Check Point
SOFTWARE TECHNOLOGIES LTD.

2020年9月10日

1530/1550设备

R80.20.XX

入门指南

Check Point
INFINITY

型号：V-80、V-80W 分类：[受保护]

Check Point版权声明

重要信息

最新文档
此文档的最新版本位于：
http://downloads.checkpoint.com/dc/download.htm?ID=88183

如需了解更多信息，请访问Check Point支持中心：
https://supportcenter.checkpoint.com

反馈
Check Point一直在致力于完善其文档。
请将您的意见发送至以下地址，以帮助我们不断改进：
cp_techpub_feedback@checkpoint.com

修订历史

日期	说明
2020年9月10日	更新了合规信息。
2020年3月2日	添加了1530型号，并更新了合规信息。
2020年1月19日	本文档的第一版

目录

引言 6

装运箱内容物 7

设置设备 8

壁挂安装 8

连接电缆 9

首次部署选项 10

设备示意图和规格 11

前面板 13

后面板 15

侧面板 16

使用首次配置向导 17

开始首次配置向导 18

欢迎 19

Zero Touch 19

身份验证详情 21

设备日期和时间设置 22

设备名称 23

安全策略管理 24

互联网连接 25

本地网络 27

无线网络 28

管理员访问 29

设备注册 30

安全管理服务器身份验证 32

安全管理服务器连接 33

软件刀片激活 34

摘要 35

Zero Touch云服务 36

U盘 37

健康与安全信息 38

支持 ***44***

引言

感谢您选择Check Point的互联网安全产品套件。Check Point产品为您的企业提供当下最新的安全解决方案。

Check Point还通过授权的培训中心、经认证的支持合作伙伴和Check Point技术支持人员所组成的网络，提供全球技术服务，包括教育服务、专业服务和支持服务，以确保您可以从安全投资中获取最大收益。

请在此处打开此文档的最新版本。

更多设备相关信息，请查看*Check Point 1500设备系列管理指南*。

如需更多技术信息，请访问Check Point支持中心。

装运箱内容物

项目	数量	说明
设备	1	1530 / 1550
LAN电缆	2	1.8m - RJ45至RJ45，CAT5e，屏蔽，STP，黑色
控制台电缆	1	1m，USB type-C转USB-2.0 type-A，黑色
电源适配器	1	AC转12VDC台式，黑色 40W，适用于有线和WiFi型号
适配器电源线	1	插头类型：美国、英国、欧盟和澳大利亚/新西兰、印度、中国、日本
橡胶垫脚	4	装在设备上
壁挂安装组件	1 2 2	包括钻孔位置贴纸。 螺丝：M4*6，桁架螺丝 螺旋锚
天线	3	WiFi天线RP-SMA型，黑色(仅限WiFi型号)
指南	1 1	*Check Point 1530/1550设备快速启动指南* *Check Point 1530/1550设备入门指南*
许可协议	1	最终用户许可协议

