

# Check Point R81 基于阿里云部署手册

上海溪盎科技有限公司

2022.10

# 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 使用新密钥登录主机

## 第四章 Gaia(底层系统)初始化

- 4.1 登陆 Gaia 系统并配置

## 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 CloudGuard 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 4 核 CPU，内存最低 16G**（因为系统是 64 位系统，建议给 4G 内存）。
- 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。

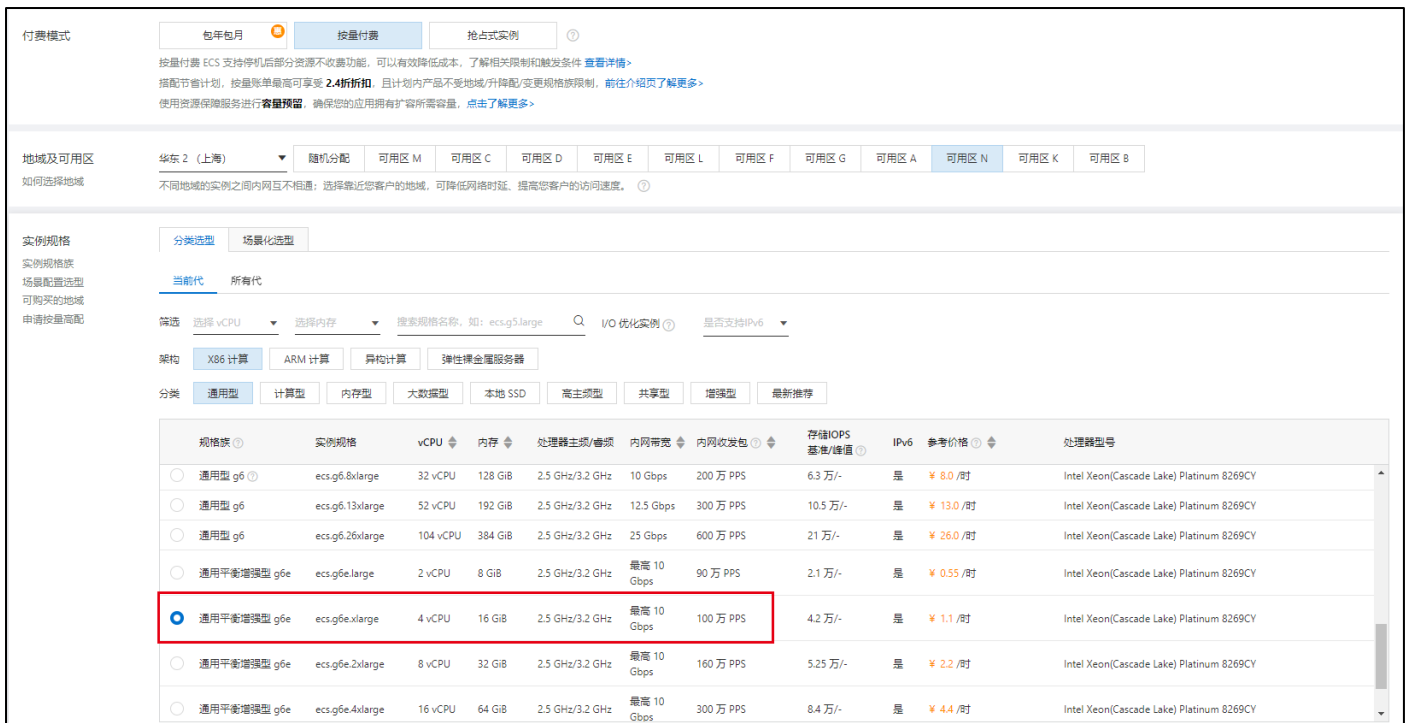
## 第二章 购买实例的相关参数

### 2.1 新建主机



### 2.2 选择地域与机型

这里建议选型计算型 4C 16G 主机起步，因为系统为 64 位系统



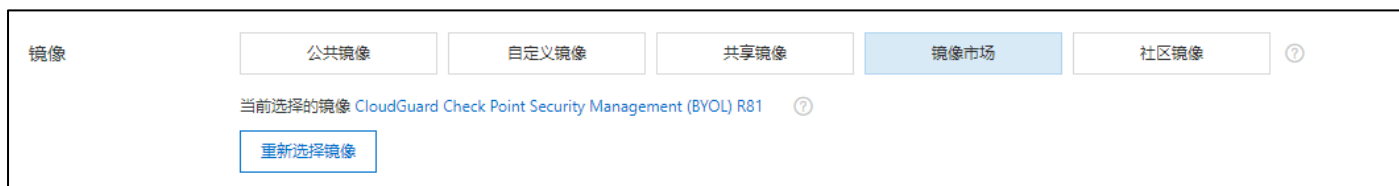
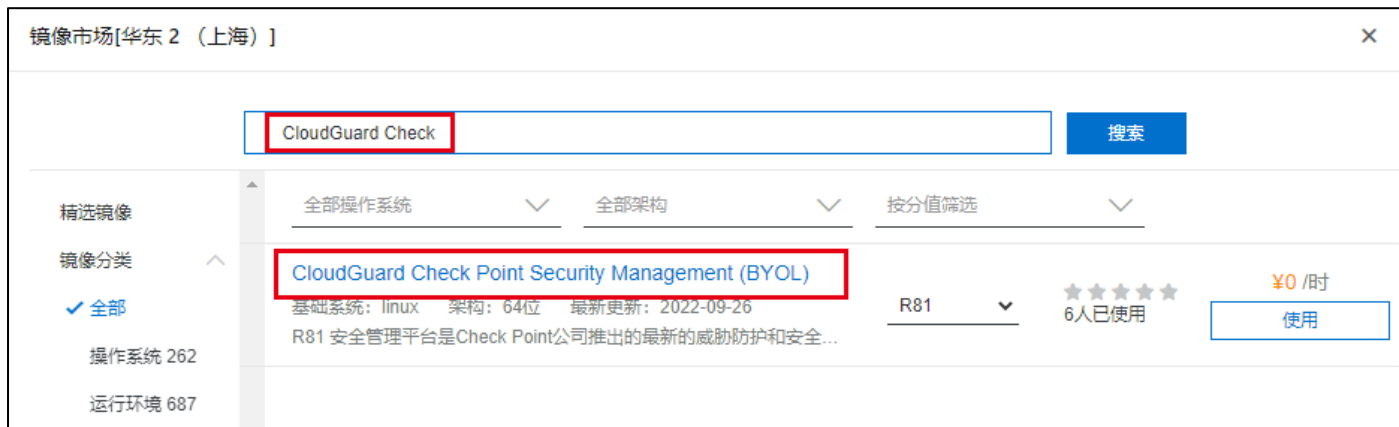
## 2.3 选择镜像

在镜像市场选择镜像

不同的镜像对应不同的实例类型：

CloudGuard Check Point Security Management (BYOL)对应实例类型是通用型 g7, g6e

CloudGuard Check Point Network Security Gateway (BYOL)对应实例类型是增强型 g7ne, g5ne



## 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



公网 IP  分配公网 IPv4 地址  
 公网带宽计费 系统会分配公网 IP，也可采用更加灵活的弹性公网 IP 方案，了解 [如何配置并绑定弹性公网 IP 地址](#)>

带宽计费模式   ?  
 带宽费用合并并在ECS实例中收取

带宽值  Mbps  
 1M 25M 50M 75M 100M

阿里云免费提供最高 5Gbps 的恶意流量攻击防护，[了解更多](#) | [提升防护能力](#)

## 2.5 设置安全组和密钥对

### 安全组可自定义

安全组  ? 安全组类似防火墙功能，用于设置网络访问控制，您也可以到管理控制台 [新建安全组](#) > [安全FAQ](#)>

安全组限制

配置安全组 **所选安全组 1). xiang\_group / sg-uf6ak2cblnw0qakdw1a9** (已有 4 个实例+辅助网卡，还可以加入 1996 个实例+辅助网卡)

请确保所选安全组开放包含 22 (Linux) 或者 3389 (Windows) 端口，否则无法远程登录ECS。您可以进入ECS控制台设置。[前往设置](#)>

### 配置密钥对

登录凭证

登录名  root

密钥对 ?   | [如何使用密钥对](#)

密钥对用于远程 SSH 连接设备。

## 2.6 确认配置信息

所选配置

基础配置 <a href="#">?</a>	付费模式： 按量付费 购买数量： 1 台	地域及可用区： 华东 2 可用区 N 镜像： <a href="#">Linux/Windows/Check Point/Debian/Canonical/Management (BYOL) R81</a> xi_lang_vpc/vpc-uf6r89m76d8zrs65jul1f	实例规格： 通用平衡增强型 g6e / ecs.g6e.large (2vCPU 8GiB) 系统盘： ESSD云盘 100GiB，PL0 (单盘IOPS性能上限1万)
网络和安全组 <a href="#">?</a>	网络： 专有网络 公网带宽： 按固定带宽 5Mbps	VPC： xi_lang_vpc/vpc-uf6r89m76d8zrs65jul1f 安全组： 1). xiang_group / sg-uf6ak2cblnw0qakdw1a9	交换机： CP-Out/vsw-uf69aq88hy7c3gagr653k/172.16.0.0/24
系统配置 <a href="#">?</a>	登录凭证： 密钥对:cp_key	实例名称： launch-advisor-20221012	实例元数据访问模式： 普通模式 (兼容加固模式)

?  ?  ?

