# 天翼云 • 云下一代防火墙

# 用户使用指南

中国电信股份有限公司云计算分公司

# 目 录

# 1 产品介绍

## 1.1 产品定义

云下一代防火墙（CT-ECFW Extended Capacity Firewall）是专门为云计算环境设计的虚拟化网络安全产品，以虚拟主机形态，提供高性价比的云安全部署方案，为客户提供了下一代防火墙、高可用性（HA）、入侵防御（IPS）、病毒过滤（AV）、服务质量保证（QoS）、云沙箱、僵尸网络 C&C 防护、IP 信誉等丰富功能。

## 1.2 术语解释

### 1.2.1 云计算

云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池（资源包括网络，服务器，存储，应用软件，服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。

### 1.2.2 NFV

NFV，即网络功能虚拟化，Network Function Virtualization。通过使用 x86 等通用性硬件以及虚拟化技术，来承载很多功能的软件处理。

### 1.2.3 虚拟化技术

虚拟化（英语：Virtualization）是一种资源管理技术，是将计算机的各种实体资源，如服务器、网络、内存及存储等，予以抽象、转换后呈现出来，打破实体结构间的不可切割的障碍，使用户可以比原本的组态更好的方式来应用这些资源。

### 1.2.4 安全策略

安全策略是网络安全设备的基本功能，控制安全域间/不同地址段间的流量转发。默认情况下，网络安全设备会拒绝设备上所有安全域/地址段之间的信息传输。

### 1.2.5 NAT

网络地址转换（Network Address Translation）简称为 NAT，是将 IP 数据包包头中的 IP 地址转换为另一个 IP 地址。当 IP 数据包通过设备时，设备会把 IP 数据包的源 IP 地址和/或者目的 IP 地址进行转换。

### 1.2.6 分布式拒绝服务（DDOS）

分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DDoS 攻击，从而占用目标大量网络资源，最终会造成目标网络瘫痪。

### 1.2.7 病毒过滤

病毒过滤功能（Anti Virus）能够为用户提供高速、高性能以及低延迟的病毒过滤解决方案。配置病毒过滤功能后，设备能够探测各种病毒威胁，例如恶意软件、恶意网站等，并且根据配置对发现的病毒进行处理。

### 1.2.8 入侵防御

入侵防御系统（Intrusion Prevention System）简称 IPS，能够实时监控多种网络攻击并根据配置对网络攻击进行阻断等操作。系统的入侵防御功能能够实现完整的基于状态的检查，从而极大降低误报率。

### 1.2.9 攻击防护

网络中存在多种防不胜防的攻击，如侵入或破坏网络上的服务器、盗取服务器的敏感数据、破坏服务器对外提供的服务，或者直接破坏网络设备导致网络服务异常甚至中断。作为网络安全设备的云下一代防火墙安全产品，具备攻击防护功能来检测各种类型的网络攻击，从而采取相应的措施保护内部网络免受恶意攻击。

### 1.2.10 云沙箱

1.2.1 当前的恶意软件大多具备强大的逃逸能力，而网络攻击可能使用零日攻击（APT）的方式，传统的防病毒引擎很难发现它们。云沙箱通过云端海量的恶意样本库、集群的虚拟执行检测引擎可以有效发现这些攻击行为，帮助客户有效的遏制由此带来的风险，如敏感信息泄露、业务中断等。

### 1.2.11 僵尸网络 C&C 防护

僵尸网络，是指采用一种或多种传播手段，使大量主机感染僵尸程序，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络，对用户的网络安全以及数据安全造成很大的威胁隐患。僵尸网络 C&C 防护功能能够根据特征库中的地址及时发现用户内网的僵尸主机，并且根据配置对发现的僵尸主机进行处理，从而避免发生进一步的威胁攻击

### 1.2.12 IP 信誉

IP 信誉包括僵尸主机、垃圾邮件、Tor 节点、失陷主机、暴力破解等特征的风险 IP，在云下一代防火墙可按照 IP 信誉特征库进行安全防护。

### 1.2.13 主备模式（HA）

部署 HA 需两台采用弹性云主机规格、云下一代防火墙版本、扩展功能完全相同进行配置，流量通过云平台所提供的虚拟 IP（VIP）进行转发。当一台设备不可用或者不能处理来自客户端的请求时，该请求会及时转到可用设备来处理，这样就保证了网络通信的不间断进行，极大地提高了通信的可靠性。

## 1.3 产品功能

### 1.3.1 功能介绍

| 产品功能 | 功能解释 |
| --- | --- |
| 应用识别 | 在进行分析报文头的基础上，结合不同的应用协议特征库综合判断所属的应用 |
| 监控统计 | 对设备数据进行统计，并以柱状图、折线图、表格、报表、日志等方式呈现出来，帮助用户通过统计数据掌握设备状况，排查问题 |
| 用户认证 | 对用户进行识别，通过认证的用户可以访问对应的管理资源 |
| 访问控制 | 划分安全区域和非安全区域，区域之间的访问基于安全策略进行控制。 |
| 入侵防御 | 实时监控多种网络攻击并根据配置对网络攻击进行阻断等操作 |
| 病毒过滤 | 探测各种病毒威胁，例如恶意软件、恶意网站等，并且根据配置对发现的病毒进行处理。 |
| 页面访问控制 | 针对不同用户的权限对页面的访问进行区别 |
| 带宽管理 | 能够管理和优化网络带宽，提高用户的网络体验和带宽资源利用率。 |
| 高可用性（HA） | 在通信线路或设备产生故障时提供备用方案，从而保证数据通信的畅通，有效增强网络的可靠性 |
| 授权管理 | 集中管理功能授权并可进行不同种类授权的统一下发 |
| 云沙箱 | 基于云端架构的恶意软件虚拟运行环境，发现未知威胁，多重静态检测引擎快速过滤正常文件及已知威胁，提升沙箱检测效率。 |
| 僵尸网络 C&C 防护 | 监控 C&C 连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏。 |
| IP 信誉 | 识别过滤各种已知风险 IP，根据配置对风险 IP 进行记录或阻断处理。 |

### 1.3.2 应用识别

- 全新一代基于应用特征、行为和关联信息的应用识别
- 支持应用类别、风险等级等多维度的应用定义

- 支持多达几千种的应用特征库
- 应用特征库支持网络实时更新

### 1.3.3 监控统计

- 支持 URL 日志、NAT 日志、会话日志、威胁日志等
- 支持实时流量统计和分析功能
- 支持安全事件统计功能
- 支持应用的多维度统计监控，包括应用风险、类别、特征、所用技术等
- 支持云应用的多维统计监控
- 支持报表功能
- 支持日志本地存储

### 1.3.4 用户认证

- 支持本地用户认证
- 支持外部服务器用户认证(RADIUS、LDAP、MS AD)
- 支持 AD/LDAP 用户/组织结构同步
- 支持 Web 认证
- 支持 MS AD 用户组同步
- 支持 Web 认证后的 SSO

### 1.3.5 访问控制

- 基于深度应用识别的访问控制
- 基于应用/角色的安全策略
- 丰富的路由特性
- 强大的 NAT 及 ALG

### 1.3.6 入侵防御

- 基于状态、精准的高性能攻击检测和防御
- 实时攻击源阻断、IP 屏蔽、攻击事件记录
- 支持针对 HTTP、SMTP、IMAP、POP3、VOIP 等几十种协议和应用的攻击检测和防御
- 支持自定义入侵防御特征

- 提供预定义防御配置模板
- 提供几千种特征的攻击检测和防御，特征库支持网络实时更新

### 1.3.7 病毒过滤

- 基于流、低延时、高并发、高性能的病毒过滤
- 支持大病毒文件的扫描
- 实时病毒连接阻断，病毒事件记录
- 支持常见病毒传输协议 HTTP、FTP 及各种邮件协议扫描
- 超百万的病毒特征库，病毒库可以在线更新、本地更新

### 1.3.8 页面访问控制

- 基于角色、时间、优先级、页面类型等条件的 Web 网页访问控制
- 支持自定义 URL 类别
- 支持千万级的URL 特征库，URL 库支持网络实时更新

### 1.3.9 带宽管理

- 根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan 等信息划分管道
- 支持两层八级管道嵌套的带宽限制和保证
- 支持最大带宽限制、最小带宽保证、每 IP 或每用户的最大带宽限制和最小带宽保证
- 基于时间和优先级的差分服务，支持带宽均分策略
- 对剩余带宽根据优先级进行弹性分配
- 主动抑制服务器端传送流量

### 1.3.10 高可用性 (HA)

- 主/备模式（A/P）
- 支持配置、会话同步
- 支持 128 组HA 数量
- 支持修改虚拟MAC 地址

### 1.3.11 授权管理

- 支持迁移，重装时，不更换授权文件

- 支持公网授权验证方式
- 支持内网授权验证方式
- 支持授权自动分发
- 支持授权回收、授权调度。

### 1.3.12 云沙箱

- 支持 SMTP、POP3、IMAP4、FTP 等协议类型的检测。
- 支持 APK、JAR、MS-OFFICE、PDF、SWF、RAR、ZIP 等文件类型的检测
- 对 PE 文件在上传云沙箱前进行文件可信证书检测
- 在云沙箱配置中新增全局、profile、预定义及自定义等配置选项
- 独立出沙箱日志类型展示、支持行为报告 PDF 文件导出

### 1.3.13 僵尸网络 C&C 防护

- 通过监控 C&C 连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏
- 定期僵尸网络服务器地址升级更新
- 支持 C&C IP 和域名两种方式检测
- 支持 TCP 和HTTP、DNS 协议检测
- 支持 C&C IP 和域名白名单

### 1.3.14 IP 信誉

- 对僵尸肉鸡、垃圾邮件发送者、Tor 节点、失陷主机、暴力破解等风险 IP 的流量进行识别和过滤
- 可对不同类别风险 IP 流量进行记录日志、丢弃数据包或阻断一定时间。
- 定期 IP 信誉特征库升级更新

## 1.4 产品优势

### 1.4.1 具有全面适应能力的软件防火墙

在虚拟化环境中，用户的计算、存储、数据资源都是运行在服务器的虚拟机上，在考虑安全防护的设计时，云下一代防火墙安全产品可在虚拟机上实现快速灵活的部署，支持在VMware、KVM、XEN、Hyper-V 等主流虚拟化平台上运行，可串联或单臂连接到虚拟网络中（如：虚拟应用服务器前端的网关，或者是 VPC 网络的边界网关），为虚拟网络或应用提供专业的边界网络安全防护功能。

以虚拟化的形式部署设备，能够克服物理防火墙的限制，在虚拟化环境中可部署于更加靠近 VM 的位置，对于 VM 主机内部流量进行过滤，实现同时对于南北向和东西向流量的安全防护。同时，用户可以根据网络搭建需求，弹性调配和管理网络资源等，并且能够按需进行灵活迁移，充分发挥虚拟化优势。

### 1.4.2 拥有专业 NGFW 安全防护功能

云下一代防火墙安全产品拥有与 NGFW 相同的操作系统，具有丰富的网络安全防护功能，对网络威胁进行防御，能够满足企业分支及公有云多租户环境中的网络安全需求。

- 具备精细化应用管控，可为用户提供多维的应用风险分析和筛选，以及灵活的安全控制，包括策略阻止、会话限制、应用引流和智能流量管理等。同时，还具备入侵防御、病毒过滤、攻击防护、NAT 等功能，满足客户对安全访问、应用识别和控制等需求。
- 具备 HA 组网能力，满足配置和会话同步的要求，从而实现高可靠的冗余部署，保障用户业务的不间断连续运营。

### 1.4.3 结合云平台的安全可视化管理

数据中心在云化过程中给网络安全管理带来了挑战，云下一代防火墙安全产品进行便捷的虚拟网络管理，为云环境中的独立租户提供专属的安全隔离和策略保护。同时，可实现基于快照的系统快速恢复，在虚拟设备出现问题或宕机的情况下，可通过快照存储的上一时间的配置进行快速恢复，即刻就能在原有虚拟机或者新的虚拟机上启动虚拟防火墙设备。

云下一代防火墙安全产品具有一致的管理界面，图形化交互直观易用。具备各种日志记录查询功能，能够有效记录网络情况，并提供实时流量和安全事件的报表统计功能，帮助管理员全面掌握网络运行状态，提高运维效率。

### 1.4.4 提供多种自动化部署方案

云下一代防火墙安全产品适合在公有云和私有云中部署，可为公有云和私有云客户提供自动化的网络安全解决方案，抵御外部的网络攻击。借助虚拟化的优势特性，云下一代防火墙安全产品可按需自动化部署和扩展安全服务资源，并可与现有的云计算管理平台进行紧密整合，将管理和安全防护能力直接深入到虚拟化架构中，可伴随着客户或虚拟业务资源的需求增长和缩减。

可为具有开发能力的客户提供完成初始化部署的方案，并提供二次开发对接接口；可为 OpenStack 的客户提供替换源生 vRouter 以及 FWaaS 的整体交付方案；可为致力于方案解耦的客户提供符合国际化标准的开源开放 NFV 集成方案。

# 2 购买指南

## 2.1规格

云下一代防火墙分为基础功能和扩展功能，基础功能必选，扩展功能可选。

| 基础功能 | 扩展功能（选购） | | |
|---|---|---|---|
| | 带宽管理（QoS） | 防病毒（AV） | URL 过滤 |
| 包括应用识别、监控统计、入侵防御（IPS）、应用层访问控制、用户认证等功能 | 应用层流量带宽控制 | 防病毒功能及最新病毒特征库 | URL 特征库 |
| | 云沙箱<br>（仅适用旗舰版） | 僵尸网络C&C 防护<br>（仅适用旗舰版） | IP 信誉<br>（仅适用旗舰版） |
| | 未知威胁安全防护 | 阻断僵尸网络/勒索软件等高级威胁进一步破坏 | IP 信誉库 |

云下一代防火墙分为三个版本，不同版本的最大处理流量、最大并发连接数、每秒新建连接数不同。对应所需的云主机配置也不同。详见下表，

| 版本 | 最大处理流量 | 最大并发连接数 | 每秒新建连接数 | 云主机配置 |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 基础版 | 100M | 50K | 20K | 2 核 CPU+2G 内存+40G 系统盘 |
| 高级版 | 200M | 250K | 40K | 2 核 CPU+4G 内存+40G 系统盘 |
| 旗舰版 | 4G | 2500K | 80K | 4 核 CPU+8G 内存+40G 系统盘+100G 数据盘 |

云下一代防火墙按照不同版本为基础功能和扩展功能分别定价。

| 版本 | 基础功能 | 防病毒（AV） | 带宽管理（QoS） | URL 过滤 | 云沙箱 | 僵尸网络 C&C 防护 | IP 信誉 |
|---|---|---|---|---|---|---|---|
| 基础版 | 1546 元/个/月 | 213 元/个/月 | 133 元/个/月 | 133 元/个/月 | 无 | 无 | 无 |
| 高级版 | 3866 元/个/月 | 533 元/个/月 | 333 元/个/月 | 333 元/个/月 | 无 | 无 | 无 |
| 旗舰版 | 7733 元/个/月 | 1066 元/个/月 | 666 元/个/月 | 666 元/个/月 | 243 元/个/月 | 243 元/个/月 | 243 元/个/月 |