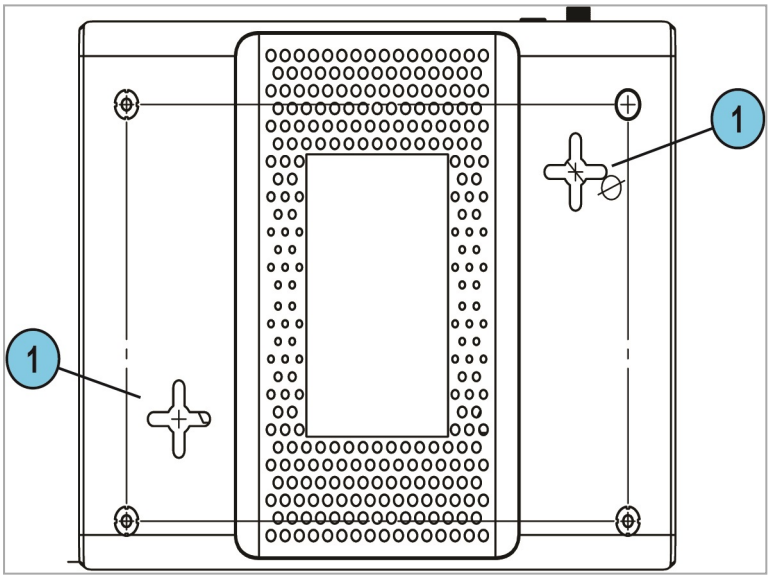
设置设备

1. 从装运箱中取出Check Point 1530/1550设备，并将其放在桌面上。
2. **可选** - 撕掉设备前面板上的透明保护贴纸。
3. 将天线连接到对应型号设备(仅限WiFi型号)。
4. 找到标为LAN1的网络接口。该接口预配置IP地址192.168.1.1。

壁挂安装

如要将设备安装到墙上：

1. 将壁装贴纸贴在墙上，然后钻两个螺丝孔。
2. 在墙上插入2个螺旋锚。
3. 将配件包中的2个螺丝(M4*6)装到墙上。
4. 安装设备，并确认2个螺钉是否牢牢固定在设备上。



密钥	项目	说明
1	设备底部孔	此处安装螺钉。

连接电缆

1. 将电源装置连接到设备和电源插座。

   电源装置连接到插座后，按后面板的开/关按钮即可打开设备。

2. 打开设备后，前面板上的电源LED将短暂亮起红色，

   然后变为蓝色并开始闪烁。这表示系统正在启动并安装固件。

   当LED常亮蓝色时，即可以登录设备。

   注 - 如果出现警报或错误，LED会亮起红色。

3. 将标准网络电缆连接到设备后面板上的LAN1端口，以及PC上的网络适配器。

4. **选项：将控制台电缆连接到设备后部的控制台端口，以及受支持终端上的USB端口。**