使用期限  设置自动释放服务时间 ECS实例将在您预约的时间点进行释放，实例释放后数据及IP地址不会被保留且无法找回，请谨慎操作。

服务协议  [《云服务器ECS 服务条款》](#) | [《镜像商品使用条款》](#)  
 您可以[点此查看购买须知](#)。  
 订单对应的发票信息，请在 管理控制台-费用中心-[发票管理](#) 中查看。  
 云产品默认禁用 TCP 25 端口和基于此端口的邮箱服务，特殊情况需报审核核后使用，[查看详情](#)>

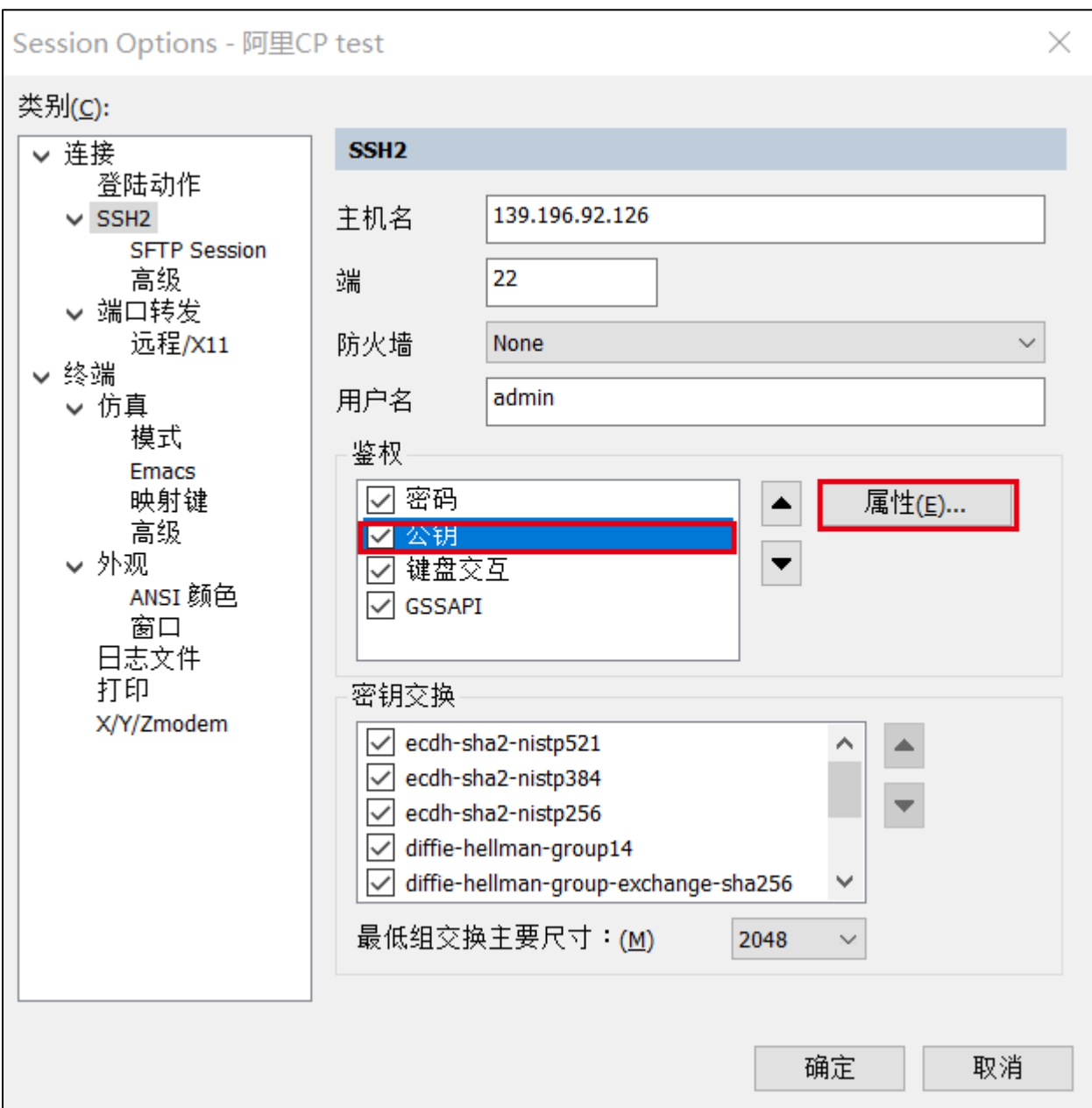
配置完就可以开通了



## 第三章 SSH 远程连接主机

### 3.1 使用新密钥文件登录主机

使用 SecureCRT 远程工具，配置会话



## 选择对应的文件

公钥属性

使用全局公钥设置(U)       使用会话公钥设置(K)

会话设置(S)

使用身份或证书文件(E)

C:\Users\admin\Documents\cp\_key.pem ...

使用个人存储证书(CAPI)(S)

CAPI    DLL: ...

要使用的证书    <Try all certificates> ...

使用证书作为原始 SSH2 密钥（服务器不支持 x.509）(I)

指纹 (%1):

SHA-2: d7:70:0c:bf:a4:c0:e7:2d:18:26:1e:ae:bc:28:d8:ba:5b:82:55:7e:54:32:99:3c  
SHA-1: a3:42:03:13:3f:99:61:af:ae:66:3e:fb:82:de:7c:62:eb:9f:84:00  
MD5: 4b:a5:dc:dd:30:71:e6:e7:b5:7f:b4:eb:a5:54:1e:c1

< ... >

创建身份文件(I)...    上传(O)    导出公钥(X)...    更改通行短语(P)...

确定

取消

## 点击跳过，进入系统

输入安全外壳密码

admin@139.196.92.126 需要一个密码。请输入密码。

用户名    admin

密码(P):

保存密码(S)

确定

取消

跳过(K)



```
This system is for authorized use only.  
Last login: Wed Oct 12 04:08:37 2022 from 101.87.178.177  
You have logged into the system.  
By using this product you agree to the terms and conditions  
as specified in https://www.checkpoint.com/download\_agreement.html  
In order to configure your system, please access the web UI and finish the First Time Wizard.  
iZuf6275hb3571p00cq4jjZ>
```

配置 admin 密码

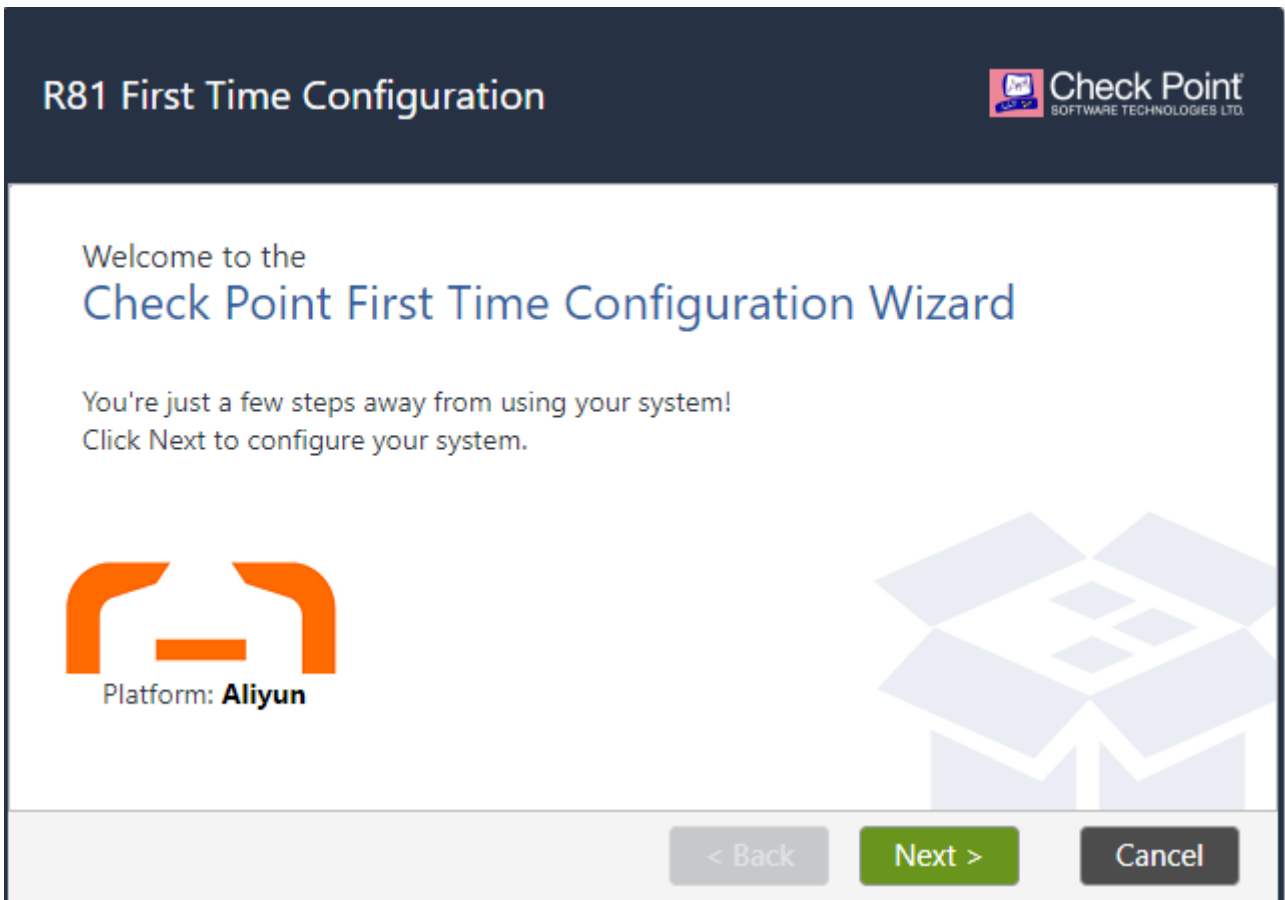
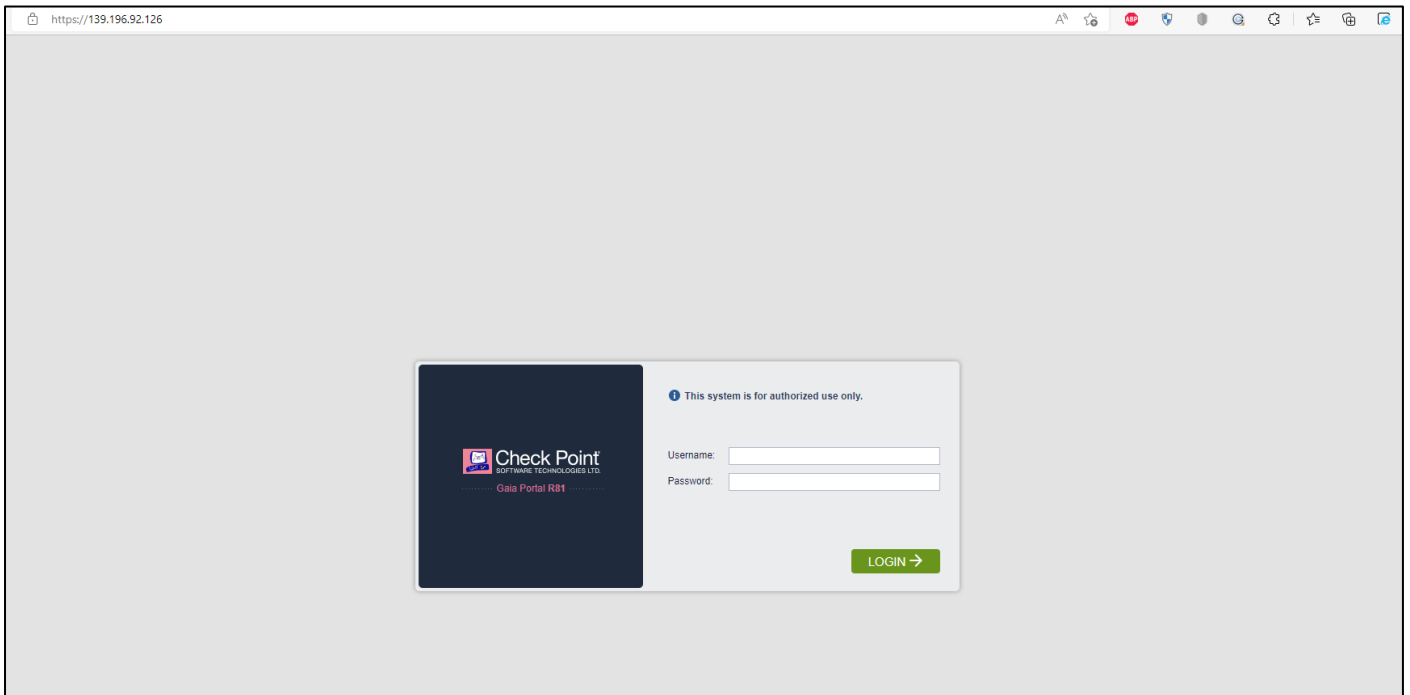
```
iZuf6275hb3571p00cq4jjZ> set user admin password  
New password:  
Verify new password:  
iZuf6275hb3571p00cq4jjZ>
```

