

华为云部署 CloudGuard

配置文档

目录

1	概述.....	3
1.1	产品介绍	3
1.2	安装要求及注意事项	3
2	购买并配置网络与主机.....	4
2.1	创建 VPC.....	4
2.2	创建 gateway.....	5
2.3	创建 Management	7
2.4	更改安全组	7
3	初始化及配置防火墙.....	8
3.1	初始化 Management	8
3.2	初始化 Management	10
3.3	下载并登陆到 SmartConsole	14
3.4	在 Management 上增加 Gateway	15
3.5	配置 Gateway	17
3.6	配置策略	19
3.7	安装策略	21

1 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,连接到混合云数据丢失防护保护敏感数据免遭窃取或意外丢失;
- 4) 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。
- 5) 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。

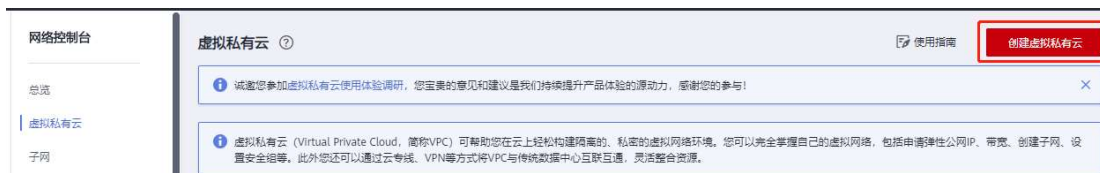
1.2 安装要求及注意事项

- 1) 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)。
- 2) 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。
- 3) 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。

2 购买并配置网络与主机

2.1 创建 VPC

登录到控制台，选择 VPN，创建一个 VPC 网络



按照自身需求，创建 VPC

基本信息

区域: 华南-广州

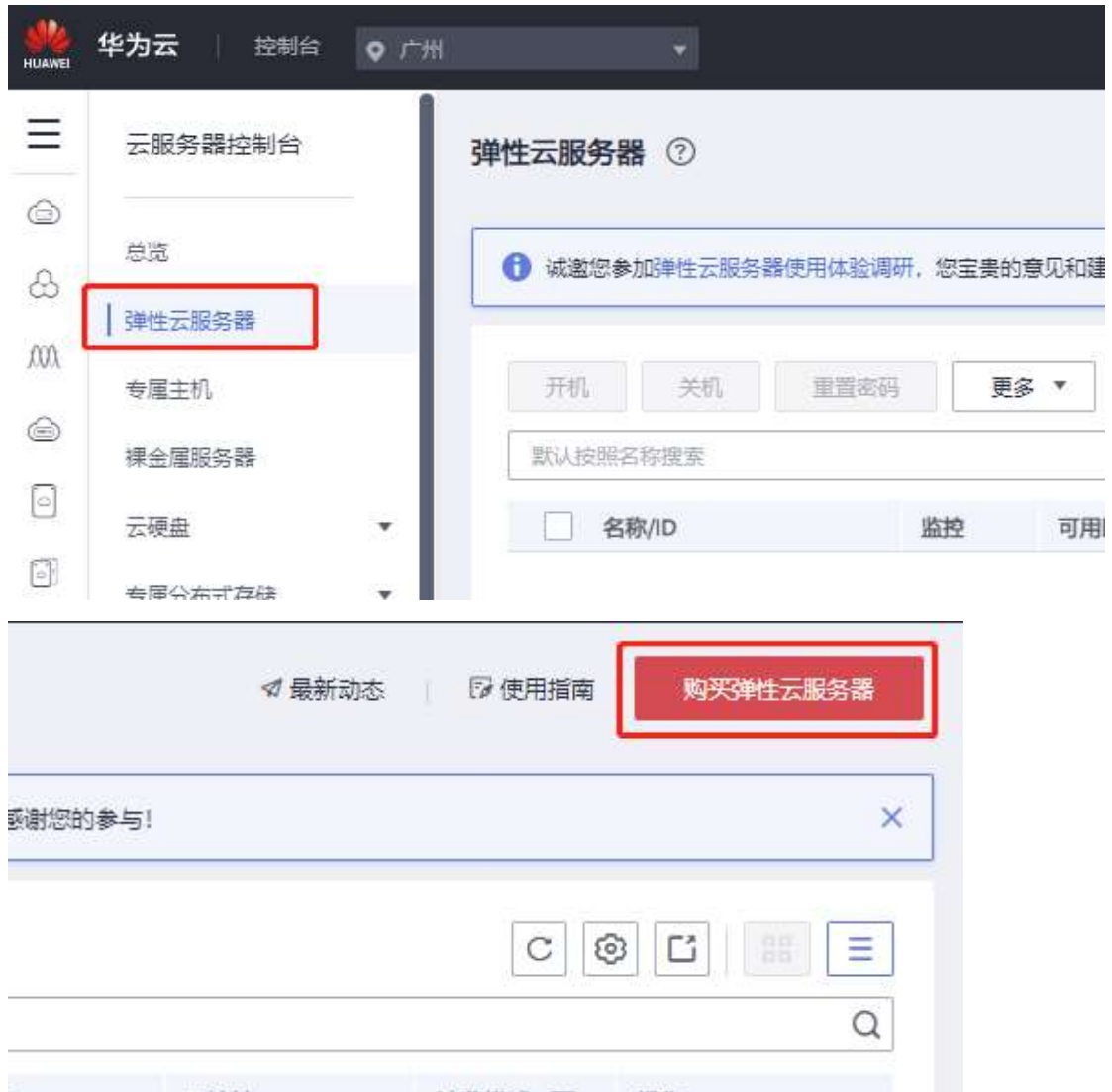
名称: vpc-8b37

网段: 172 · 16 · 10 · 0 / 24

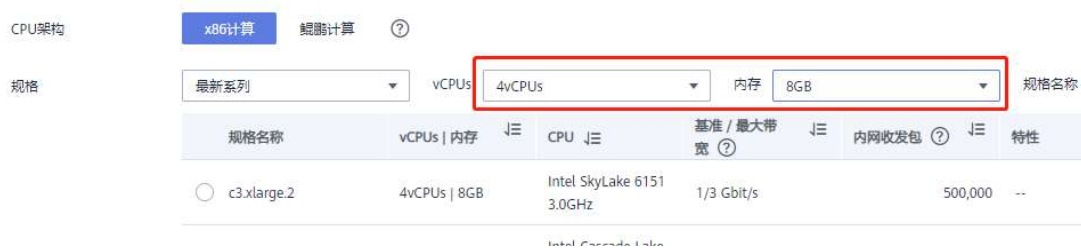
建议使用网段: 10.0.0.0/8-24 (选择) 172.16.0.0/12-24 (选择) 192.168.0.0/16-24 (选择)

高级配置 ▾ 标签

2.2 创建 gateway



选择规格



选择市场镜像，选择 gateway 版本

镜像

公共镜像 私有镜像 共享镜像 **市场镜像**

copy_cn-north-1_checkpoint-r8040-gateway(100GB) C 新建私有镜像

使用私有镜像创建弹性云服务器前，请查看操作系统已知问题。

系统盘

通用型SSD - 100 + GB IOPS上限2,300, IOPS突发上限8,000 ?

