Key Pair 权限（Mac 或 Linux 系统）.....11

3、创建网络防火墙.....12

4、设置路由.....13

4.1、创建 ingress route table.....13

4.2、创建网络防火墙路由表.....13

4.3、创建服务器子网路由表.....13

三、实验步骤.....14

3.1、验证连通性.....14

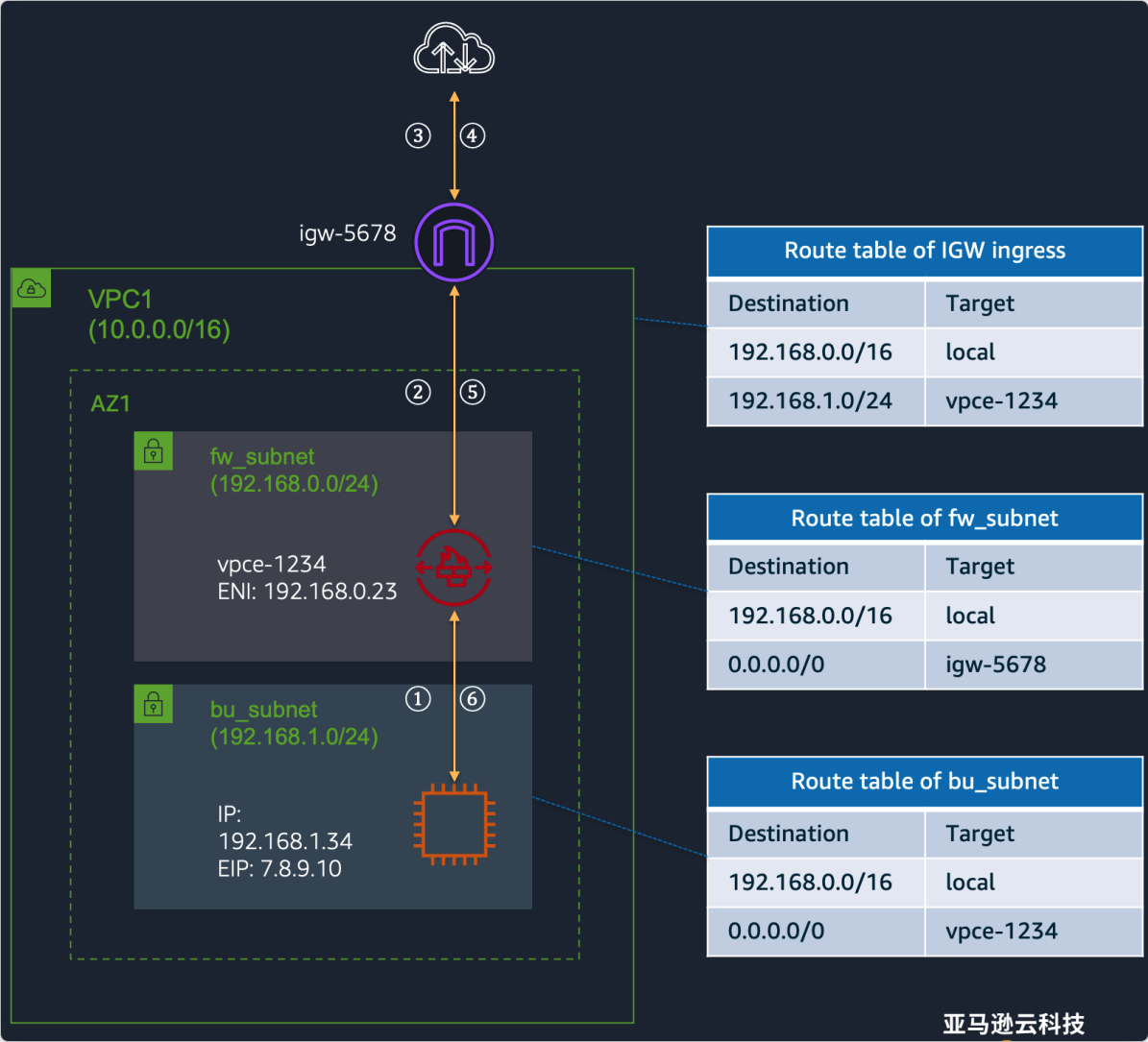
3.2、实验一、无状态规则组，拒绝 ssh 访问目标服务器。.....14

3.3、实验二、有状态规则验证，允许远端 ssh 到目标服务器.....17

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。.....21

一、实验拓扑

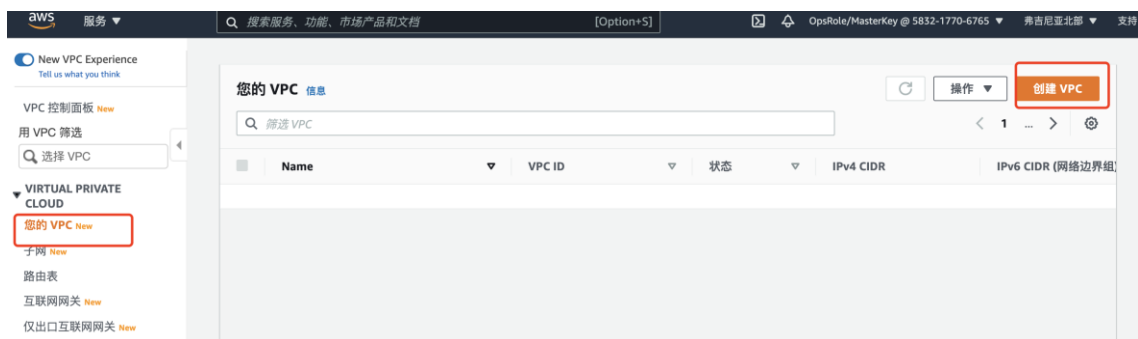
实验采用单 AZ 分布式部署模式



## 二、实验准备

### 1、创建实验 VPC

#### 1.1、创建 VPC



## 创建 VPC 信息

VPC 是由 AWS 对象(如 Amazon EC2 实例)填充的 AWS 云的隔离部分。

### VPC 设置

#### 名称标签 – 可选

使用“Name”键和您指定的值创建一个标签。

szsd-vpc

#### IPv4 CIDR 块 信息

192.168.0.0/16

#### IPv6 CIDR 数据块 信息

- ☒ 无 IPv6 CIDR 块
- ☐ Amazon 提供的 IPv6 CIDR 块
- ☐ 我拥有的 IPv6 CIDR

#### 租期 信息

默认

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

New VPC Experience  
Tell us what you think

VPC 控制面板 New

用 VPC 筛选

Q 选择 VPC

VIRTUAL PRIVATE CLOUD

您的 VPC New

子网 New

路由表

子网 (7) 信息

Q 筛选子网

操作

创建子网

	Name	子网 ID	状态	VPC	IPv4 CIDR
<input type="checkbox"/>	-	subnet-63718705	Available	vpc-0a939170	172.31.0.0/20
<input type="checkbox"/>	-	subnet-7e810033	Available	vpc-0a939170	172.31.16.0/20
<input type="checkbox"/>	mkt210-pubsub	subnet-05992e65731e1f5aa	Available	vpc-06a844636f1342736   mk...	10.0.1.0/24
<input type="checkbox"/>	-	subnet-e5c935c4	Available	vpc-0a939170	172.31.80.0/20
<input type="checkbox"/>	-	subnet-4a2a33e0	Available	vpc-0a939170	172.31.48.0/20

VPC > 子网 > 创建子网

## 创建子网 信息

### VPC

#### VPC ID

在此 VPC 中创建子网。

vpc-0fb3c2e31ca102215 (szsd-vpc)