保存退出，进行初始化


```
iZuf6275hb3571p00cq4jjZ> save config  
iZuf6275hb3571p00cq4jjZ>
```

## 第四章 Gaia (底层系统) 初始化

### 4.1 登陆 Gaia 系统



## Deployment Options

 Check Point  
SOFTWARE TECHNOLOGIES LTD.


Setup

Continue with R81 configuration

Installation


Install from Check Point cloud  
 Install from USB device

Recovery

Import existing snapshot 

< Back   Next >   Cancel

## Management Connection

 Check Point  
SOFTWARE TECHNOLOGIES LTD.

Interface: eth0

Configure IPv4:

IPv4 address:

Subnet mask:

Default Gateway:

Configure IPv6:

IPv6 Address:


Mask Length:

Default Gateway:

< Back   Next >   Cancel

## 配置主机名

### Device Information



Host Name:

Domain Name:

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:


#### Proxy Settings

Use a Proxy server

Address:

Port:

### Date and Time Settings



Set time manually:

Date:

Time:  :

Time Zone:

Use Network Time Protocol (NTP):

Primary NTP server:  Version:

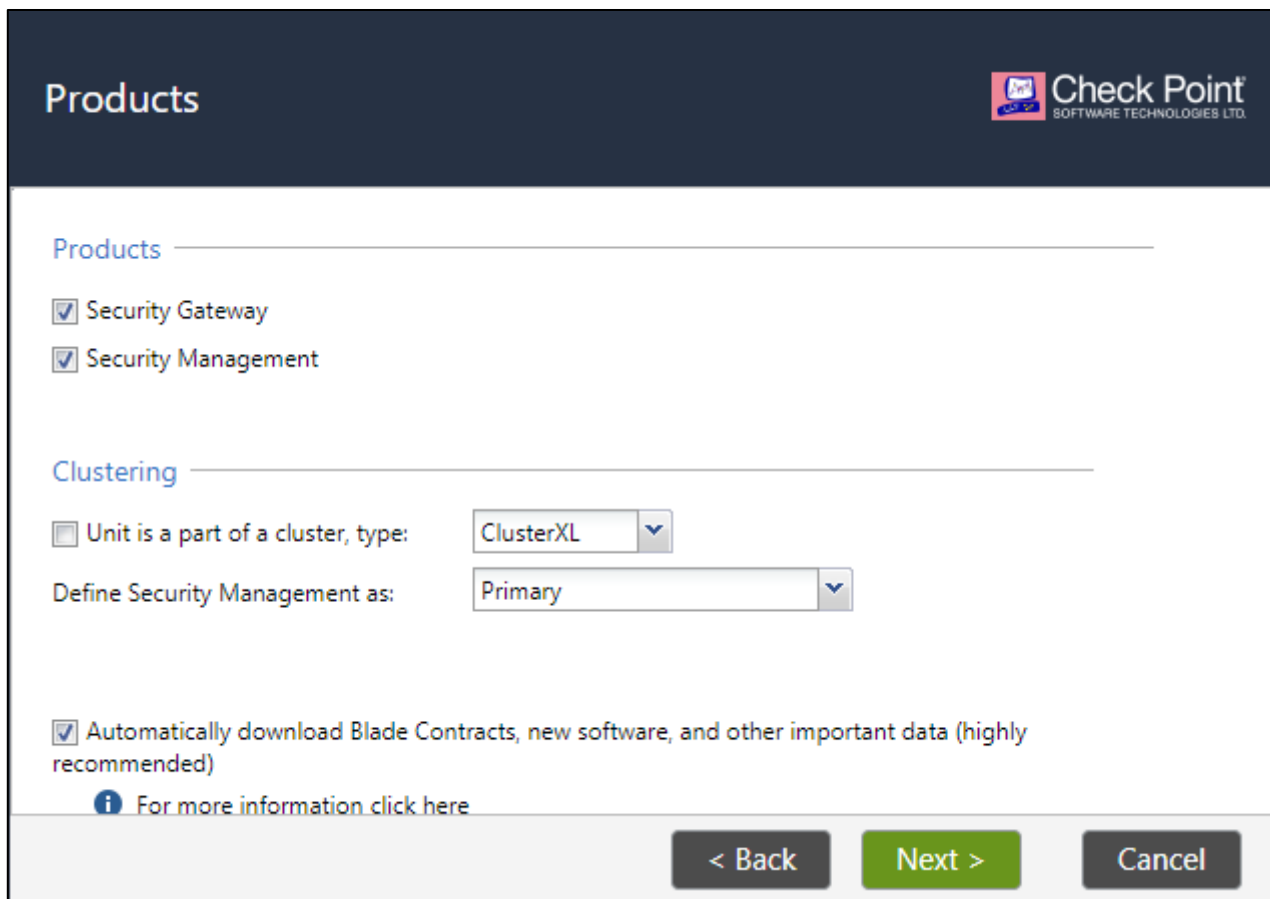
Secondary NTP server:  Version:

Time Zone:

根据需要选择安装的产品类型

- Security Gateway: 安全网关 (防火墙)
- Security Management: 管理服务器

通常是二选一，不建议两个产品装在同一台云主机上。



The screenshot shows the 'Products' configuration screen in the Check Point installation wizard. The interface is dark-themed with a white content area. At the top left, the word 'Products' is displayed in white. At the top right, the Check Point logo and 'SOFTWARE TECHNOLOGIES LTD.' are visible. Below the title, there are two sections: 'Products' and 'Clustering'. In the 'Products' section, two checkboxes are checked: 'Security Gateway' and 'Security Management'. In the 'Clustering' section, there are two dropdown menus: 'Unit is a part of a cluster, type:' set to 'ClusterXL' and 'Define Security Management as:' set to 'Primary'. Below these, there is a checked checkbox for 'Automatically download Blade Contracts, new software, and other important data (highly recommended)'. At the bottom, there is an information icon and a link 'For more information click here'. At the very bottom, there are three buttons: '< Back' (disabled), 'Next >' (active/highlighted), and 'Cancel' (disabled).

## Security Management GUI Clients

GUI clients can log into the Security Management from:

Any IP Address

This machine  
IP address:

Network  
IP Address:   
Subnet:

Range of IPv4 addresses:  
 -

< Back   Next >   Cancel

## First Time Configuration Wizard Summary

Your device will be configured with the following products:

