

# Check Point R80.20 基于腾讯云的部署 2019.4.1

金锐同创（北京）科技股份有限公司

# 目录

## 第一章 概述

- 1.1 产品介绍
- 1.2 安装要求及注意事项

## 第二章 购买实例的相关参数

- 2.1 新建主机
- 2.2 选择地域与机型
- 2.3 选择镜像
- 2.4 选择存储和带宽
- 2.5 设置安全组和主机
- 2.6 确认配置信息

## 第三章 配置主机网络

- 3.1 登陆 VNC
- 3.2 登陆 checkpoint 命令行
- 3.3 配置网络地址及默认路由

## 第四章 Gaia(底层系统)初始化

- 4.1 登陆 Gaia 系统并配置（以红圈标注为建议）

## 第五章 通过 SmartConsole 配置防火墙的相关功能

- 5.1 下载并安装 SmartConsole 客户端
- 5.2 Get 底层的拓扑及接口地址信息
- 5.3 定义接口域并关闭接口地址防欺骗功能
- 5.4 编辑策略
- 5.5 开启内网段的 SNAT
- 5.6 下发策略并生效

## 第一章 概述

### 1.1 产品介绍

Check\_Point\_vSEC 提供行业领先的威胁防护安全保护，以确保即使遭遇最复杂的攻击，也能保障腾讯公有云和混合云网络的安全。完全集成式安全保护包括：

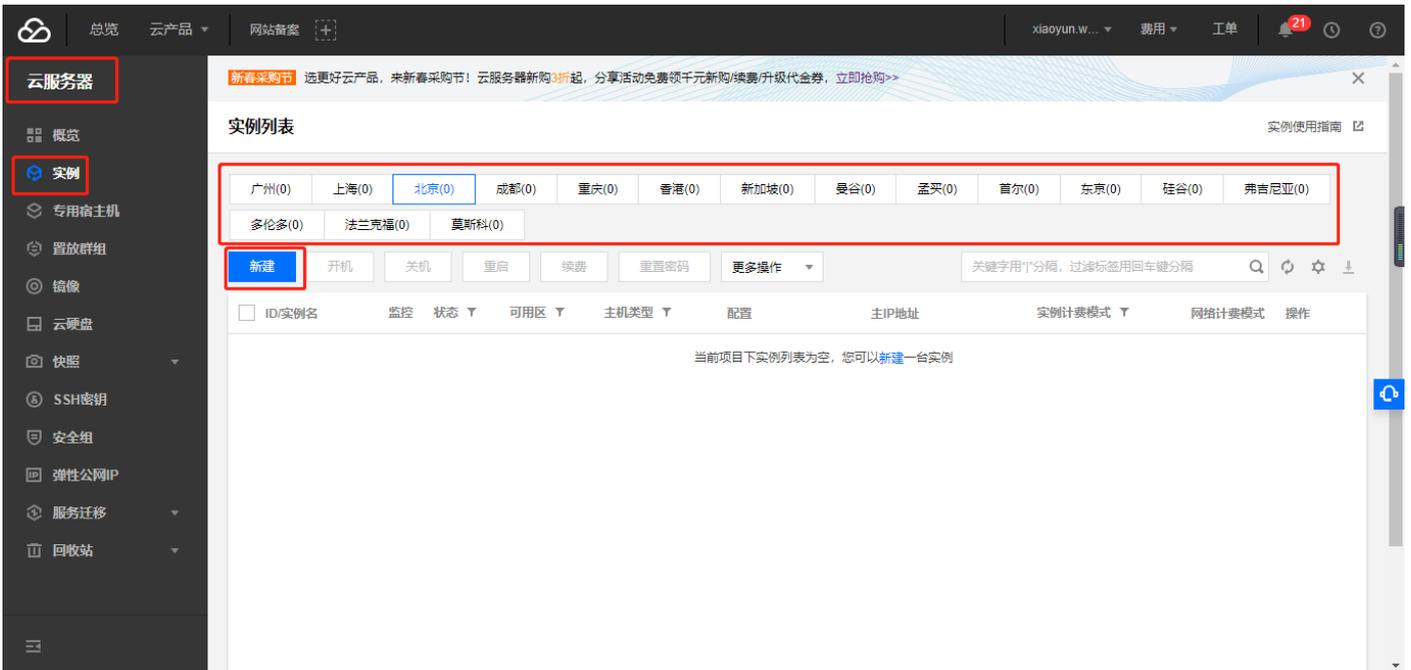
1. **防火墙、入侵防护系统 (IPS)、防病毒和防僵尸网络技术**保护云中服务免遭未经授权访问，并阻止攻击
2. **应用程序控制**帮助阻止应用程序层拒绝服务 (DoS) 攻击，并保护混合云服务安全
3. **移动访问**允许移动用户使用具有双重身份验证和设备配对的 SSL 加密连接，连接到混合云
4. **数据丢失防护**保护敏感数据免遭窃取或意外丢失
5. **SandBlast 零日保护沙盒**技术提供最高级的保护，防范恶意软件和零日攻击本地和混合云基础设施的集中化管理通过单一控制台对云和本地安全进行集中配置与监控，统一安全策略管理，达到所有公司数据安全轨迹的一致性。与来自物理基础设施的日志记录一样，混合云工作负载流量会被记录，并可在同一仪表板中轻松查看。这可确保跨混合云和物理网络应用适当级别的保护。
6. **整合性日志记录和报告** Check Point 跨云和本地网络整合监控、日志记录和报告功能。可针对云工作负载流量生成安全报告，以跟踪整个混合云网络的安全合规性，从而简化报告和审核流程。通过单个仪表板集中安全管理的各个方面，如策略管理、日志记录、监控、事件分析和报告，安全管理员可全面了解整个组织的安全状态。

### 1.2 安装要求及注意事项

- 购买主机的配置要求**建议选择 2 核 CPU，内存最低 4G**（因为系统是 64 位系统，建议给 4G 内存）。
- **系统默认用户名和密码为 admin/admin**，在初始化引导时有密码修改。
- 产品授权方式分为试用版本和正式版本，镜像本身默认提供给用户 15 天的试用期，在此期间所有的功能都可以正常试用。试用期过后如果没有新的授权，所有的功能均不能使用。正式版本需要您购买相应的许可服务。

## 第二章 购买实例的相关参数

### 2.1 新建主机



### 2.2 选择地域与机型

这里建议最低配置 4G 内存，因为系统是 64 位系统



## 2.3 选择镜像

### 在镜像市场选择镜像



## 2.4 选择存储和带宽

### 根据自己需求购买相关的硬盘和宽带速度



## 2.5 设置安全组和主机

### 安全组可自定义

快速配置 | 自定义配置

1.选择地域与机型    2.选择镜像    3.选择存储和带宽    **4.设置安全组和主机**    5.确认配置信息

所属项目: 默认项目

安全组: 新建安全组 | **已有安全组**

**sg-4j6zm1zx | 放通全部端口** 使用指引 这里我们选择了默认安全组，也可以根据自己需求进行更改

如您有业务需要放通其他端口，您可以 [新建安全组](#)

安全组规则: 入站规则 | 出站规则

来源	协议端口	策略	备注
0.0.0.0/0	TCP:22	允许	一键放通入站规则

费用: 配置费用 **0.73元/小时** (阶梯计费) | 带宽费用 **0.80元/GB**

[上一步](#) | [下一步: 确认配置信息](#)

咨询·建议

### 实例名称不填，登陆密码保留原始

1.选择地域与机型    2.选择镜像    3.选择存储和带宽    **4.设置安全组和主机**    5.确认配置信息

实例名称: 可选，不填默认未命名 你还可以输入60个字符

登录方式: 设置密码 | 立即关联密钥 | 自动生成密码 | **保留镜像设置**

注: 创建后，您可使用自定义镜像内登录信息(密钥/密码)登录。

安全加固:  免费开通   
 安装组件免费开通DDoS防护和云镜主机防护 [详细介绍](#)

云监控:  免费开通   
 免费开通云产品监控、分析和实施告警，安装组件获取主机监控指标 [详细介绍](#)

定时销毁:  开启定时销毁   
 开启定时销毁后，系统将在设定时间点自动销毁机器

[高级设置](#)

费用: 配置费用 **0.69元/小时** (阶梯计费) | 带宽费用 **0.80元/GB**

[上一步](#) | [下一步: 确认配置信息](#)

咨询·建议

## 2.6 确认配置信息

配置完就可以开通了

1.选择地域与机型    2.选择镜像    3.选择存储和带宽    4.设置安全组和主机    **5.确认配置信息**

▼ 存储和带宽 100GB系统盘; 按使用流量: 5Mbps [编辑](#)