   a. 将Flow control(流量控制) 设置为**None**。

   b. 如要获取控制台驱动程序，请单击：https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

   c. 验证MD5和SHA256是否如下所示：

      - MD5 - c0b27c9b0f3a3ed53927a4857853a2cb
      - SHA 256 - 5d8fa117cd499a50cab895f35d50d108a61e80b6a3f6d2ecbffa8949085b8f2e

5. **如果您使用外部调制解调器：**

   将以太网电缆连接到设备后面板上的WAN端口，然后插入外部调制解调器或路由器的PC/LAN网络端口。连接以太网后，设备前面板上的互联网LED将亮起。

注 - 在电源周期(打开和关闭) 之间，等待10秒。

首次部署选项

在首次部署网关时，您可以使用多种不同的选项：

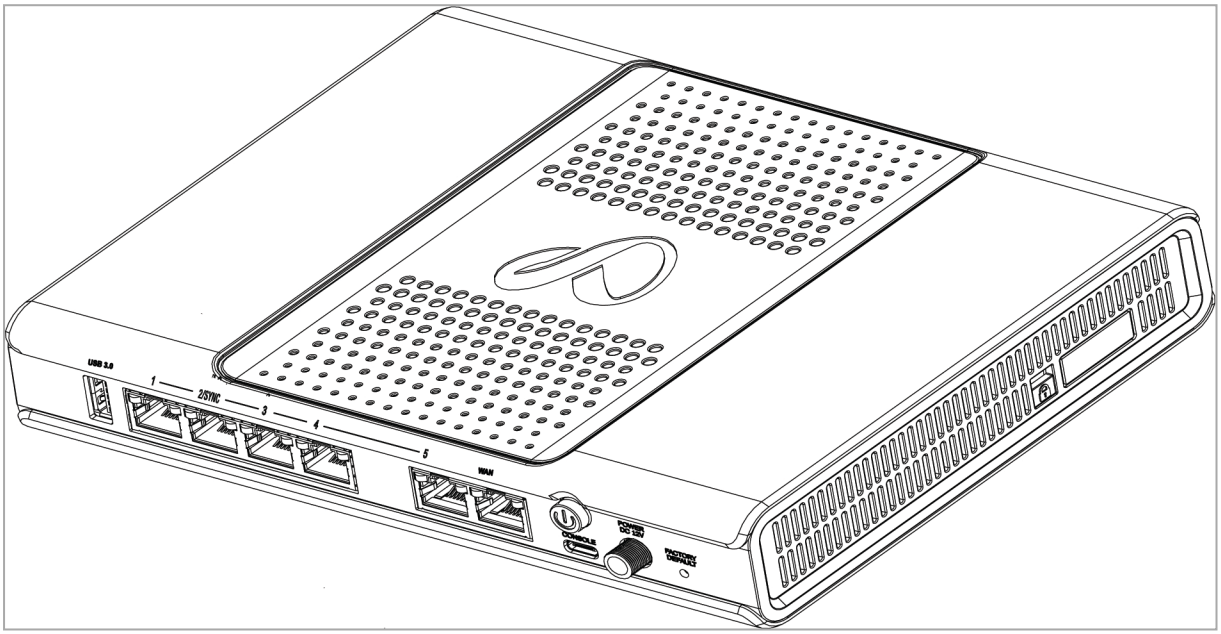
- *"使用首次配置向导"在本页17*
- *"Zero Touch云服务"在本页36*
- *"U盘"在本页37*