#### 已关联的 VPC CIDR

IPv4 CIDR

192.168.0.0/16

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

Name

值 - 可选

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

## 子网 2, 共 2 个

### 子网名称

使用“名称”键和您指定的值创建一个标签。

szsd-svr-sub

名称最多可包含 255 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

192.168.1.0/24

### ▼ 标签 - 可选

#### 键

Name

#### 值 - 可选

szsd-svr-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

取消

创建子网

完成创建后，修改服务器子网为 public 子网

您已成功创建 2 个子网: subnet-072b9040bcb94a4f5, subnet-0074cbfc4172b8fc7

### 子网 (1/2) 信息

筛选子网

子网 ID: subnet-072b9040bcb94a4f5 子网 ID: subnet-0074cbfc4172b8fc7 清除筛选条件

	Name	子网 ID	状态	VPC	IPv4 CIDR	IPv6 CIDR	地址
<input checked="" type="checkbox"/>	szsd-svr-sub	subnet-0074cbfc4172b8fc7	Available	vpc-0fb3c2e31ca102215   szs...	192.168.1.0/24	-	
<input type="checkbox"/>	szsd-fw-sub	subnet-072b9040bcb94a4f5	Available	vpc-0fb3c2e31ca102215   szs...	192.168.0.0/24	-	

操作

- 查看详细信息
- 创建日志
- 修改自动分配 IP 设置
- 编辑 IPv6 CIDR
- 编辑网络 ACL 关联
- 编辑路由表关联
- 共享子网
- 管理标签
- 删除子网

VPC > 子网 > subnet-0074cbfc4172b8fc7 > 修改自动分配 IP 设置

## 修改自动分配 IP 设置 信息

启用自动分配 IP 地址设置，以便为该子网中的新网络接口自动请求公有 IPv4 或 IPv6 地址。

### 设置

子网 ID

subnet-0074cbfc4172b8fc7

自动分配 IPv4 信息

☒ 启用自动分配公有 IPv4 地址

自动分配客户拥有的 IPv4 地址 信息

☐ 启用自动分配客户拥有的 IPv4 地址  
由于未找到客户拥有的池，选项已禁用。

取消 

保存

### 1.3、创建 Internet Gateway 并关联到 VPC

New VPC Experience  
Tell us what you think

VPC 控制面板 New

用 VPC 筛选

选择 VPC

VIRTUAL PRIVATE CLOUD

您的 VPC New

子网 New

路由表

互联网网关 New

#### 互联网网关 (2) 信息

创建互联网网关

<input type="checkbox"/>	Name	互联网网关 ID	状态	VPC ID	所有者
<input type="checkbox"/>	mk1210-igw	igw-0881bd5cbc2338d1b	Attached	vpc-06a844636f1342736   mk1210-vpc	583217706765
<input type="checkbox"/>	-	igw-bc5524c7	Attached	vpc-0a939170	583217706765