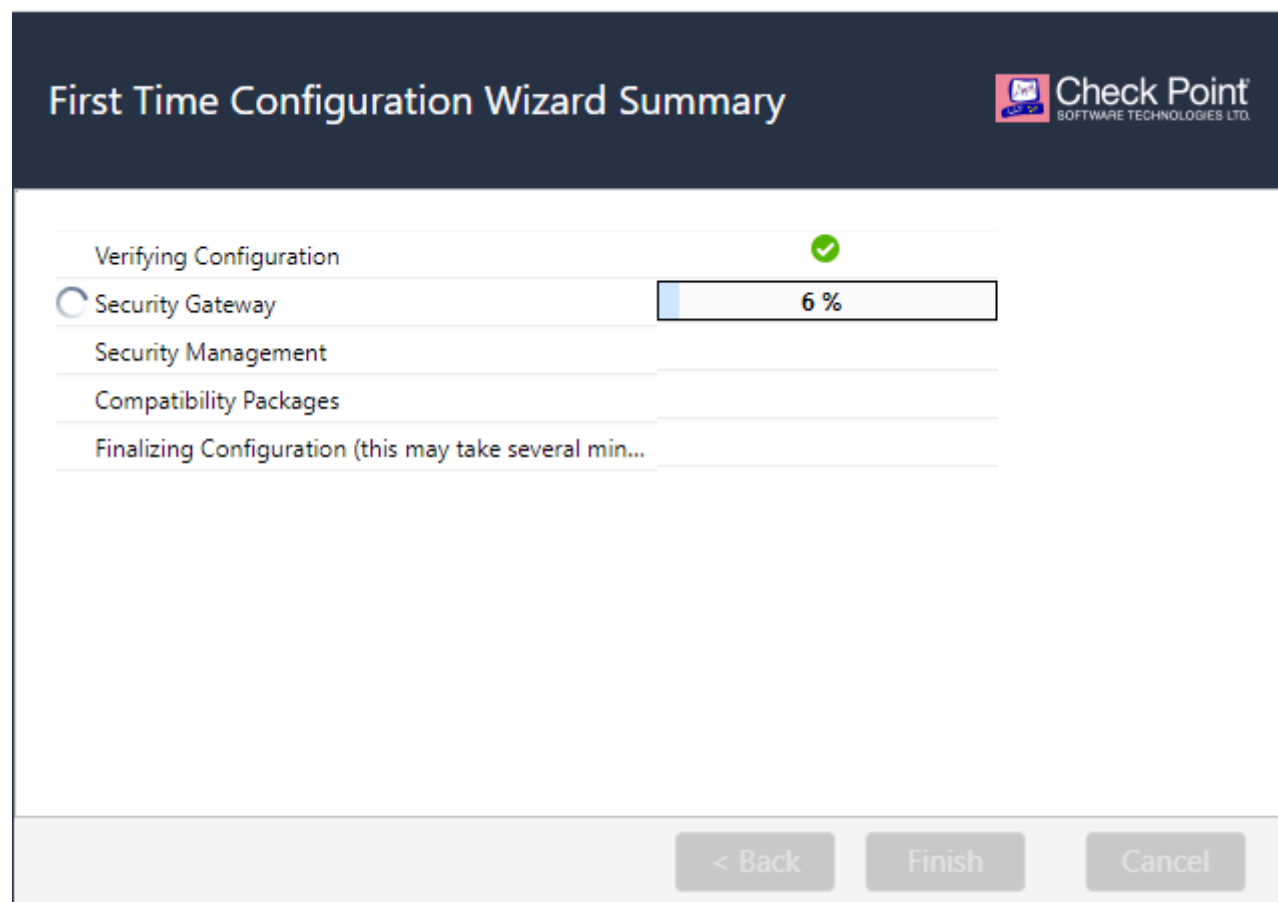
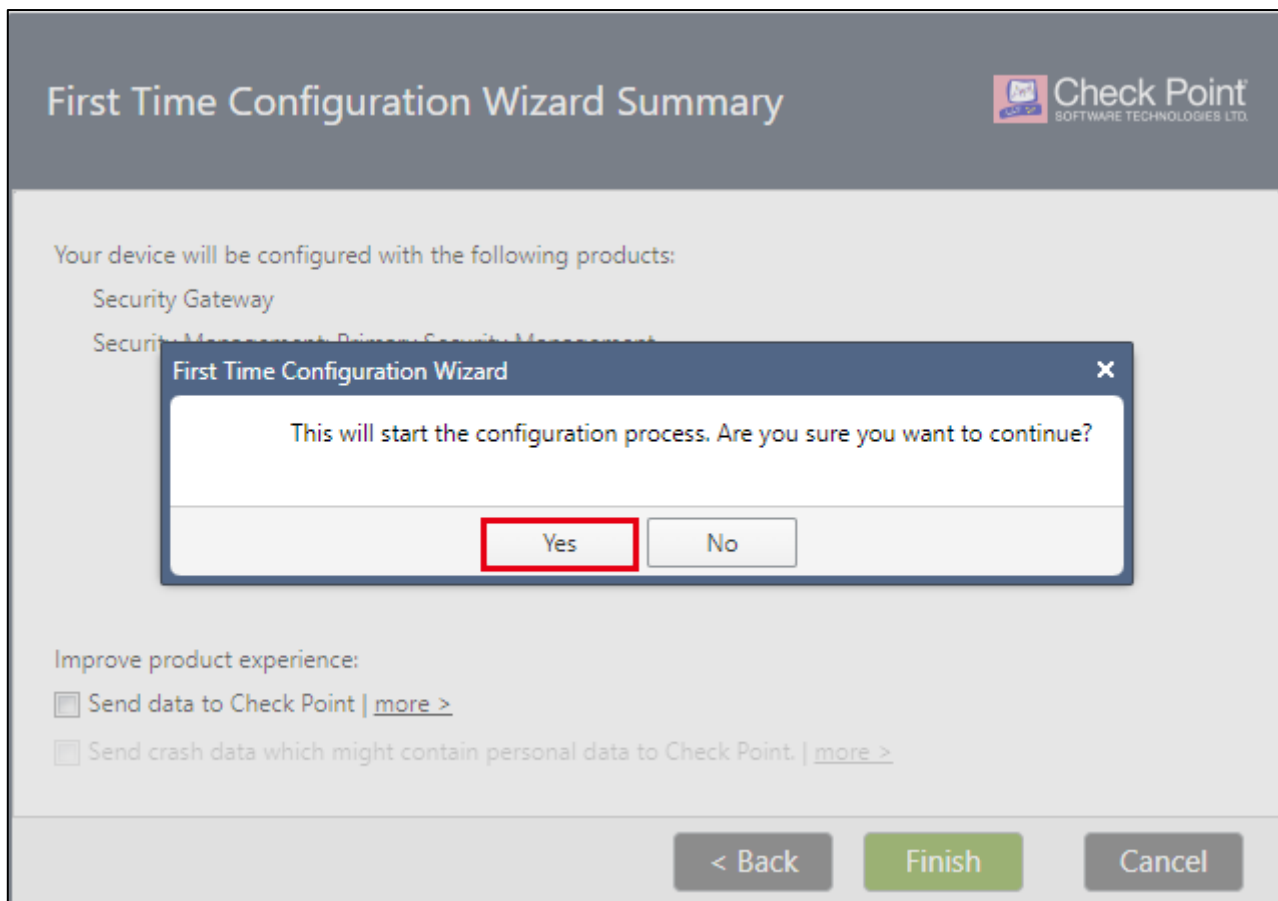
- Security Gateway
- Security Management: Primary Security Management

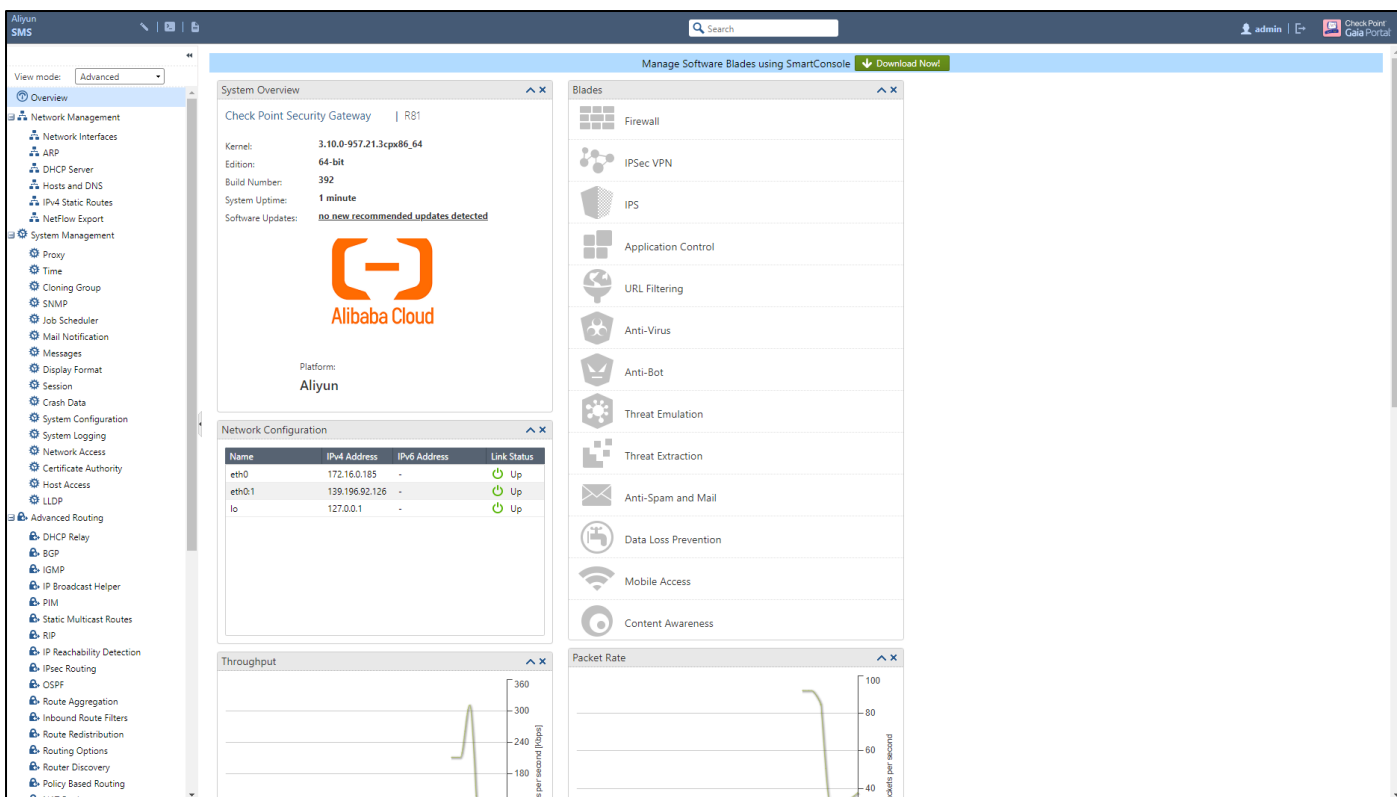
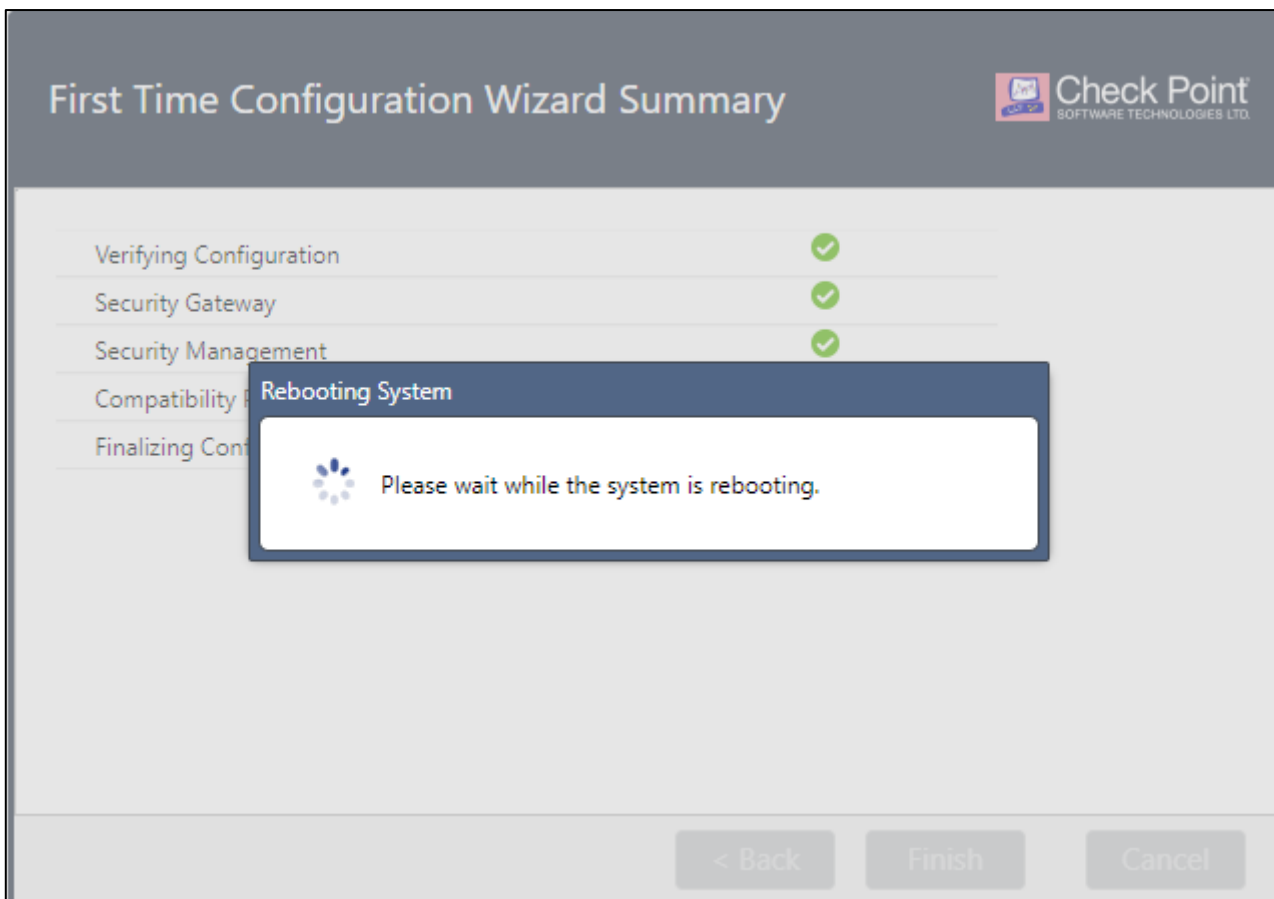
Improve product experience:

Send data to Check Point | [more >](#)

Send crash data which might contain personal data to Check Point. | [more >](#)

< Back   Finish   Cancel

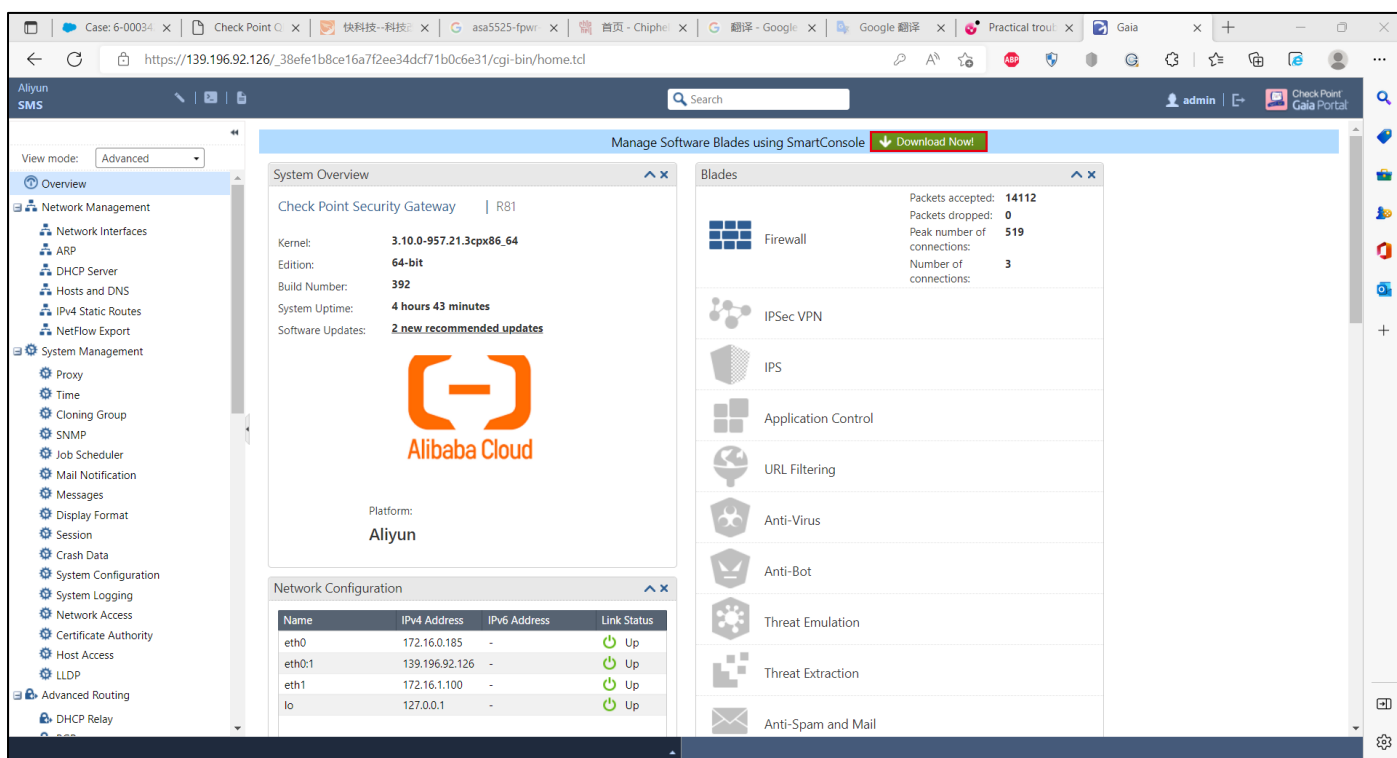




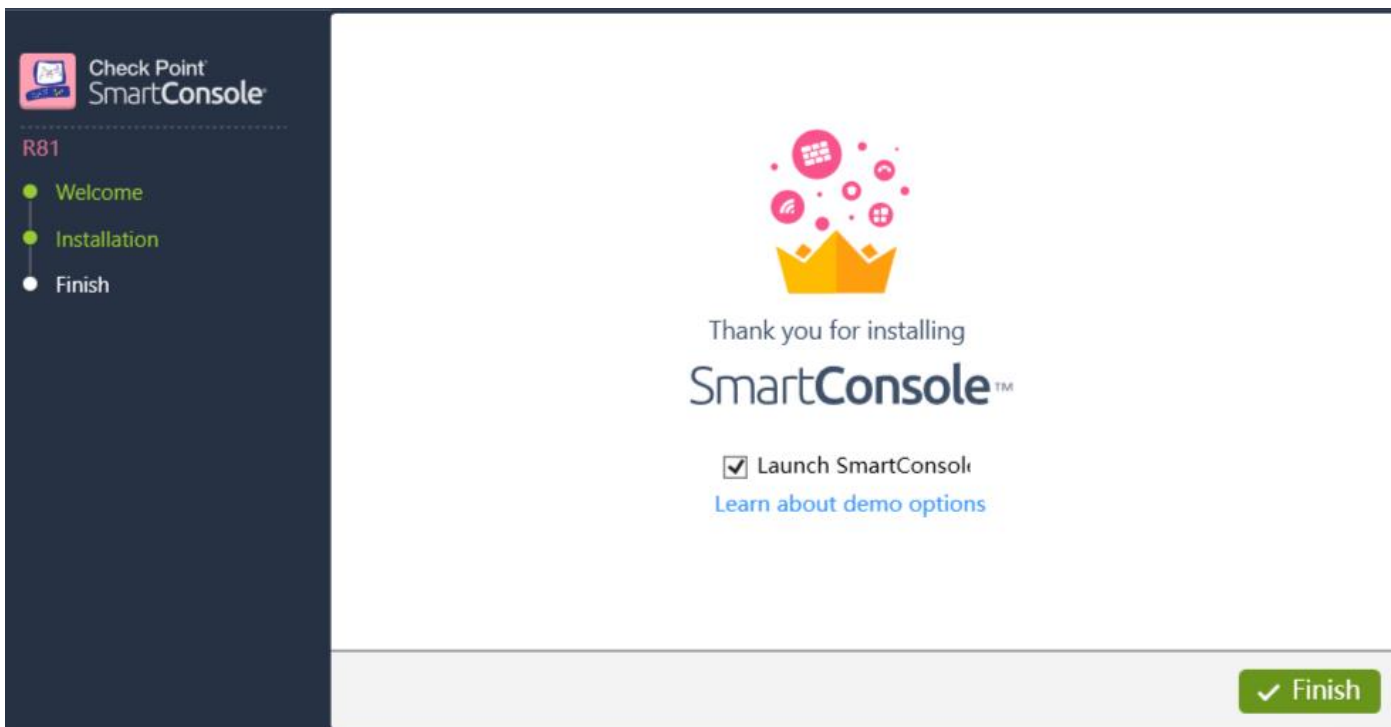