## 2.2购买

云下一代防火墙以镜像方式承载，在购买授权前需要开通一台云主机承载业务，云主机的开通过程参照 3.1 开通说明，完成云主机的部署后，即可订购产品授权。

1、在天翼云官网的产品列表找到安全产品组的云下一代防火墙，点击进入产品的介绍页面，点击【立即订购】即可进入订购页面；也可以再控制中心，找到安全产品组的云下一代防火墙，点击“  ”也可以跳转订购页面。

2、设置实例名称，选择所需版本和扩展功能（扩展功能为非必选项）。

3、选择部署方式：“单节点”为单机部署方式，“主备模式”为 HA 高可用部署方式，选择主

备模式需要准备两台云主机承载业务。

4、提供产品序列号和承载云墙的主机的弹性 IP 以及技术人联系方式。序列号获取方式参照 3.1 开通说明。

注：云下一代防火墙的开通以交付授权为完成节点，后续免费提供方案和部署支撑，请确保在购买云下一代防火墙之前，有熟悉网络环境你的对接人以及有合理的业务切割时间。


# 2.3升级

规格变更的过程会导致虚机重启、网络以及业务的中断，所以还请慎重进行规格变更。

升级操作分为规格升级和功能扩展两个部分，需要单独进行。


云下一代防火墙实例
立即购买
实例名称
版本
部署模式
扩展功能
开通时间
截止时间
授权文件
操作
高级版
主备模式
带宽管理（QoS）
URL过滤
防病毒（AV）
2020-04-21 11:32:19
2020-05-21 11:32:19
已过期
升级版本 升级功能 续订
高级版
主备模式
URL过滤
带宽管理（QoS）
防病毒（AV）
2020-04-21 11:32:27
2020-05-21 11:32:27
已过期
升级版本 升级功能 续订
共 2 条
10条/页
1
前往 1 页

1、升级版本


升级版本
实例名称:
部署模式:
主备模式
版本:
标准版
高级版
旗舰版
四层吞吐量8Gbps，七层吞吐量4Gbps，并发连接数2500K，每秒新建连接数80K；推荐最低配置：4核CPU 8G内存 40G系统盘 100G数据盘。
扩展功能:
带宽管理（QoS）
URL过滤
防病毒（AV）
序列号 1:
弹性IP 1:
序列号 2:
弹性IP 2:
联系电话:
请留一个技术人员联系电话，如有问题便于取得联系。
费用总计:
0.00元
（预计3个工作日完成升级授权，请到控制中心下载授权并做授权导入）
确 定
我已阅读，理解并接受《云下一代防火墙协议》

2、升级功能


## 2.4续订

在 console 页面实例列表点击【续订】即可进入续订的配置页面，续订操作是在原实例到期时间的基础上增加使用时长。

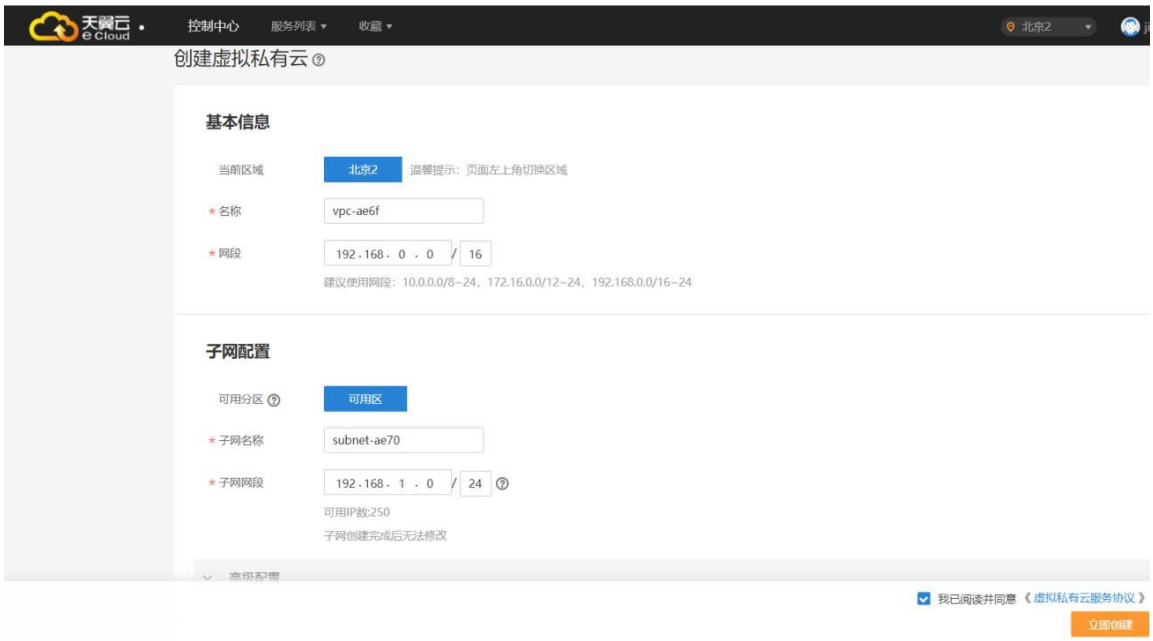

## 2.5退订

3.1.1. 除了产品试用期间可退订之外，云下一代防火墙安全产品均不支持业务退订。

# 3 快速入门

## 3.1开通说明

1、在天翼云控制台中选择并创建虚拟私有云(VPC)