VPC > 互联网网关 > 创建互联网网关

## 创建互联网网关 信息

互联网网关是将 VPC 连接到互联网的虚拟路由器。要创建新的互联网网关，请在下方指定网关的名称。

### 互联网网关设置

名称标签

使用“Name”键和您指定的值创建一个标签。

szsd-igw

### 标签 - 可选

标签是分配给 AWS 资源的标记。每个标签都由一个键和一个可选值组成。您可以使用标签来搜索和筛选资源或跟踪 AWS 成本。

键

值 - 可选

Q Name X

Q szsd-igw X

移除

添加新标签

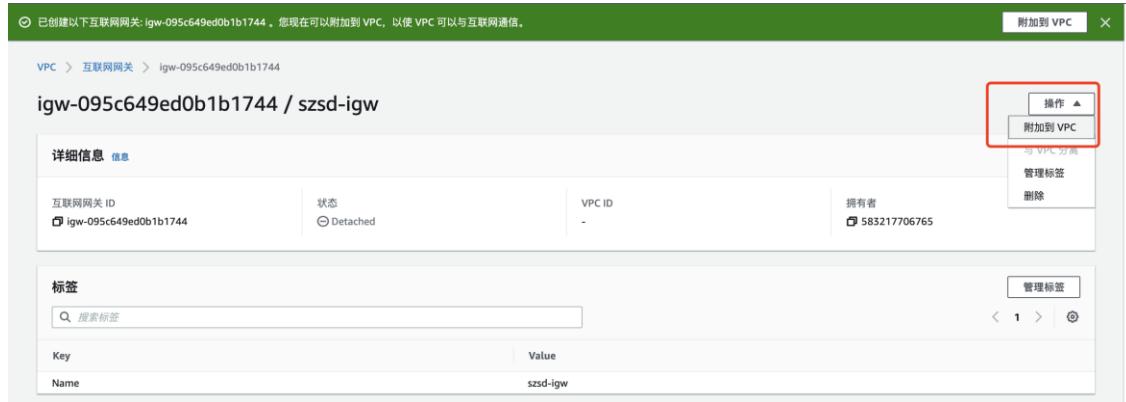
您可以再添加 49 个 标签。

取消 

创建互联网网关



## 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

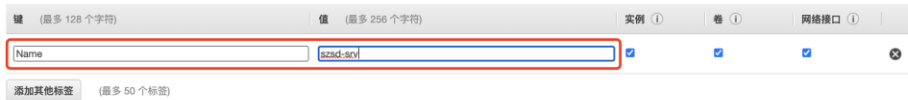


存储保持默认，点击下一步。

增加标签，方便后续使用和管理。点击下一步。

## 步骤 5: 添加标签

标签由一个区分大小写的键值对组成。例如，您可以定义一个键为“Name”且值为“Webserver”的标签。可将标签副本应用于卷和/或实例。标签将应用于所有实例和卷。有关标记 Amazon EC2 资源的信息，请参阅“了解更多”。



#### 步骤 6: 配置安全组

安全组是一组防火墙规则，用于控制您的实例的流量。在此页面上，您可以添加规则来允许特定流量到达您的实例。例如，如果您希望设置一个 Web 服务器，并允许 Internet 流量到达您的实例，请添加相应的规则来允许不受限制地访问 HTTP 和 HTTPS 端口。您可以创建一个新安全组或从下面选择一个现有安全组。有关 Amazon EC2 安全组的信息，请参阅[“了解更多信息”](#)。

分配安全组 ☒ 创建一个新的安全组

☐ 选择一个现有的安全组

安全组名称:

描述: launch-wizard-1 created 2021-03-12T09:36:24.360+08:00

类型	协议	端口范围	来源	描述
SSH	TCP	22	自定义 0.0.0.0/0	例如 SSH for Admin Desktop

添加规则

**警告**  
设置为 0.0.0.0/0 的源规则允许所有 IP 地址访问您的端口。我们建议将安全组规则设置为仅允许从已知的 IP 地址进行访问。

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。

### 选择现有密钥对或创建新密钥对

密钥对由 AWS 存储的公有密钥和您存储的私有密钥文件构成。它们共同帮助您安全地连接到您的实例。对于 Windows AMI，需使用私有密钥文件获取登录实例所需的密码。对于 Linux AMI，私有密钥文件让您通过 SSH 安全地登录实例。