▼ 安全组 sg-4j6zm1zx | 放通全部端口 [编辑](#)

▼ 设置信息 跟随镜像设置 [编辑](#)

购买数量:  1    **配置完就可以开通了**

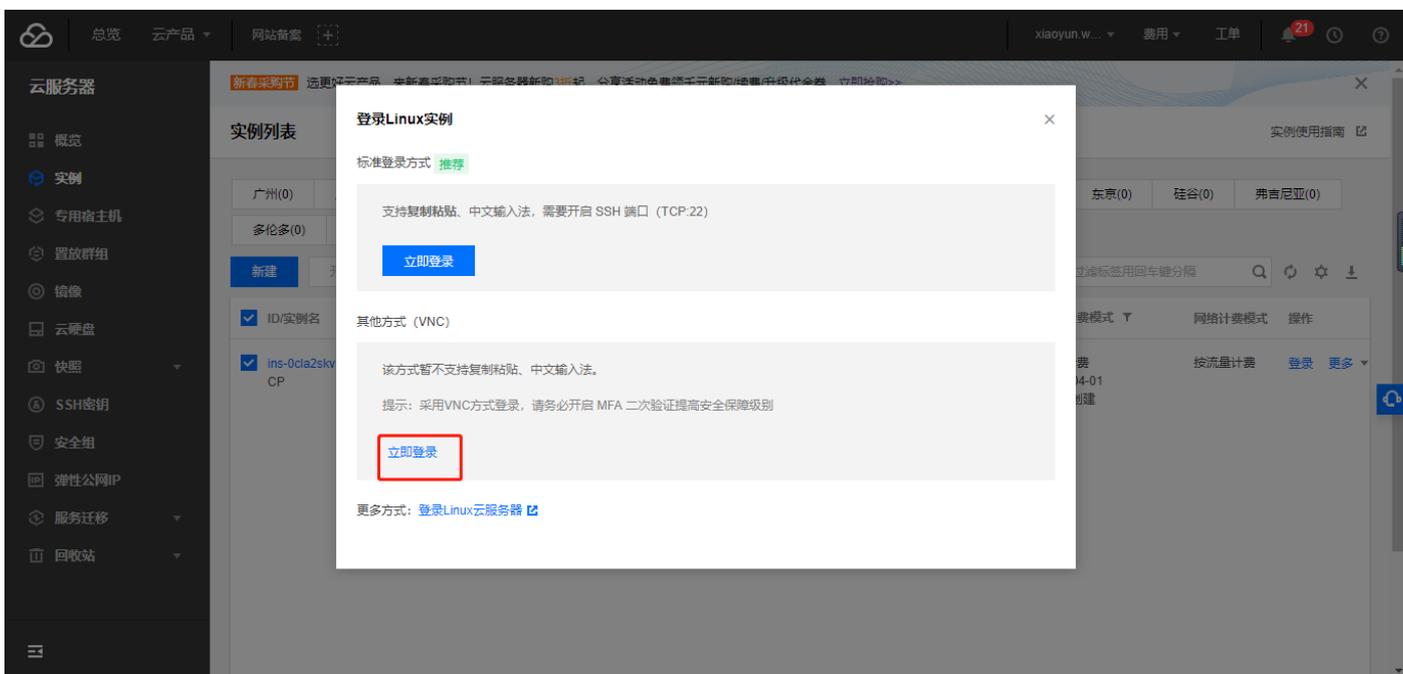
费用: 配置费用 **0.73元/小时** (阶梯计费 ⓘ) | 带宽费用 **0.80元/GB**

Tencent 腾讯开放平台 QQ物联 DNSPod 微信公众平台 腾讯优图 腾讯蓝鲸 企业QQ 腾讯微云 腾讯文档 友情链接 中国站

Copyright © 2013-2019 Tencent Cloud. All Rights Reserved. 腾讯云 版权所有 京公网安备 11010802017518 粤B2-20090059-1