增加一块数据盘 您还可以挂载 23 块磁盘 (云硬盘)

Linux实例添加的数据盘可使用脚本向导式初始化。如何操作?

配置两个不同网段的网卡，以及为主机分配公网地址

网络

vpc-8b37(172.16.0.0/24) C

subnet-8b69(172.16.0.0/24) C 手动分配IP地址 172 · 16 · 10 · 55 查看已使用IP地址

可用私有IP数量250个 ?

如需创建新的虚拟私有云，您可前往控制台创建。批量创建云服务器时，指定的IP地址为起始IP地址。

扩展网卡

增加一块网卡 您还可以增加 1 块网卡

配置名称和密码

< 弹性云服务器 自定义购买 快速购买

① 基础配置 ———— ② 网络配置 ———— ③ 高级配置 ———— ④ 确认配置

云服务器名称 **CheckPoint-Gateway** 允许重名

购买多台云服务器时，名称自动按序增加4位数字后缀。例如：输入ecs，从ecs-0001开始命名；若已有ecs-0010，从ecs-0011开始命名。

登录凭证 **密码** 密钥对 使用镜像密码

用户名 root

密码 **请牢记密码，如忘记密码可登录ECS控制台重置密码。**

确认密码

购买数量 - 1 + 您还可以创建200台云服务器。申请更多云服务器配额请单击申请扩大配额。

协议 我已经阅读并同意《华为镜像免责声明》

配置类 参考价格，实际扣费请以账单为准。 了解详情

上一步 立即购买

等待创建成功

2.3 创建 Management

同样按照上述方法，创建 Management（注意：在创建 Management 时要选择 Management 镜像，而不是 Gateway 的镜像）。Management 用于管理 Gateway。

2.4 更改安全组



添加 443 端口

添加规则 快速添加规则 删除 一键放通 入方向规则: 4 按我设置

<input type="checkbox"/>	协议端口	类型	源地址	描述	操作
<input type="checkbox"/>	全部	IPv4	Sys-default	--	修改 复制 删除
<input type="checkbox"/>	TCP : 22	IPv4	0.0.0.0/0	Permit default Linux SSH port.	修改 复制 删除
<input type="checkbox"/>	TCP : 443	IPv4	0.0.0.0/0	--	修改 复制 删除
<input type="checkbox"/>	TCP : 3389	IPv4	0.0.0.0/0	Permit default Windows remote desktop p...	修改 复制 删除

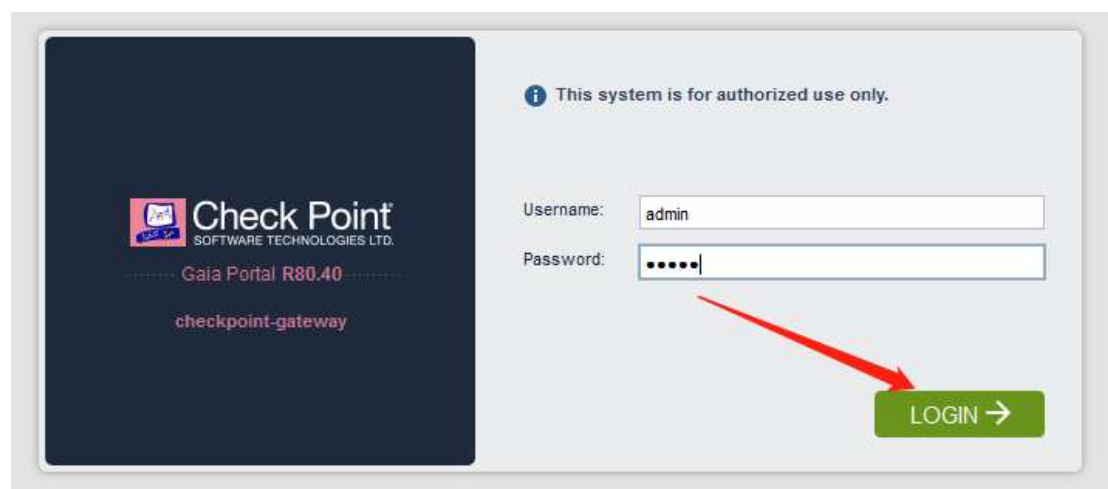
3 初始化及配置防火墙

3.1 初始化 Management

复制 Gateway 的公网地址到浏览器，以 `Https://IP` 格式打开，推荐用谷歌、火狐浏览器。



默认账户密码都是 admin



登陆进来之后设置一下用户和 SIC 的密码，两者也可以一样。IP 地址不用变，主机名称可以改一下，因为主机名一旦保存就不支持更改了

The screenshot shows the configuration wizard with the following sections:

- Authentication:** Configure the Gaia OS password for user "admin". Fields for New Password and Confirm Password are present.
- Network Configuration:** Host Name: gw-088157; IPv4 Addr (eth0): 172.16.10.55; Subnet mask: 255.255.255.0; Default Gateway: 172.16.10.253.
- SIC:** Activation Key and Confirm Activation Key fields.
- Configurations:** Enable cluster membership for this gateway.
- Checkboxes at the bottom: Automatically download Blade Contracts and other important data (highly); Improve product experience by sending data to Check Point.
- A green "Go!" button at the bottom right.