注意：所选的密钥对将添加到为此实例授权的密钥组中。了解更多关于 [从公有 AMI 删除现有密钥对](#) 的信息。

☒ 创建新 密钥对

密钥对名称



您必须下载私有密钥文件(\*.pem 文件)才能继续操作。请将其存储在安全且易于访问的位置。您无法在创建文件后再次下载此文件。

取消

启动新实例

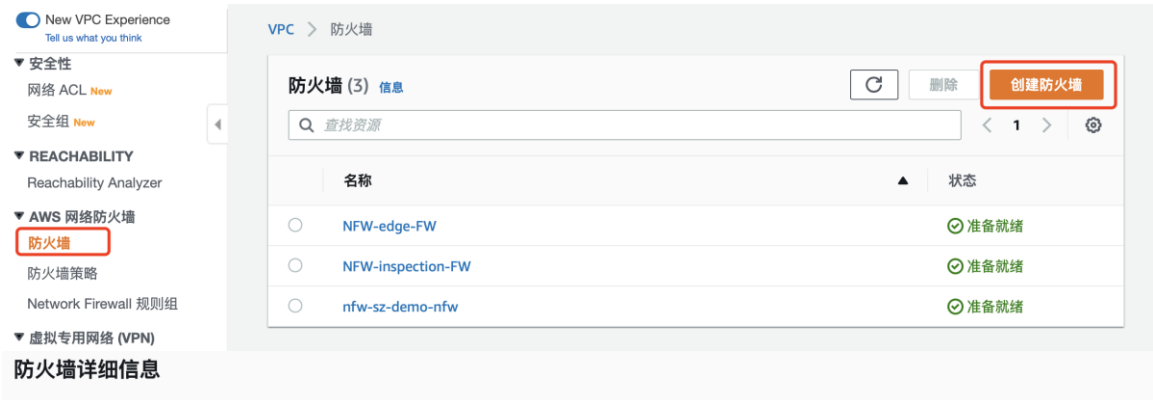
预计一分钟后，实例会完成创建并完成 2 阶段的健康检查后，进入可使用状态。可继续进行下面的实验。

## 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



名称

为防火墙输入唯一的名称。

szsd-fw

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

防火墙用于监控和控制 VPC 的网络流量。

描述可以包含 0-256 个字符。

VPC

选择要在其上创建此防火墙的 VPC。

szsd-vpc

防火墙子网

您可以在多个可用区中部署防火墙，部署到每个可用区中的一个子网上。每个子网都必须至少具有一个可用 IP 地址。

可用区

子网

us-west-2a

szsd-fw-sub

移除

添加新子网

### 已关联防火墙策略

防火墙策略包含一个规则组列表，用于定义防火墙如何检查和管理 Web 流量。您可以在创建防火墙后，配置关联的防火墙策略。

选择想要关联防火墙策略的方式

☒ 创建和关联空的防火墙策略

☐ 关联现有的防火墙策略

新的防火墙策略名称

为防火墙策略输入一个唯一的名称。

szsd-policy

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 - optional

防火墙策略用于定义防火墙如何监控和控制 VPC 的网络流量。

描述可以包含 0-256 个字符。

### 防火墙标签

键

值 - 可选

Q Name

X

Q szsd-fw

X

移除

添加新标签

您最多还可以再添加 49 个标签。

取消

创建防火墙

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

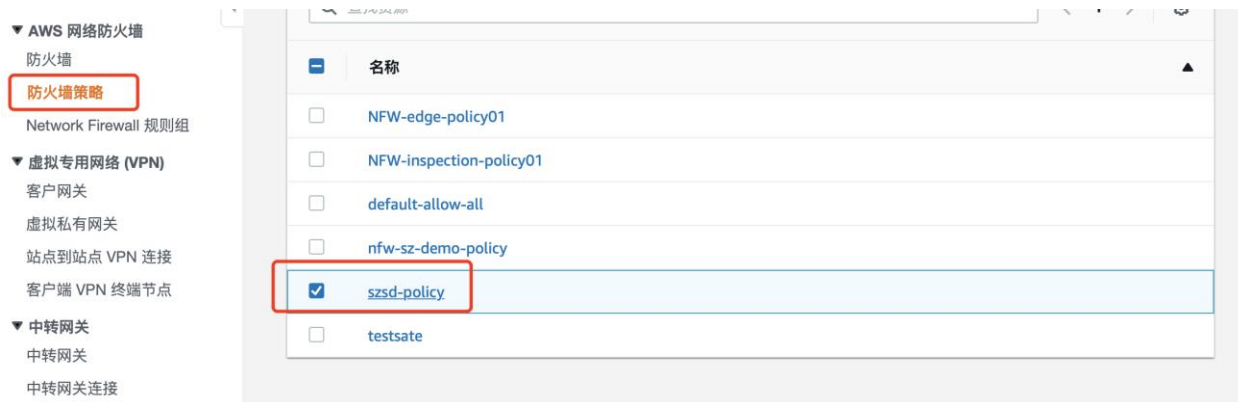
<https://aws.amazon.com/cn/premiumsupport/knowledge-center/new-user-accounts-linux-instance/>