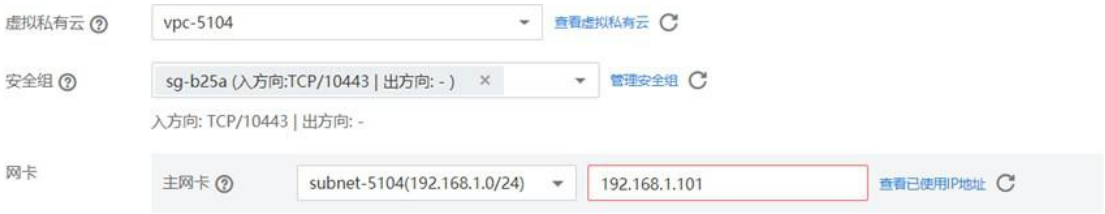




2、在控制台选择弹性云服务器，并选择购买弹性云服务器

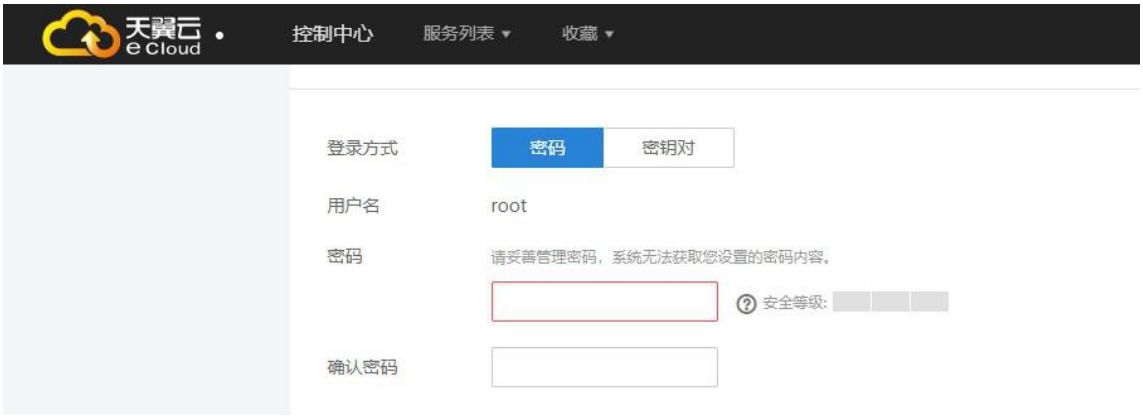

1） 计费方式根据需求去选择，区域选择应与上面所创建虚拟私有云（VPC）对应，具体系统配置还请参照云下一代防火墙安全产品规格


2） 选择云下一代防火墙安全产品的镜像，硬盘保持默认


3） 按照需求创建网卡，并选择之前所创建的虚拟私有云以及其子网，安全组（开放的端口号）这边选择默认所有（用户可根据需求去修改安全组规则）

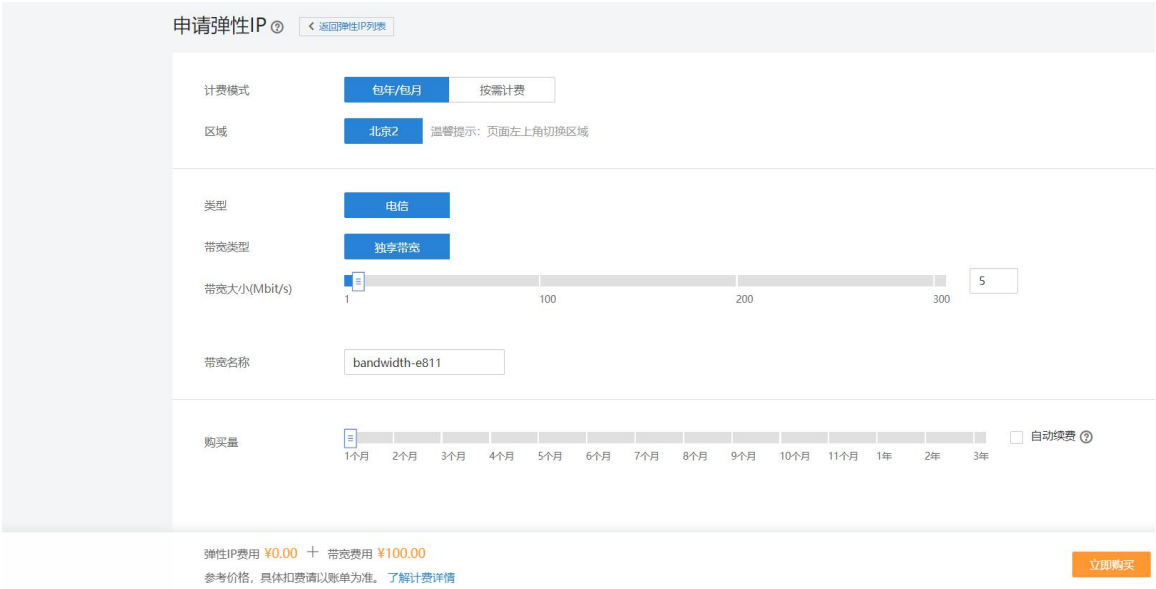



4） 给云服务器设置登陆密码，高级配置不需要配置，最终点击购买

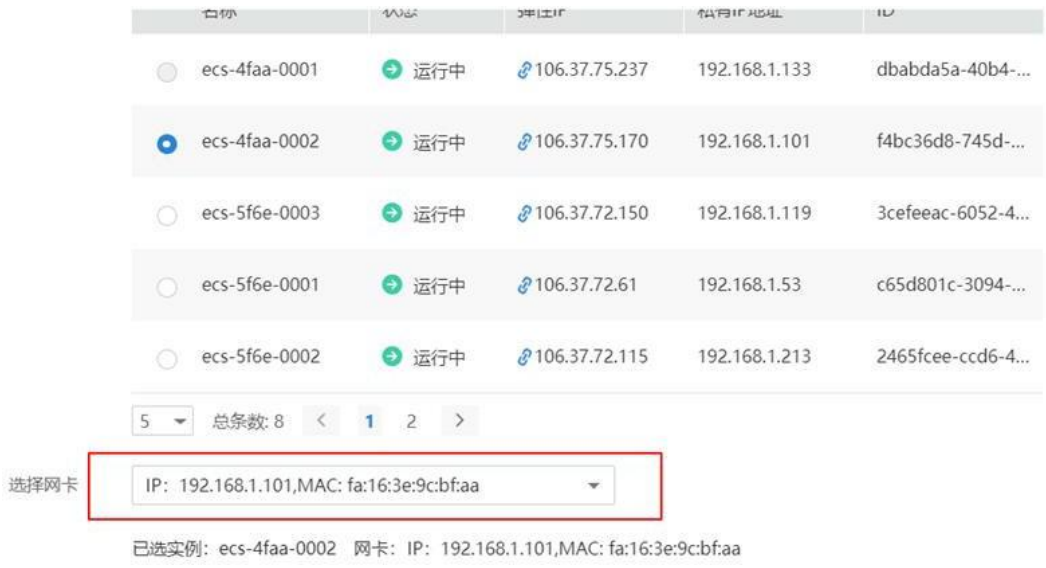



3、绑定弹性 IP

1）云下一代防火墙需要公网 IP，所以需要额外购买弹性 IP，点击网络中的弹性 IP，选择期限和带宽


2）将弹性 IP 与云下一代防火墙的管理子网绑定

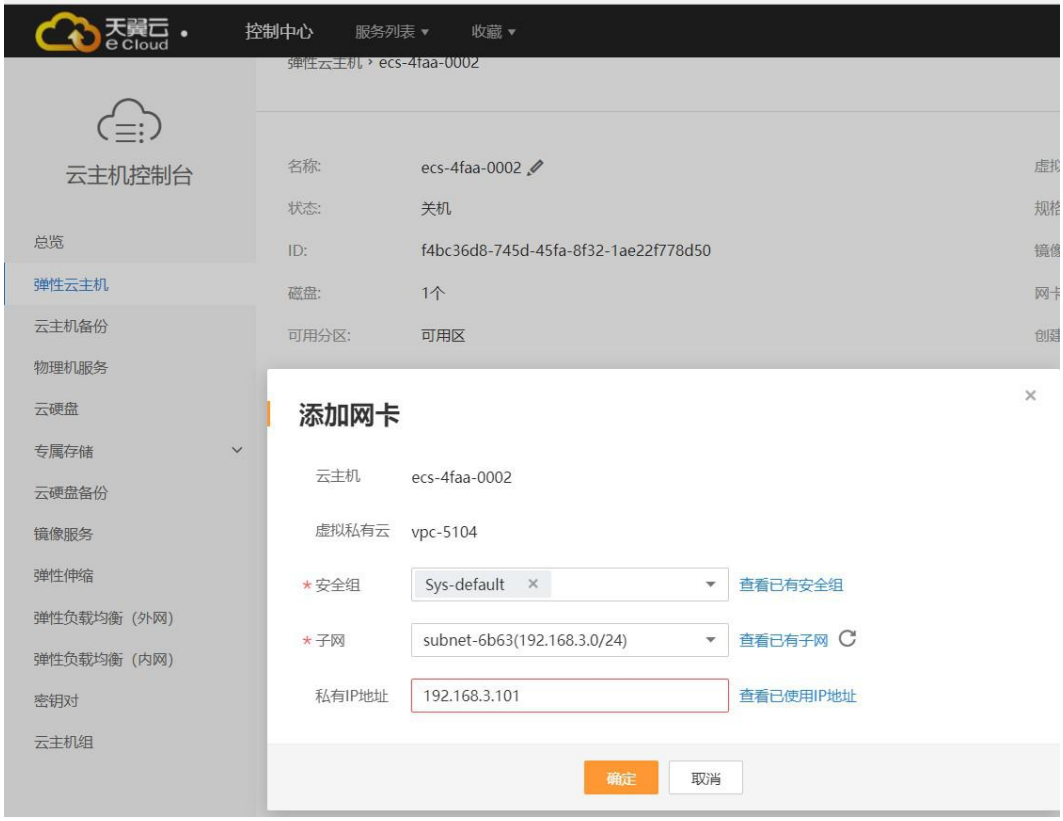




4、查看云下一代防火墙安全产品的安装情况

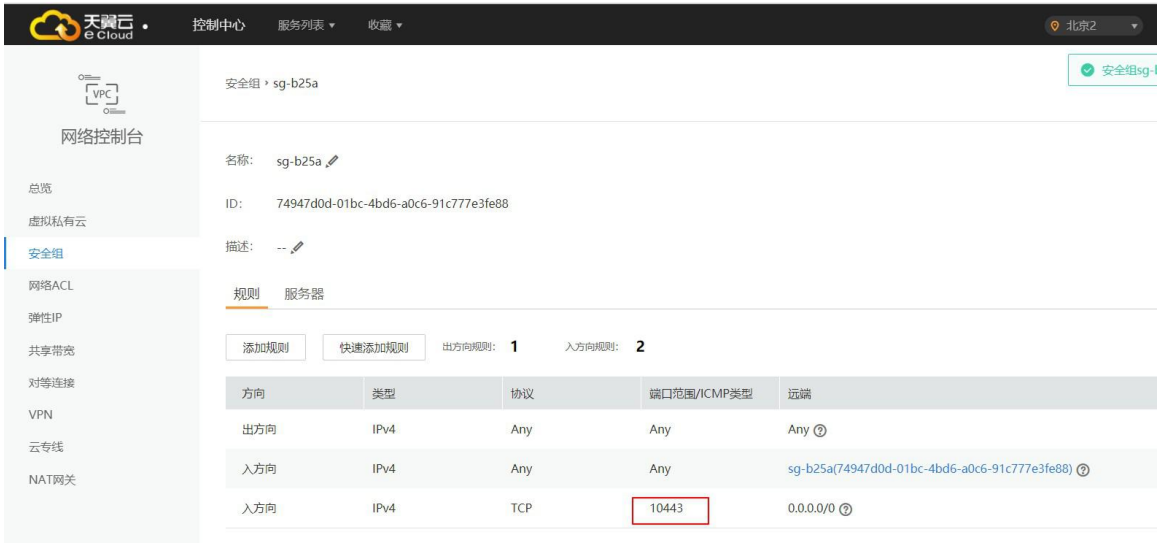

## 5、添加网卡

### 1） 如果需要添加网卡，关闭云下一代防火墙

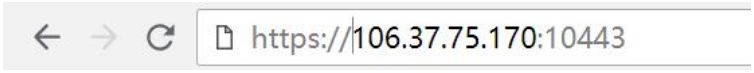

### 2） 点击关闭之后的云下一代防火墙，选择网卡并点击添加


6、在安全组下放行管理组的端口




7、用浏览器（IE11 及以上或 Chrome）https 访问所绑定的弹性公网 IP 所放行的端口号，即可操作云下一代防火墙安全产品的 WEIUI 界面




默认用户名为：请联系400客户获取

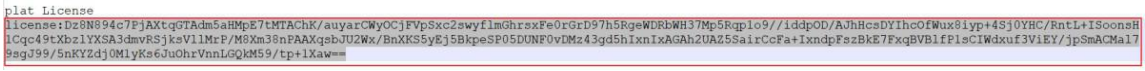
默认密码为：请联系400客户获取

8、进行授权

产品公测期间，每个云下一代防火墙产品均有 1 个月的免导入 license 试用的时间。

1）购买云下一代防火墙产品后，license 会发到天翼云账号所绑定的邮箱（如有变动可另行提供）。用户在邮箱中查看云下一代防火墙的证书 license


2）复制 license：到==的所有内容

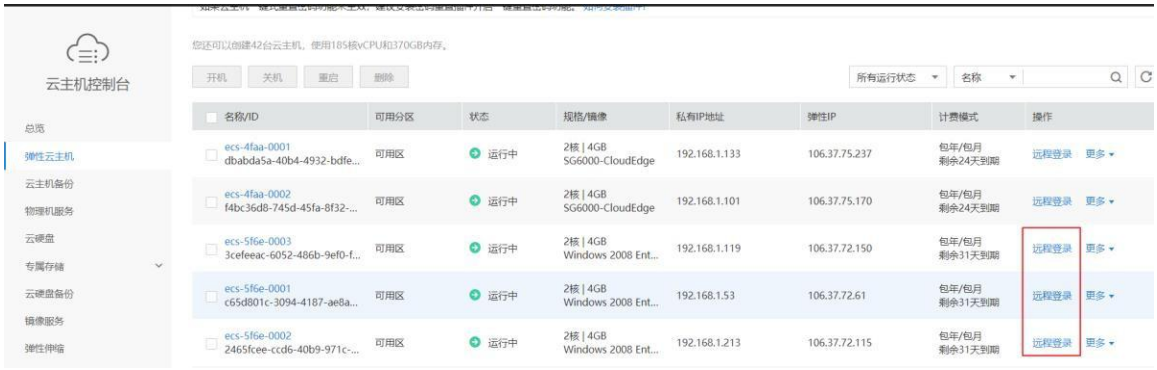


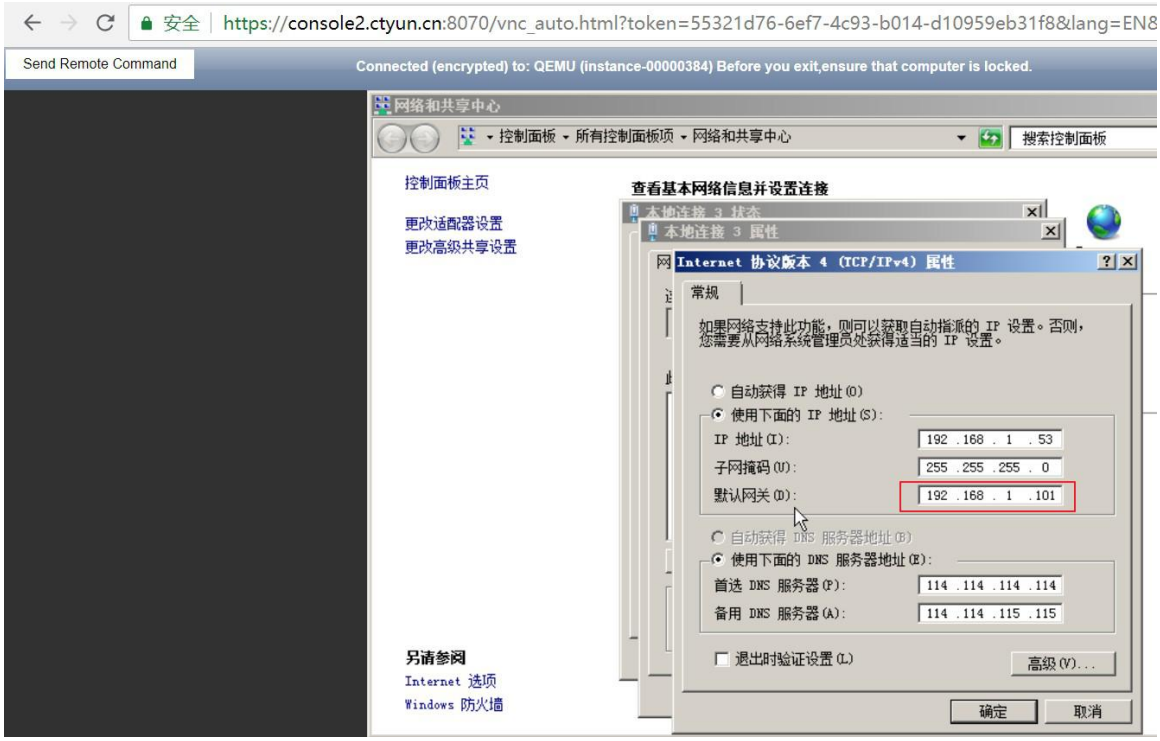

3）粘贴到云下一代防火墙的许可证手动输入框子内，并点击确认

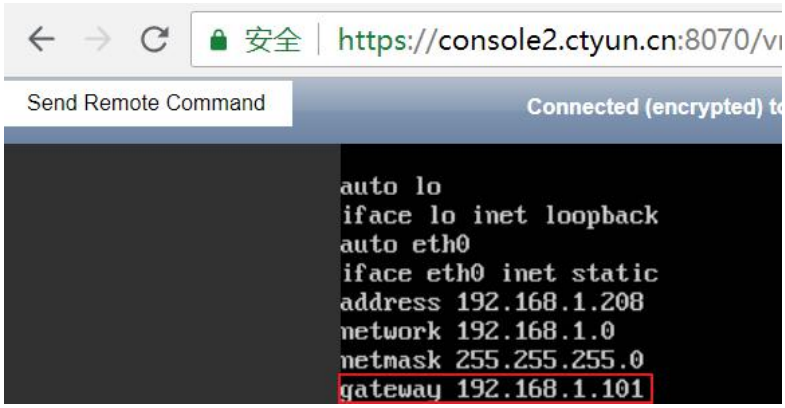

# 3.2开启防护

1、进行安全域和 IP 地址的配置，弹性 IP 绑定的接口为 trust 区域，IP 地址要与天翼云所配置的网卡地址一致


2、在虚拟私有云（VPC）内的所有服务器上修改网关，网关指向云下一代防火墙安全产品





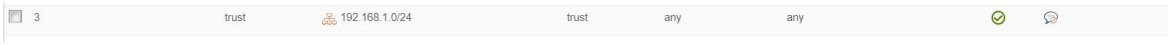

# 3.3安全设置

在云下一代防火墙安全产品上配置一条访问控制策略（此处配置的为全通策略）。由于全通策略缺乏一定的安全性，所以在客户业务运行正常的情况下，还请自行根据需求更换为明细的安全策略，如果采用全通策略，请直接略过明细的安全策略配置步骤。


1、在云下一代防火墙安全产品上配置 SNAT 策略

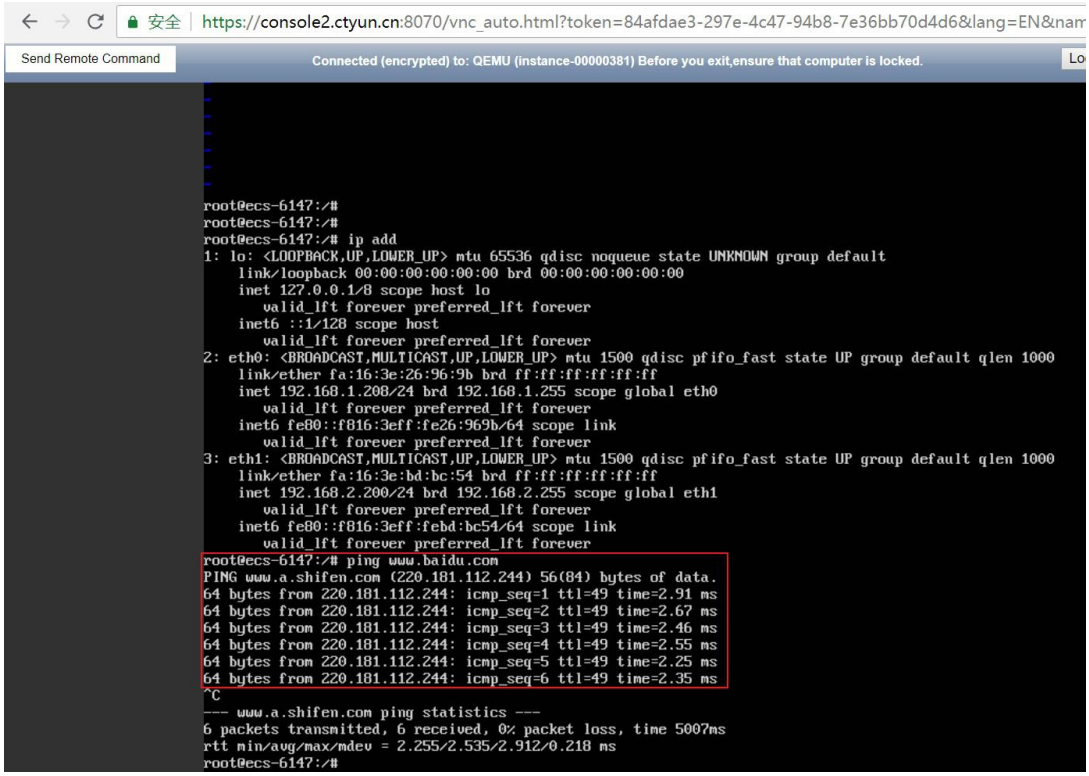
1） 分别对应 VPC 内的服务器，这里将出流量源地址转换成出接口 IP（云下一代防火墙安全产品 e0/0 接口地址）。


2） 明细的安全策略配置：设置 SNAT 的安全策略，放行内网访问外网的数据流量




3） 关闭所创建云下一代防火墙安全产品的源/目的检查（点击弹性云服务器名称进入网卡选项）

4）验证 SNAT 策略，配置完 SNAT 后服务器可以访问外网


2、在云下一代防火墙安全产品上配置三条 DNAT 策略

1）将访问弹性 IP 所绑定的 e0/0 接口地址（192.168.1.101）的 FTP 服务、SSH 服务、远程控制服务映射到内部环境中的服务器（192.168.1.53、192.168.1.208、192.168.1.213），如果采用全通策略，请直接略过明细的安全策略配置步骤。