## 第五章 通过 SmartConsole 配置防火墙的相关功能



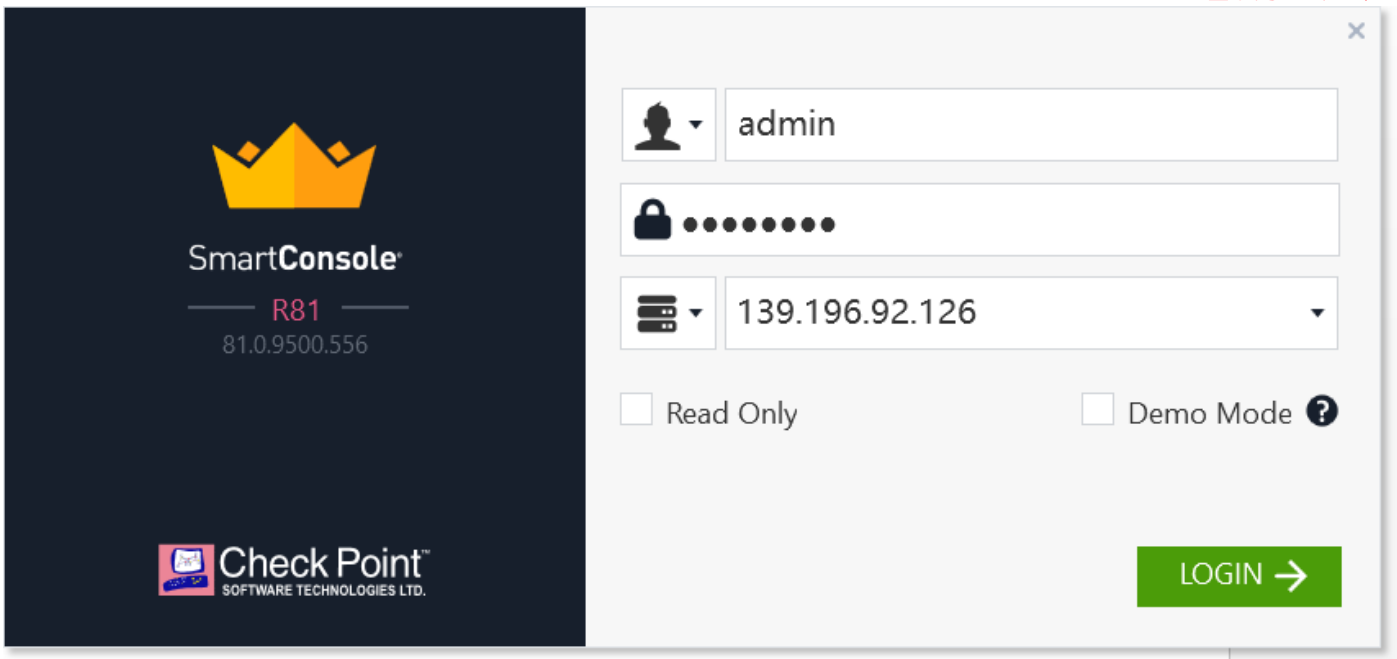
## 5.1 下载和安装 SmartConsole 客户端



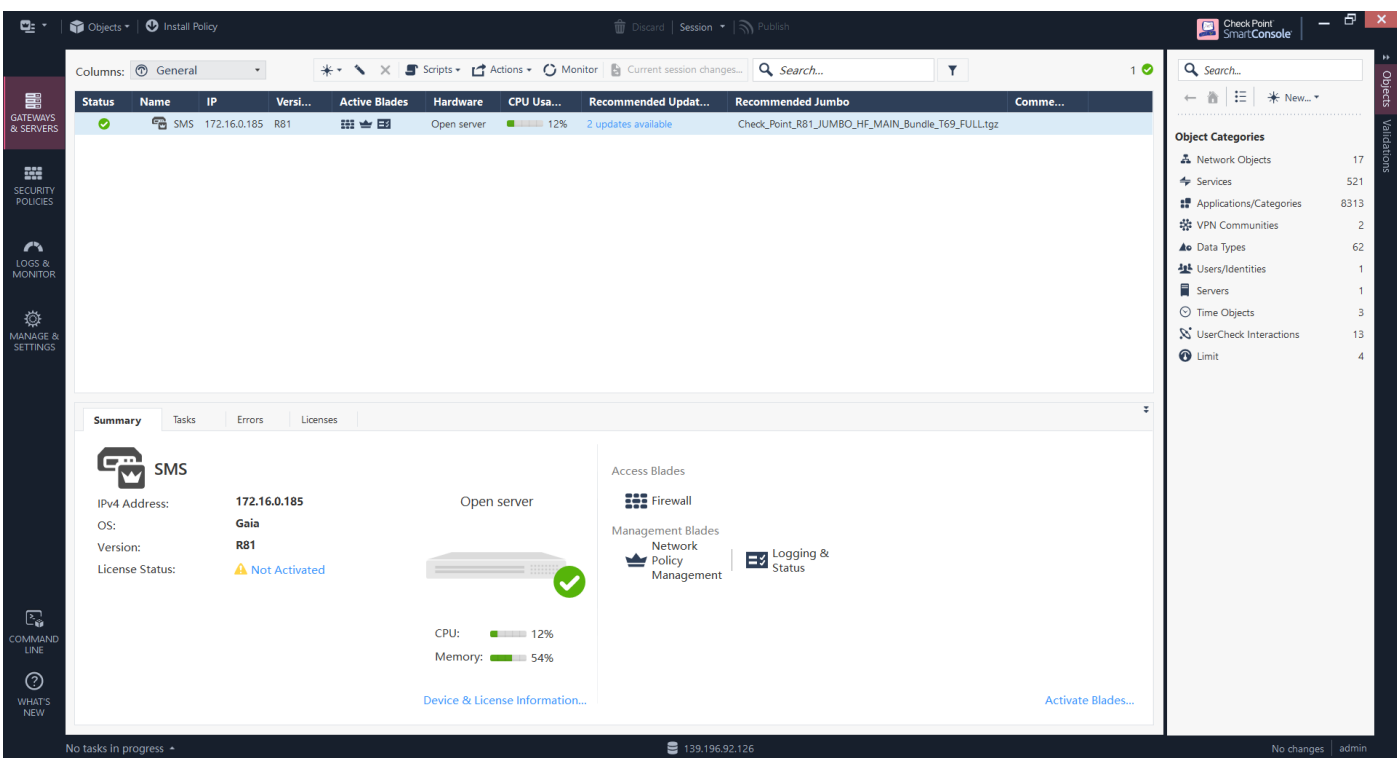
## 安装 SmartConsole



## 登陆 SmartConsole

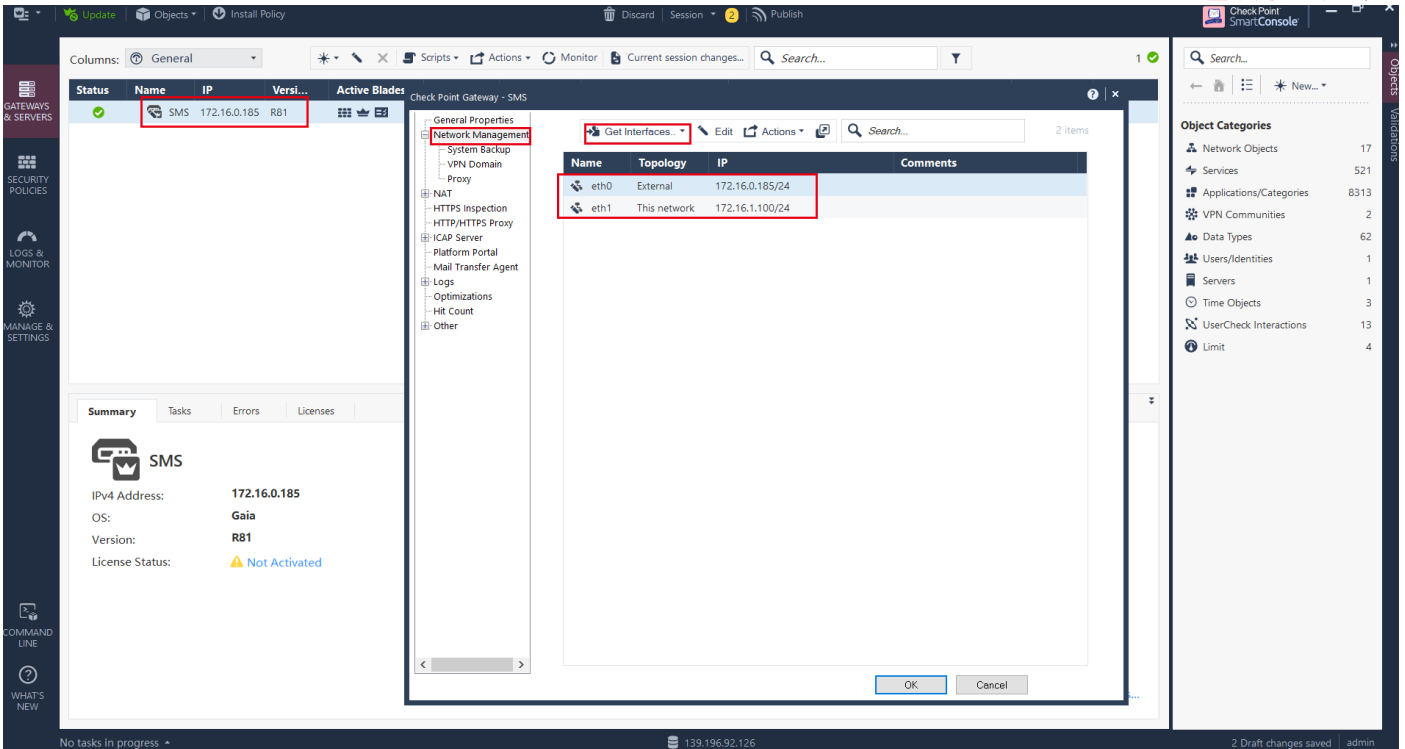