Windows 参考如下链接 ssh 访问 EC2

[https://docs.aws.amazon.com/zh\\_cn/AWSEC2/latest/UserGuide/putty.html](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



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

编辑

要对不匹配任何无状态规则的数据包执行的操作。

对完整数据包的操作	对分段数据包的操作
转发至有状态规则组	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。

添加规则

信息

在规则组中添加所需的无状态规则。所添加的每个规则都会在以下“规则”表中列出。

优先级

首先评估优先级较低的规则。规则组中的每个规则都必须具有唯一的优先级设置。

1

协议

传输协议检查以下内容。

选择选项

TCP

×

Protocol: 6

源

源 IP 地址和地址检查范围(以 CIDR 表示法显示)。

任何 IPv4 地址

▼

0.0.0.0/0

源端口范围

源端口和端口检查范围。这仅适用于 TCP 和 UDP 协议。

任何端口

▼

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 IPv4 地址

▼

0.0.0.0/0

目标端口范围

目标端口和端口检查范围。这仅适用于 TCP 和 UDP 协议。

自定义

▼

22

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。

-

▼

添加规则

规则 (1)

删除

查找资源

< 1 > ⚙

	优先级	协议	源	目标	源端口范围	目标端口范围	操作	自定义操作	掩码	标记
<input type="radio"/>	1	TCP	0.0.0.0/0	0.0.0.0/0	0-65535	22	放弃	-	-	-

取消

创建并添加

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。

▼ REACHABILITY

Reachability Analyzer

▼ AWS 网络防火墙

防火墙

防火墙策略

**Network Firewall 规则组**

▼ 虚拟专用网络 (VPN)

客户网关

虚拟私有网关

站点到站点 VPN 连接

客户端 VPN 终端节点

▼ 中转网关

中转网关

中转网关连接

中转网关路由表

中转网关多播

网络管理器

▼ 流量镜像

名称	类型
<input type="checkbox"/> Default-allow-all	stateless
<input type="checkbox"/> domainlist	stateful
<input type="checkbox"/> nfw-sz-demo-rule	stateful
<input type="checkbox"/> nfw-sz-demo-stateless	stateless
<input checked="" type="checkbox"/> <b>szsd-stateless-rg</b>	stateless
<input type="checkbox"/> test2	stateful

规则 (1)

**编辑规则**

优先级	协议	源	目标	源端口范围	目标端口范围	操作	自定义操作
1	TCP	0.0.0.0/0	0.0.0.0/0	0-65535	22-22	放弃	-

VPC > Network Firewall 规则组 > szsd-stateless-rg > 编辑规则

## 编辑规则 信息

选择一个要编辑或删除的规则。要添加新规则，请选择“添加规则”。

规则 (1)	优先级	协议	源	目标	源端口范围	目标端口范围	操作	自定义操作	掩码	标记
<input checked="" type="radio"/>	1	TCP	0.0.0.0/0	0.0.0.0/0	0-65535	22-22	放弃	-	-	-