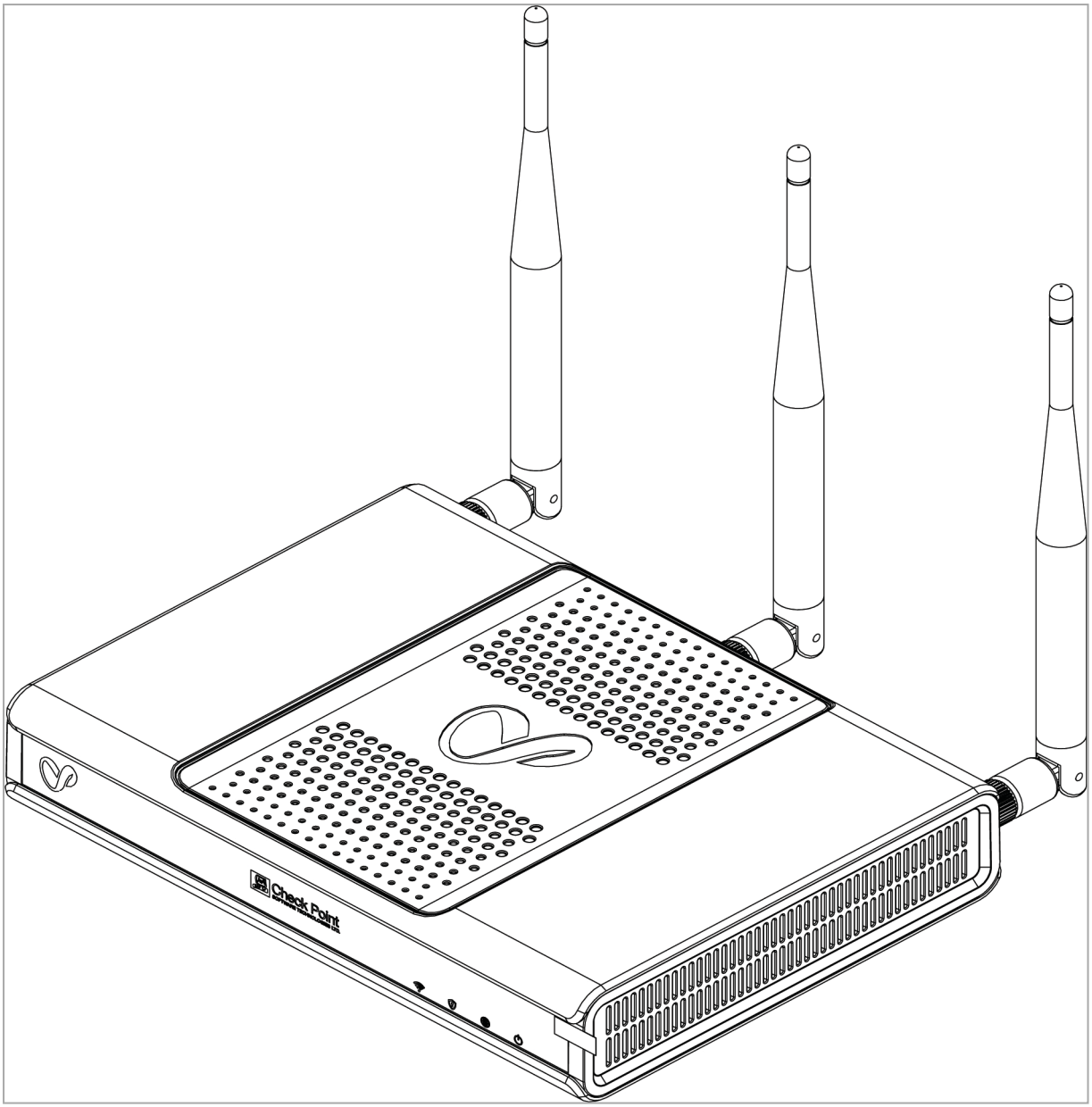
设备示意图和规格

本部分介绍了1530/1550型号的前面板、后面板和侧面板的不同功能：

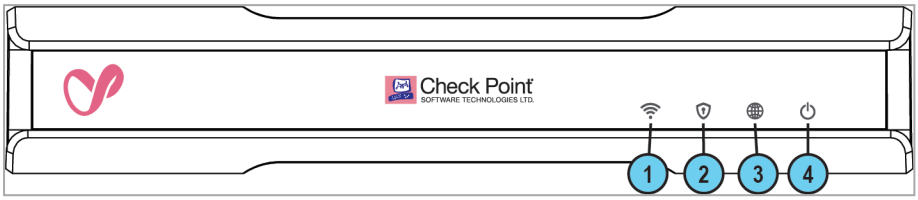
- 有线
- WiFi(带天线)

注 - 根据您具备的设备型号，以下部分规格可能会有所不同。




Check Point

前面板



注 - 仅有一组LED。这些LED会根据发生的活动，亮起不同的颜色。

表格：LED

密钥	项目	图标	说明
1	WiFi LED (仅限WiFi型号)		■ **关** - WiFi关闭 ■ **蓝色** - WiFi开启，并正常运行 ■ **红色** - WiFi错误/警报
2	管理LED		■ **关** - 无管理 ■ 颜色 - 参见下方
3	互联网LED		■ **关** - 无互联网连接 ■ **闪烁蓝色** - 尝试连接到互联网。 ■ **蓝色** - 已连接 ■ **闪烁红色** - 连接失败
4	电源LED(状态)		■ **常亮蓝色** - 正常运行 ■ **闪烁蓝色** - 正在启动和安装固件。在该过程完成后，LED将常亮蓝色。 ■ **红色** - 错误/警报 **注** - 设备首次打开时，该LED亮起红色。

管理LED显示重试机制的状态：

操作	管理LED活动
Zero Touch正在运行。	闪烁红色(慢速)
已成功连接至Zero Touch云服务器，并保存部署脚本。	闪烁红色(快速)
Zero Touch过程已完成。无需激活SMP。	LED关闭
激活睡眠时间。	闪烁蓝色(慢速)
重新激活。	闪烁蓝色(快速)
SMP已连接。	常亮蓝色。
SMP模式关闭。	LED关闭