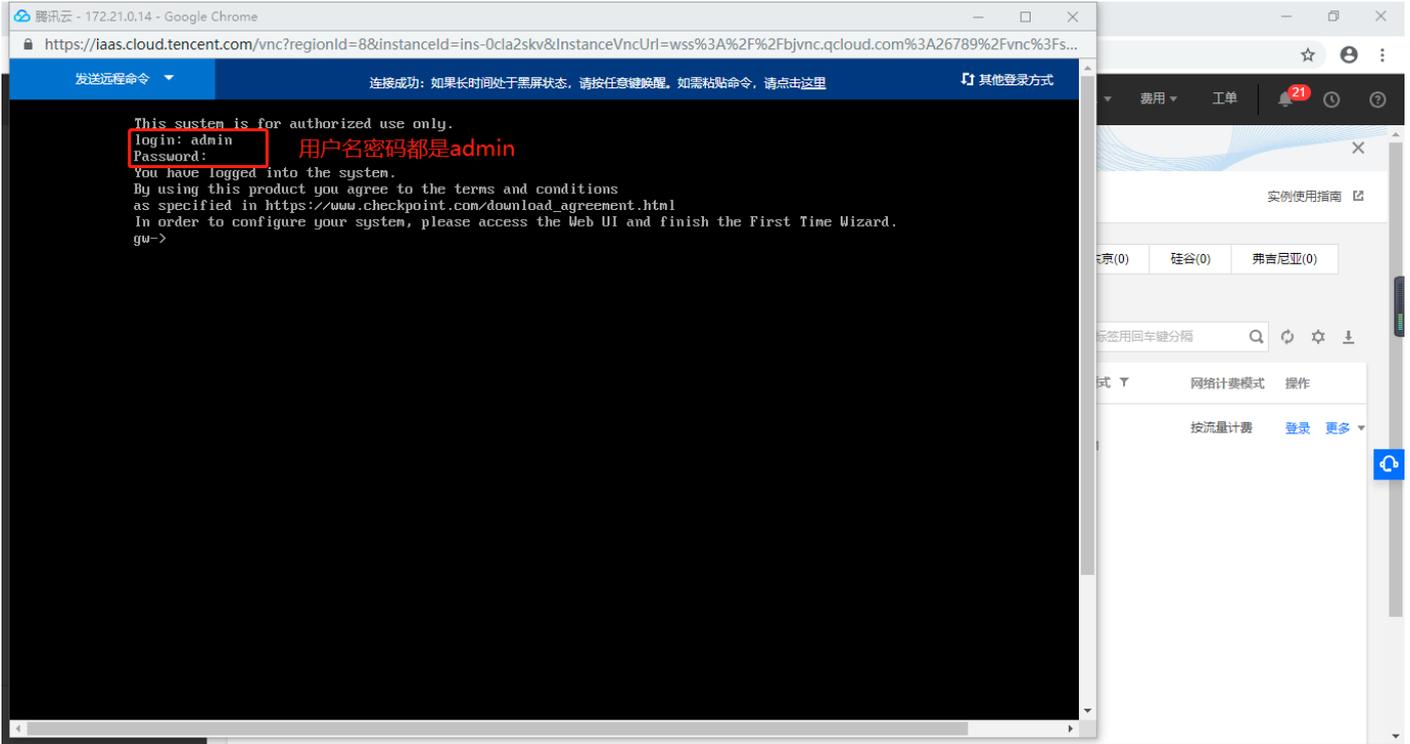
## 第三章 配置主机网络

### 3.1 登陆 VNC



### 3.2 登陆 checkpoint 命令行

用户名和密码都是 admin



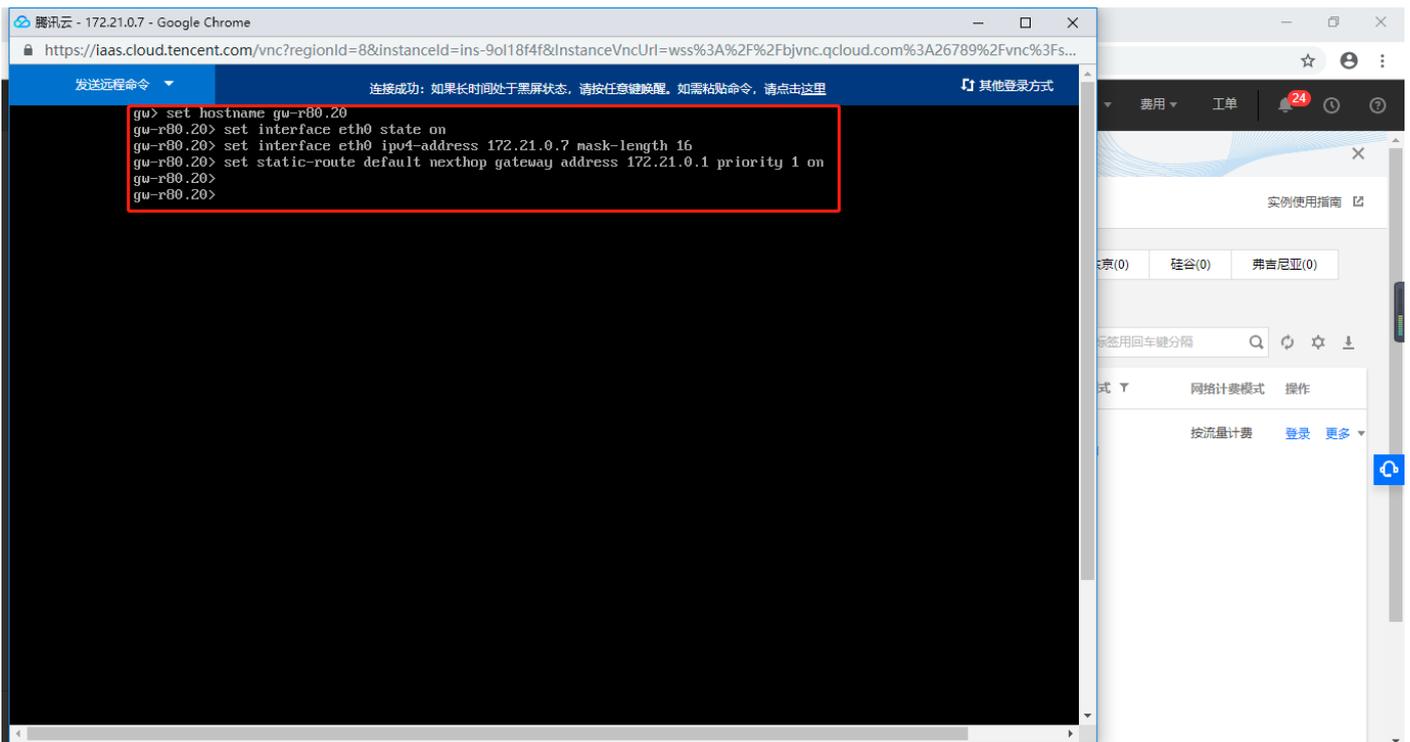
### 3.3 配置网络地址及默认路由

Set hostname gw-r80.20 (这里必须配置用户名带有破折号(-)和句号(.))

Set interface eth0 state on (先打开 eth0 端口的状态)

Set interface eth0 ipv4-address 172.21.0.7 mask-length 16 (配置接口地址 )

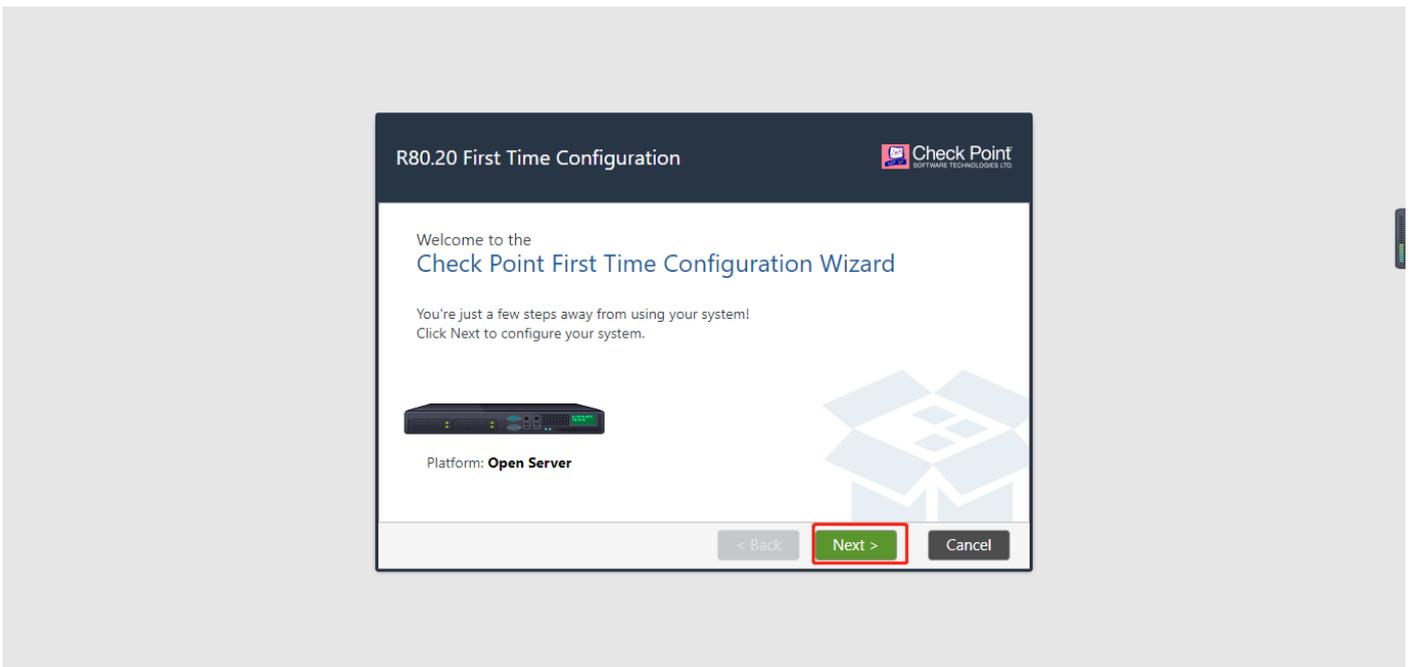
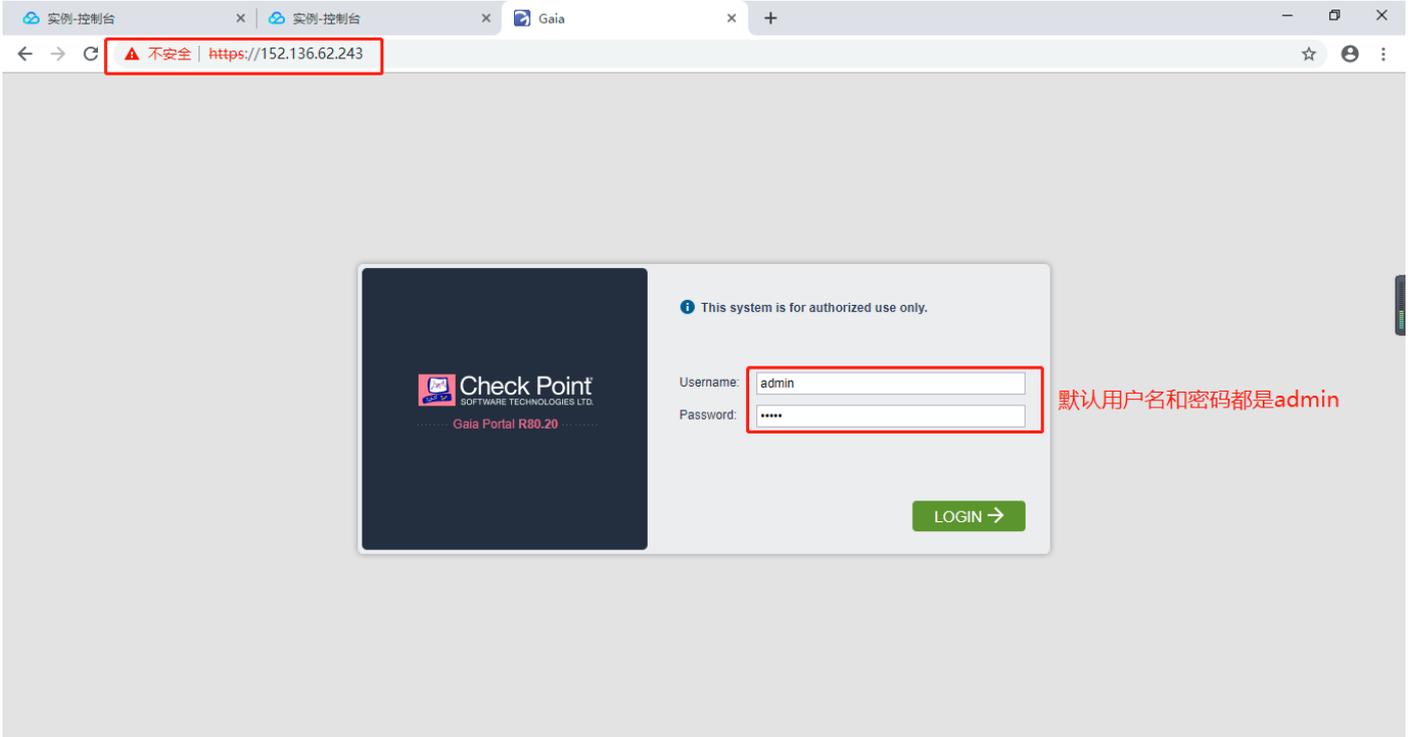
Set static-route default nexthop gateway address 172.21.0.1 priority 1 on (配置默认路由)



## 第四章 Gaia (底层系统) 初始化

### 4.1 登陆 Gaia 系统

接下来以红圈标注为建议设置



### Deployment Options

Check Point  
SOFTWARE TECHNOLOGIES LTD.