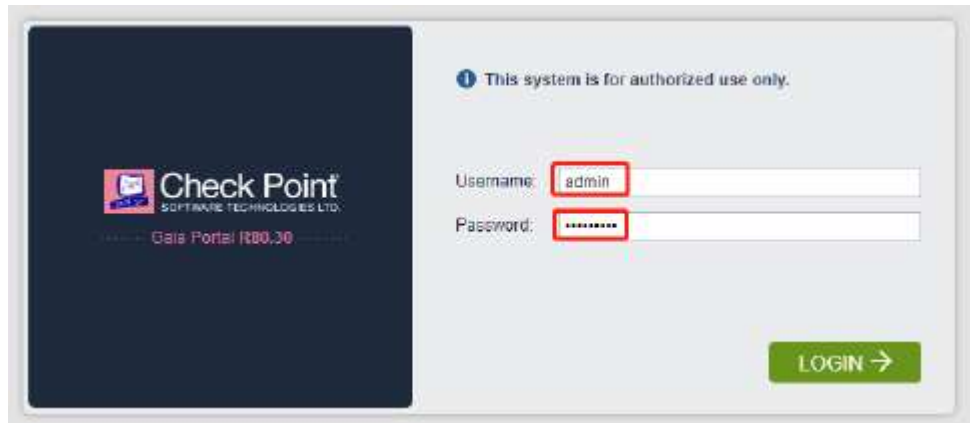
配置完成后是这样的

The screenshot shows the Open Server web interface with the following components:

- System Overview:** Check Point Security Gateway | R80.30. Kernel: 3.10.0-693.el7.x86_64; Edition: 64-bit; Build Number: 273; System Uptime: 4 hours 46 minutes; Software Updates: 2 new recommended updates.
- Blades:** Firewall (Packets accepted: 329070, Packets dropped: 72, Peak number of connections: 534, Number of connections: 11); IPSec VPN; IPS (Attacks Detected: 0); Application Control; URL Filtering; Anti-Virus (Signature last updated: 0, Viruses detected: 0, Scanned Hosts: 2, Weeks: 1, Infected Hosts: 0); Anti-Bot (Gateway is up to date, Database version: 1908291546, Package date: Thu, Aug 29, 08:00:00 2019).
- Network Configuration Table:**

Name	IPv4 Address	IPv6 Address	Link Status
eth0	172.16.10.56	-	Up
eth1	172.16.20.170	-	Up

3.2 初始化 Management



This system is for authorized use only.

Check Point
SOFTWARE TECHNOLOGIES LTD.
Gala Portal R80.30

Username:

Password:

LOGIN →



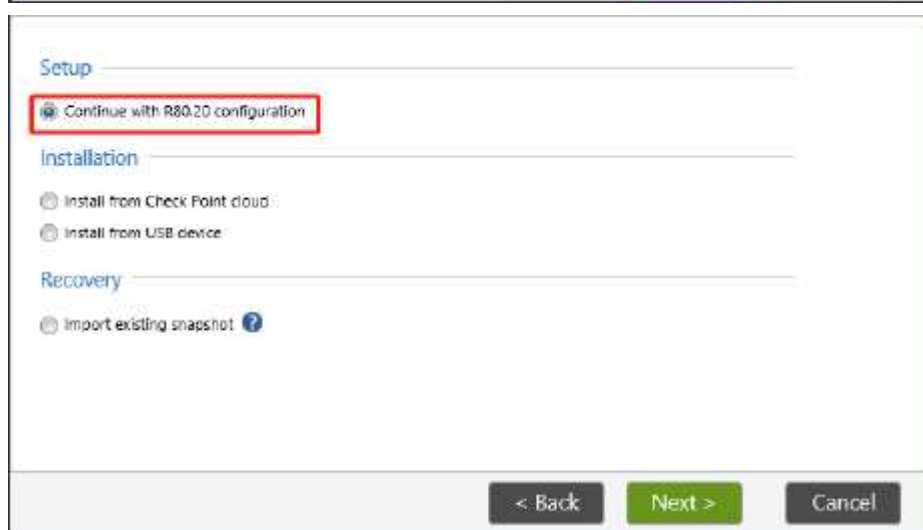
Welcome to the
Check Point First Time Configuration Wizard

You're just a few steps away from using your system!
Click Next to configure your system.



Platform: **Open Server**

< Back **Next >** Cancel



Setup

Continue with R80.20 configuration

Installation

Install from Check Point cloud

Install from USB device

Recovery

Import existing snapshot ?

< Back **Next >** Cancel

更改默认密码

Authentication Details

Change the default administrator password:

Password:

Confirm Password:

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

按照向导继续下一步

Installation Type

Security Gateway and/or Security Management

Multi-Domain Server

< Back Next > Cancel

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

然后默认下一步直到完成

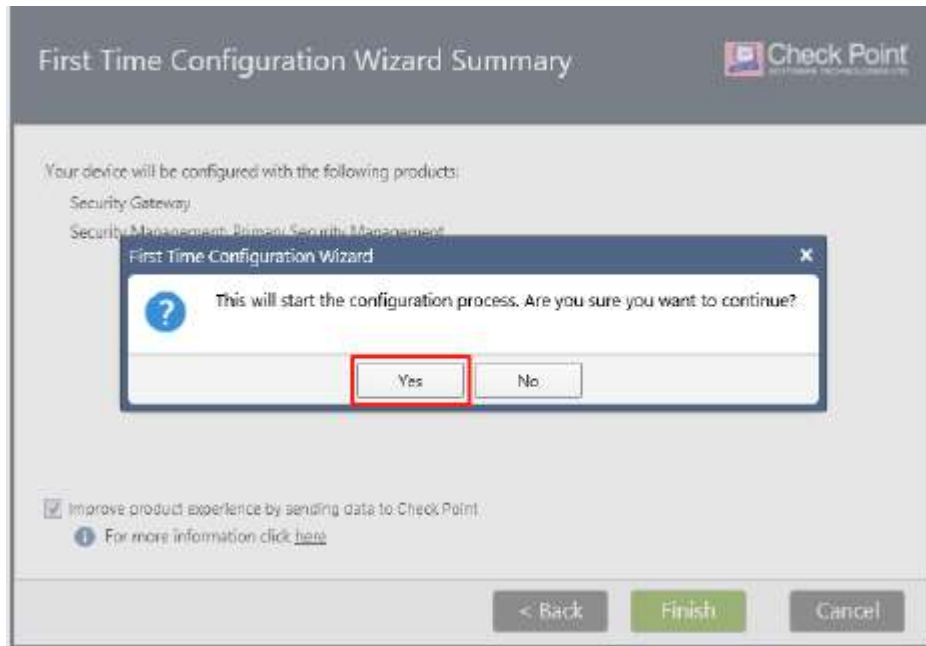
First Time Configuration Wizard Summary

Your device will be configured with the following products:

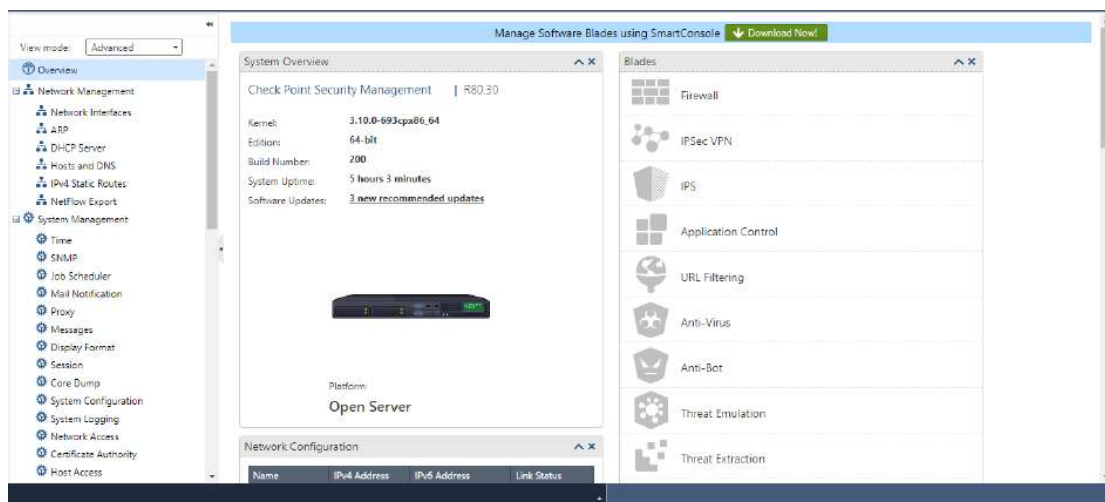
- Security Gateway
- Security Management: Primary Security Management

Improve product experience by sending data to Check Point
For more information click [here](#)