操作	管理LED活动
网关无法连接到SMP，并将退出重试脚本。	常亮红色。

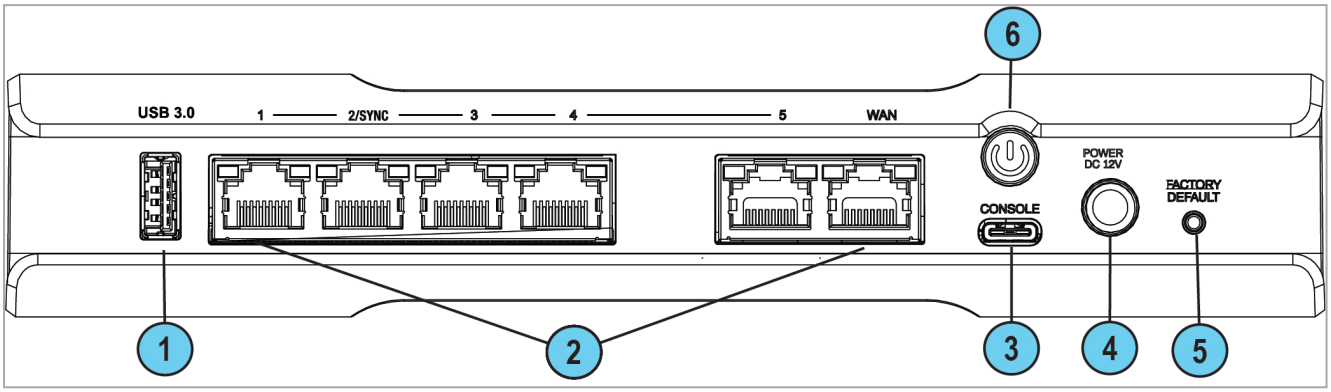
重试前的等待时间：

失败	等待时间
第1次	2分钟
第2次	4分钟
第3次	8分钟
第4次	16分钟
后续次数	每16分钟重试一次，直到成功激活云服务

下表介绍了网络LED(RJ45 WAN和LAN端口) 。各端口使用双色LED显示链路/活动和速度，从10M至1GbE。

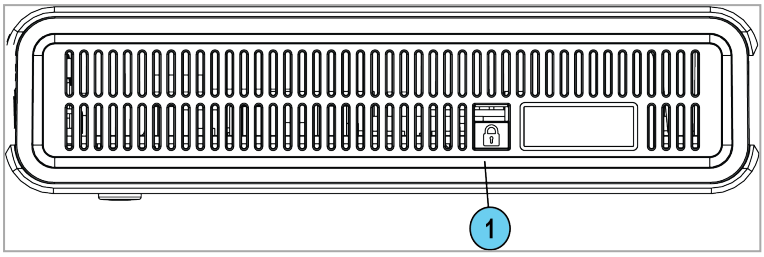
RJ45	LED1(绿色)	LED2(琥珀色)
无链路	关	关
1G链路	打开	关
1G活动	闪烁	打开
100M链路	打开	关
100M活动	闪烁	关
10M链路	打开	关
10M活动	闪烁	关

后面板



密钥	项目	说明
1	USB端口3.0	用于软件下载。
2	LAN和WAN端口1 GbE	LAN端口1-5，LAN 2/同步 WAN端口1。
3	控制台	此处插入串行控制台电缆。波特率：115200。
4	电源线插座	此处插入电源适配器线。
5	出厂默认设置	长按按钮12秒，将设备恢复至出厂默认设置。
6	电源按钮	按电源按钮打开或关闭设备。