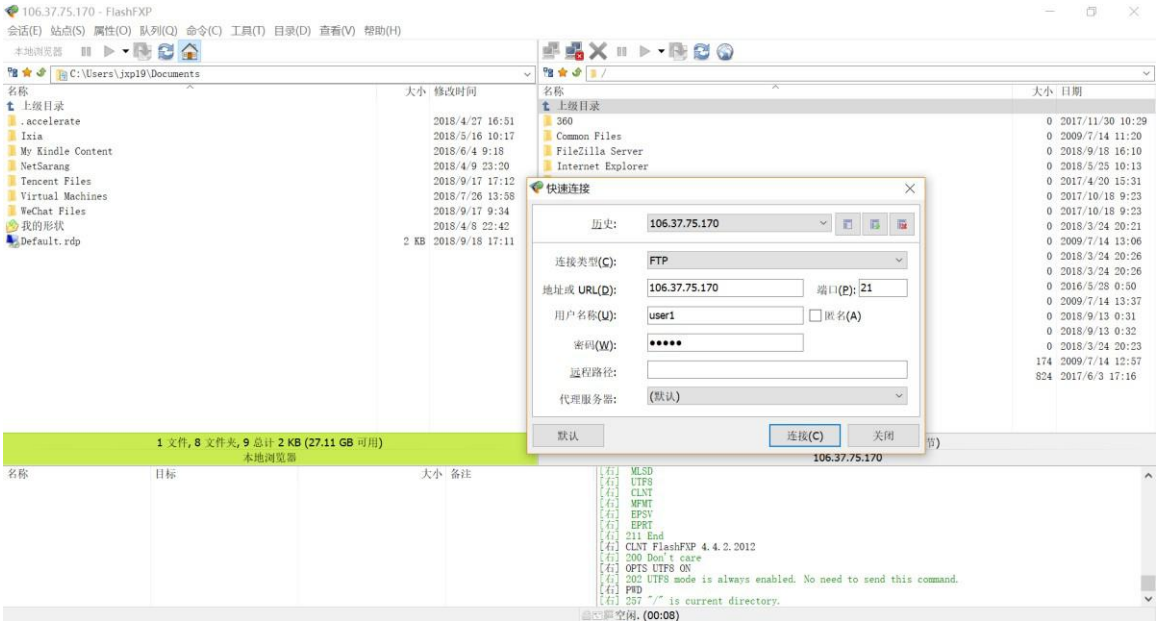

| ID | 状态 | 源地址 (原始) | 目的地址 (原始) | 服务 | 转换为 | 端口 | SLB | HA 组 | 日志 | 描述 | 命中数 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | Any | 192.168.1.101 | RDP | 192.168.1.213 | 0 | | 0 | 关闭 | | 91 |
| 2 | | Any | 192.168.1.101 | FTP | 192.168.1.53 | 0 | | 0 | 关闭 | | 57 |
| 3 | | Any | 192.168.1.101 | ssh-new | 192.168.1.208 | 22 | | 0 | 关闭 | | 1 |

2）明细的安全策略配置：对应上述目的 NAT 分别设置 3 条安全策略，放行 FTP 服务、SSH 服务、远程控制服务，目的 IP 设置的是 NAT 转换前的 IP 地址

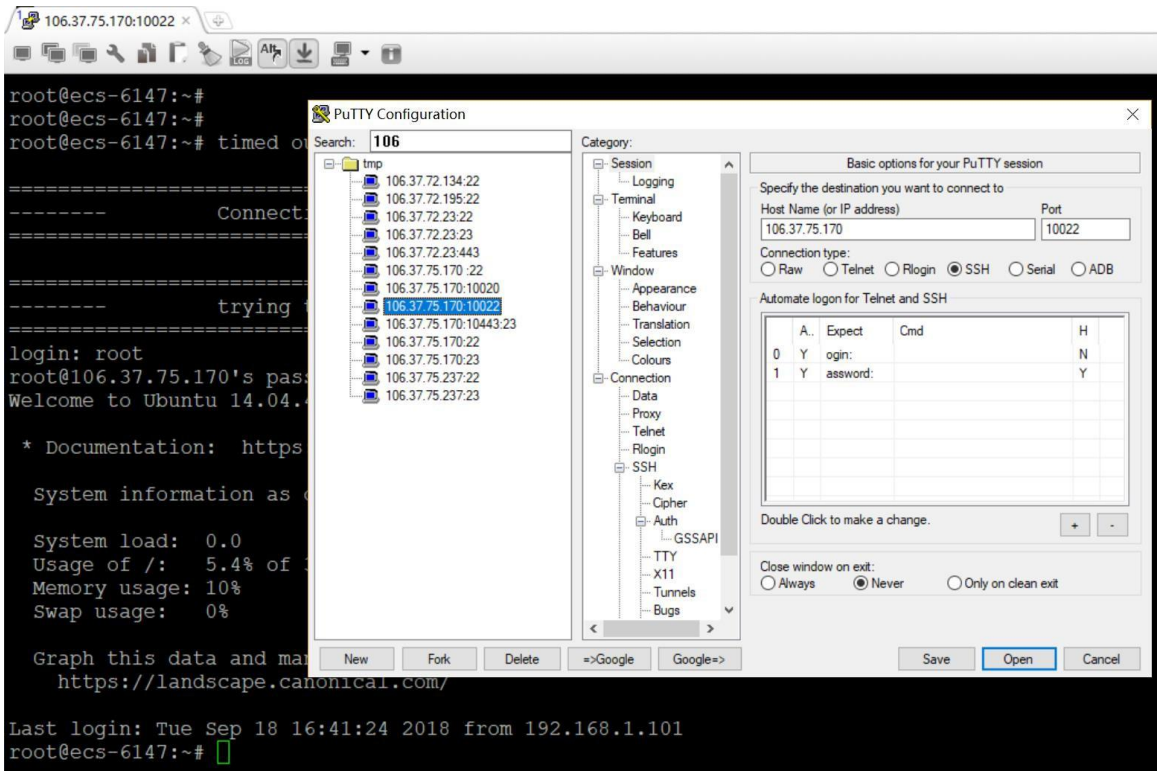
| ID | 名称 | 源 | | | 目的 | | 服务 | 应用 | 动作 | 会话 | 防护状态 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 安全域 | 地址 | 用户 | 安全域 | 地址 | | | | | |
| 9 | | trust | 36.111.88.33/32 | | trust | 192.168.1.101/32 | RDP | | | | |
| 6 | | trust | 36.111.88.33/32 | | trust | 192.168.1.101/32 | ssh-10020 | | | | |
| 5 | | trust | 36.111.88.33/32 | | trust | 192.168.1.101/32 | FTP | | | | |

3）验证 DNAT 策略，通过公网可以远程登陆到内网的服务器

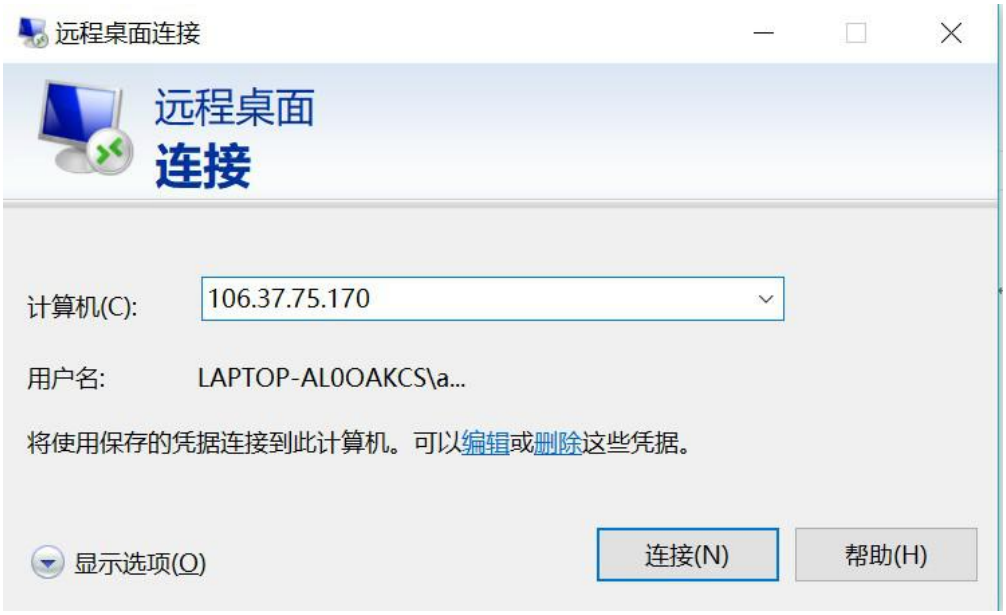
- FTP 服务




- SSH 服务

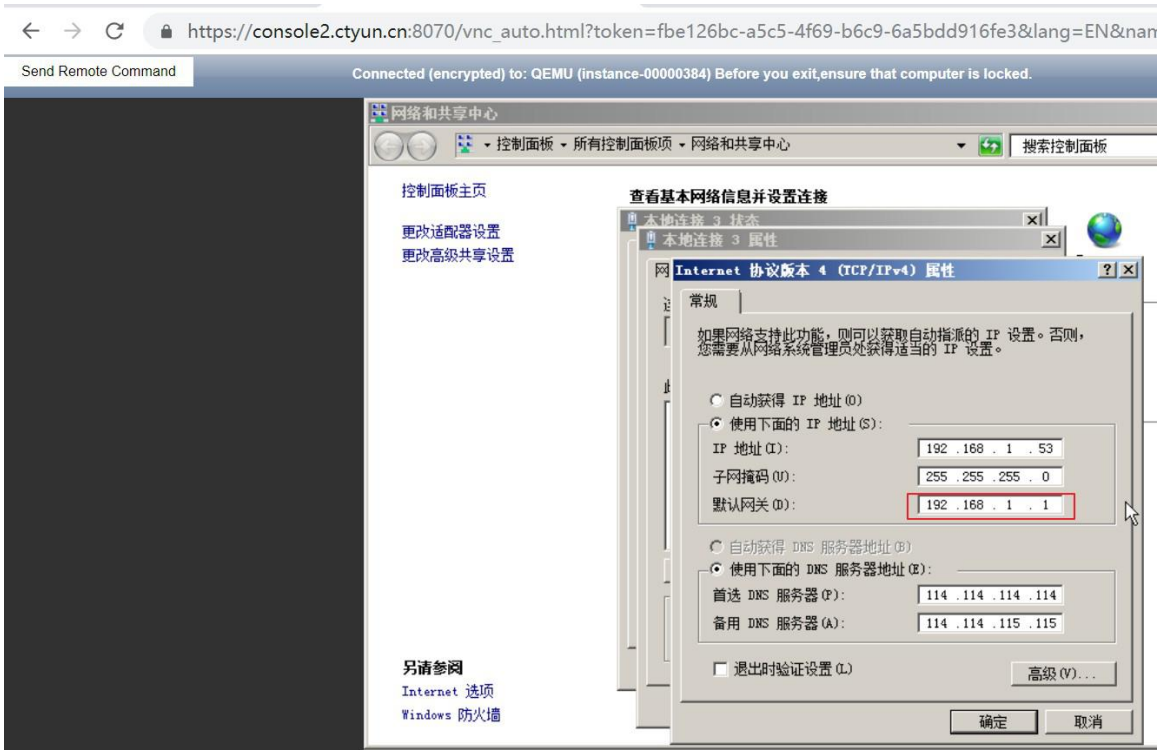


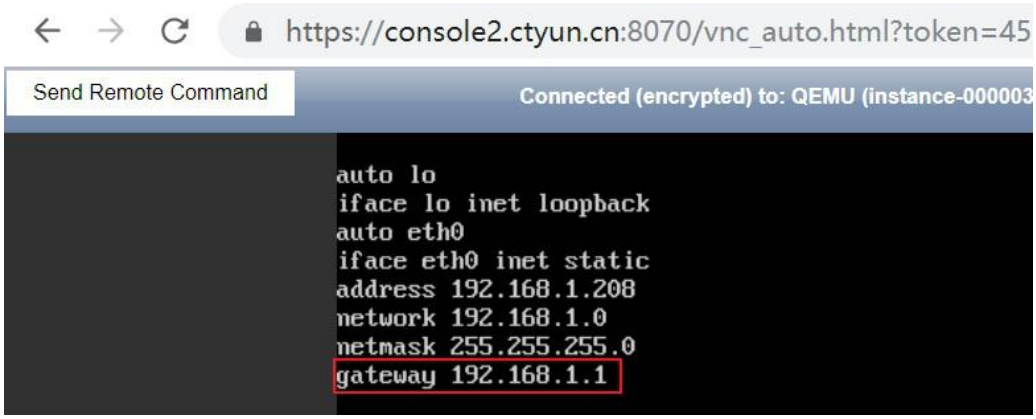

■ 远程控制服务




# 3.4 停止防护

在虚拟私有云（VPC）内的所有服务器上修改网关，网关指向子网默认网关，子网默认网关还请在虚拟私有云（VPC）内查看子网。

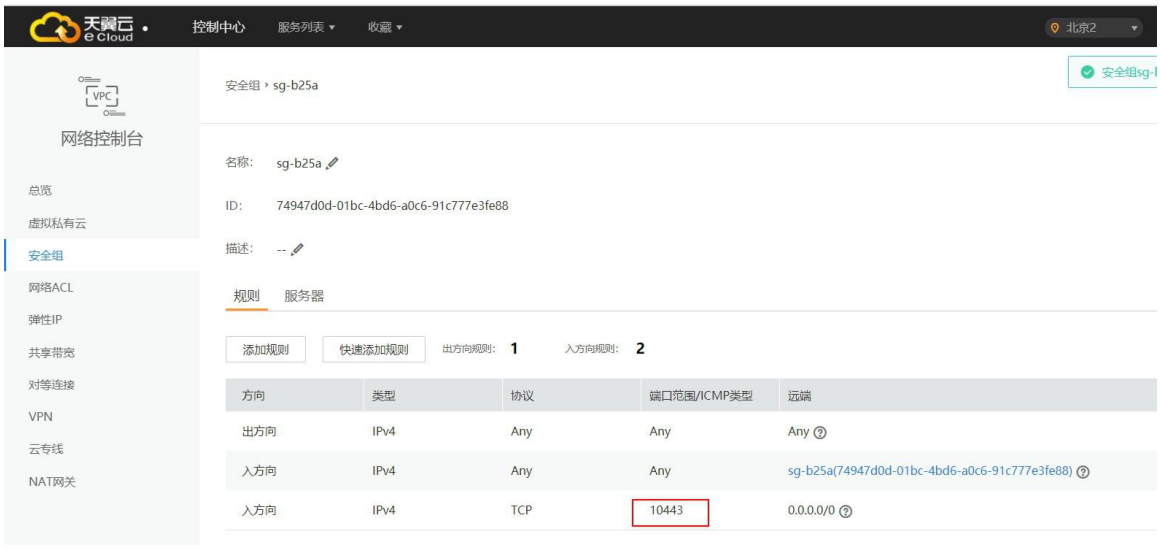

https://console2.ctyun.cn:8070/vnc_auto.html?token=fbe126bc-a5c5-4f69-b6c9-6a5bdd916fe3&lang=EN&nam
Send Remote Command
Connected (encrypted) to: QEMU (instance-00000384) Before you exit,ensure that computer is locked.
网络和共享中心
控制面板 ▸ 所有控制面板项 ▸ 网络和共享中心
搜索控制面板
控制面板主页
更改适配器设置
更改高级共享设置
查看基本网络信息并设置连接
本地连接 3 状态
本地连接 3 属性
Internet 协议版本 4 (TCP/IPv4) 属性
常规
如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。
自动获得 IP 地址(O)
使用下面的 IP 地址(S):
IP 地址(I): 192 .168 . 1 . 53
子网掩码(U): 255 .255 .255 . 0
默认网关(D): 192 .168 . 1 . 1
自动获得 DNS 服务器地址(B)
使用下面的 DNS 服务器地址(E):
首选 DNS 服务器(P): 114 .114 .114 .114
备用 DNS 服务器(A): 114 .114 .115 .115
退出时验证设置(L)
高级(V)...
确定
取消
另请参阅
Internet 选项
Windows 防火墙


https://console2.ctyun.cn:8070/vnc_auto.html?token=45
Send Remote Command
Connected (encrypted) to: QEMU (instance-000003
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
address 192.168.1.208
network 192.168.1.0
netmask 255.255.255.0
gateway 192.168.1.1

