华为云部署 **CloudGuard**

配置文档

目录

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

2.2 创建 gateway

选择规格

选择市场镜像，选择 gateway 版本

配置两个不同网段的网卡，以及为主机分配公网地址

配置名称和密码

等待创建成功

2.3 创建 Management

同样按照上述方法，创建 Managemen（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

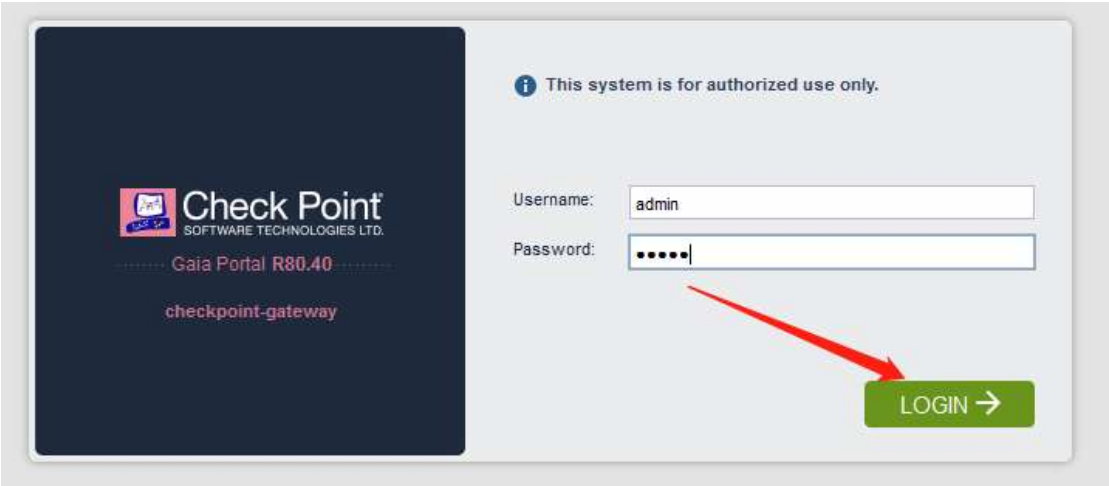
添加 443 端口

3 初始化及配置防火墙

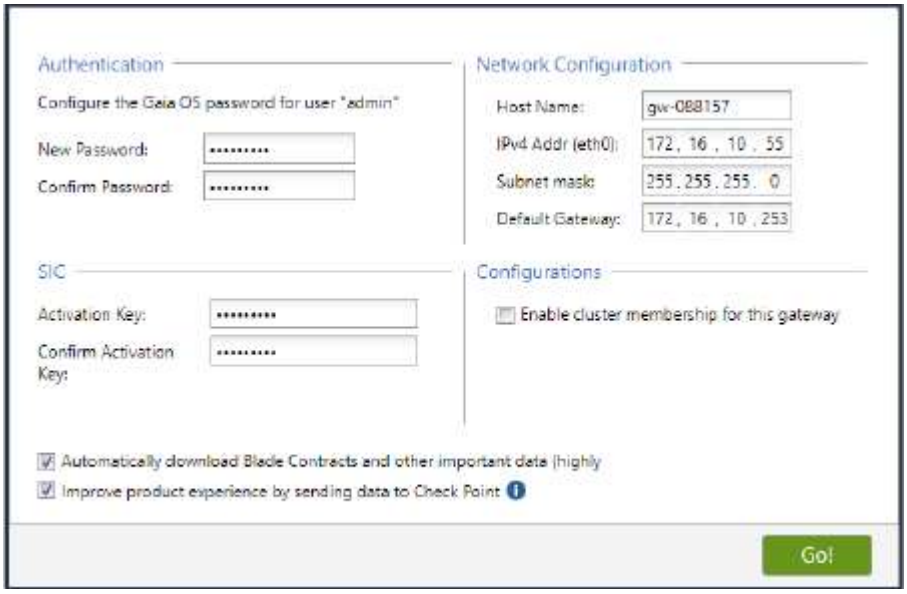
3.1 初始化 Management

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。

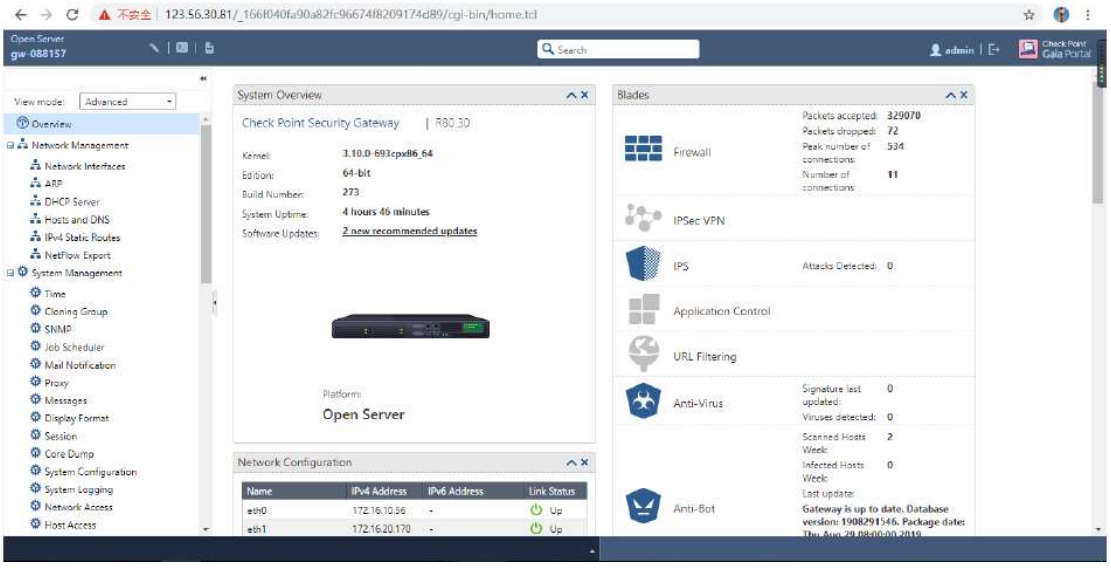
默认账户密码都是 admin



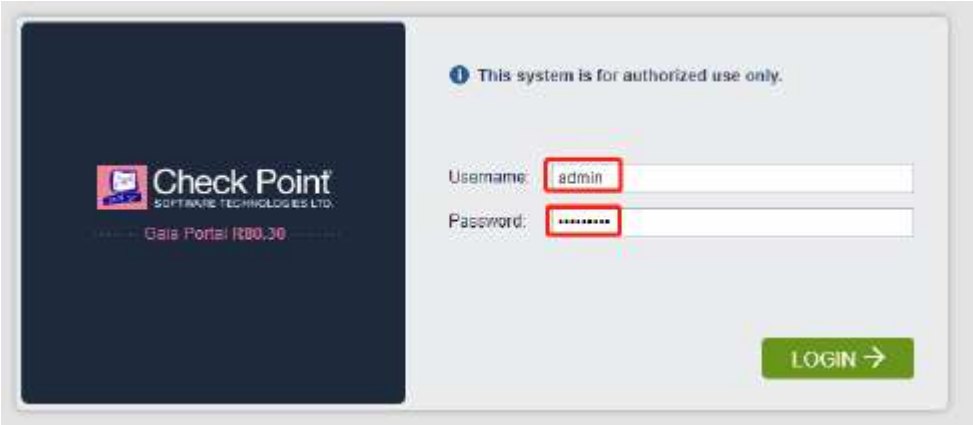
登陆进来之后设置一下用户和 SIC 的密码，两者也可以一样。IP 地址不用变，主机名称可以改一下，因为主机名一旦保存就不支持更改了