Setup

Continue with R80.20 configuration

Installation

Install from Check Point cloud  
 Install from USB device

Recovery

Import existing snapshot ?

< Back   **Next >**   Cancel

### Authentication Details

Check Point  
SOFTWARE TECHNOLOGIES LTD.

Change the default administrator password:

Password:  Good

Confirm Password:  更改密码

It is strongly recommended to use both uppercase and lowercase characters as well as one of the following characters in the password: !@#\$%^&\*()-\_+=;

< Back   **Next >**   Cancel

### Management Connection

Interface: eth0

Configure IPv4:

IPv4 address:

Subnet mask:

Default Gateway:

Configure IPv6:

IPv6 Address:

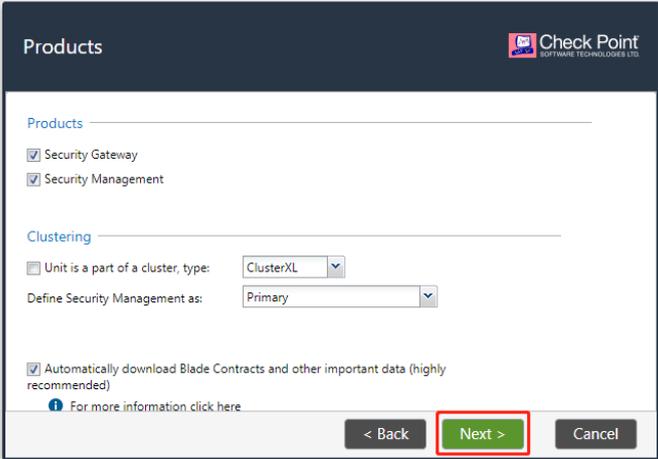
Mask Length:

Default Gateway:

### Installation Type

Security Gateway and/or Security Management

Multi-Domain Server



**Products** 

Products

- Security Gateway
- Security Management

Clustering

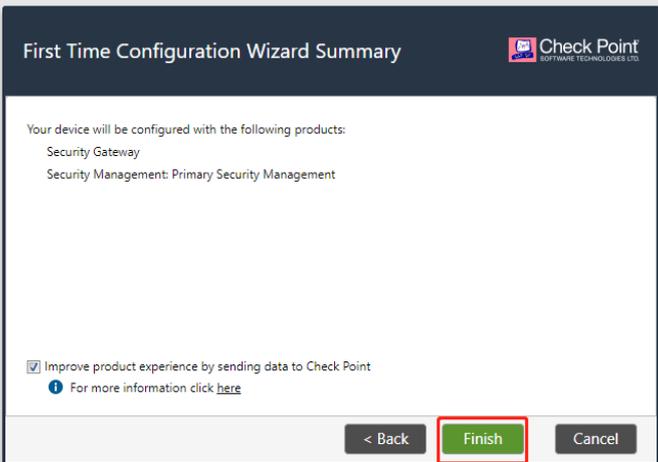
Unit is a part of a cluster, type: ClusterXL

Define Security Management as: Primary

Automatically download Blade Contracts and other important data (highly recommended)

 For more information click here

< Back **Next >** Cancel



**First Time Configuration Wizard Summary** 

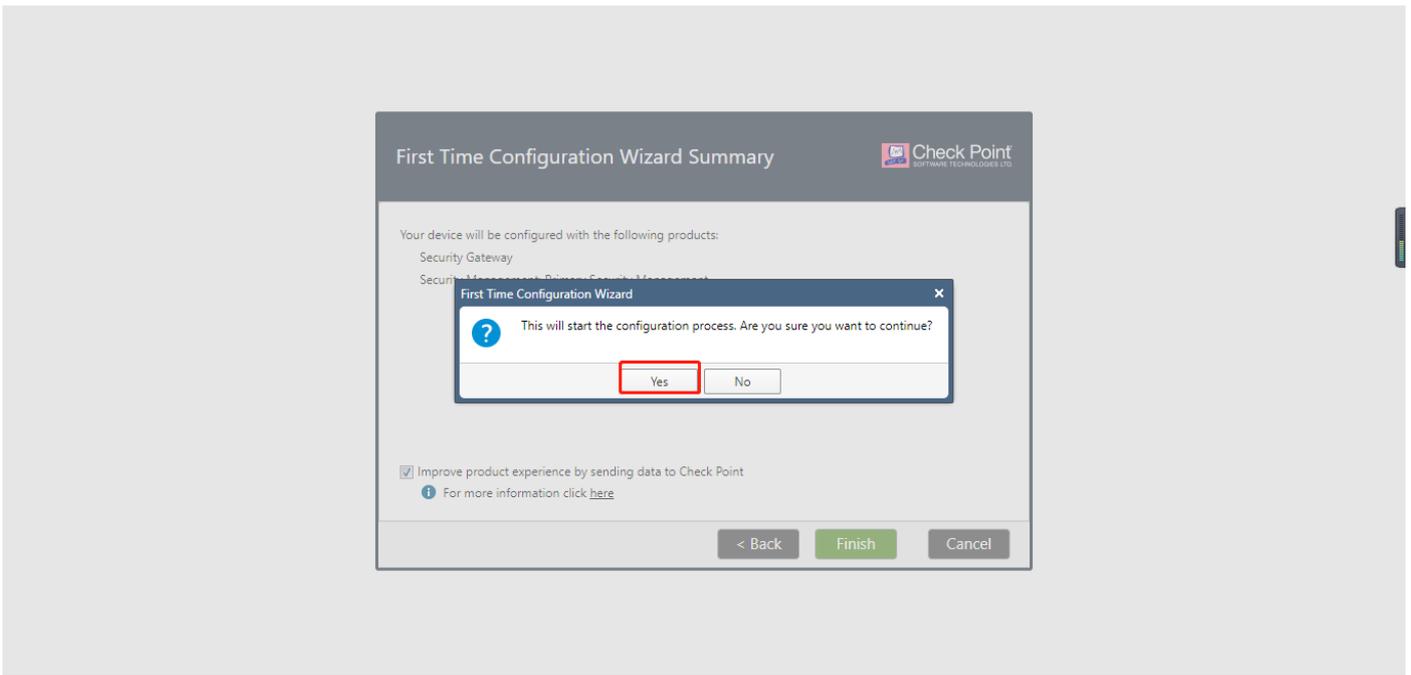
Your device will be configured with the following products:

- Security Gateway
- Security Management: Primary Security Management

Improve product experience by sending data to Check Point

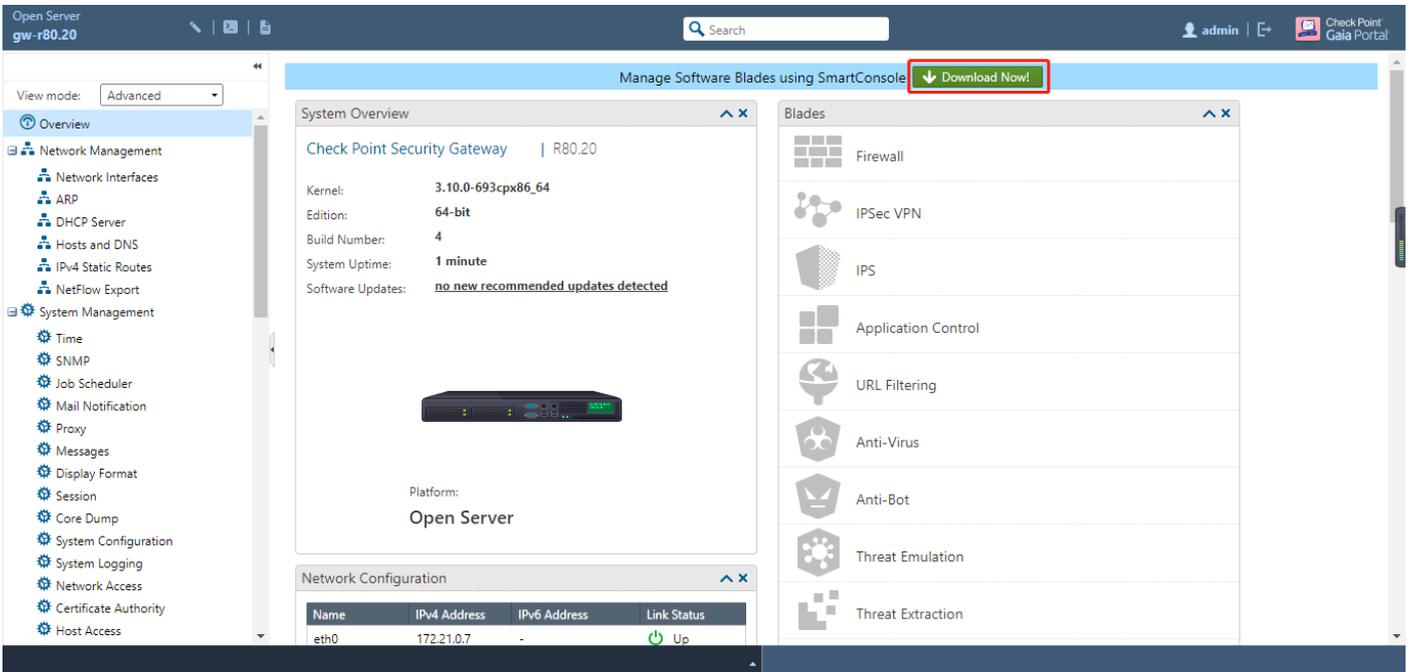
 For more information click [here](#)