## SmartConsole 主页面

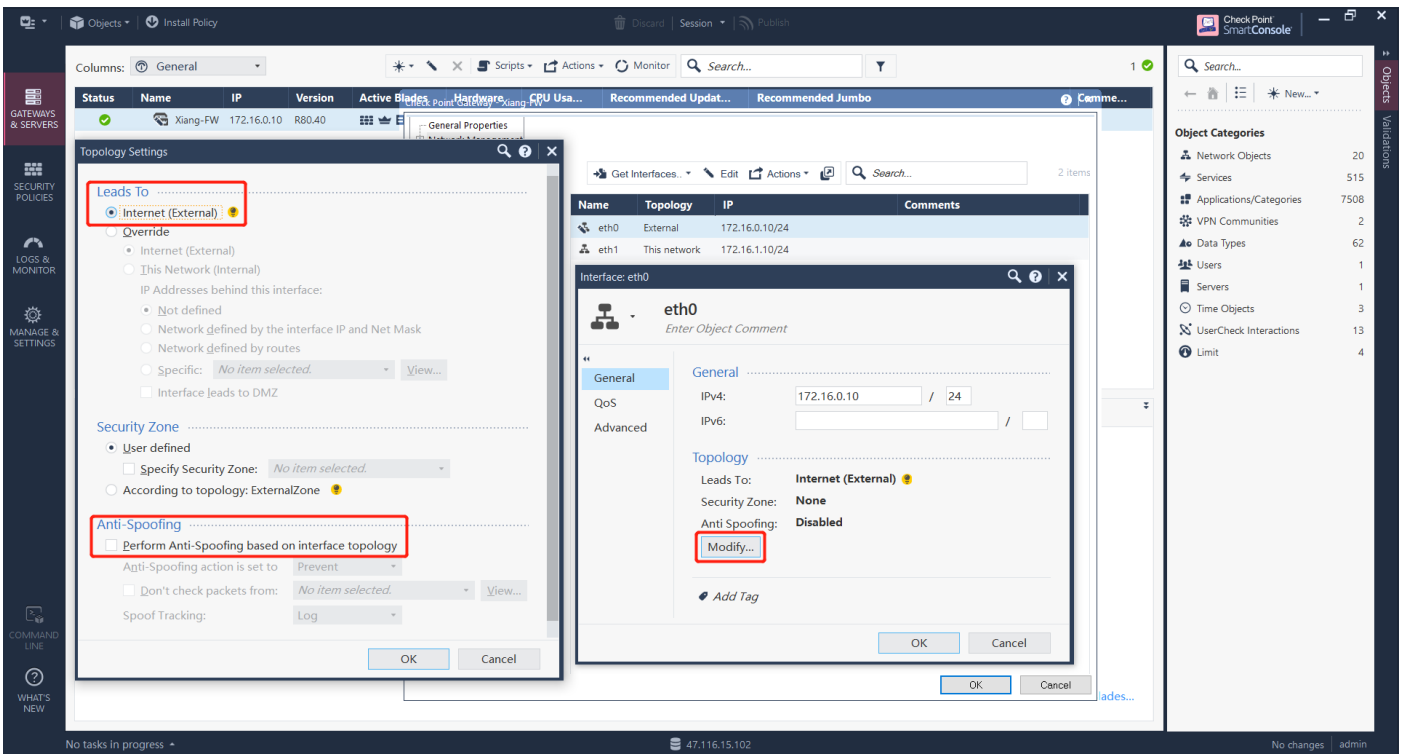


## 5.2 Get 底层的拓扑信息

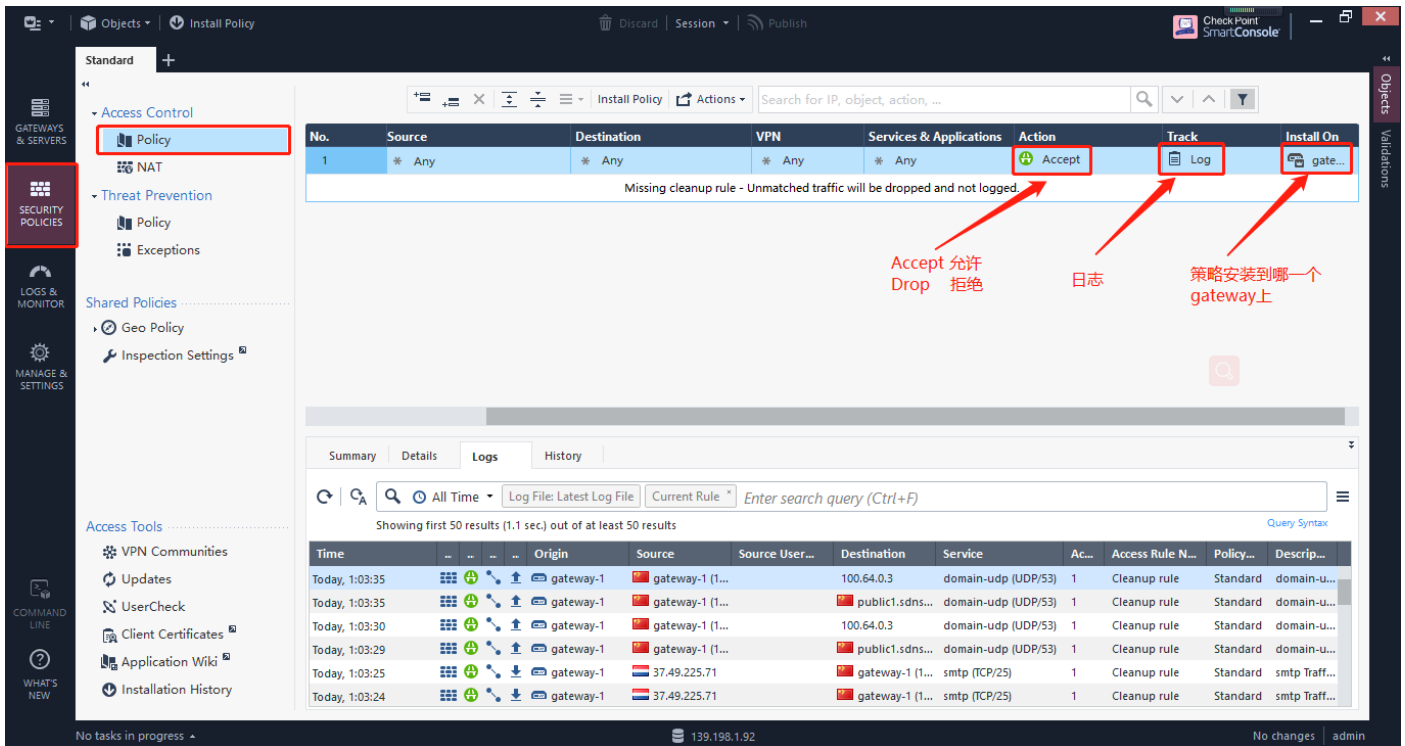
让上层 FW 获取底层接口信息及拓扑



### 5.3 定义接口域并关闭接口地址防欺骗功能

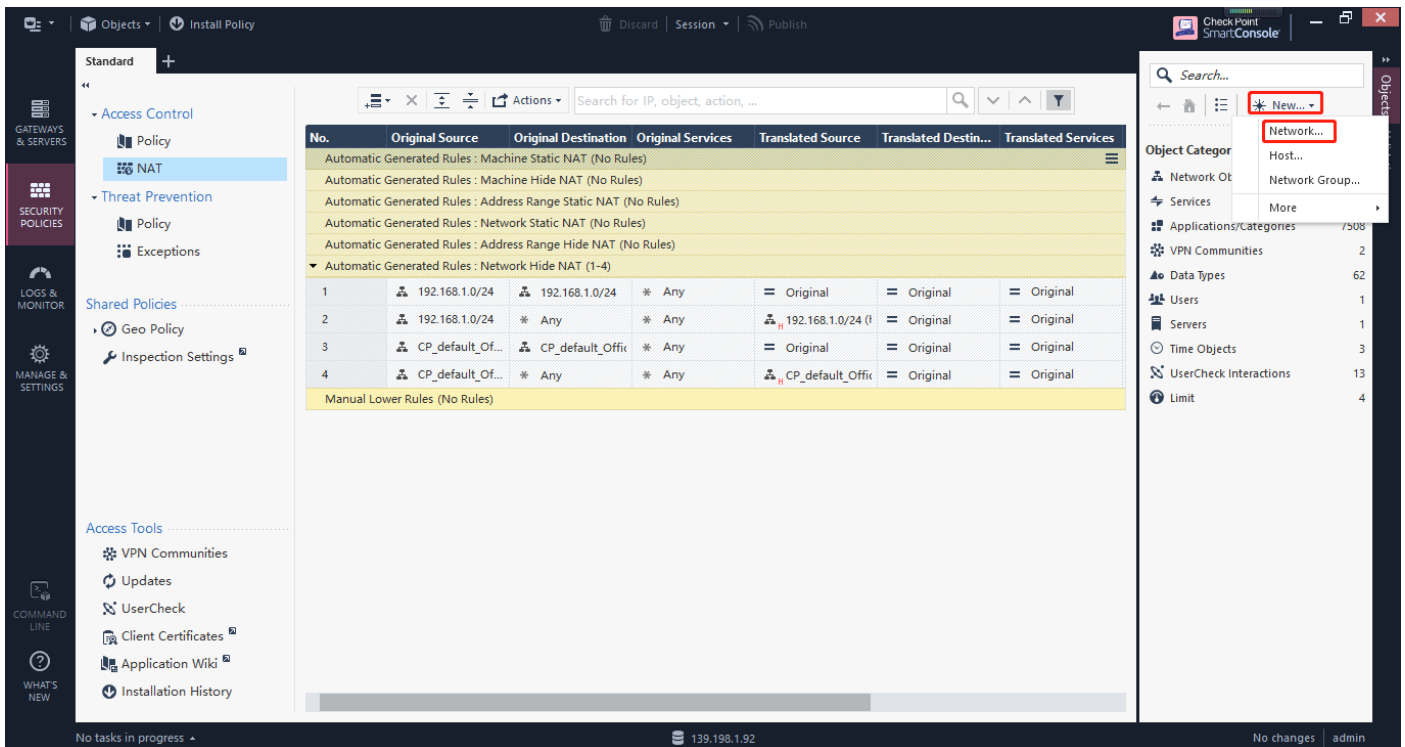


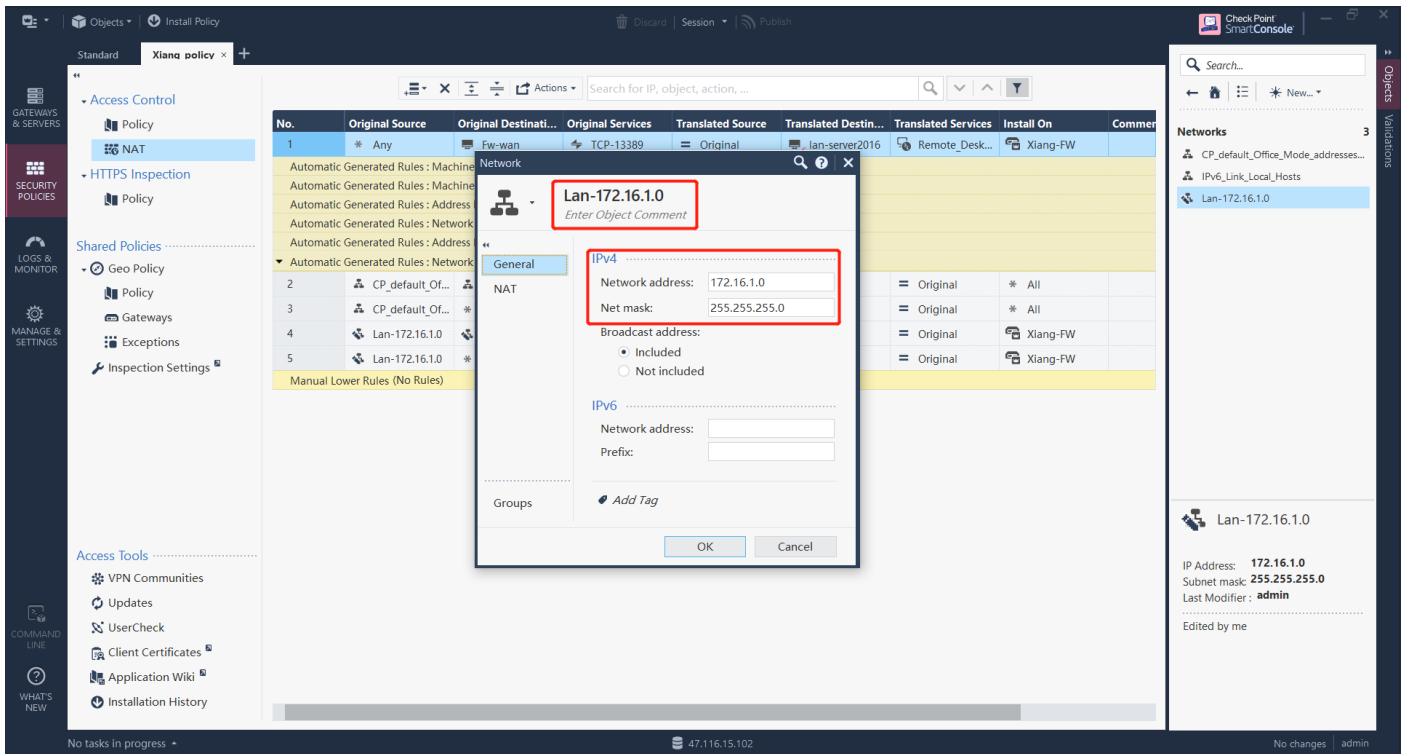