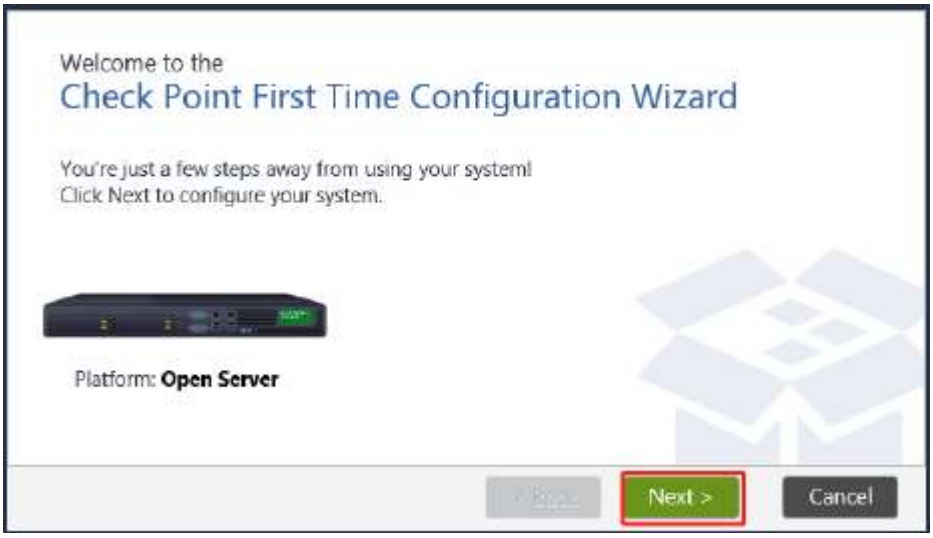


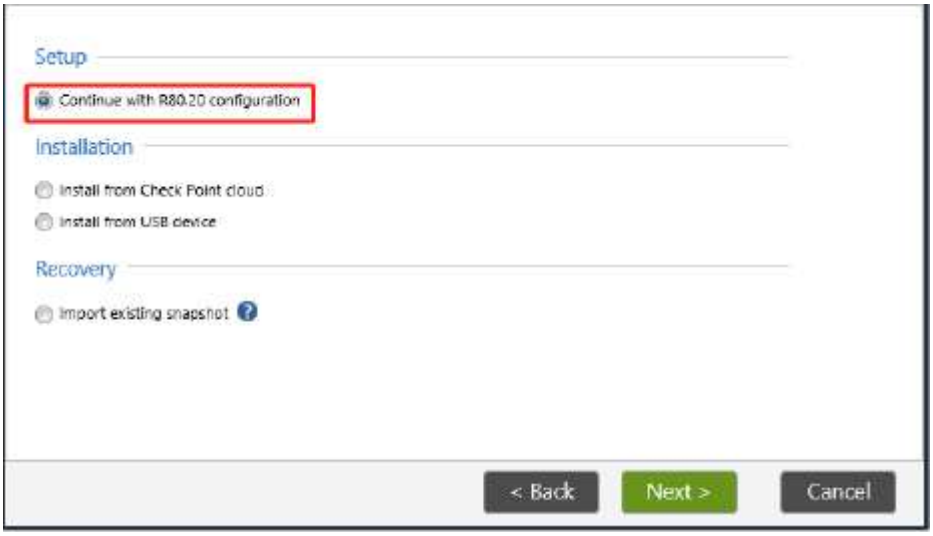
配置完成后是这样的



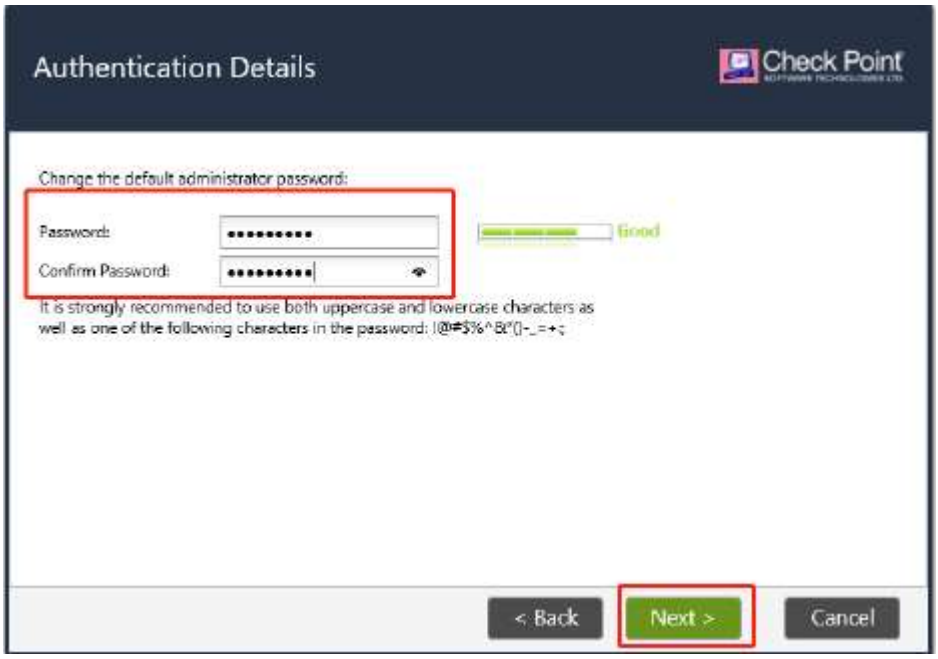
3.2 初始化 Management



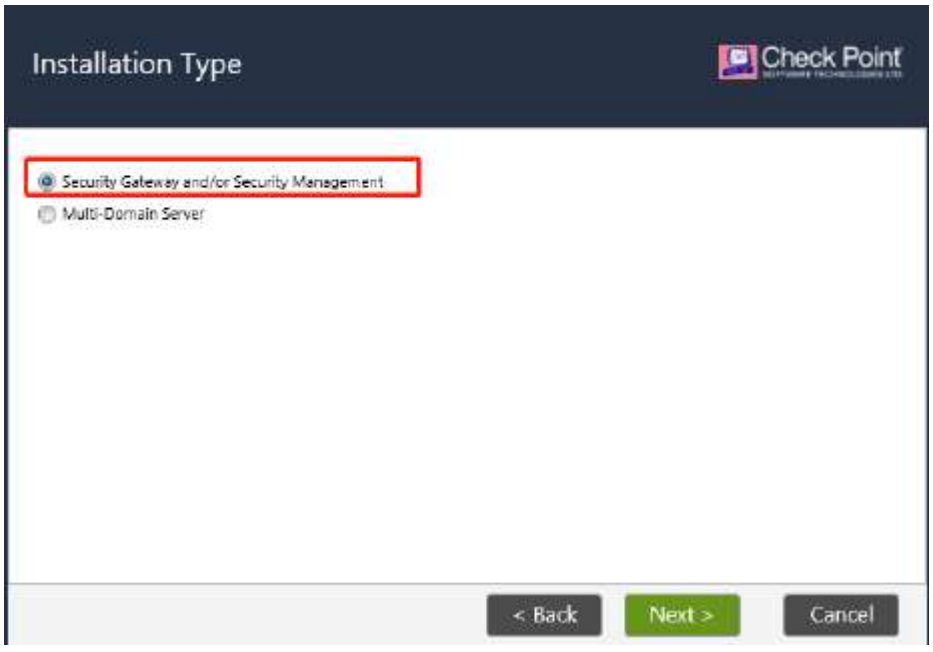


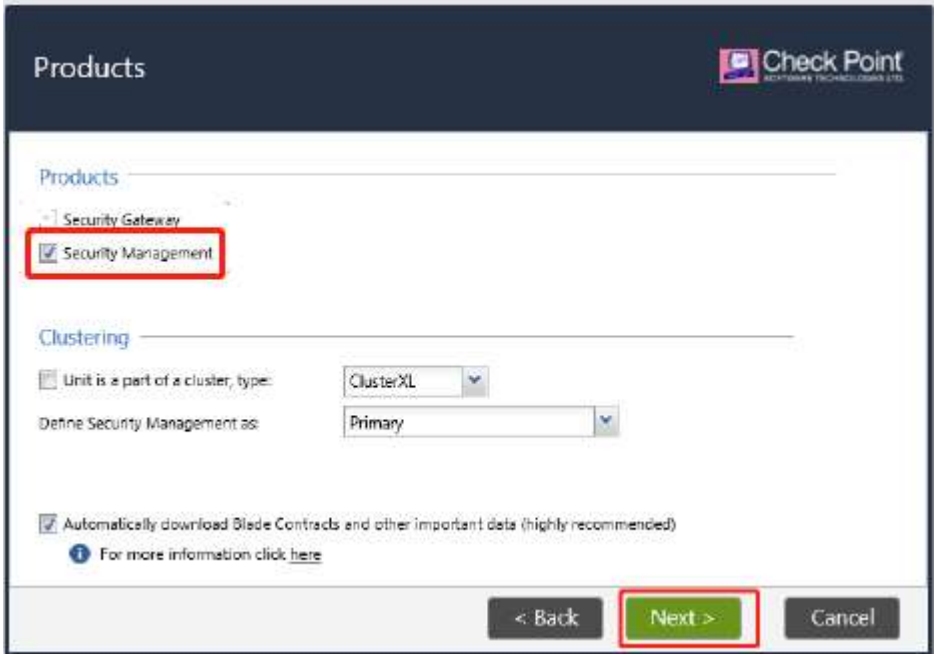


更改默认密码

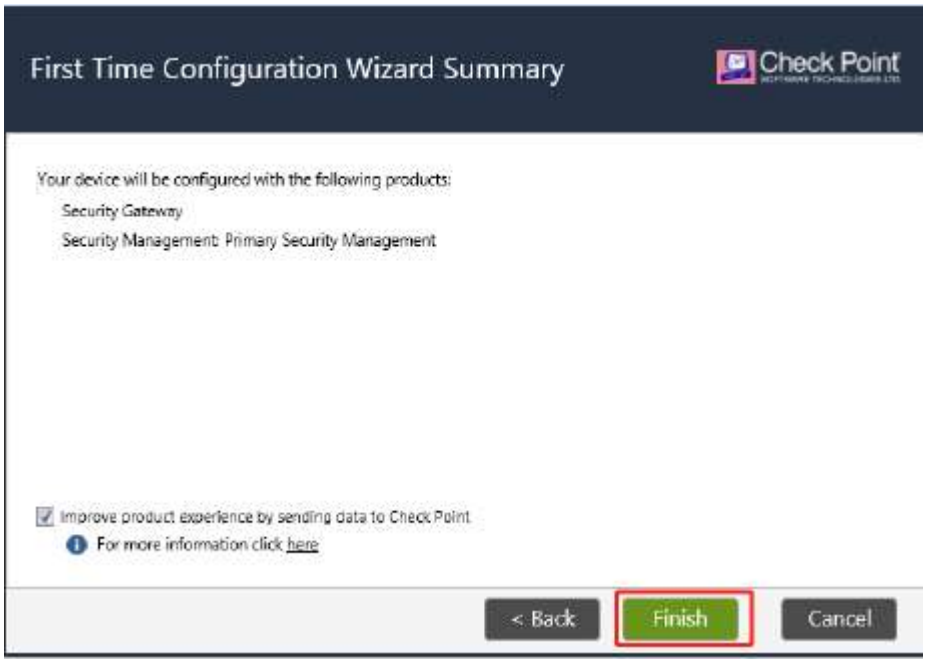


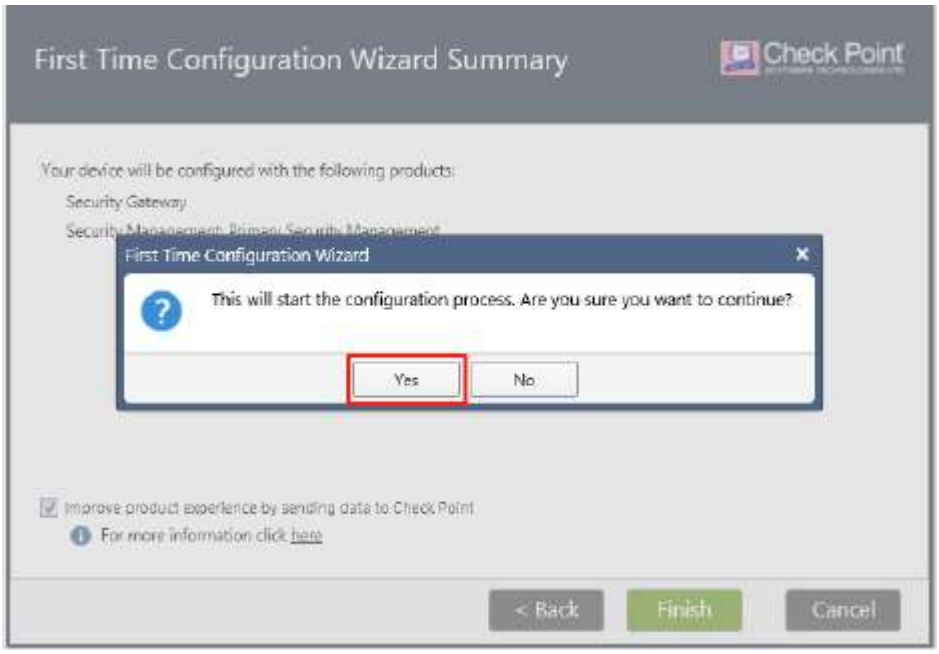
按照向导继续下一步



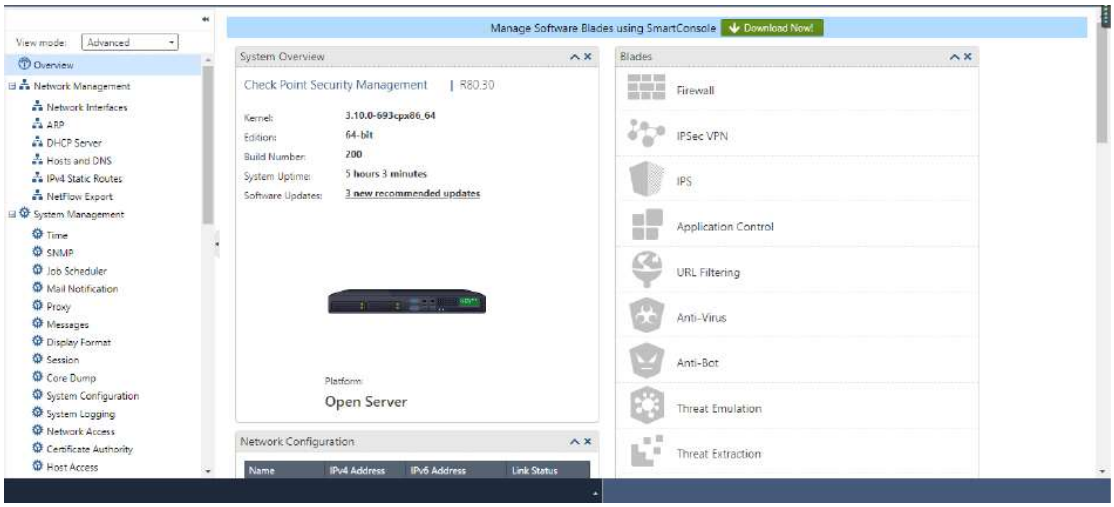


然后默认下一步直到完成

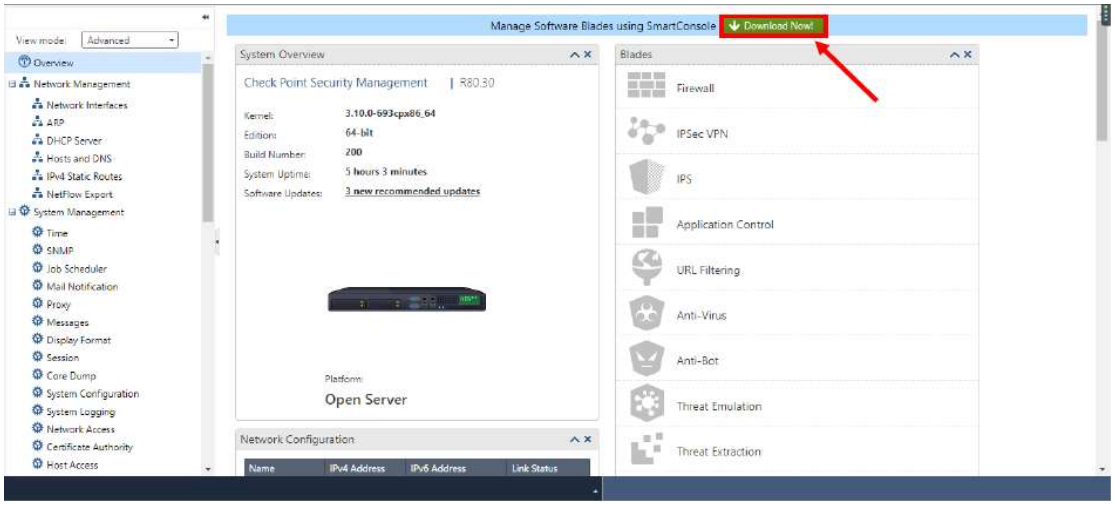