< Back **Finish** Cancel

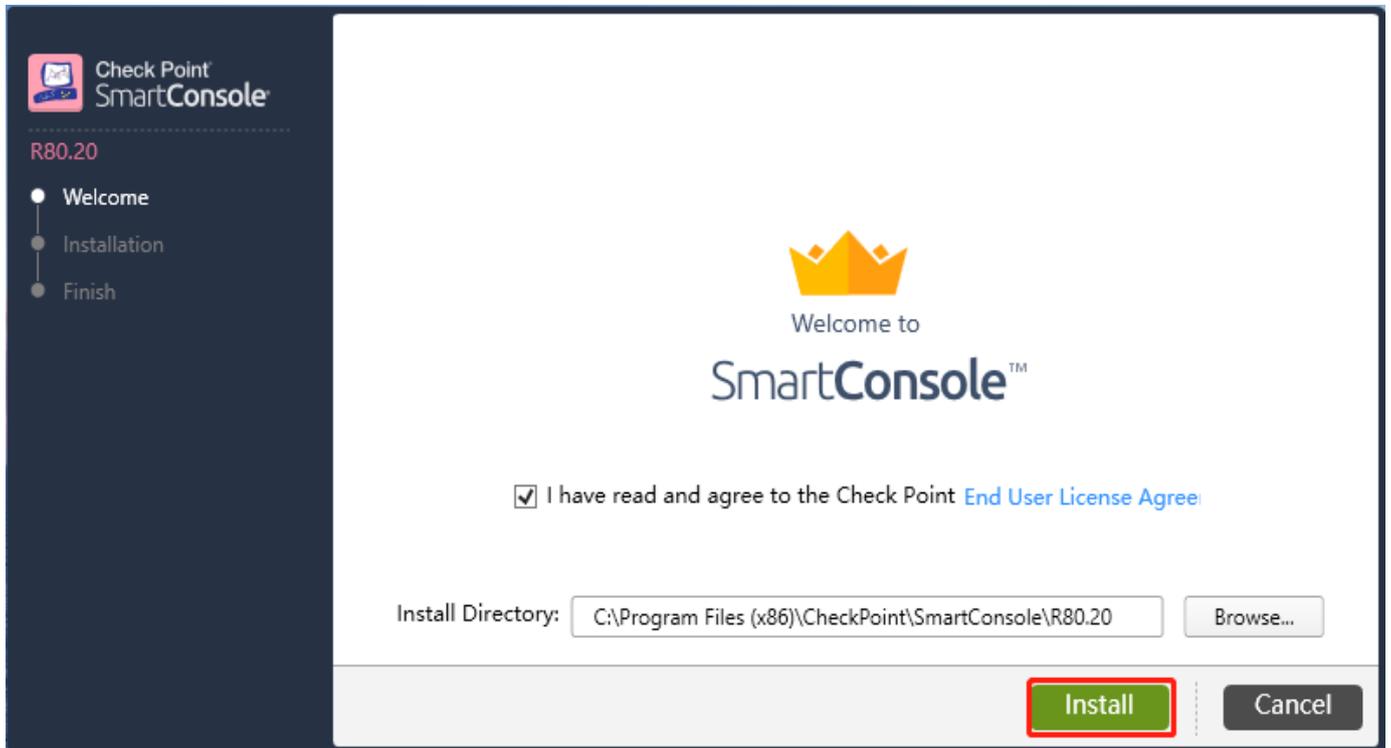


## 第五章 通过 SmartConsole 配置防火墙的相关功能

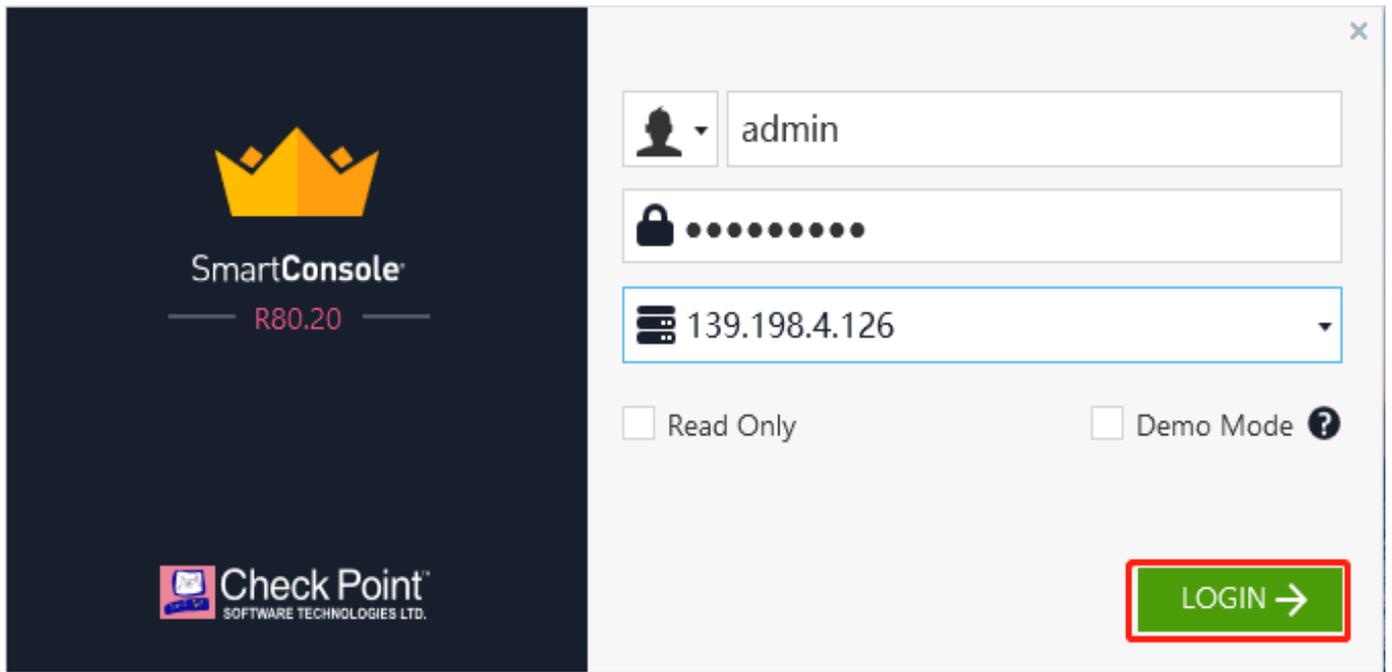
### 5.1 下载和安装 SmartConsole 客户端



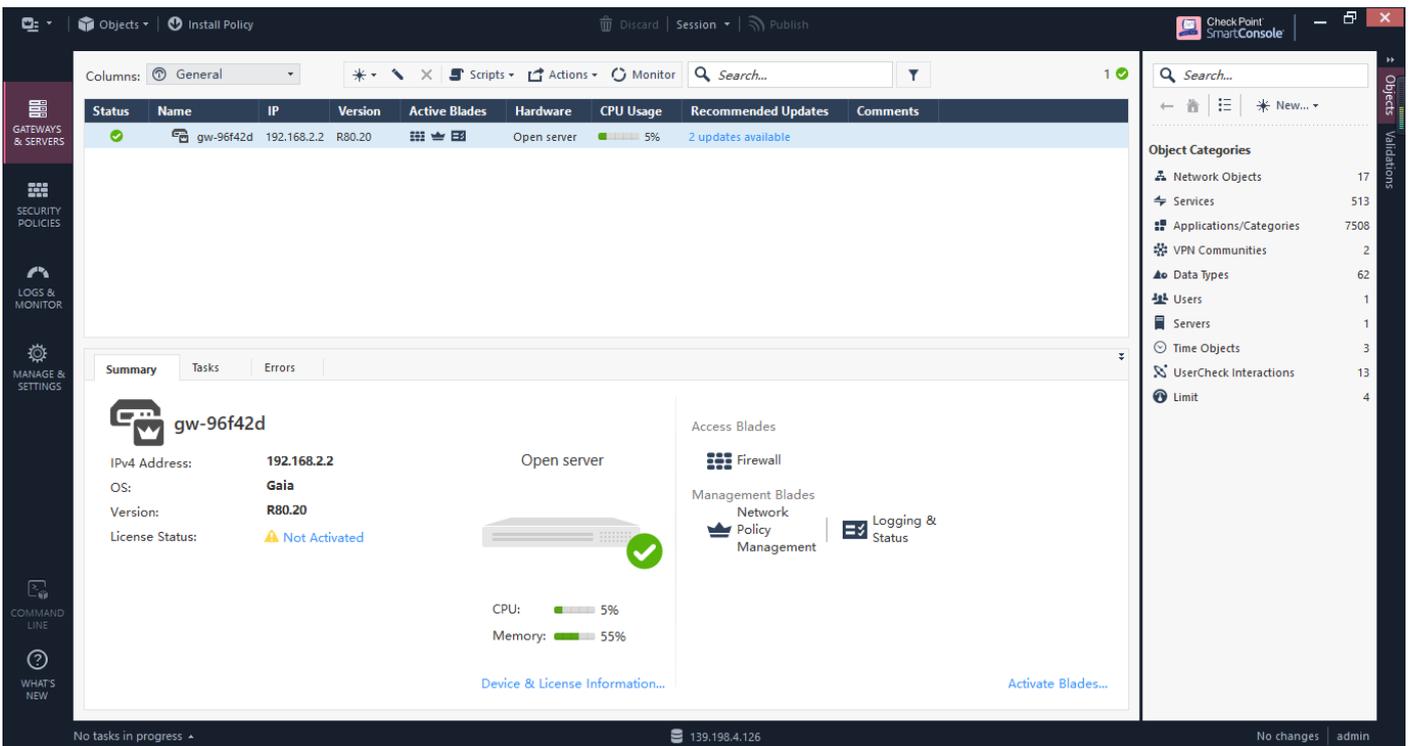