## 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

### ▼ REACHABILITY

Reachability Analyzer

### ▼ AWS 网络防火墙

防火墙

防火墙策略

**Network Firewall 规则组**

### ▼ 虚拟专用网络 (VPN)

客户网关

虚拟私有网关

站点到站点 VPN 连接

客户端 VPN 终端节点

VPC > Network Firewall 规则组

Network Firewall 规则组 (6) 信息

创建网络防火墙规则组

<input type="checkbox"/>	名称	类型
<input type="checkbox"/>	Default-allow-all	stateless
<input type="checkbox"/>	domainlist	stateful
<input type="checkbox"/>	nfw-sz-demo-rule	stateful

VPC > Network Firewall 规则组 > 创建网络防火墙规则组

## 创建网络防火墙规则组 信息

### 规则组类型

☒ 有状态规则组

使用有状态规则组来检查通信流量上下文中的数据。

☐ 无状态规则组

使用无状态规则组检查单个数据包自身，而不在通信流量上下文中。

### 有状态规则组

#### 名称

为在您的有状态规则组中唯一的规则组输入名称。

szsd-statefull-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数来估计有状态规则组的容量需求。更新规则组时不能更改或超出设置。

1000

此容量必须大于或等于 1 且小于 10000。

#### 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
<input type="radio"/>	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。

DHCP 选项集 New

弹性 IP New

托管前缀列表 New

终端节点

终端节点服务

NAT 网关 New

对等连接

▼ 安全性

网络 ACL New

安全组 New

▼ REACHABILITY

Reachability Analyzer

▼ AWS 网络防火墙

防火墙

防火墙策略

Network Firewall 规则组

▼ 虚拟专用网络 (VPN)

客户网关

虚拟私有网关

站点到站点 VPN 连接

客户端 VPN 终端节点

▼ 中转网关

中转网关

中转网关连接

中转网关路由表

VPC > 防火墙策略

防火墙策略 (5) 信息

🔍 查找资源

< 1 > ⚙️

<input type="checkbox"/>	名称
<input type="checkbox"/>	NFW-edge-policy01
<input type="checkbox"/>	NFW-inspection-policy01
<input type="checkbox"/>	default-allow-all
<input type="checkbox"/>	nfw-sz-demo-policy
<input checked="" type="checkbox"/>	szsd-policy

New VPC Experience  
Tell us what you think

DHCP 选项集 New

弹性 IP New

托管前缀列表 New

终端节点

终端节点服务

NAT 网关 New

对等连接

▼ 安全性

网络 ACL New

安全组 New

▼ REACHABILITY

Reachability Analyzer

▼ AWS 网络防火墙

防火墙

防火墙策略

Network Firewall 规则组

▼ 虚拟专用网络 (VPN)

客户网关

虚拟私有网关

站点到站点 VPN 连接

客户端 VPN 终端节点

▼ 中转网关

中转网关

中转网关连接

中转网关路由表

szsd-policy 信息

Network Firewall 规则组 详细信息

无状态规则组 (1)

编辑优先级

删除

添加规则组 ▼

< 1 > ⚙️

<input type="checkbox"/>	优先级 ▲	名称 ▼	容量 ▼
<input type="checkbox"/>	1	szsd-stateless-rg	1000

无状态默认操作 编辑

要对不匹配任何无状态规则的数据包执行的操作。

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

有状态规则组 (0)

删除

添加规则组 ▲

创建并添加新的有状态规则组

将有状态规则组添加到防火墙策略

<input type="checkbox"/>	名称 ▼	容量 ▼
--------------------------	------	------

VPC > 防火墙策略 > szsd-policy > 添加我自己的有状态规则组

将有状态规则组添加到防火墙策略 信息

选择并添加您希望位于防火墙策略中的有状态规则组。

📘 防火墙策略可以与多个防火墙关联。修改防火墙策略会影响引用该策略的所有防火墙。  
要使用为您管理的规则组，请参阅 [AWS 合作伙伴网络 \(APN\) 集成](#)。

有状态规则组 (5)