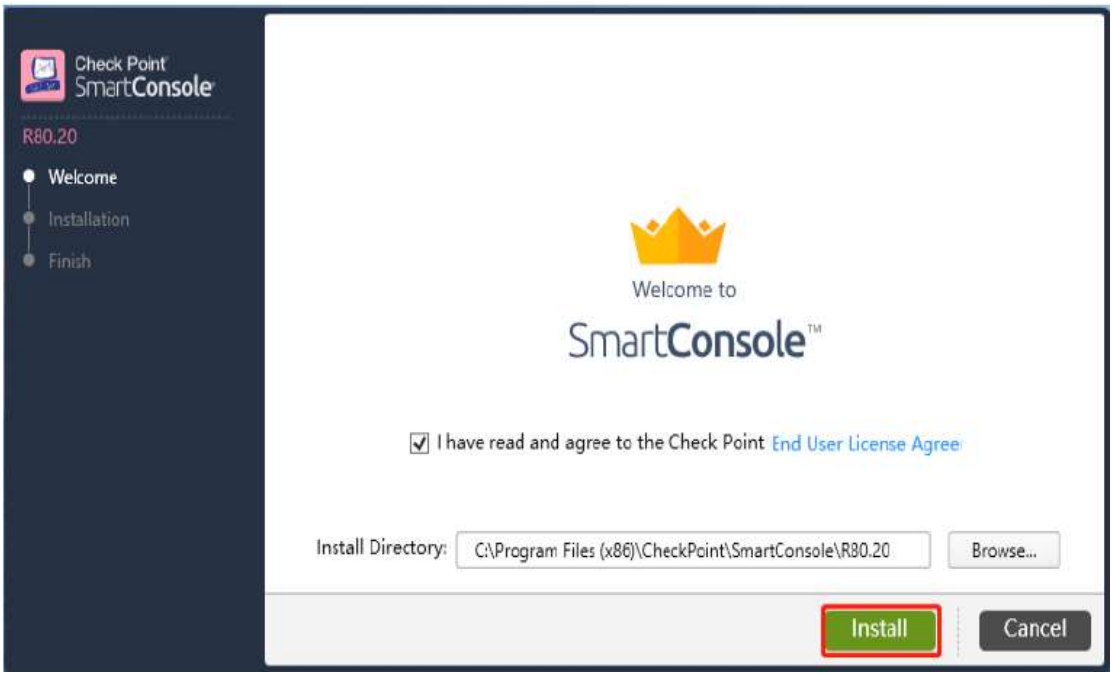
等待初始化完成后，重新登录网址即可见到和 gateway 一样的页面。



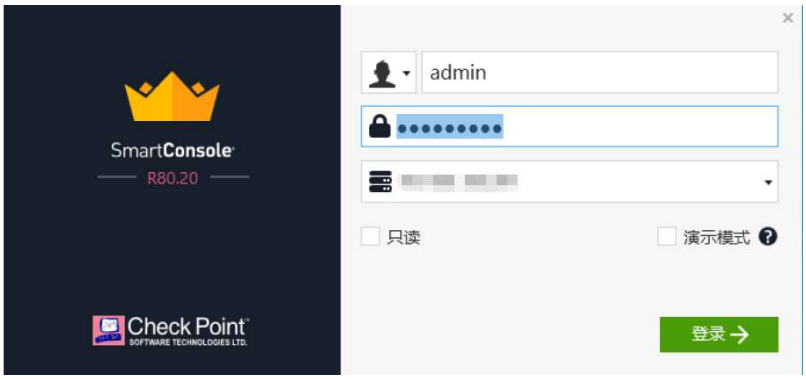
3.3 下载并登陆到 SmartConsole

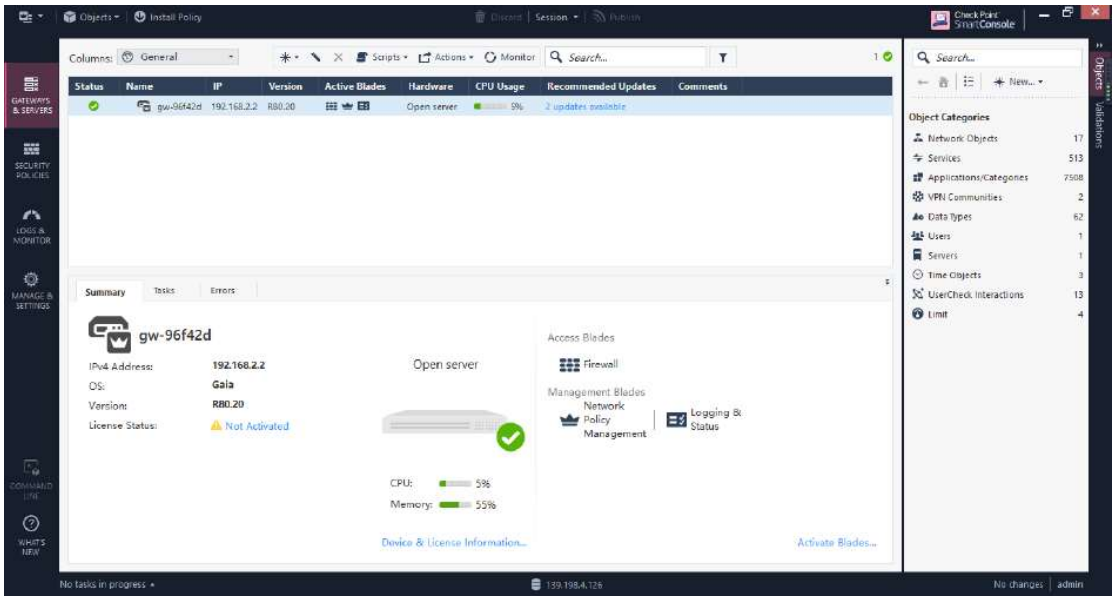


按照向导默认安装



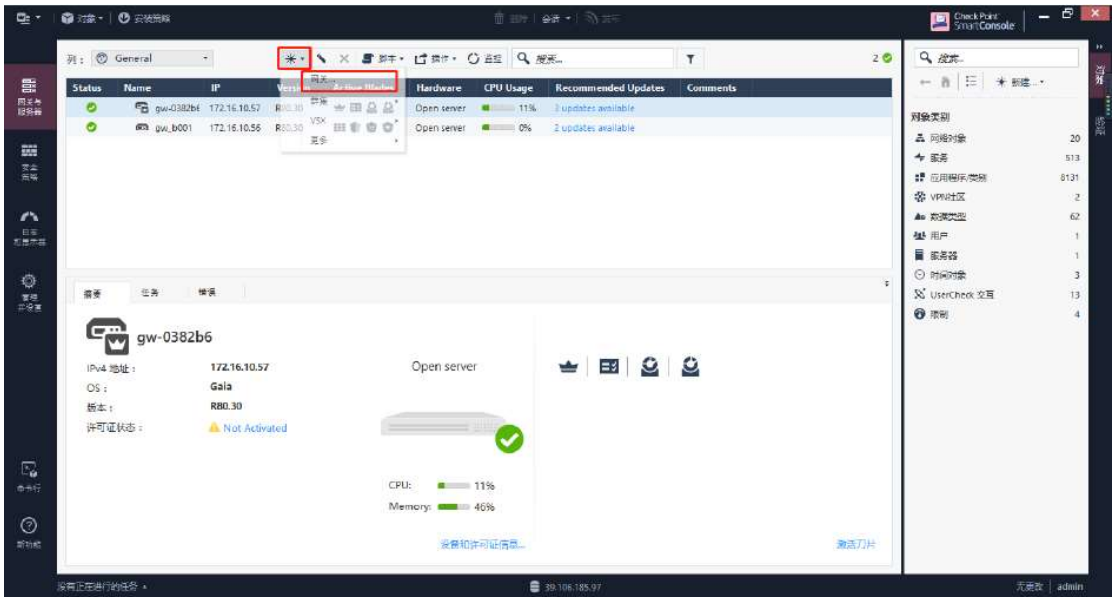
安装完成后，输入 Management IP、用户名和密码，点击登陆

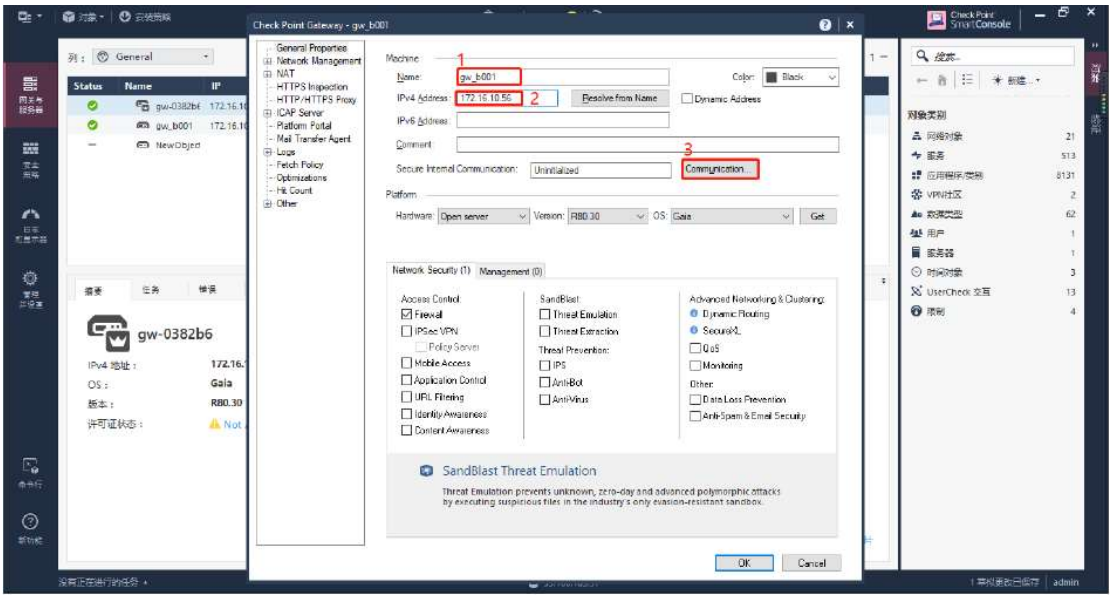


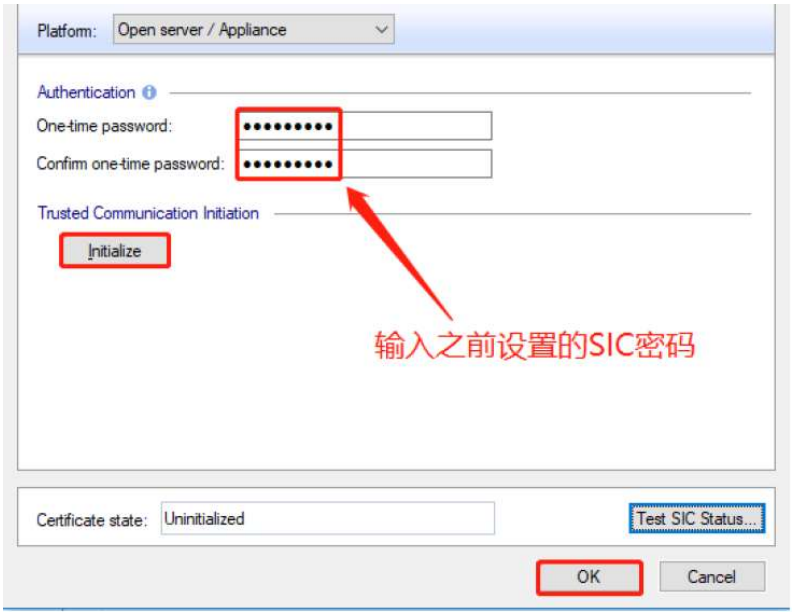


3.4 在 Management 上增加 Gateway

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