## 5.4 编辑策略



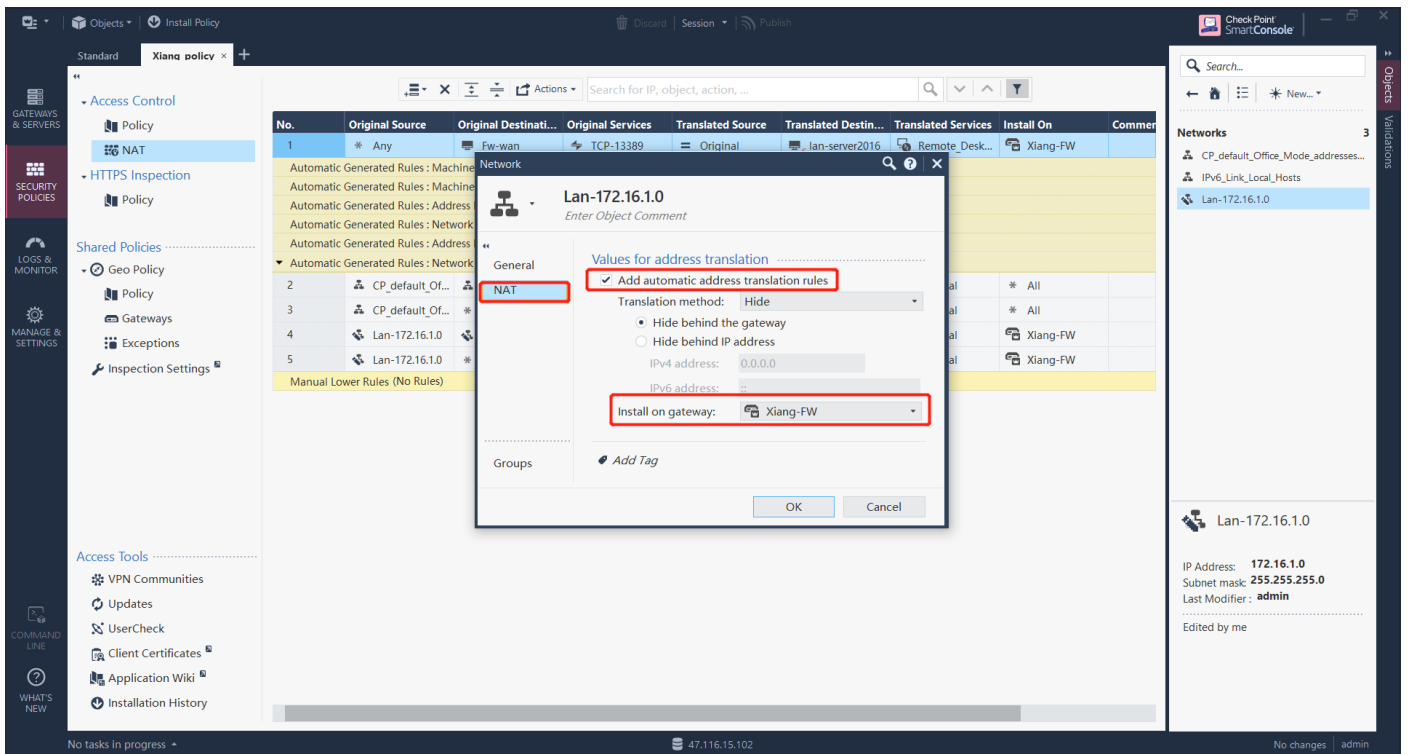
## 5.5 开启内网段的 SNAT

首先新建内网网路地址段

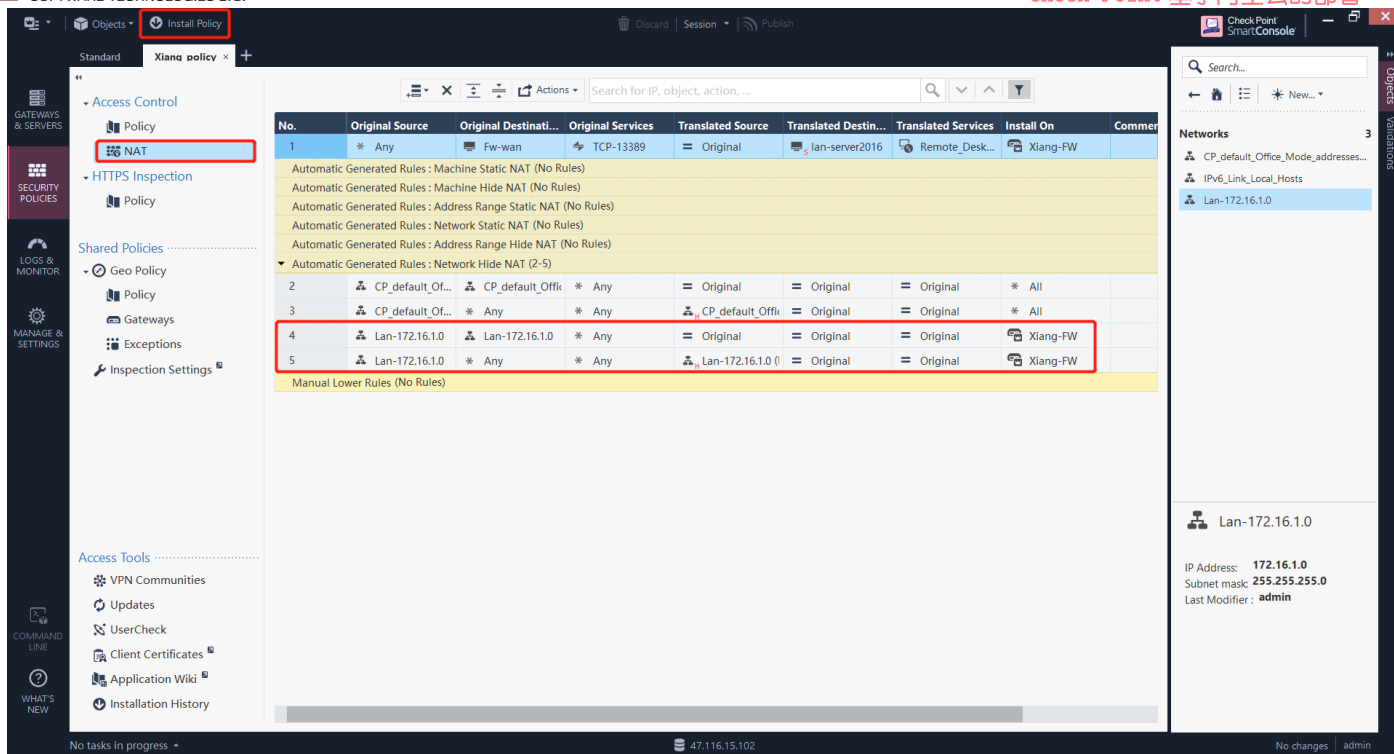




## 开启 NAT



## 5.6 下发策略并生效



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

yejf@zenitera.com