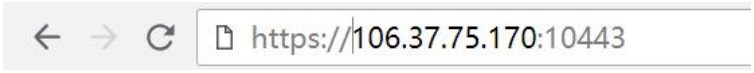

# 4 操作指南

## 4.1 配置登陆方式

1） 在安全组下放行管理的端口




2） 用浏览器（IE11 及以上或 Chrome）https 访问所绑定的弹性公网 IP 所放行的端口号，即可操作云下一代防火墙安全产品的 WEIUI 界面




# 4.2 配置接口配置

1） 在 WEBUI 界面进行安全域和 IP 地址的配置， IP 地址要与天翼云所配置的网卡地址一致。


2） 在 WEBUI 界面中查看 IP 地址


# 4.3 配置静态路由

1） 在网络中选择路由，并点击静态路由


2） 设置静态路由，指向相对应的下一跳


# 4.4 配置安全策略

1） 在策略中选择安全策略


2） 配置安全策略

# 4.5 配置内网访问外网的 SNAT 策略

1） 在云下一代防火墙安全产品上配置一条访问控制策略（此处配置的为全通策略）。由于全通策略缺乏一定的安全性，所以在客户业务运行正常的情况下，还请自行根据需求更换为明细的安全策略，如果采用全通策略，请直接略过明细的安全策略配置步骤。

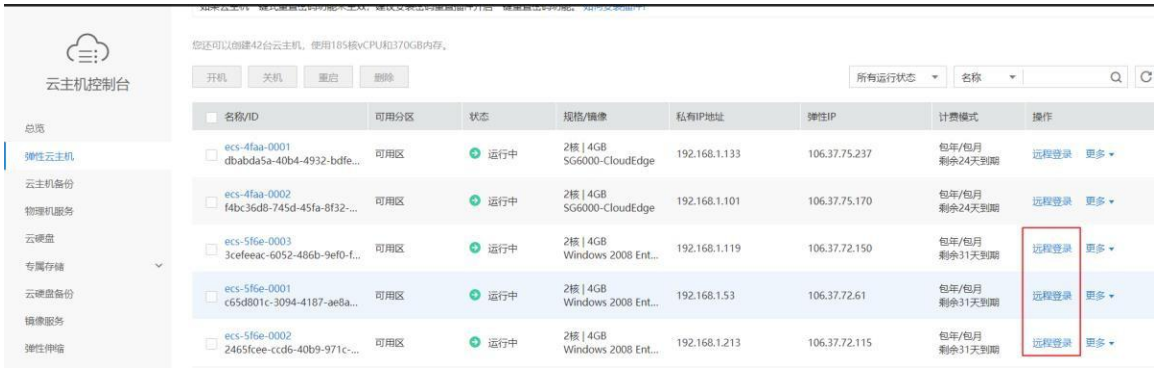

2） 在云下一代防火墙安全产品上配置 SNAT 策略，对应拓扑中的三台服务器，这里将出流量源地址转换成出接口 IP（云下一代防火墙安全产品 e0/0 接口地址）。

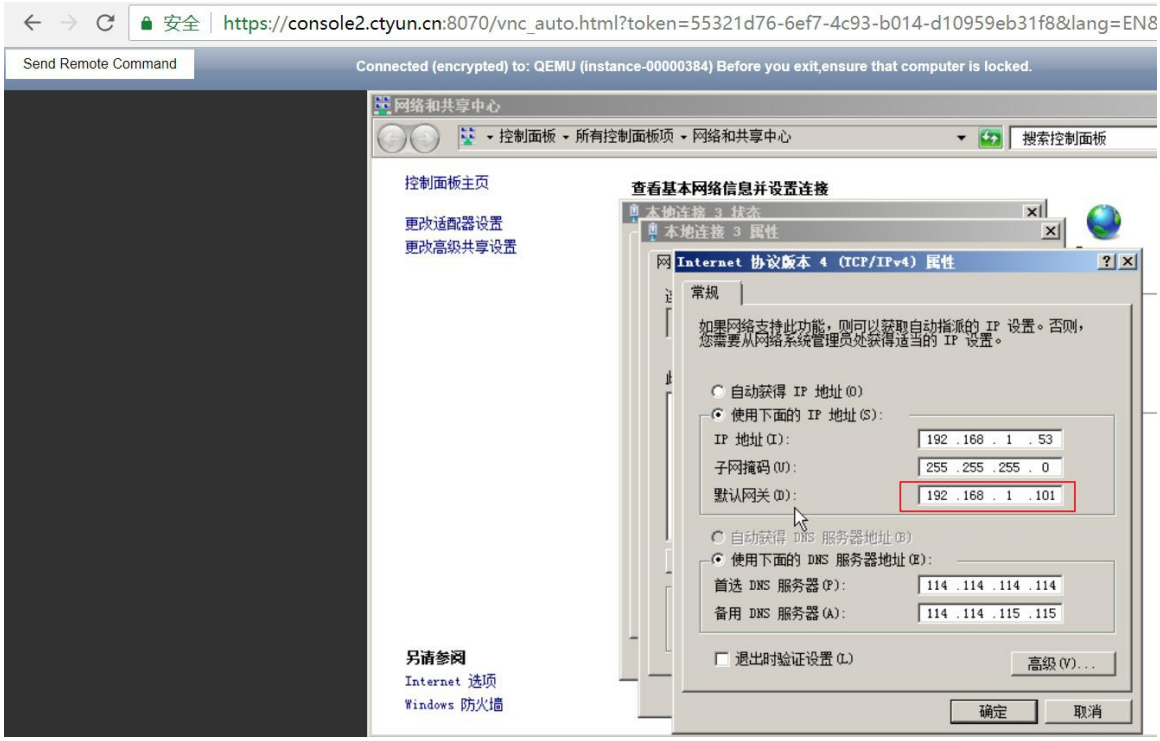

3） 明细的安全策略配置：设置 SNAT 的安全策略，放行内网访问外网的数据流量

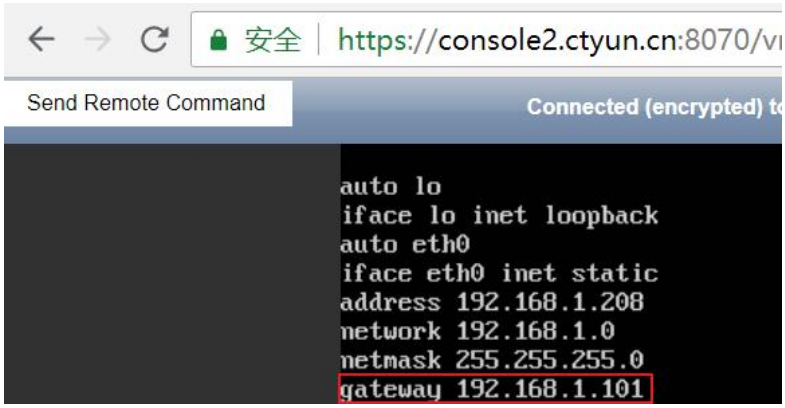



4） 关闭所创建云下一代防火墙安全产品的源/目的检查（点击弹性云服务器名称进入网卡选项）

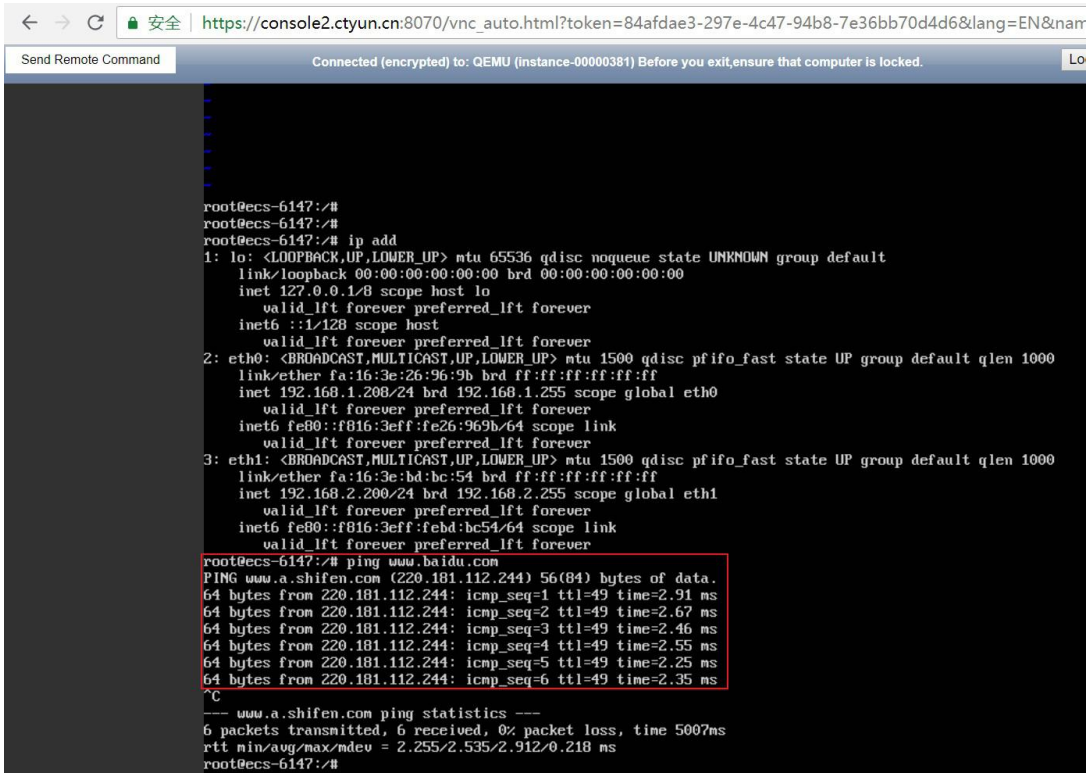

5） 在虚拟私有云（VPC）内的所有服务器上修改网关，网关指向云下一代防火墙安全产品






6） 验证 SNAT 策略，配置完 SNAT 后服务器可以访问外网


# 4.6 配置外网访问内网的 DNAT 策略

1） 在云下一代防火墙安全产品上配置三条 DNAT 策略，将访问弹性 IP 所绑定的 e0/0 接口地址（192.168.1.101）的 FTP 服务、SSH 服务、远程控制服务映射到内部环境中的服务器（192.168.1.53、192.168.1.208、192.168.1.213），如果采用全通策略，请直接略过明细的安全策略配置步骤。

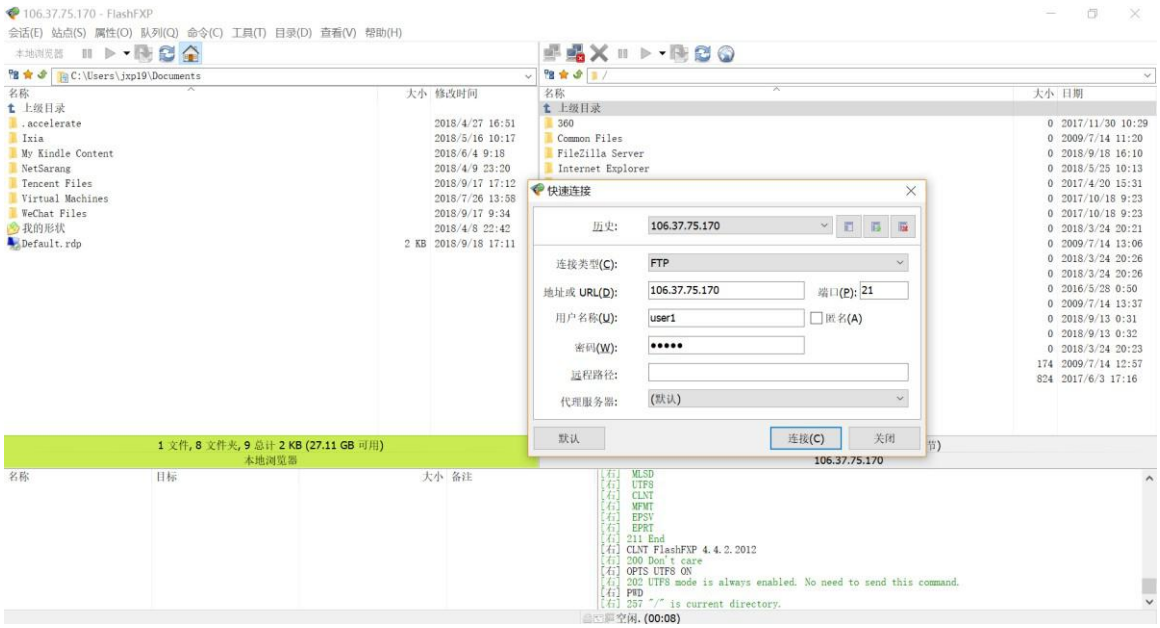

| ID | 状态 | 源地址 (原始) | 目的地址 (原始) | 服务 | 转换为 | 端口 | SLB | HA 组 | 日志 | 描述 | 命中数 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | Any | 192.168.1.101 | RDP | 192.168.1.213 | 0 | | 0 | 关闭 | | 91 |
| 2 | | Any | 192.168.1.101 | FTP | 192.168.1.53 | 0 | | 0 | 关闭 | | 57 |
| 3 | | Any | 192.168.1.101 | ssh-new | 192.168.1.208 | 22 | | 0 | 关闭 | | 1 |

2） 明细的安全策略配置：对应上述目的 NAT 分别设置 3 条安全策略，放行 FTP 服务、SSH 服务、远程控制服务，目的 IP 设置的是 NAT 转换前的 IP 地址