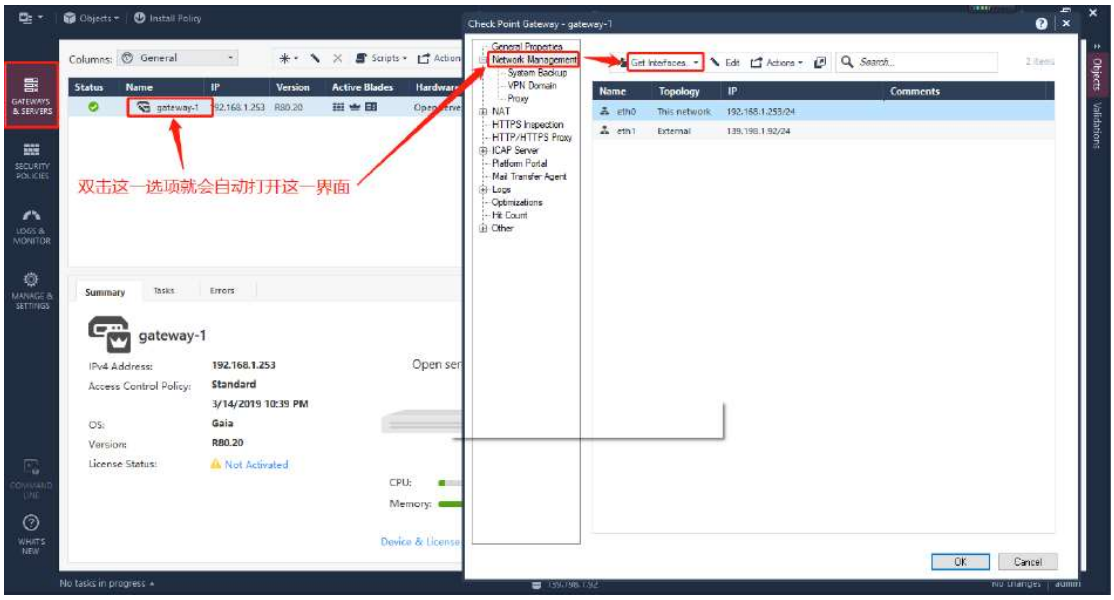

Check Point Gateway - gw_b001
General Properties
Network Management
NAT
HTTPS Inspection
HTTP/HTTPS Proxy
ICAP Server
Platform Portal
Mail Transfer Agent
Logs
Fetch Policy
Optimizations
Hit Count
Other
Machine
Name: gw_b001
IPv4 Address: 172.16.10.56
IPv6 Address:
Comment:
Color: Black
Resolve from Name
Dynamic Address
Secure Internal Communication: Uninitialized
Communication...
1
2
3
Platform
Hardware: Open server
Version: R80.30
OS: Gaia
Get
Network Security (7)
Management (0)
Access Control
Firewall
IPSec VPN
Policy Server
Mobile Access
Application Control
URL Filtering
Identity Awareness
Content Awareness
SandBlast
Threat Emulation
Threat Extraction
Threat Prevention
IPS
Anti-Bot
Anti-Virus
Advanced Networking & Clustering
Dynamic Routing
SecureXL
QoS
Monitoring
Other
Data Loss Prevention
Anti-Spam & Email Security
SandBlast Threat Emulation
Threat Emulation prevents unknown, zero-day and advanced polymorphic attacks by executing suspicious files in the industry's only evasion-resistant sandbox.
OK
Cancel
gw-0382b6
IPv4 地址：
OS：
Gaia
版本：
R80.30
admin


Platform:
Open server / Appliance
Authentication
One-time password:
Confirm one-time password:
Trusted Communication Initiation
Initialize
输入之前设置的SIC密码
Certificate state:
Uninitialized
Test SIC Status...
OK
Cancel