### 安装 SmartConsole



## 登陆 SmartConsole

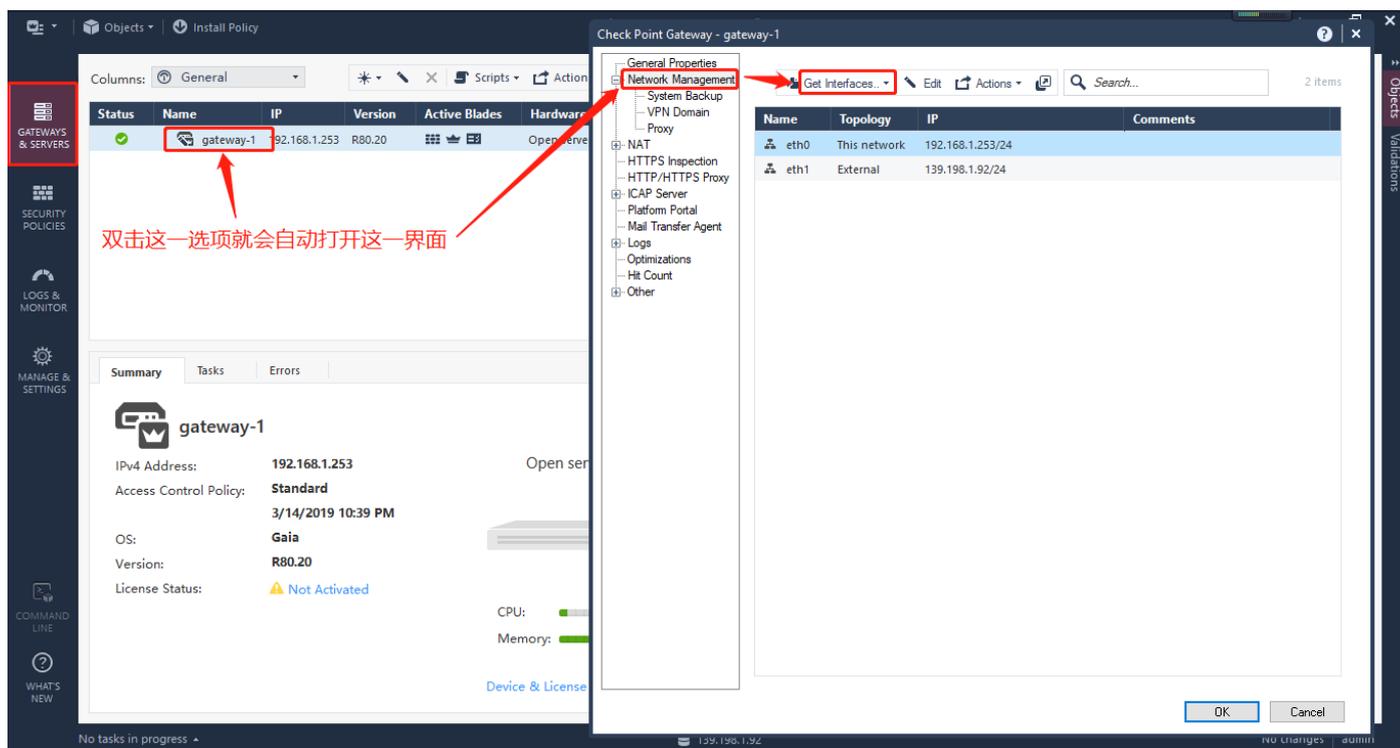


## SmartConsole 主页面

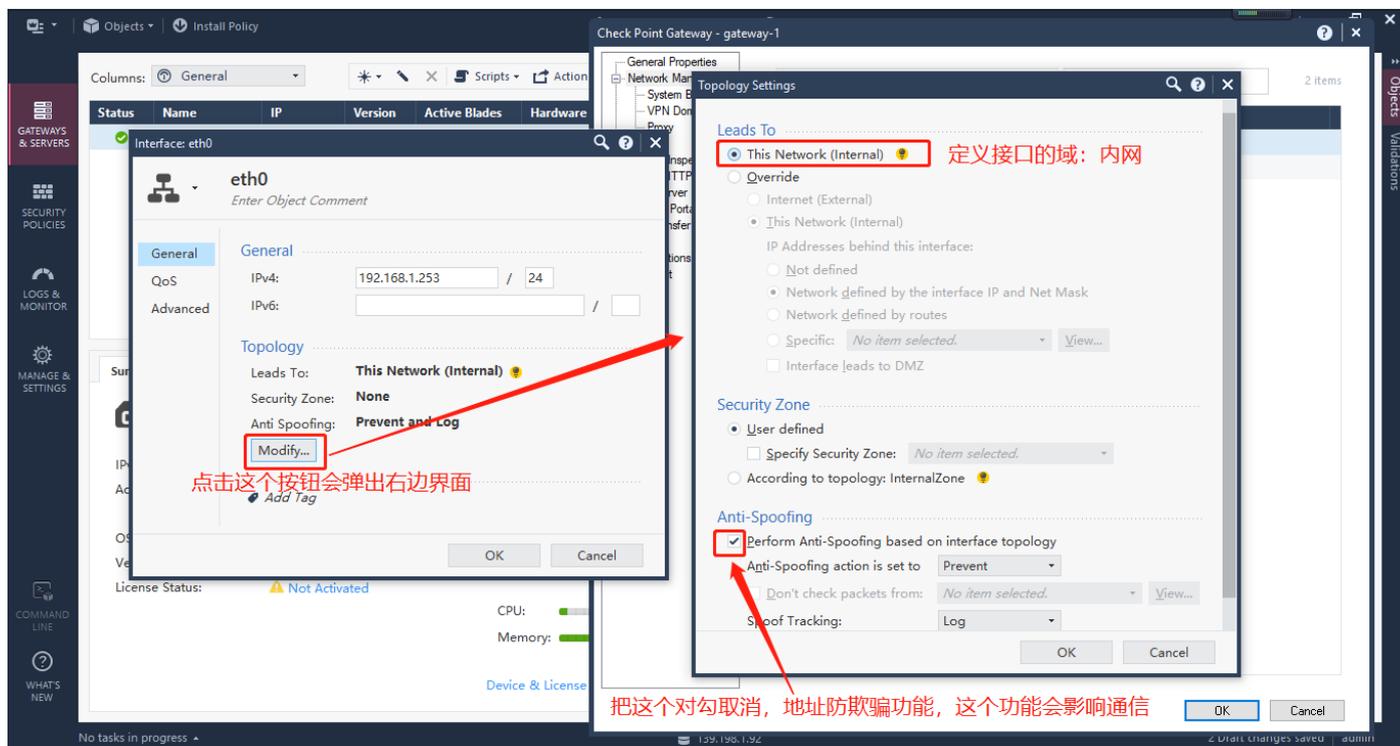


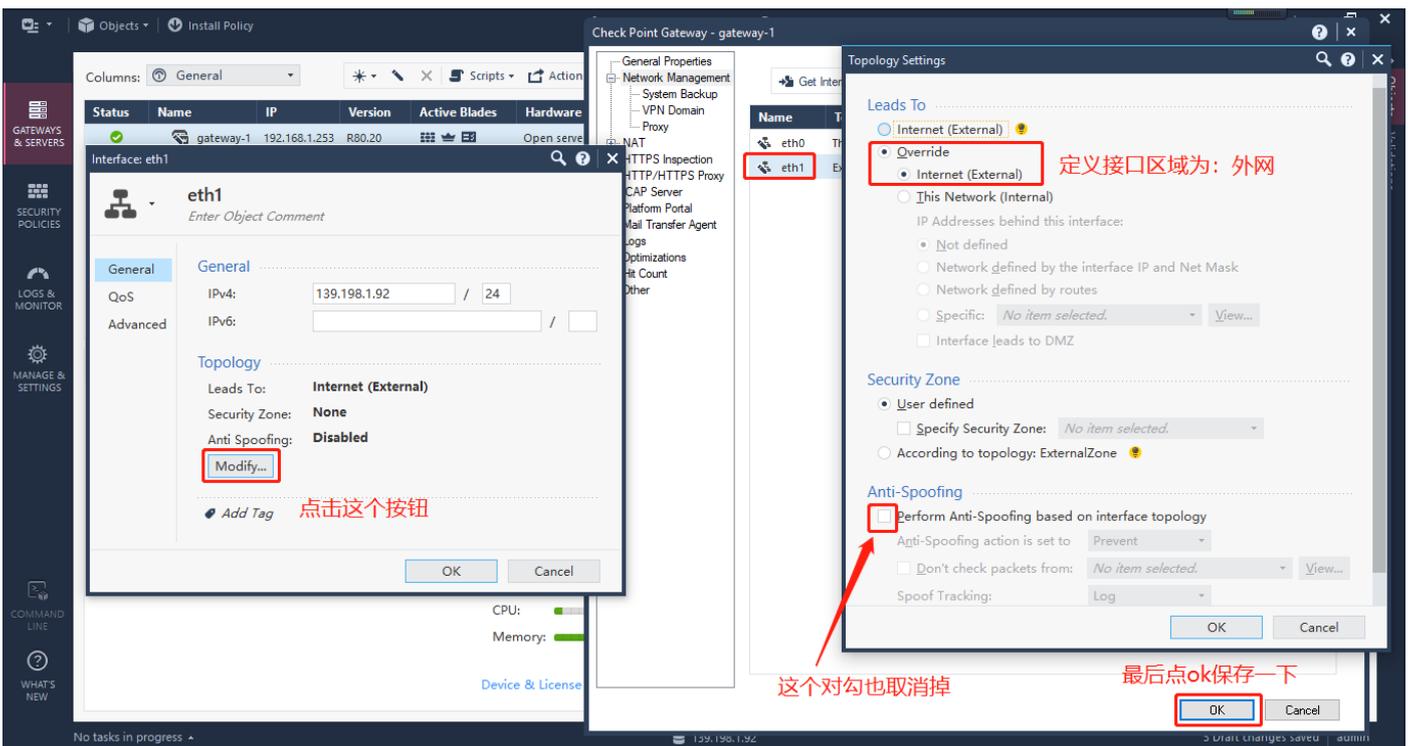
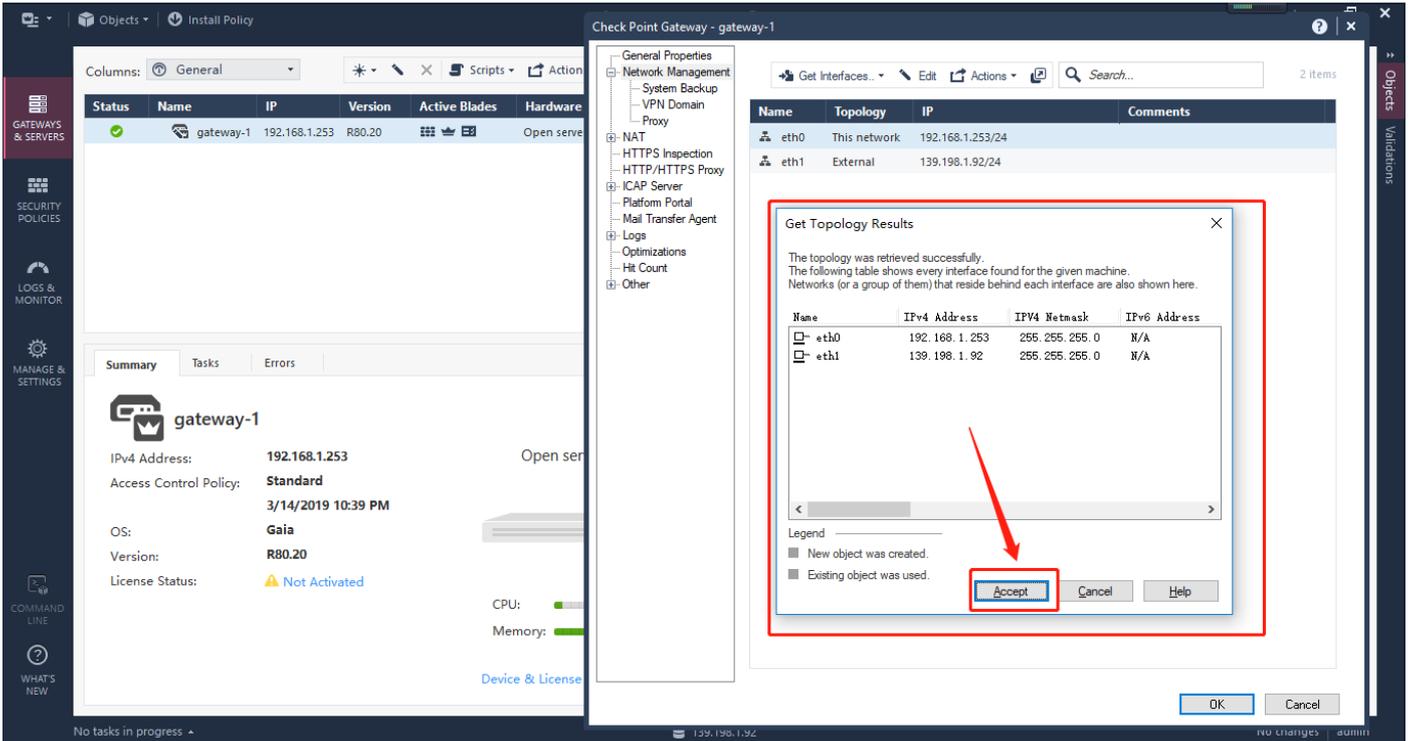
## 5.2 Get 底层的拓扑信息

让上层 FW 获取底层接口信息及拓扑



## 5.3 定义接口域并关闭接口地址防欺骗功能





## 5.4 编辑策略

Accept 允许 拒绝

日志

策略安装到哪一个 gateway 上

No.	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	* Any	* Any	* Any	* Any	Accept	Log	gate...