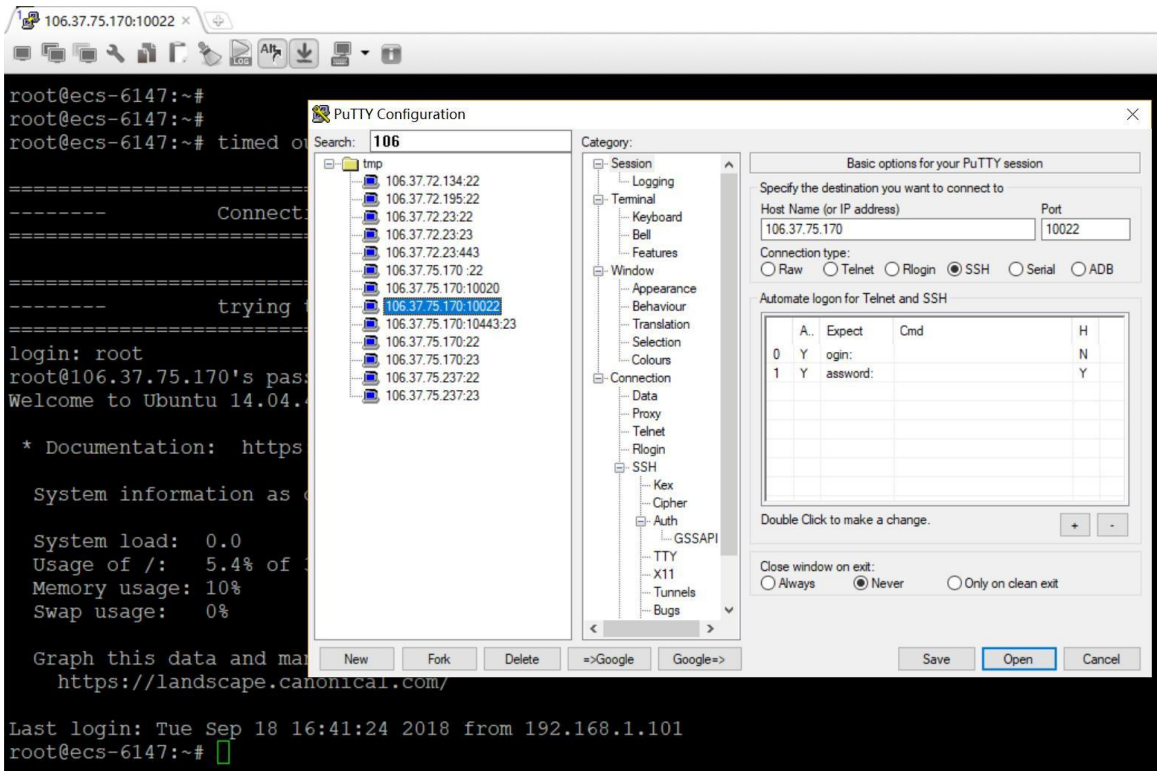
| ID | 名称 | 源 | | | 目的 | | 服务 | 应用 | 动作 | 会话 | 防护状态 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 安全域 | 地址 | 用户 | 安全域 | 地址 | | | | | |
| 9 | | trust | 36.111.88.33/32 | | trust | 192.168.1.101/32 | RDP | | | | |
| 6 | | trust | 36.111.88.33/32 | | trust | 192.168.1.101/32 | ssh-10020 | | | | |
| 5 | | trust | 36.111.88.33/32 | | trust | 192.168.1.101/32 | FTP | | | | |

3） 验证 DNAT 策略，通过公网可以远程登陆到内网的服务器

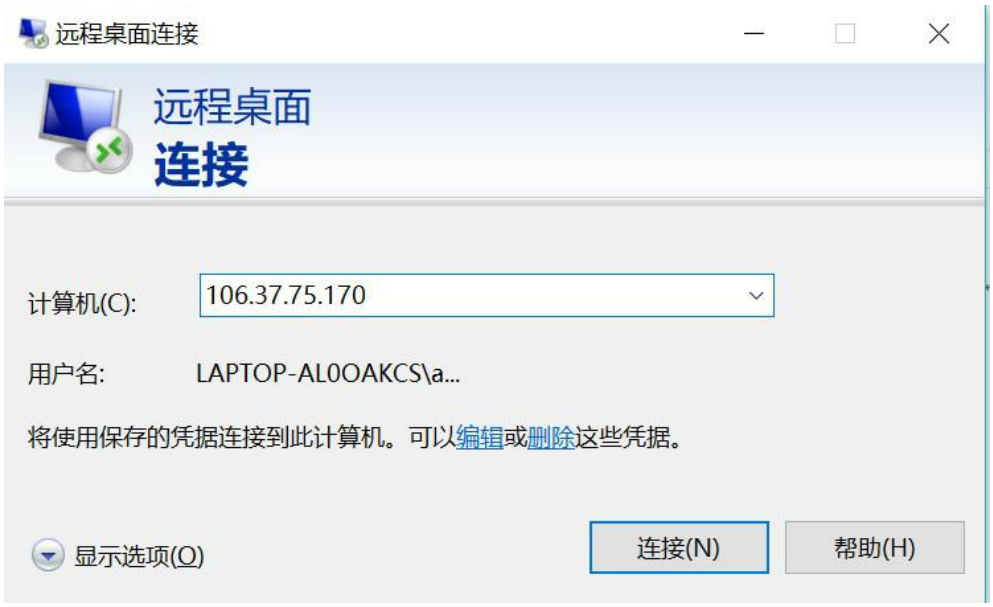
■ FTP 服务




■ SSH 服务


106.37.75.170:10022
root@ecs-6147:~#
root@ecs-6147:~#
root@ecs-6147:~# timed
PuTTY Configuration
Search: 106
Category:
tmp
106.37.72.134:22
106.37.72.195:22
106.37.72.23:22
106.37.72.23:23
106.37.72.23:443
106.37.75.170 :22
106.37.75.170:10020
106.37.75.170:10022
106.37.75.170:10443:23
106.37.75.170:22
106.37.75.170:23
106.37.75.237:22
106.37.75.237:23
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Kex
Cipher
Auth
GSSAPI
TTY
X11
Tunnels
Bugs
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
106.37.75.170
10022
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
ADB
Automate logon for Telnet and SSH
Expect
Cmd
ogin:
assword:
Double Click to make a change.
Close window on exit:
Always
Never
Only on clean exit
New
Fork
Delete
=>Google
Google=>
Save
Open
Cancel
login: root
Welcome to Ubuntu 14.04.
* Documentation:
System information as
System load: 0.0
Memory usage: 10%
Swap usage: 0%
https://landscape.canonical.com/
Last login: Tue Sep 18 16:41:24 2018 from 192.168.1.101
root@ecs-6147:~#

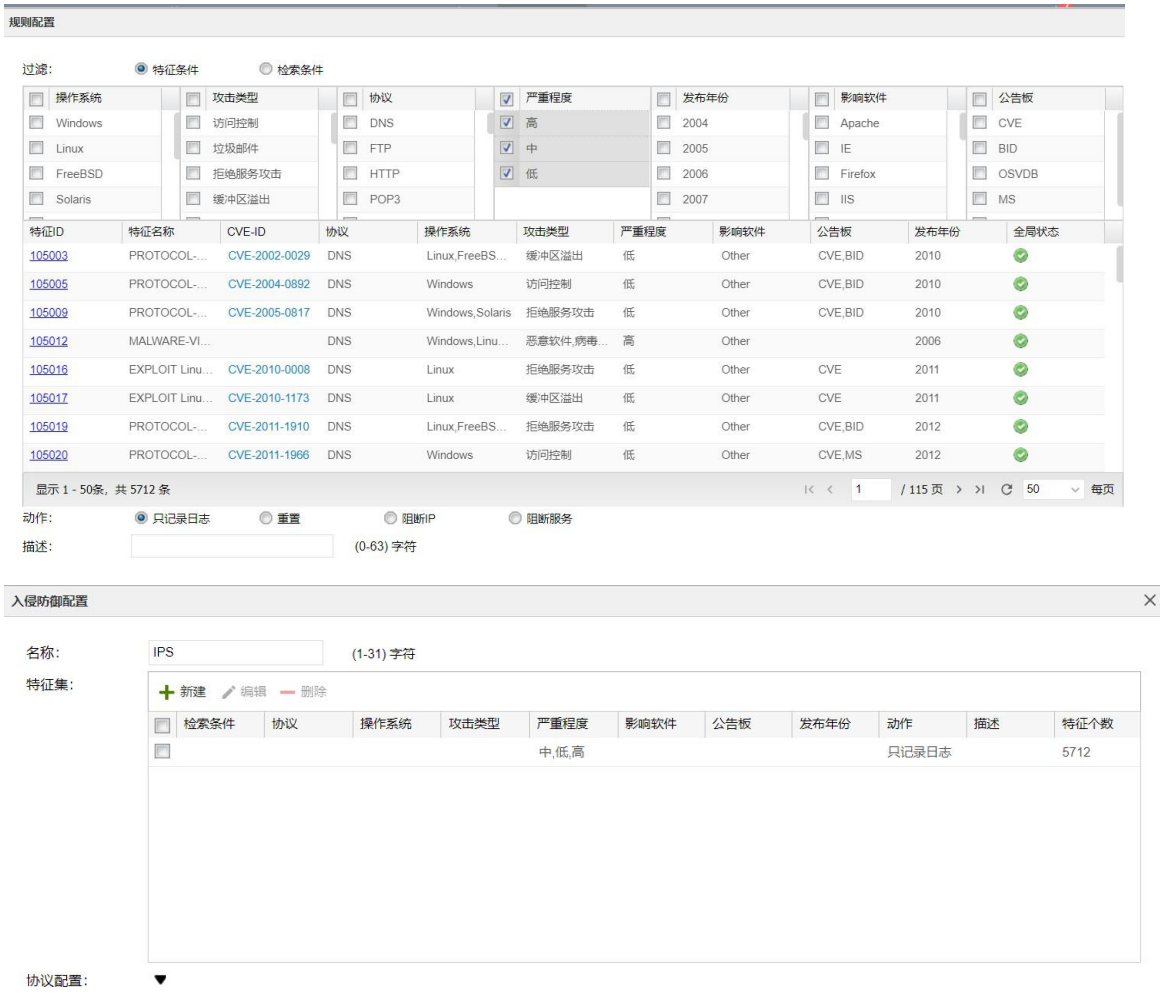
■ 远程控制服务


远程桌面连接
远程桌面
连接
计算机(C):
106.37.75.170
用户名:
LAPTOP-AL0OAKCS\a...
将使用保存的凭据连接到此计算机。可以编辑或删除这些凭据。
显示选项(O)
连接(N)
帮助(H)