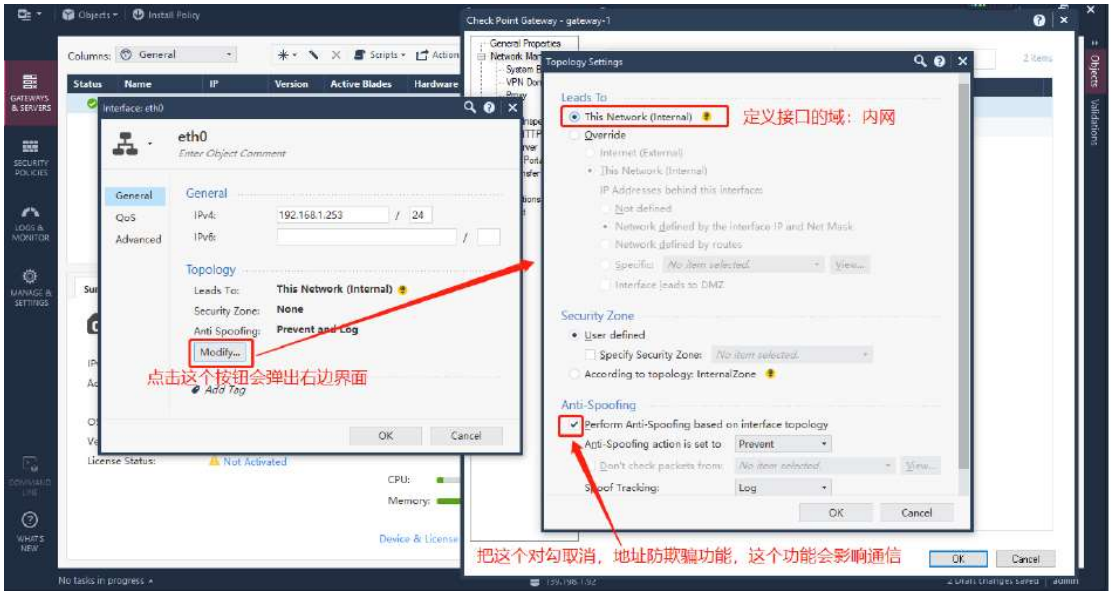
3.5 配置 Gateway

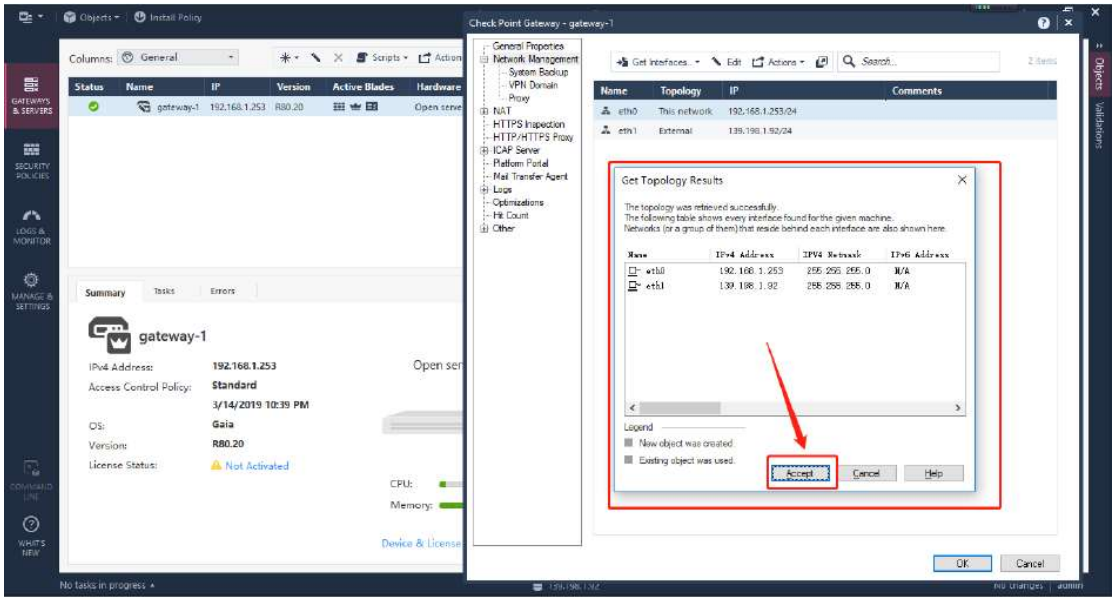
配置接口及关闭接口地址防欺骗功能

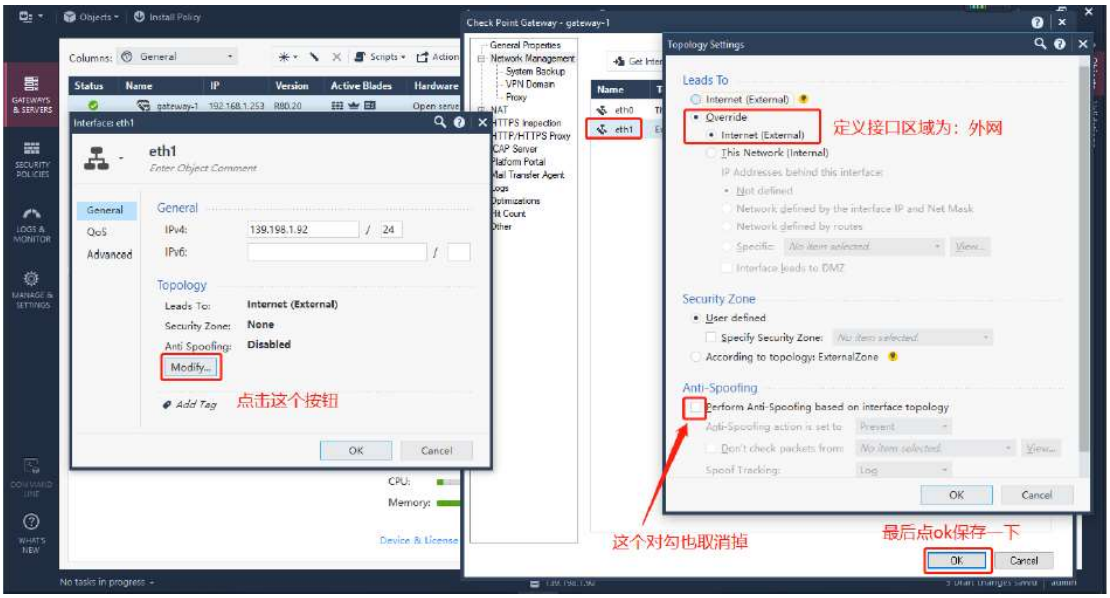
让上层 FW 获取底层接口信息及拓扑



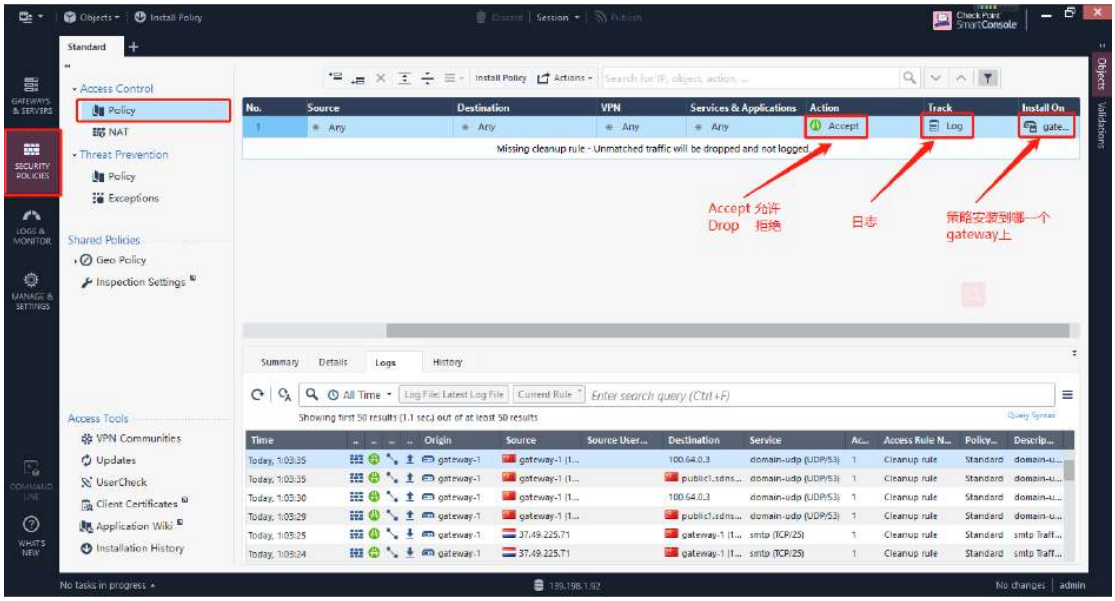
定义接口域，并关闭接口地址防欺骗功能



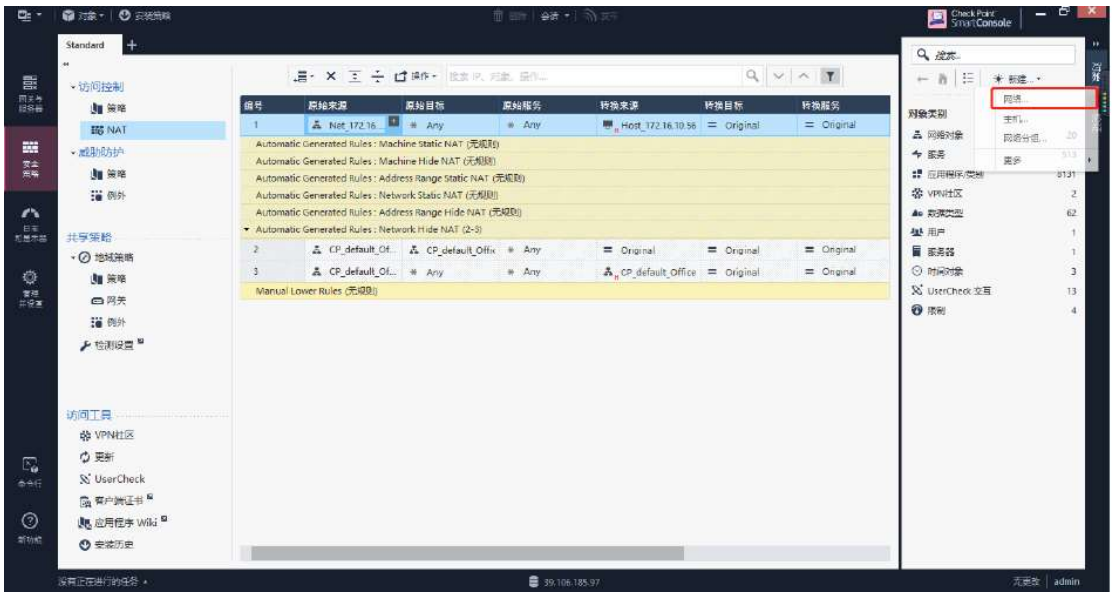

Get Topology Results
Accept
Cancel
Help
OK
Cancel

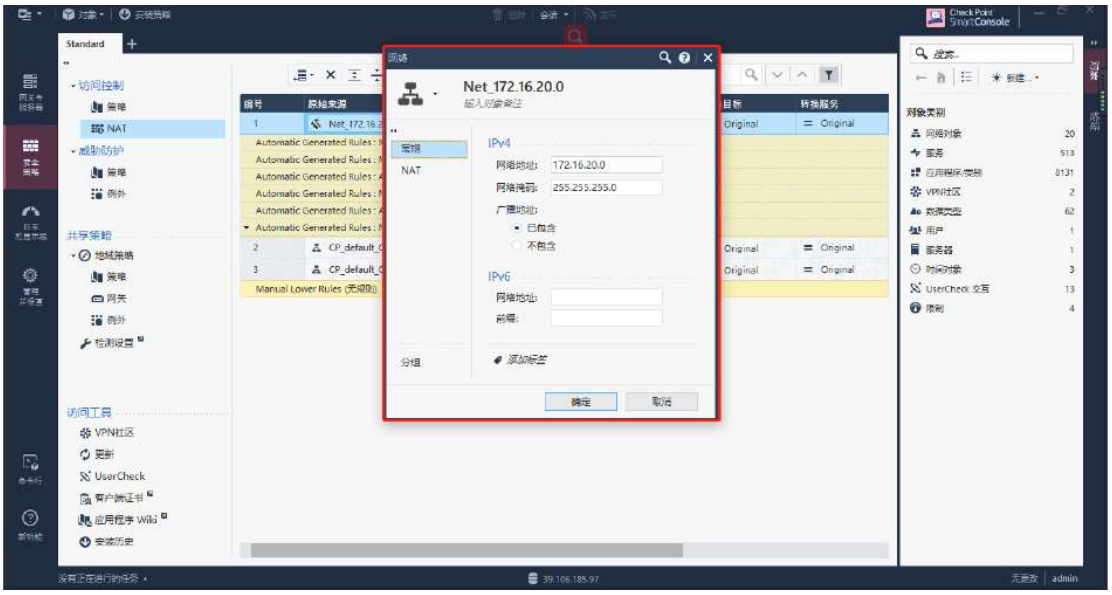

eth1
Modify...
点击这个按钮
Topology Settings
Leads To
Override
Internet (External)
定义接口区域为：外网
Anti-Spoofing
Perform Anti-Spoofing based on interface topology
这个对勾也取消掉
最后点ok保存一下
OK
Cancel

3.6 配置策略

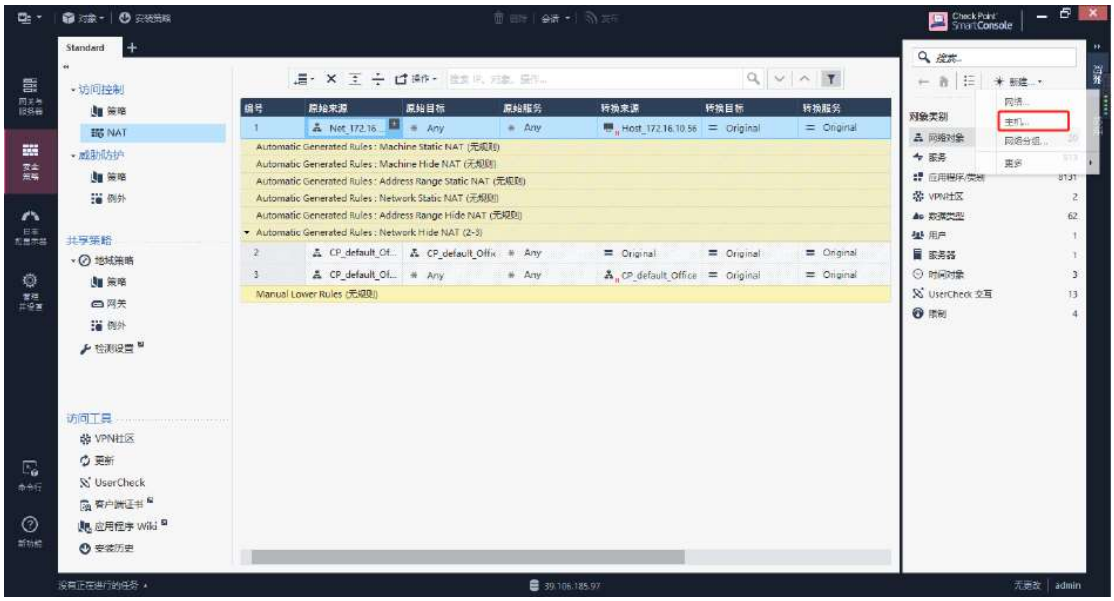


增加内网网段对象




Net_172.16.20.0
常规
NAT
IPv4
网络地址: 172.16.20.0
网络掩码: 255.255.255.0
广播地址:
已包含
不包含
IPv6
网络地址:
前缀:
分组
添加标签
确定
取消

增加主机对象


Standard
访问控制
策略
NAT
威胁防护
策略
例外
共享策略
地域策略
策略
网关
例外
检测设置
访问工具
VPN社区
更新
UserCheck
客户端证书
应用程序 Wiki
安装历史
Automatic Generated Rules : Machine Static NAT (无规则)
Automatic Generated Rules : Machine Hide NAT (无规则)
Automatic Generated Rules : Address Range Static NAT (无规则)
Automatic Generated Rules : Network Static NAT (无规则)
Automatic Generated Rules : Address Range Hide NAT (无规则)
Automatic Generated Rules : Network Hide NAT (2-3)
Manual Lower Rules (无规则)
网络...
主机...
网络组...
更多

3.7 安装策略

至此，初始化配置成功。