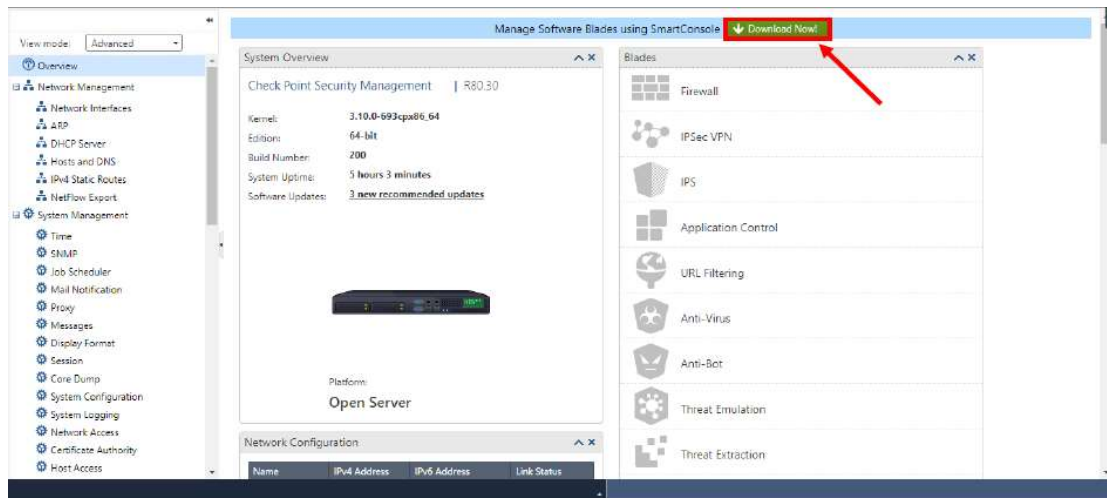
< Back **Finish** Cancel



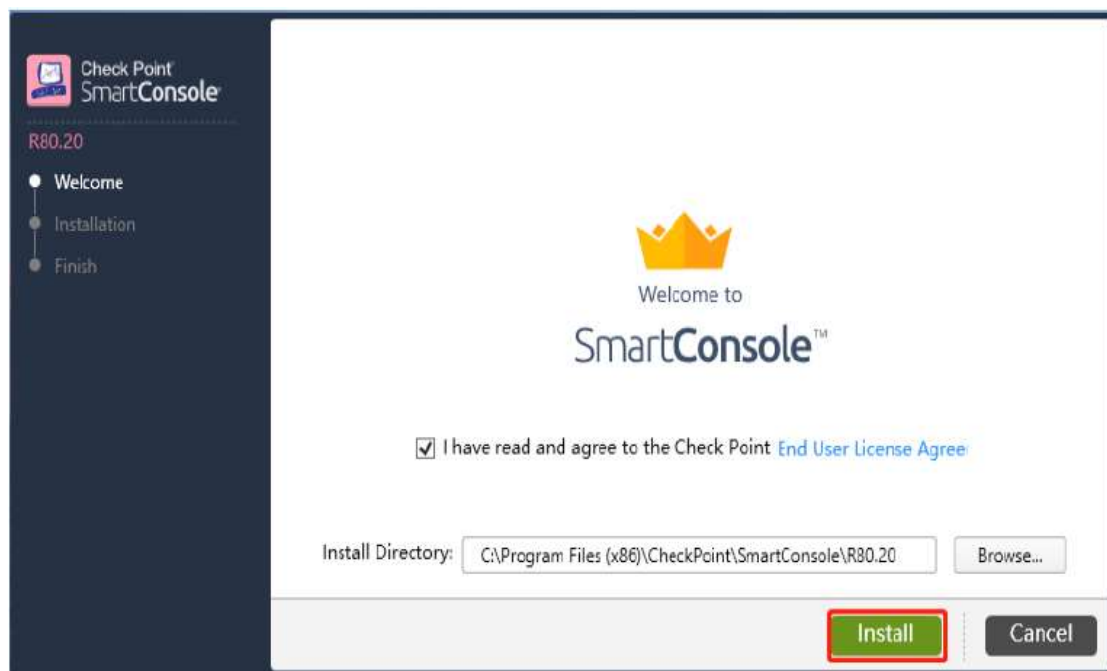
等待初始化完成后，重新登录网址即可见到和 gateway 一样的页面。



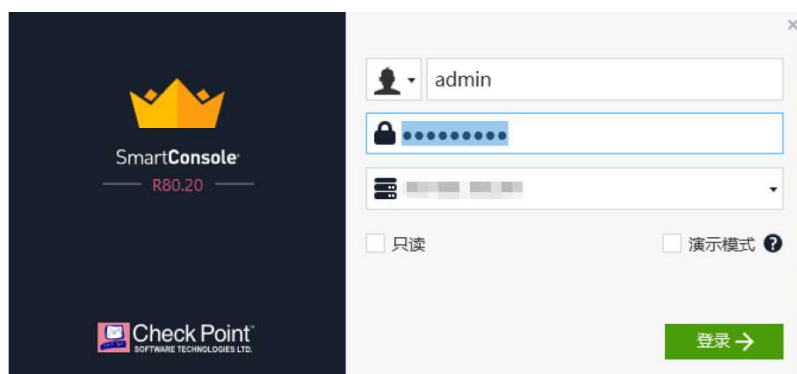
3.3 下载并登陆到 SmartConsole