# 4.7 配置入侵防御

1. 创建 IPS 模板

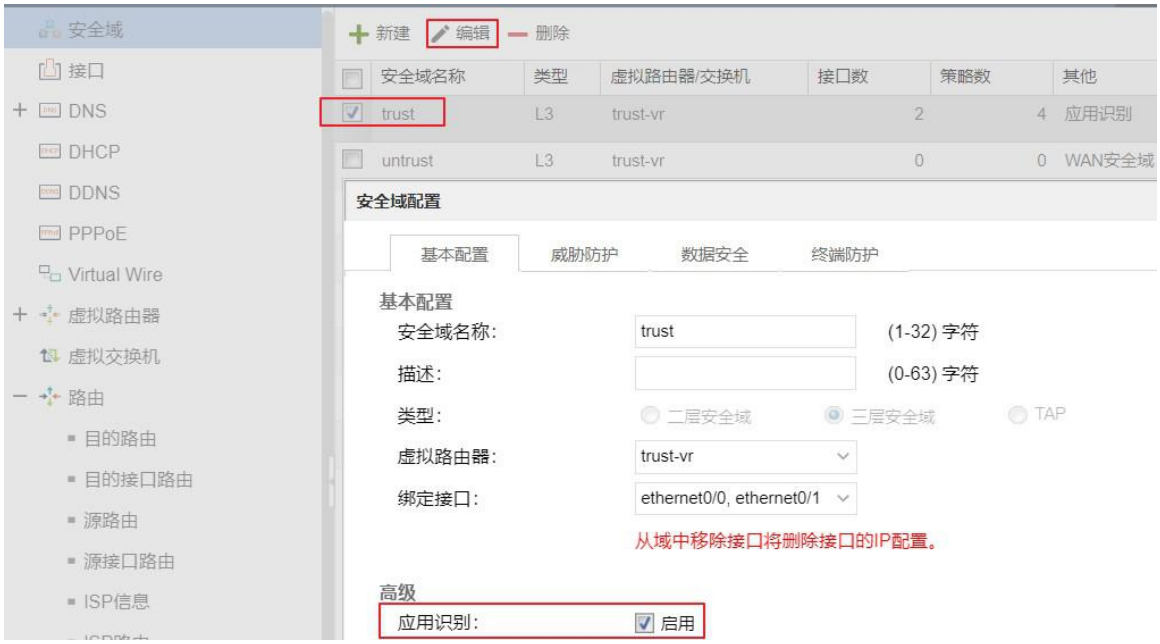

2. 编辑 IPS 模板并按照需求进行特征库的选择




3. 针对模板进行协议配置


4. 按照需求开启SQL 注入、XSS 注入

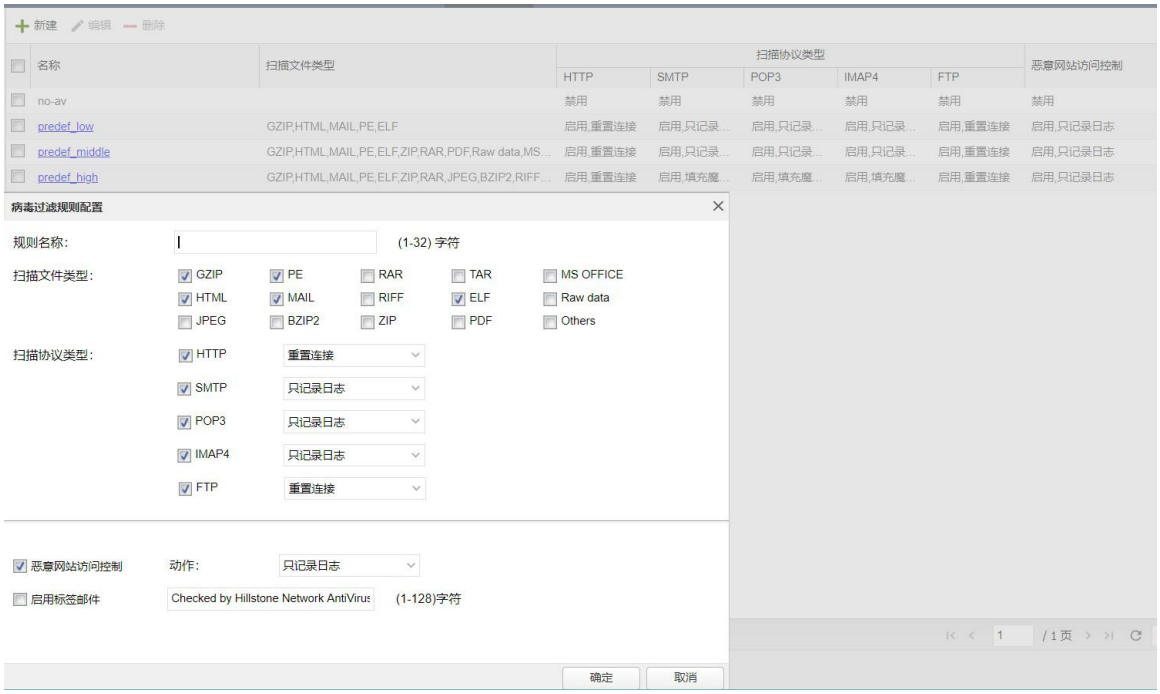

5. 在区域调用此IPS 模板，入侵防御生效。



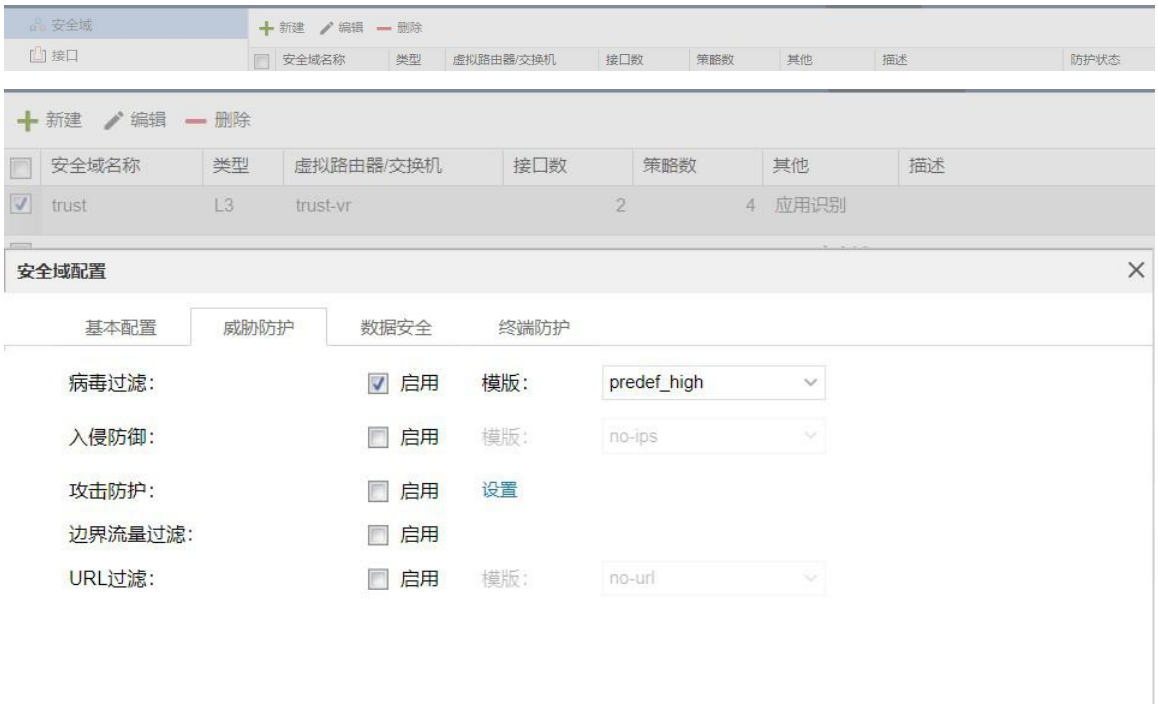


# 4.8 配置病毒防御

1. 选择病毒过滤模板，并按照需求进行模板创建和修改



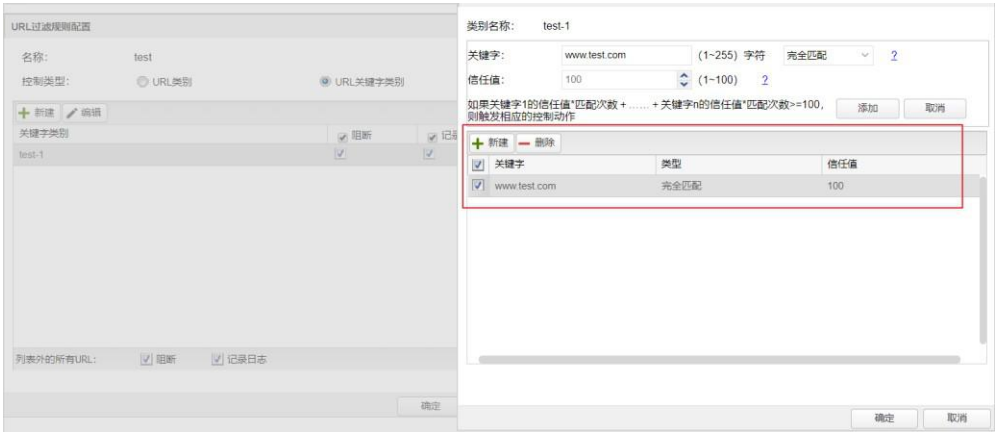

## 2. 在安全域下调用病毒防御模板



# 4.9 配置 URL 过滤

1. 新建URL 过滤名称以及 test-1 规则

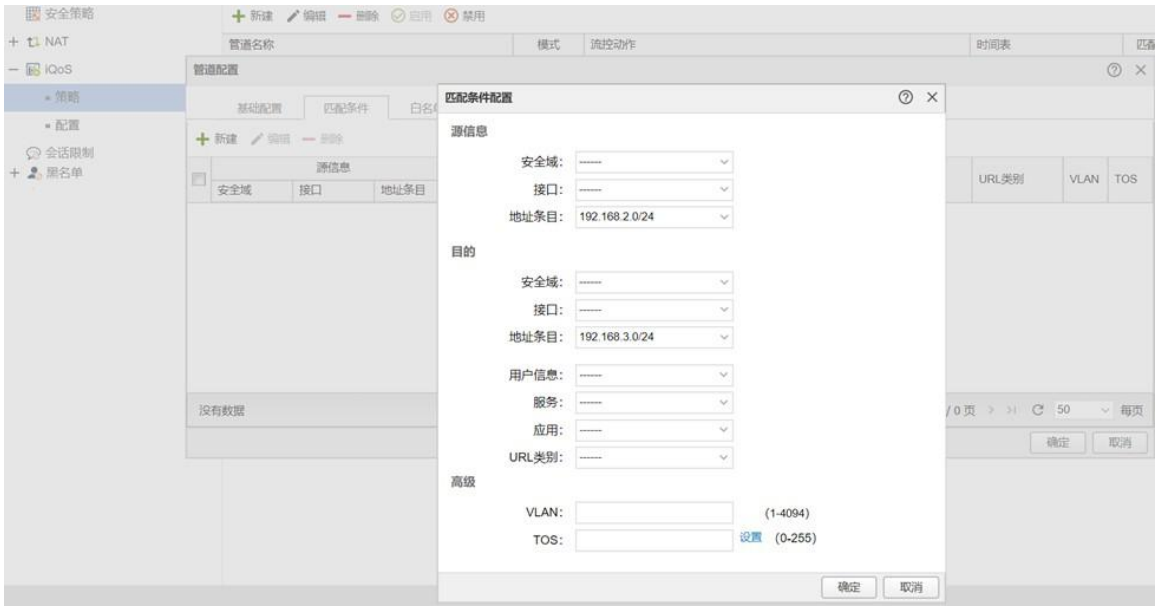

2. 设置URL 过滤的规则（test-1）



3. 在安全策略中调用URL 过滤模板


# 4.10 配置应用层流量带宽控制 QOS

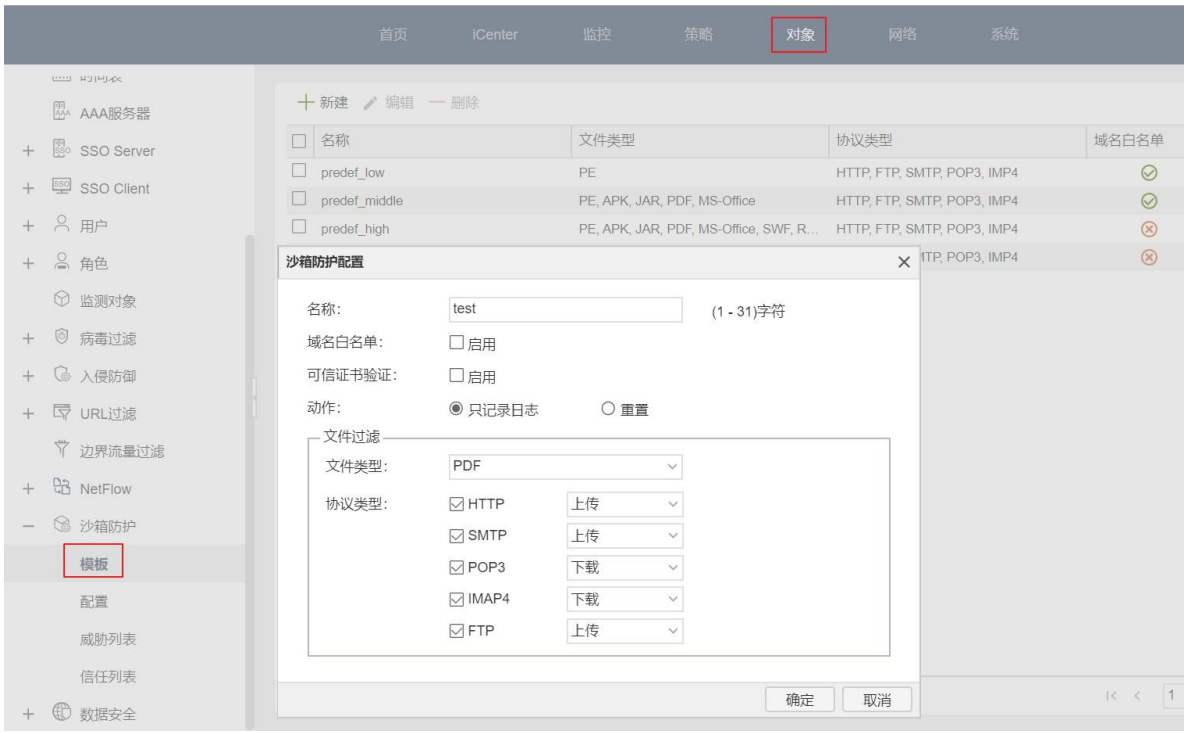
1) 支持针对某IP 或者某角色进行带宽限制，正向和反向是按照源地址到目的地址进行划分