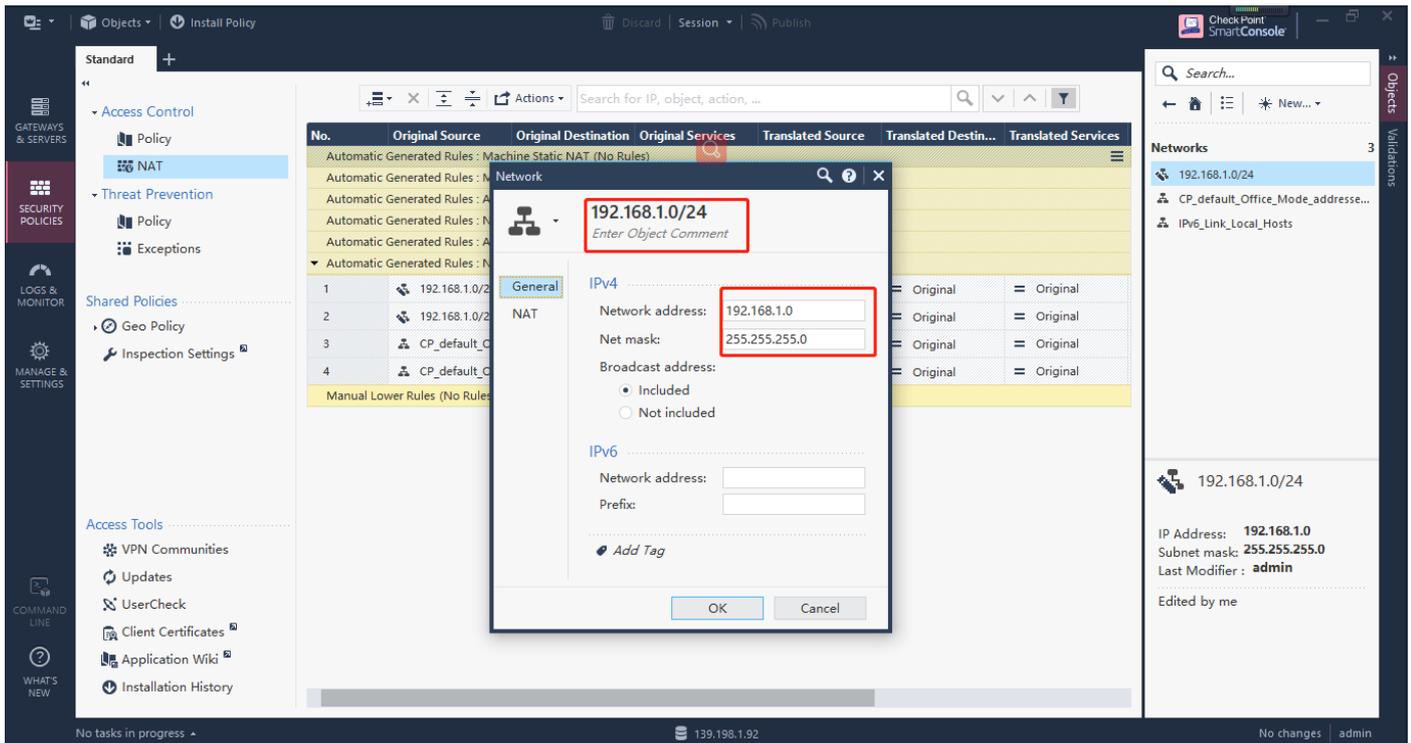
Missing cleanup rule - Unmatched traffic will be dropped and not logged.

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Descrip...
Today, 1:03:35	gateway-1	gateway-1 (1...		100.64.0.3	domain-udp (UDP/53)	1	Cleanup rule	Standard	domain-u...
Today, 1:03:35	gateway-1	gateway-1 (1...		public1.sdns...	domain-udp (UDP/53)	1	Cleanup rule	Standard	domain-u...
Today, 1:03:30	gateway-1	gateway-1 (1...		100.64.0.3	domain-udp (UDP/53)	1	Cleanup rule	Standard	domain-u...
Today, 1:03:29	gateway-1	gateway-1 (1...		public1.sdns...	domain-udp (UDP/53)	1	Cleanup rule	Standard	domain-u...
Today, 1:03:25	gateway-1	37.49.225.71		gateway-1 (1...	smtp (TCP/25)	1	Cleanup rule	Standard	smtp Traff...
Today, 1:03:24	gateway-1	37.49.225.71		gateway-1 (1...	smtp (TCP/25)	1	Cleanup rule	Standard	smtp Traff...

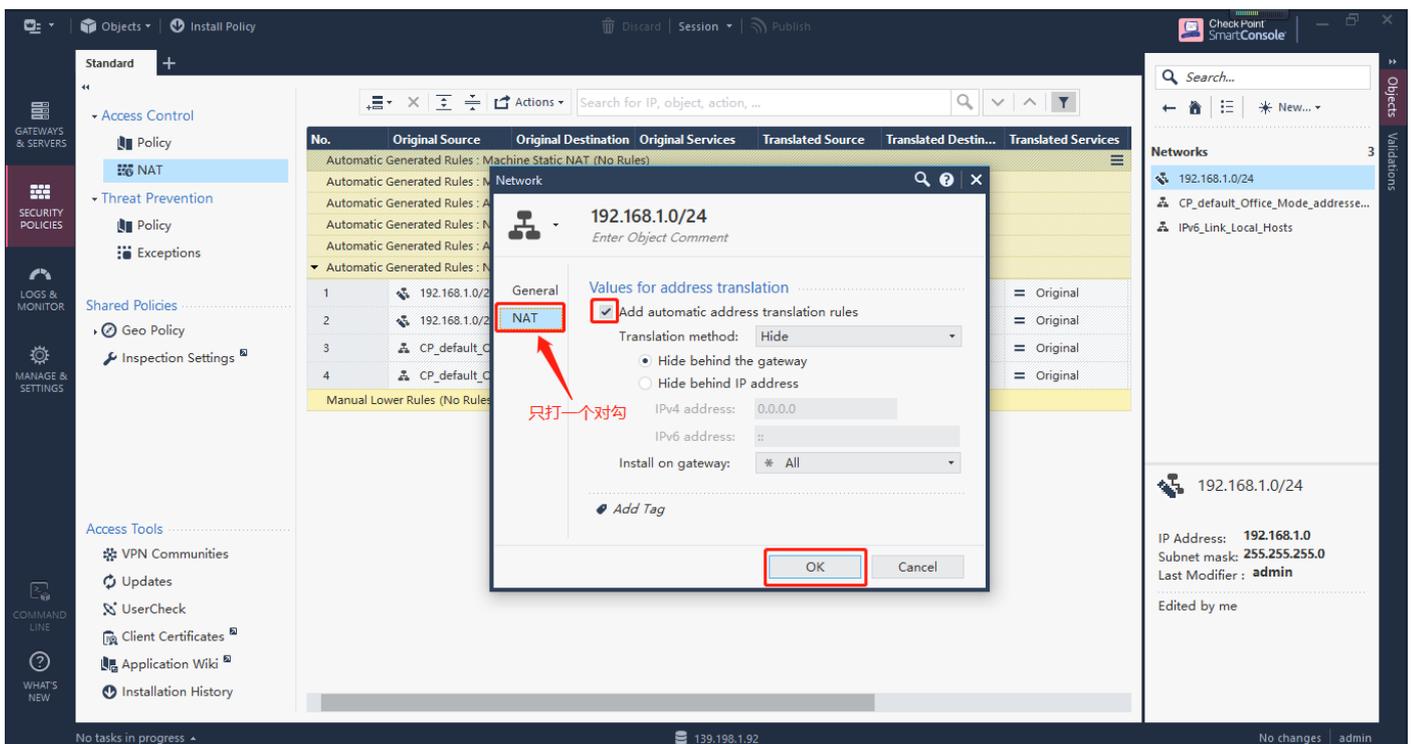
## 5.5 开启内网段的 SNAT

首先新建内网路地址段

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services
1	192.168.1.0/24	192.168.1.0/24	* Any	= Original	= Original	= Original
2	192.168.1.0/24	* Any	* Any	192.168.1.0/24 (f	= Original	= Original
3	CP_default_Of...	CP_default_Offic	* Any	= Original	= Original	= Original
4	CP_default_Of...	* Any	* Any	CP_default_Offic	= Original	= Original



## 开启 NAT



## 5.6 下发策略并生效

最关键一步，下发策略，也就是保存并生效

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services
Automatic Generated Rules : Machine Static NAT (No Rules)						
Automatic Generated Rules : Machine Hide NAT (No Rules)						
Automatic Generated Rules : Address Range Static NAT (No Rules)						
Automatic Generated Rules : Network Static NAT (No Rules)						
Automatic Generated Rules : Address Range Hide NAT (No Rules)						
Automatic Generated Rules : Network Hide NAT (1-4)						
1	192.168.1.0/24	192.168.1.0/24	* Any	= Original	= Original	= Original
2	192.168.1.0/24	* Any	* Any	192.168.1.0/24 (I	= Original	= Original
3	CP_default_Of...	CP_default_Offic	* Any	= Original	= Original	= Original
4	CP_default_Of...	* Any	* Any	CP_default_Offic	= Original	= Original
Manual Lower Rules (No Rules)						

有这两条NAT，证明开启成功，剩下那两条是系统自动的不用管

注：只要内部计算机的网关指向防火墙的内部接口地址，内网计算机就可以上网了

有问题请联系相关的技术人员