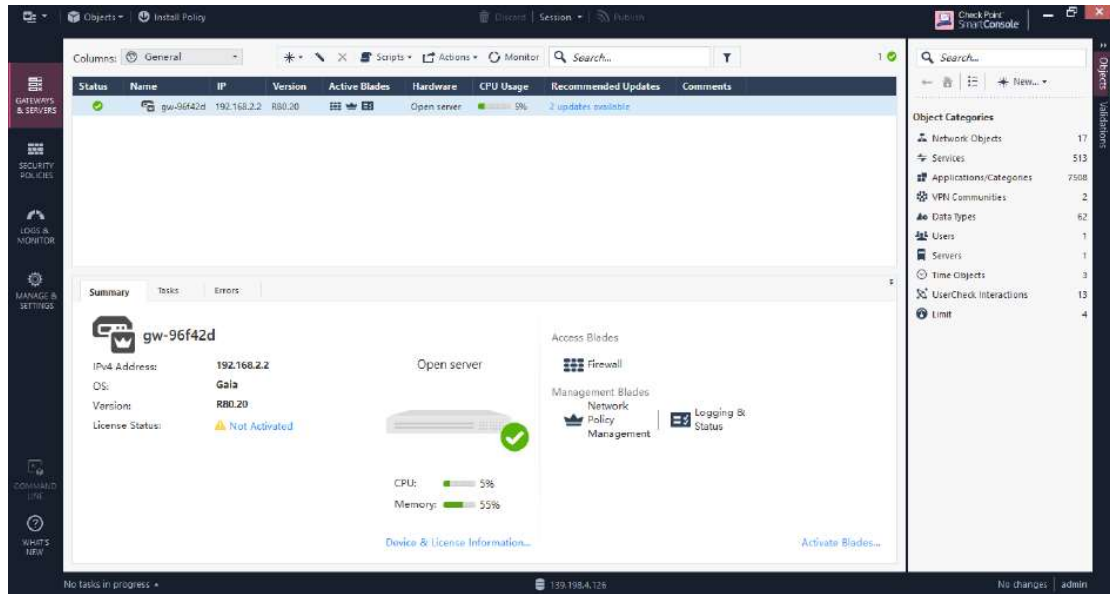


按照向导默认安装



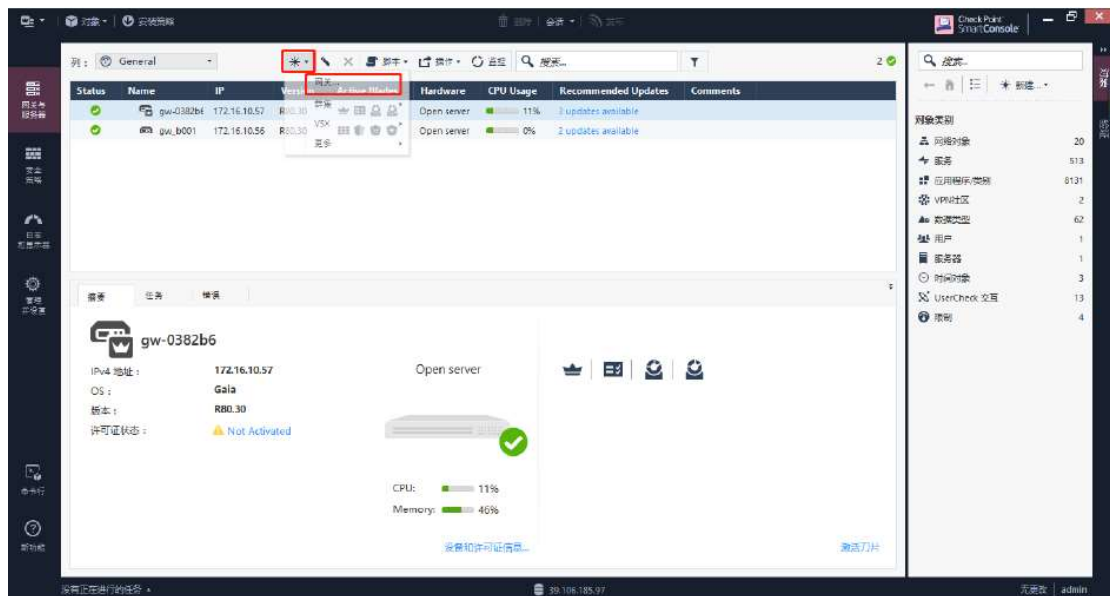
安装完成后，输入 Management IP、用户名和密码，点击登陆

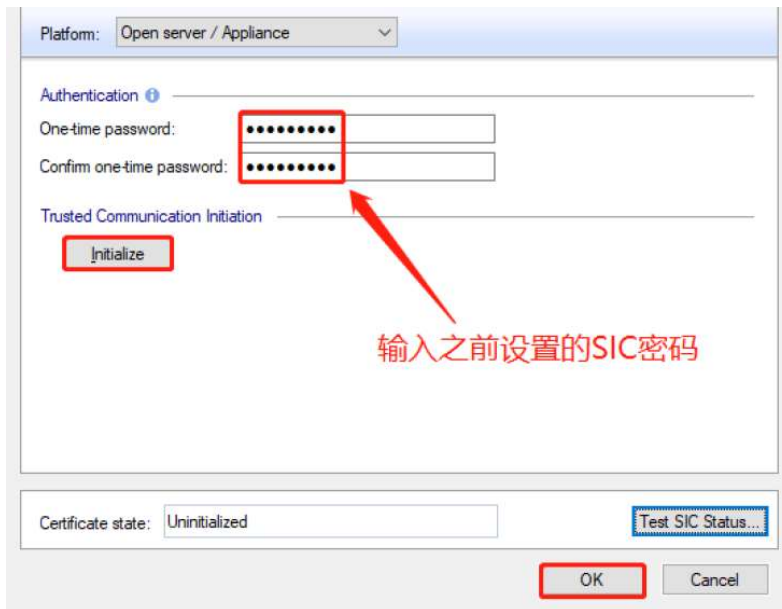
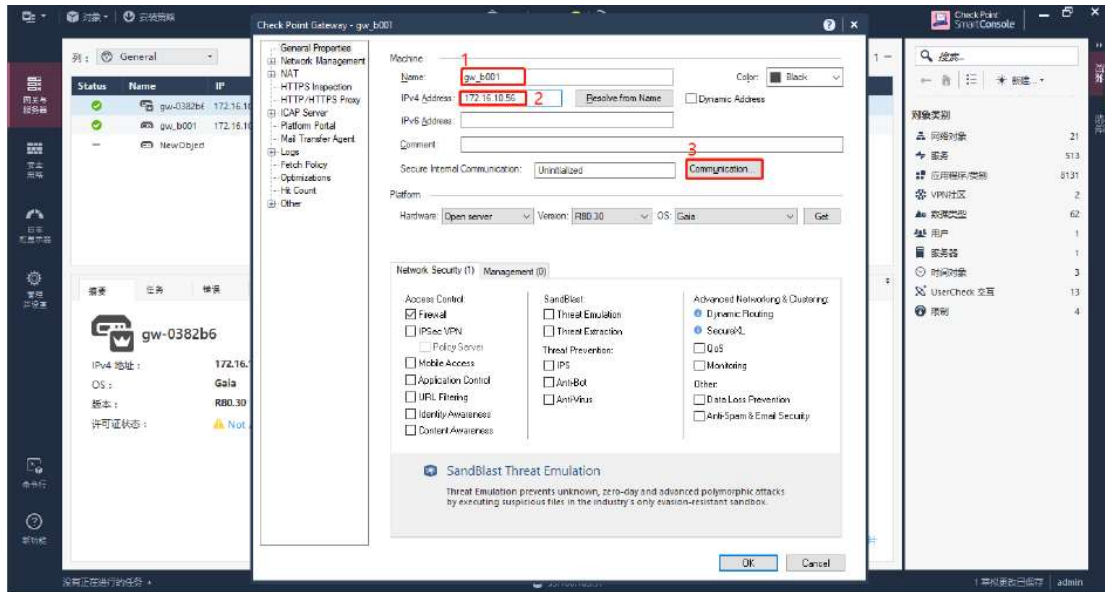