侧面板



密钥	项目	说明
1	防盗插槽。	此处插入防盗电缆。请参考Kensington和Sunbox TL-623M电缆。

使用首次配置向导

使用首次配置向导配置Check Point 1530/1550设备。

如要关闭向导并保存已配置的设置，请单击**Quit**。

注 - 在首次配置向导中，您可能无法看到本指南中所述的所有页面。向导中显示的页面取决于您的设备型号和您选择的选项。

开始首次配置向导

如要在完成硬件设置后，首次配置Check Point 1530/1550设备，请使用首次配置向导。

如果您因为以下情况未完成向导，则向导将在您连接到设备后再次运行：

- 浏览器窗口关闭。
- 在您运行向导时，设备会重启。

在完成向导后，您可以使用WebUI(Web用户界面) 更改使用首次配置向导配置的设置，并配置高级设置。

如要打开WebUI，请在浏览器中输入以下其中一个地址：

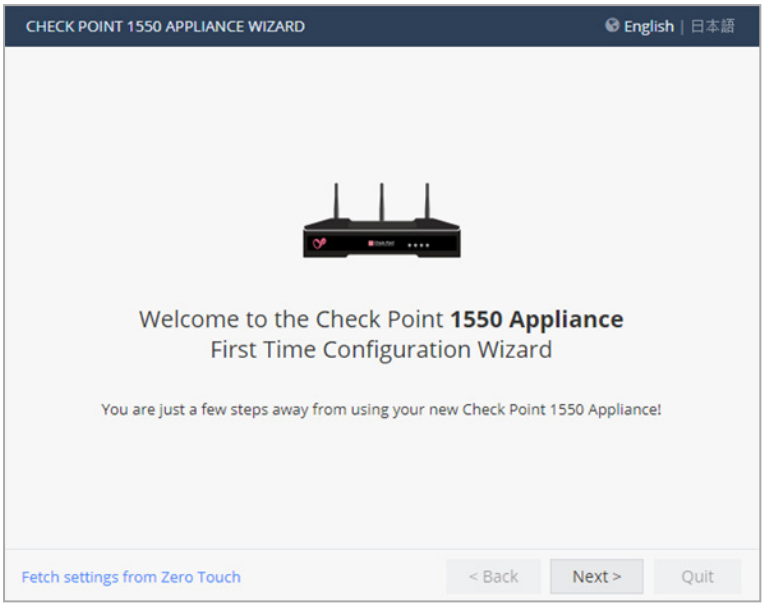
- https://my.firewall
- https://192.168.1.1:4434

如果屏幕上显示安全警告消息，请确认并继续。

首次配置向导将运行。

欢迎

Welcome页面列有产品介绍，并且会显示您的设备名称。



您可以连接到Zero Touch服务器，以自动从云端提取设置。

如要更改WebUI应用程序的语言：

选择页面顶部的语言链接。

注 - 仅允许使用英语作为输入语言。

Zero Touch

借助Zero Touch，网关可以在首次连接至互联网后，自动从云端提取设置。

注 - 如果您使用代理服务器连接至互联网，则无法使用Zero Touch。

如果网关通过DHCP连接至互联网，则无需额外操作即可提取Zero Touch设置。如果没有可用的DHCP服务，则您必须运行首次配置向导，配置**Internet Connection**设置，然后从Zero Touch服务器提取设置。

如要连接到Zero Touch服务器：

1. 在**Welcome**页面，单击**Fetch Settings from the cloud**。
2. 在打开的窗口中，单击**OK**，以确认您想要继续。
3. **Internet connection**页面将打开。配置您的互联网连接，并单击**Connect**。
4. **Fetching settings from the cloud**窗口将打开，并显示**Connecting to the service provider**状态。此过程需要几分钟时间。
5. 如果连接失败，屏幕上将显示一条错误消息。可能的错误包括：

- 互联网连接配置有误。
- 互联网连接是通过代理服务器。
- Zero Touch已在运行。
- Zero Touch服务已经完成。
- 首次配置向导已经完成。
- Zero Touch服务被禁用。

  如适用，立即单击**Retry**以重新连接。

6. 连接到服务器后，系统将自动下载和安装设置。**Fetching settings from the cloud**窗口会显示状态。安装完成可能需要几分钟的时间。
7. 单击**完成**。

注 - 如果检测到内部网络(LAN)和使用DHCP (WAN)返回的IP之间发生冲突，将自动更改存在冲突的LAN地址。如果已更改存在冲突的LAN IP地址，系统日志中会显示一条消息。

当您重新连接到WebUI，或者单击**Refresh**后，浏览器将打开以显示安装过程状态。

网关下载并成功应用设置后，将不会再次连接到Zero Touch服务器。

身份验证详情

在**Authentication Details**页面，输入所需的详情，以登录Check Point 1530/1550 WebUI 应用程序，或者如果向导异常终止：