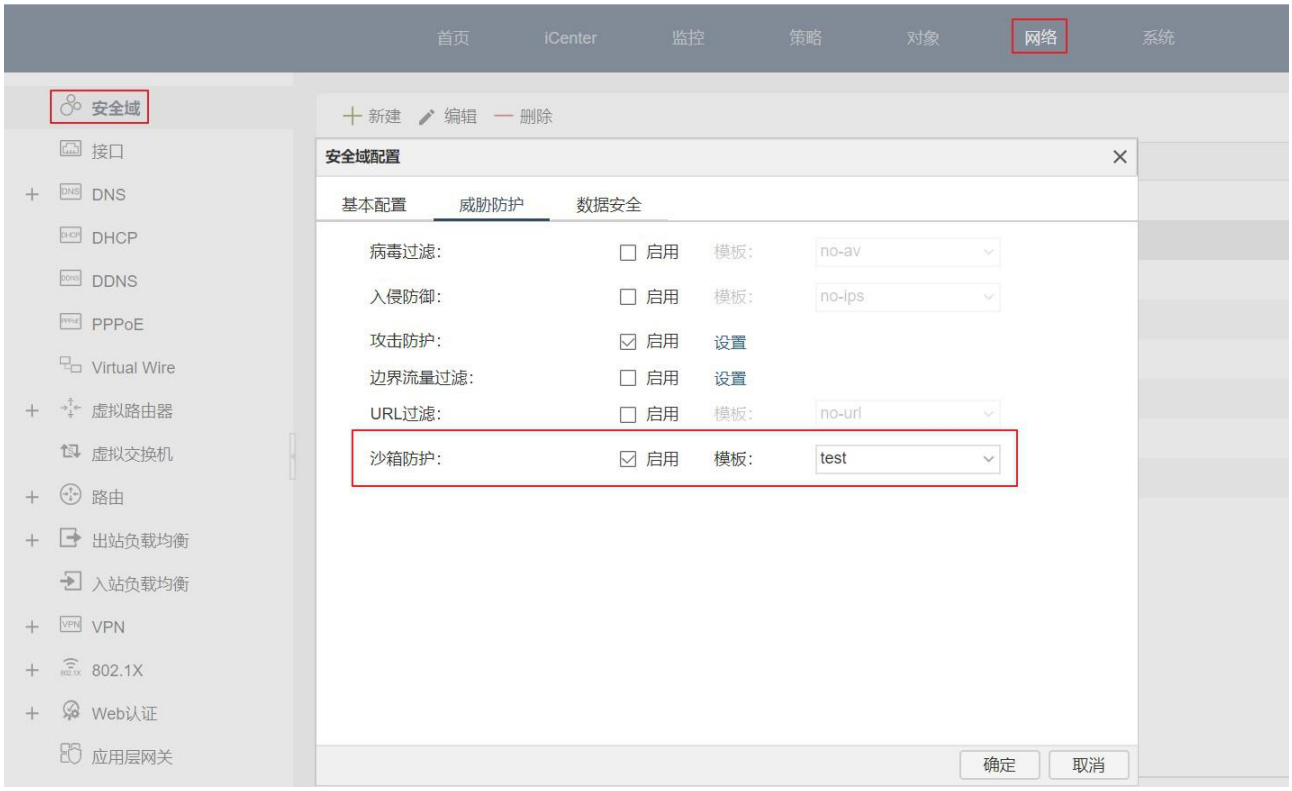

2) 按照需求设置限速


# 4. 11 配置云沙箱

1) 新建云沙箱的模板



2）在安全域或者安全策略下调用云沙箱模板

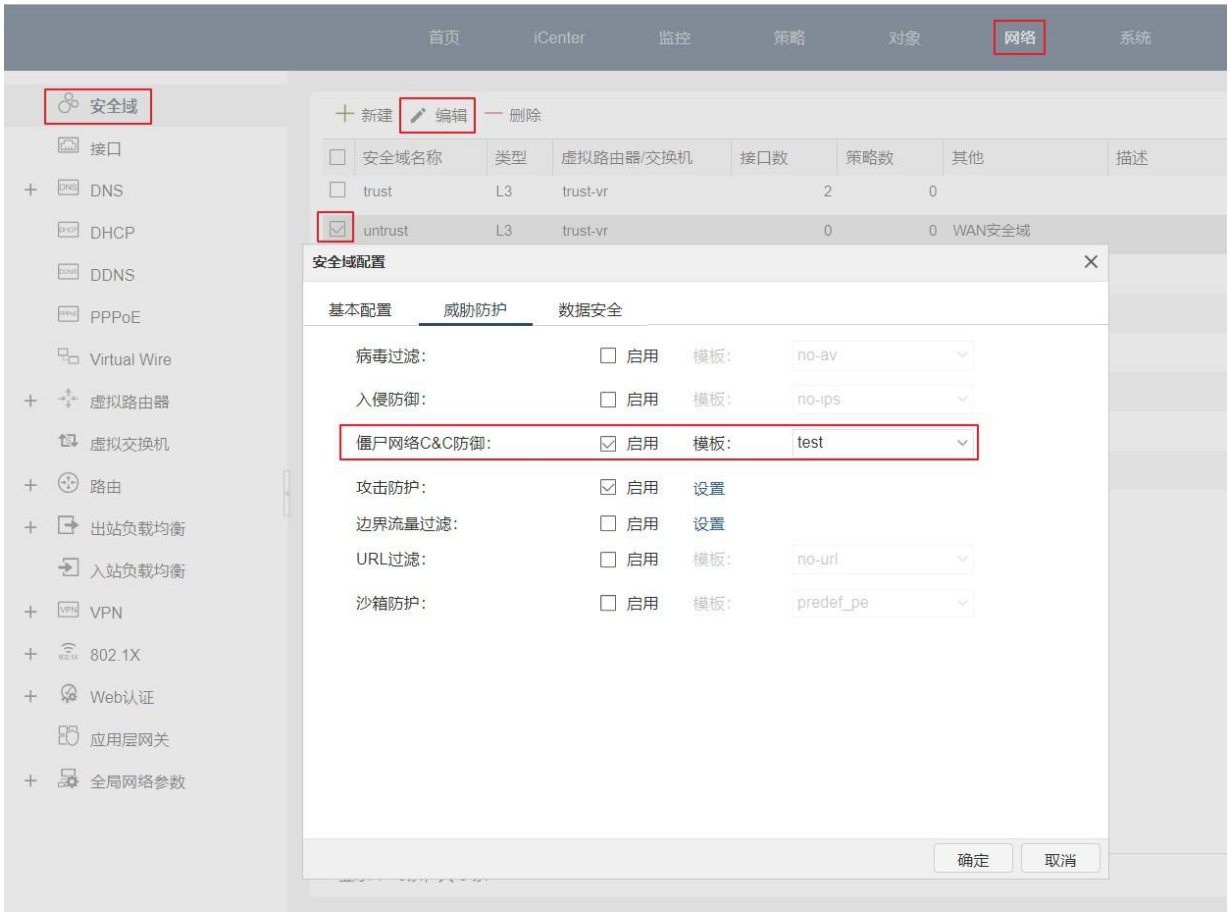




# 4.12 配置僵尸网络 C&C 防护

1）新建僵尸网络C&C 防护的模板


2) 在安全域/安全策略下调用模板




# 4.13 配置 IP 信誉

1）在网络-安全域-威胁防护-边界流量过滤下配置 IP 信誉

# 5 常见问题

## 5.1 功能类

### 5.1.1 云下一代防火墙有什么功能

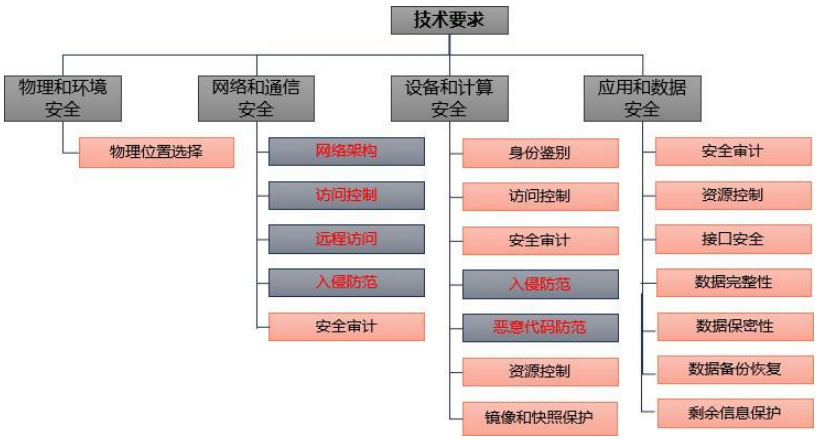
天翼云防火墙是业内最专业的防火墙，拥有多种功能：

1) 访问控制：能够基于传统“五元组”、时间、安全域、应用等维度进行精细化控制。
2) 流量识别：拥有专业的应用识别特征库，可将流量识别为具体应用并进行统计呈现。
3) 入侵检测：拥有专业的恶意威胁特征库，对各类型网络攻击进行阻断。
4) 网络功能：支持“静态路由”、“动态路由”、“网络地址转换 NAT 功能”等，可以轻松融入客户网络。
5) 其他安全功能：网络病毒查杀、流量带宽控制、页面访问控制等

更多功能详见：https://www.ctyun.cn/help/qslist/2172 《天翼云云下一代防火墙用户使用指南》

### 5.1.2 云下一代防火墙是否能满足等保三级要求

首先要明确一点，等保要求不光是对技术及产品的要求，同时也是对企业安全管理制度上存在要求。技术上可以通过多种安全产品来实现，云下一代防火墙可以满足 GB/T 22239.2（等级保护云计算安全扩展要求） 里部分“网络和通信安全”“设备和计算安全”，见下图标红字体部分。



### 5.1.3 云下一代防火墙和阿里云的云防火墙有什么区别

天翼云云下一代防火墙从规格上来看更加便宜、性能更高。功能对比如下图：

| | 阿里云-云防火墙-高级版 | 天翼云-云下一代防火墙 |
|---|---|---|
| 应用识别 | 不支持 | 支持3000+应用识别 |
| 监控统计 | 仅支持五元组日志 | 支持流量、用户、应用等统计，可以使用柱状图、折线图、表格、报表、日志等方式呈现 |
| 用户认证 | 不支持 | 支持用户认证 |
| 访问控制 | 3-4层访问控制 | 2-7层访问控制 |
| 入侵防御 | 支持常见攻击的防御 | 检测通过NSS LAB认证，综合检测率全球第一 |
| 病毒过滤 | 不支持 | 支持，通过购买AV授权实现 |
| 带宽控制 | 不支持 | 支持，通过购买QOS授权实现 |
| 页面访问控制 | 不支持 | 支持，通过购买URL授权实现 |
| 高可用性 | 不支持 | 支持 |

### 5.1.4 云下一代防火墙安全产品有几个规格？

云下一代防火墙安全产品分为标准版、高级版和旗舰版，三个版本基本功能相同但性能不同，扩展功能标准版和高级版相同，旗舰版增加了更多的防护选配功能。所需弹性云主机的配置也不同，上述三个版本均可购买额外的安全扩展功能。

### 5.1.5 云下一代防火墙安全产品能否进行规格变更？

支持标准版升至高级版或旗舰版，高级版升至旗舰版，变更前还请确认如下三点：

1） 规格变更的过程会导致虚机重启、网络以及业务的中断

2） 确认云下一代防火墙所在的弹性云主机配置满足高级版所需配置，配置需求请参照官网

3） 需提前缴纳规格变更差价

### 5.1.6 云下一代防火墙安全产品价值优势有哪些？

| | | |
|---|---|---|
| **引导点** | | 1. 引导统一威胁管理的安全防护机制<br>2. 引导 IP、应用相互嵌套的流控功能<br>3. 引导基于公有云环境下的 HA 部署方案 |
| **战略要点** | **公司** | 专业的防火墙厂商，12 年的技术积累以及产品成熟度高 |
| | **资质** | 1. 连续多年入选 Gartner 防火墙魔力象限<br>2. NSS Labs 推荐级最佳下一代防火墙 |
| | **功能** | 1. 全并行软硬件架构，基于多核硬件处理架构和拥有自主知识产权的64位操作系统，实现软硬件全并行操作<br>2. 依靠二层单播技术实现公有云环境下的 HA 部署<br>3. 基于状态、精准的高性能攻击检测和防御引擎<br>4. 支持深度应用识别技术，能够准确识别数千种网络应用<br>5. 支持丰富的用户认证方式，包括 TACACS+、RADIUS、LDAP 等外部服务器用户认证，以及本地认证、Web 认证等<br>6. 带宽管理支持基于五元组、应用的多层嵌套，可满足复杂场景下的流量控制功能。 |
| | **性能** | 1. 性能高：依靠专有算法在每个 CPU 核上处理所有安全功能，并可将会话负载均分到所有内核，实现最优化的多核并行处理<br>2. 云下一代防火墙在具备全面安全防护的同时提供了低延时、高可靠性的部署方案，实现用户带来更快速的安全体验。 |

### 5.1.7 云下一代防火墙安全产品涉及到等保三级中哪些条例？

云下一代防火墙中涉及到了等保三级中的虚拟化安全，具体条例如下：

① 符合 GB/T22239.2 中关于不同云租户间隔离的要求

② 符合 GB/T22239.2 中关于识别、监控虚拟机之间、虚拟机与物理机之间、虚拟机与宿主机之间的流量要求。

③ 符合 GB/T22239.2 中关于根据承载的业务系统安全保护等级划分资源池，并实现资源池之间的隔离

④ 符合 GB/T22239.2 中关于提供开放接口，允许接入第三方安全产品，实现云租户的网络之间、安全区域之间、虚拟机之间的网络安全防护的要求

⑤ 符合 GB/T22239.2 中关于虚拟机迁移时，访问控制策略随其迁移和依据安全策略控制虚拟机间的访问的要求

⑥ 符合 GB/T22239.2 中关于检测到云租户对外的攻击行为，并能记录攻击类型、攻击时间、攻击流量和发布到互联网的有害信息进行实时监测和告警的要求

### 5.1.8 云下一代防火墙安全产品的适用场景有哪些？

① 金融行业业务场景：某互联网金融服务公司作为快速成长中的金融服务公司，考虑到业务的发展、云端基础网络的可靠性、部署运维的便捷性以及性价比多个方面因素，选择利用云计算技术，从而实现了实现业务动态增长的同时保障业务的长期安全稳定运行。

② 政企行业业务场景：多个市级公安警务云，充分利用云下一代防火墙的微隔离可视化技术，实现警务云安全加固，对云内几十个业务系统、系统内关键业务虚机进行隔离、防护，从而符合行业安全技术标准，规定要求。

③ 医疗行业业务场景：某医院门急诊项目为银医通项目，该项目为军区总医院门诊和急诊提供计算服务，门急诊的应用部署在虚拟化平台上，传统方案无法进行有效的安全防护，需要采用更完善的安全防护方式。

## 5.2 开通类

### 5.2.1 哪些资源池可以支持开通云下一代防火墙

**以下节点均可以部署云下一代防火墙**

北京/内蒙 1、2/上海 1、2、3/广州 1、2、3/厦门 1、2/成都 2/西安/长沙/南京/福州 2/沈阳/武汉节点/贵州/福州/杭州/深圳/广州 4/苏州/郑州/青岛/西安 2/上海 4/芜湖/南宁/长沙 2/南昌/成都 3/乌鲁木齐/昆明/海口/重庆/武汉 2/兰州/西宁/太原/石家庄/中卫/长春/天津/北京 2/哈尔滨节点

### 5.2.2 如何开通云下一代防火墙安全产品？

需要提前购买弹性云主机，在官网选择云下一代防火墙安全产品规格及时长，并进行购买，开通之后会收到通知。

### 5.2.3 弹性 IP 与弹性云主机一同购买，如何对弹性 IP 解绑？

详情请咨询客服。

### 5.2.4 我需要部署几台云下一代防火墙

云下一代防火墙可以采用单机部署模式也可以一组双机部署模式（高可靠模式）。

网络结构复杂或者需要保护的云主机过多，可以选择多台或者多组。

### 5.2.5 开通云下一代防火墙业务是否会造成业务中断

创建云下一代防火墙不会造成断网，当串联部署到网络中时会有业务中断的时间，需要提前通知业务部门告知割接时间。

# 5.3 操作类

## 5.3.1 云下一代防火墙安全产品无法启动或连接怎么办？

请修改 VPC 内所有服务器的默认网关，网关还请参照虚拟私有云（VPC）内的子网信息，如果依旧存在问题，请联系客服。

## 5.3.2 云下一代防火墙是怎么实现入侵防御以及病毒过滤？

入侵防御和病毒过滤是基于安全域进行配置，并按照协议和特征进行匹配，同时可根据威胁程度进行日志提醒。

## 5.3.3 在云下一代防火墙如何添加云主机进行安全防护？

需要分别按照路由、源 NAT（SNAT）、目的 NAT（DNAT），云主机网关进行对应配置，配置完成之后即可实现安全防护。

## 5.3.4 在云下一代防火墙上如何添加明细策略？

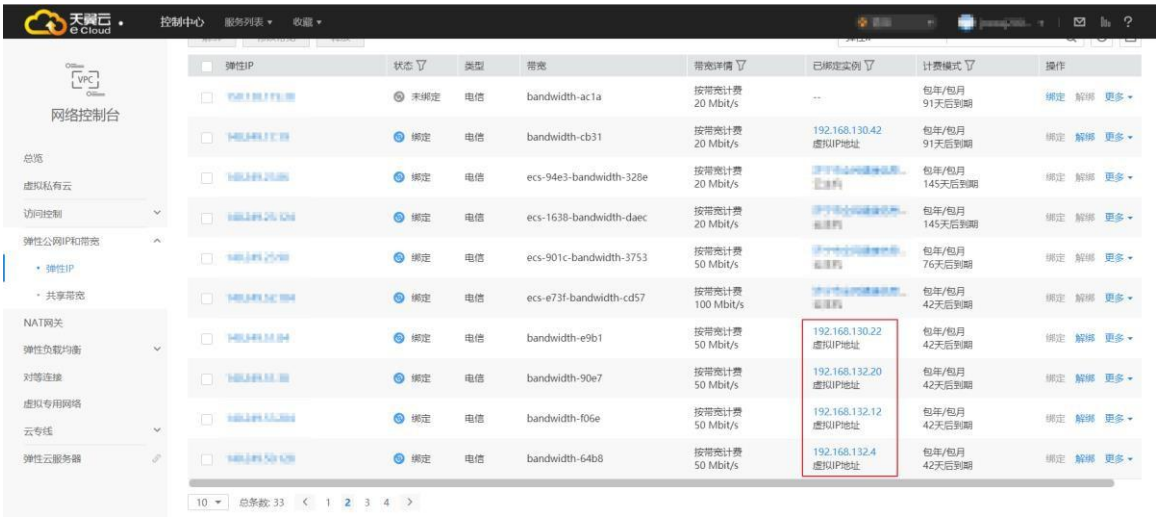
选择安全策略并按照安全域、地址、服务、应用、策略动作、策略优先级进行配置。

## 5.3.5 在 HA 模式的云下一代防火墙上需要分别进行配置吗？

仅需要在主墙上进行配置，配置以及会话会自动同步至备墙。

## 5.3.6 如何查看 HA 模式的云下一代防火墙所绑定的弹性 IP 吗？

HA 模式下弹性 IP 绑定至虚拟 IP 中，可通过控制台下的弹性 IP 进行跳转。




### 5.3.7 云下一代防火墙如何更新特征库？

下列条件会导致云下一代防火墙无法更新特征库，在检查完毕之后点击立即在线升级：

1） 云下一代防火墙无法访问互联网。

2） 云下一代防火墙上缺少 DNS 的相关配置。

3） 云下一代防火墙上缺少对应功能的许可。