3.4 在 Management 上增加 Gateway

因为 Gateway 和 Management 系统是分开的，所以这里要在 Management 上增加 Gateway

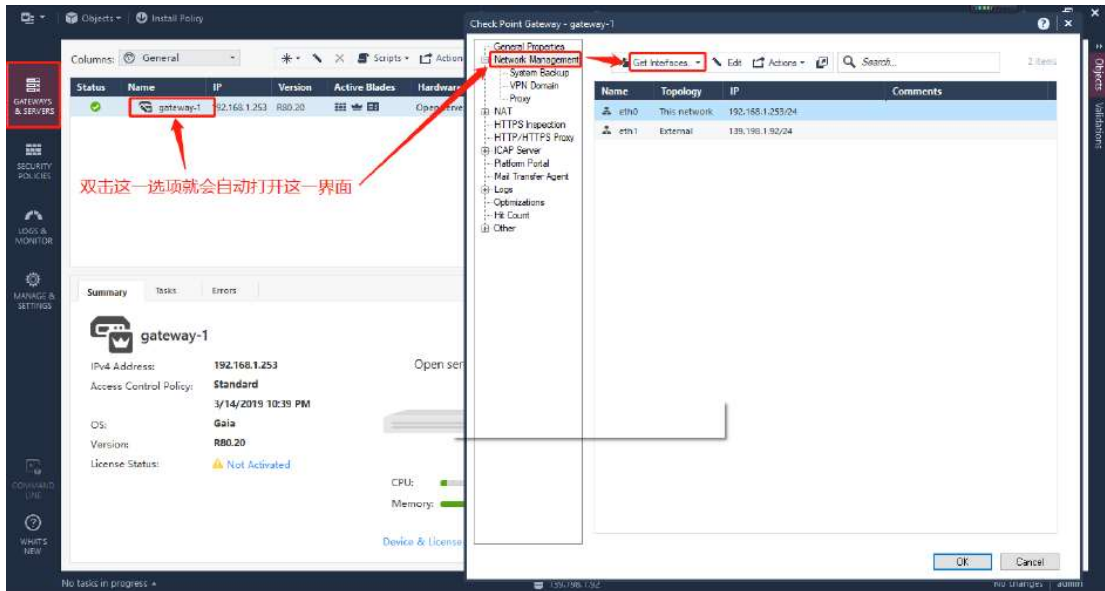




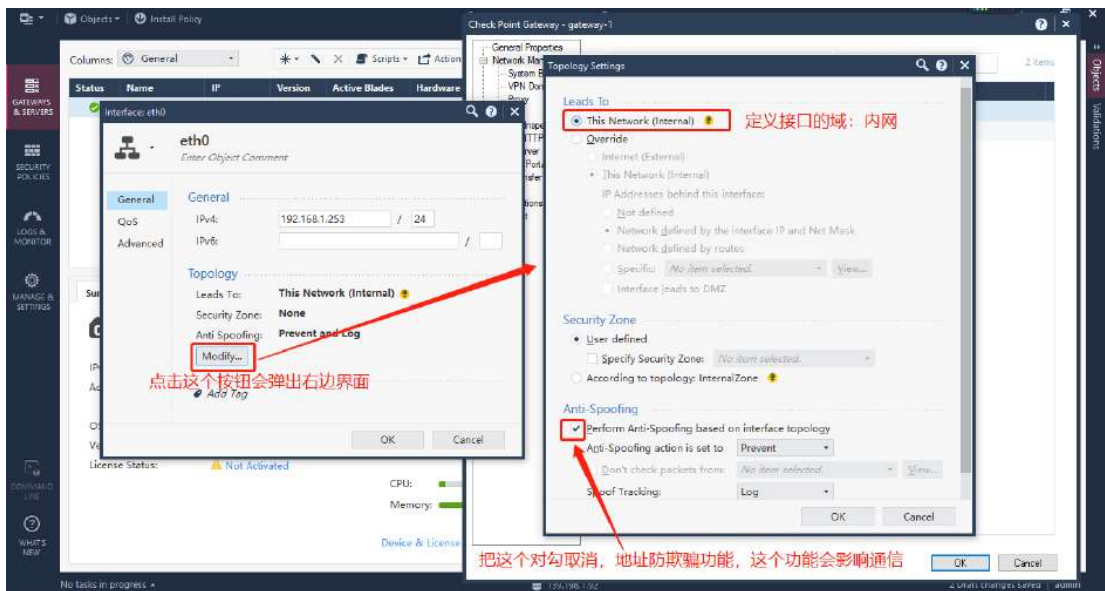
3.5 配置 Gateway

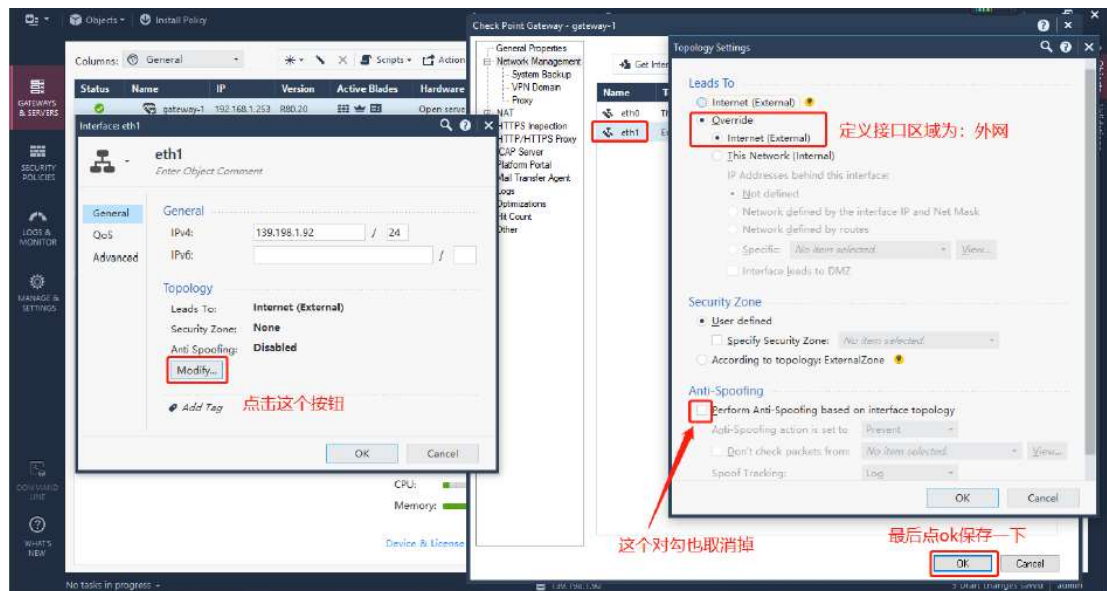
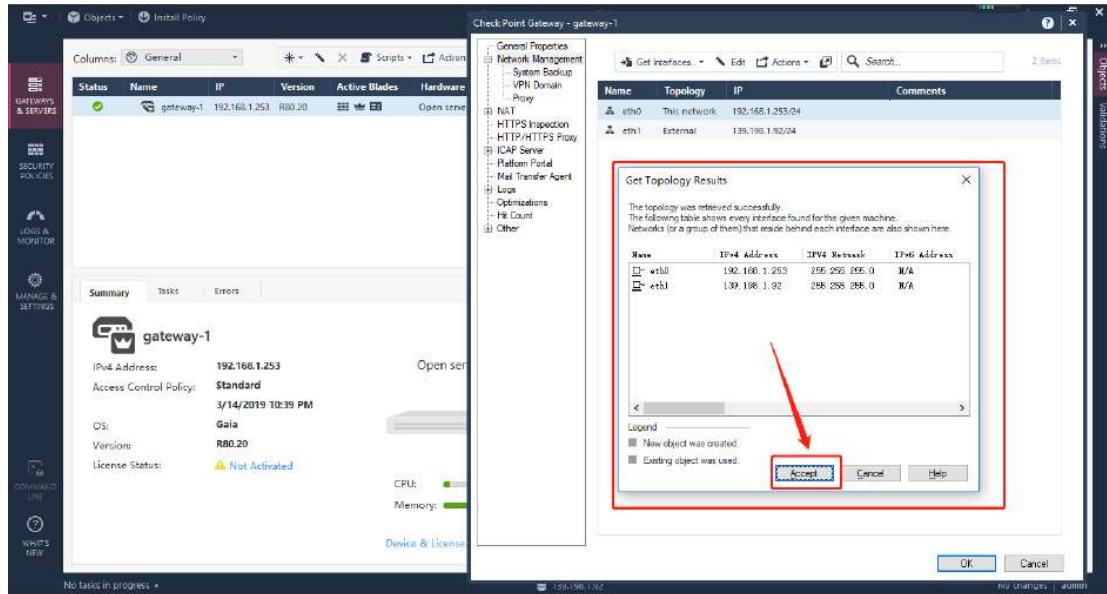
配置接口及关闭接口地址防欺骗功能