🔍 Find resources

< 1 > ⚙️

<input type="checkbox"/>	Name
<input type="checkbox"/>	domainlist
<input type="checkbox"/>	nfw-sz-demo-rule
<input type="checkbox"/>	szsd-domain-filter-rg
<input checked="" type="checkbox"/>	szsd-statefull-rg
<input type="checkbox"/>	test2

取消 添加有状态规则组

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

#### 有状态规则组

##### 名称

为在您的有状态规则组中唯一的规则组输入名称。

szsd-domain-filter-rgl

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数来估计有状态规则组的容量需求。更新规则组时不能更改或超出设置。

1000

此容量必须大于或等于 1 且小于 10000。

##### 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。

#### 域列表 信息

##### 源域来名

列出要对其执行操作的域名。

.amazon.com

每行输入一个域名。

##### 协议

选择要检查的协议。

☒ HTTP

☒ HTTPS

##### 操作

当请求与此组中的域名匹配时要执行的操作。

☐ 允许

☒ 拒绝

取消

创建有状态规则组

将有状态规则组，关联到 szsd-policy。

DHCP 选项集 New

弹性 IP New

托管前置列表 New

终端节点

终端节点服务

NAT 网关 New

对等连接

▼ 安全性

网络 ACL New

安全组 New

▼ REACHABILITY

Reachability Analyzer

▼ AWS 网络防火墙

防火墙

防火墙策略

Network Firewall 规则组

▼ 虚拟专用网络 (VPN)

VPC > 防火墙策略

防火墙策略 (6) 信息

🔍 查找资源

< 1 > ⚙️

<input type="checkbox"/>	名称
<input type="checkbox"/>	NFW-edge-policy01
<input type="checkbox"/>	NFW-inspection-policy01
<input type="checkbox"/>	default-allow-all
<input type="checkbox"/>	nfw-sz-demo-policy
<input checked="" type="checkbox"/>	szsd-policy

New VPC Experience  
Tell us what you think

DHCP 选项集 New

弹性 IP New

托管前置列表 New

终端节点

终端节点服务

NAT 网关 New

对等连接

▼ 安全性

网络 ACL New

安全组 New

▼ REACHABILITY

Reachability Analyzer

▼ AWS 网络防火墙

防火墙

防火墙策略

Network Firewall 规则组

▼ 虚拟专用网络 (VPN)

客户网关

虚拟私有网关

站点到站点 VPN 连接

客户端 VPN 终端节点

▼ 中转网关

中转网关

中转网关连接

中转网关路由表

szsd-policy 信息

Network Firewall 规则组 详细信息

无状态规则组 (1)

编辑优先级

删除

添加规则组 ▼

< 1 > ⚙️

<input type="checkbox"/>	优先级 ▲	名称	容量 ▼
<input type="checkbox"/>	1	szsd-stateless-rg	1000

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。

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

有状态规则组 (0)

删除

添加规则组 ▲

创建并添加新的有状态规则组

将有状态规则组添加到防火墙策略

<input type="checkbox"/>	名称	容量 ▼
--------------------------	----	------

VPC > 防火墙策略 > szsd-policy > 添加我自己的有状态规则组

将有状态规则组添加到防火墙策略 信息

选择并添加您希望位于防火墙策略中的有状态规则组。

🔔 防火墙策略可以与多个防火墙关联。修改防火墙策略会影响引用该策略的所有防火墙。  
要使用为您管理的规则组，请参阅 [AWS 合作伙伴网络\(APN\)集成](#)。

有状态规则组 (5)

🔍 Find resources

编辑规则组 📄

🔄

< 1 > ⚙️

<input type="checkbox"/>	Name
<input type="checkbox"/>	domainlist
<input type="checkbox"/>	nfw-sz-demo-rule
<input checked="" type="checkbox"/>	szsd-domain-filter-rg
<input type="checkbox"/>	szsd-statefull-rg
<input type="checkbox"/>	test2

取消 添加有状态规则组

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。