让上层 FW 获取底层接口信息及拓扑

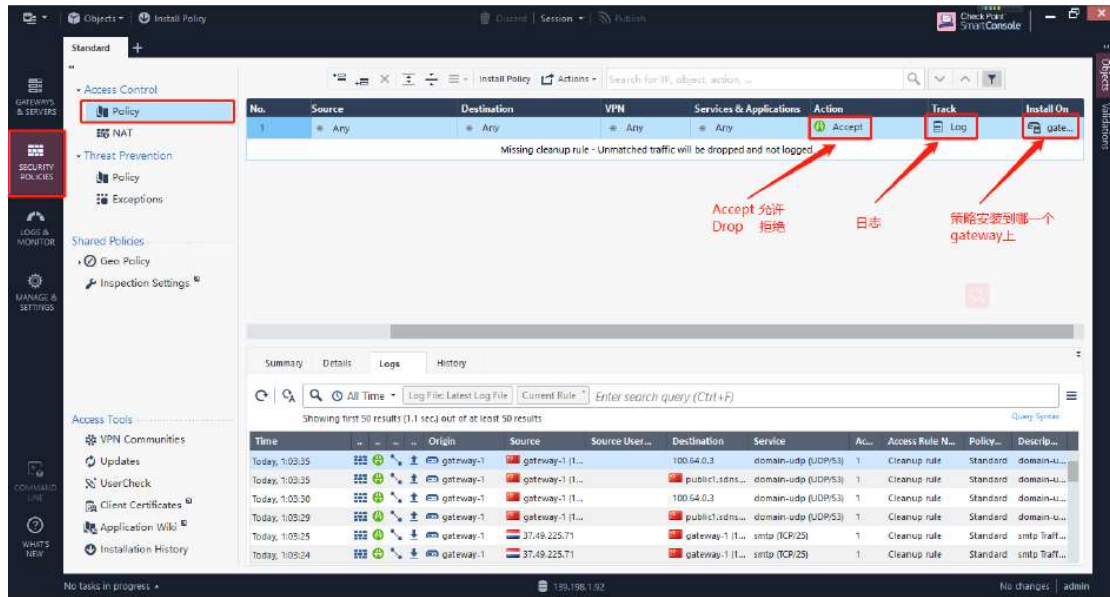


定义接口域，并关闭接口地址防欺骗功能

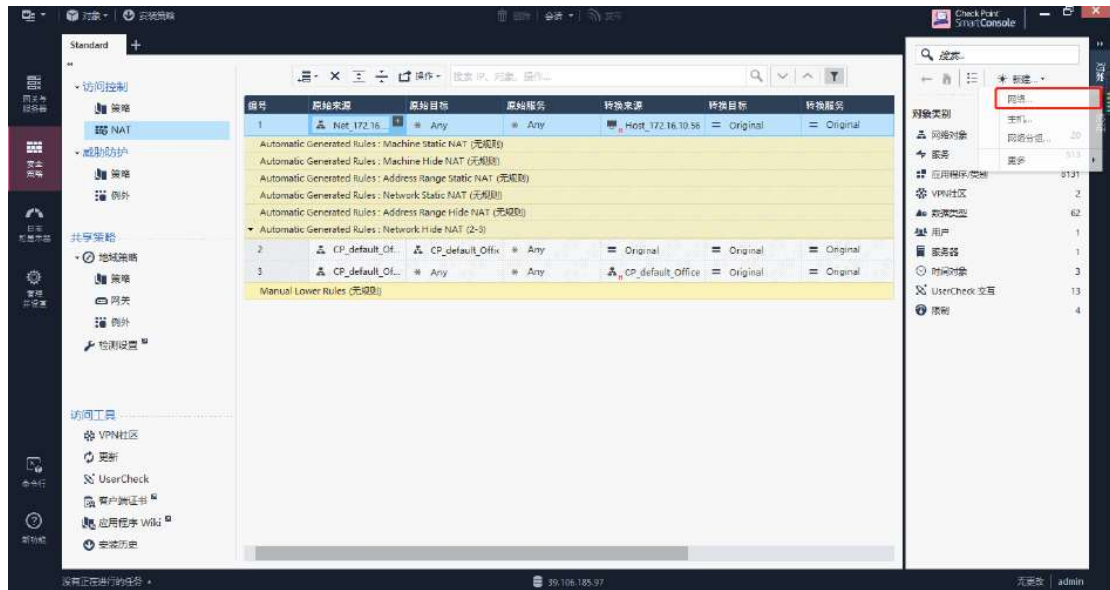


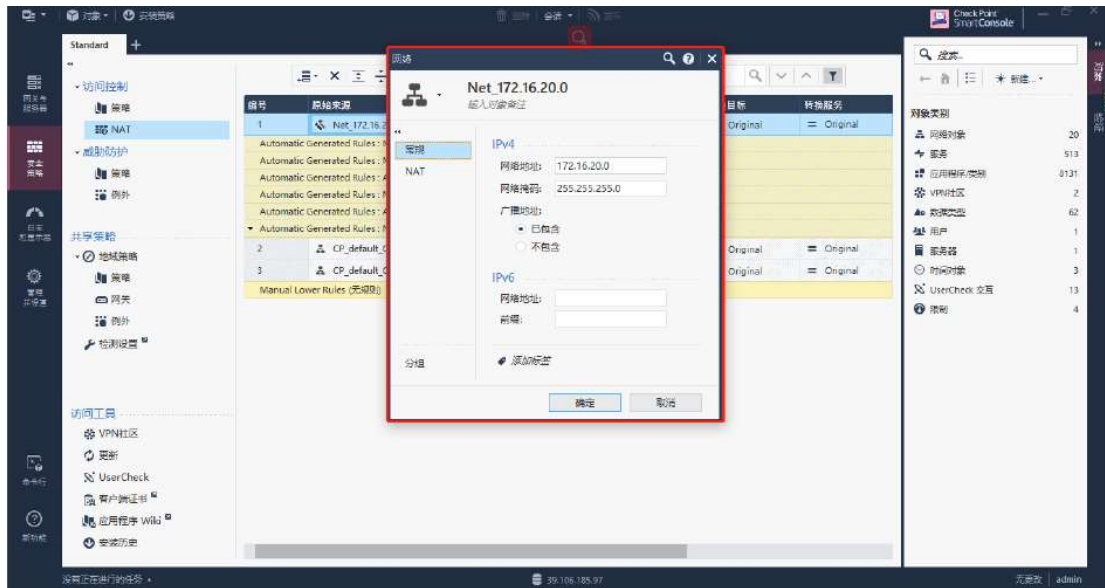


3.6 配置策略

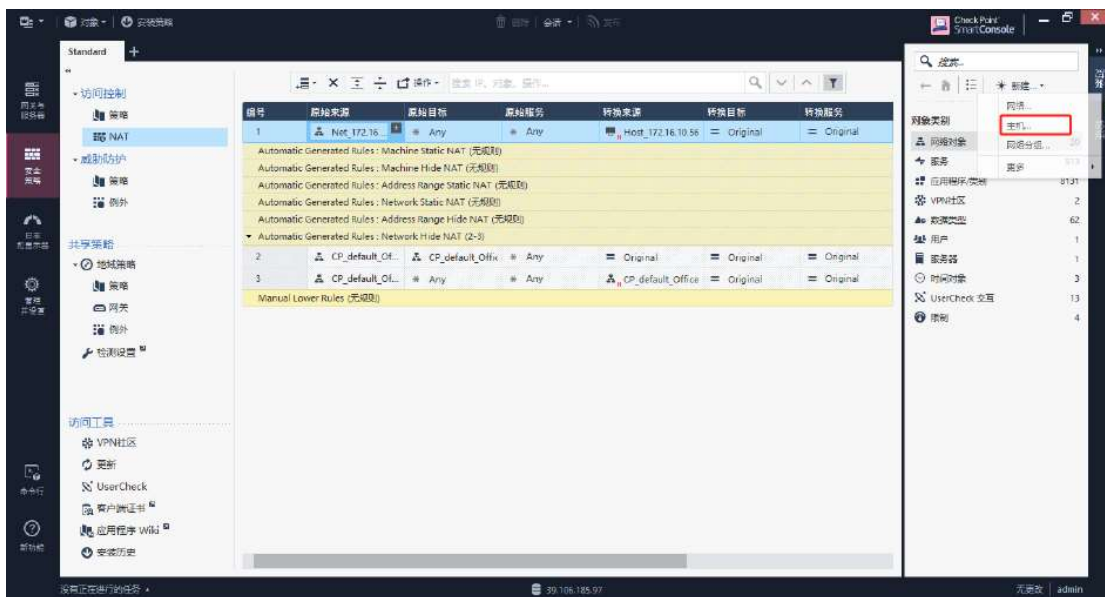


增加内网网段对象





增加主机对象



3.7 安装策略



至此，初始化配置成功。