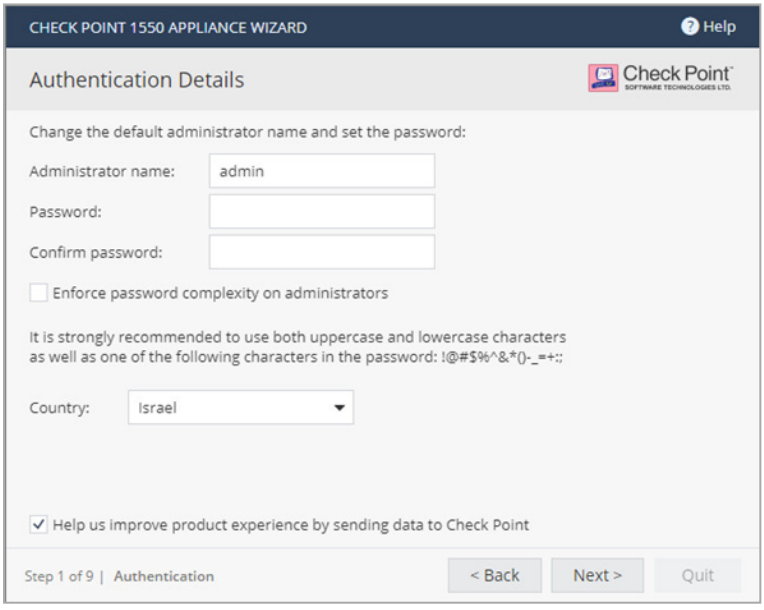
- **Administrator Name** - 我们建议您更改默认的管理员的“admin(管理员)”登录名称。该名称区分大小写。
- **Password** - 至少包含6个字符的强密码，其中至少一个大写字母、一个小写字母和一个特殊字符。使用**密码强度**计量表，测量您设置的密码的强度。

  注 - 该计量表只是一种指示器，并不能强制创建包含特定数量字符或字符组合的密码。如要强制执行密码复杂性，请勾选此复选框。
- **Confirm Password** - 再次输入密码。
- **Country** - 从列表中选择一个国家/地区 (针对无线网络型号) 。

  由于各地区的法规有所差异，无线频率和参数要取决于许可证设置的国家/地区。

  如果您正在使用试用许可证，则在所有区域仅可进行**基本无线电设置**。**Summary**页面和**Device > License**页面上将显示一条警告消息，表示未应用所选的无线电设置。有关基本无线电设置的更多信息，请参见sk159693。

  如果您选择了一个国家/地区，并安装了一张有效的许可证，但设备的无线区域与您所选的国家/地区不符，系统会显示一条警告消息，而您则必须编辑国家/地区信息。如果国家/地区与无线区域相符，您将可以查看完整设置。

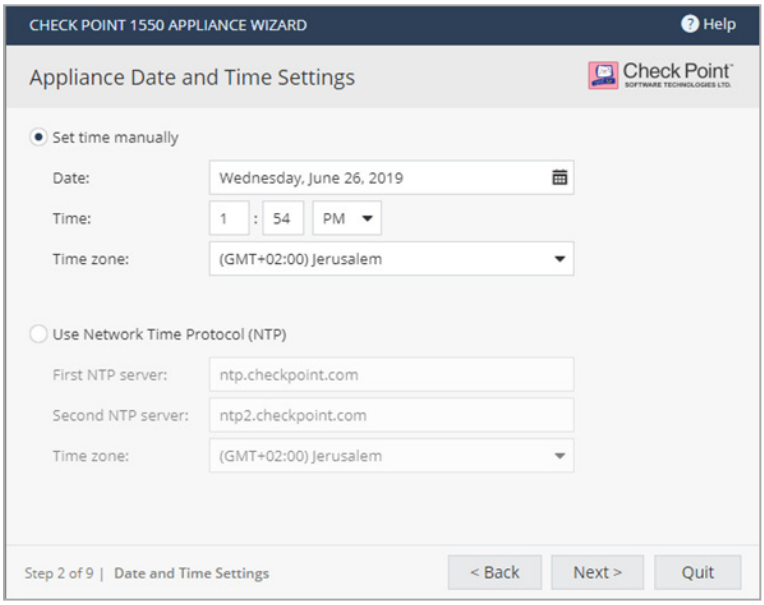


设备日期和时间设置

在**Appliance Date and Time Settings**页面，手动配置设备的日期、时间和时区设置，或者使用网络时间协议选项。

在手动设置时间时，默认将使用主机设置的日期和时间值。如必要，请更改时区设置，以正确显示您所在的位置。默认自动启用夏令时。您可以在WebUI应用程序的**Device** > **Date and Time**页面对其进行更改。

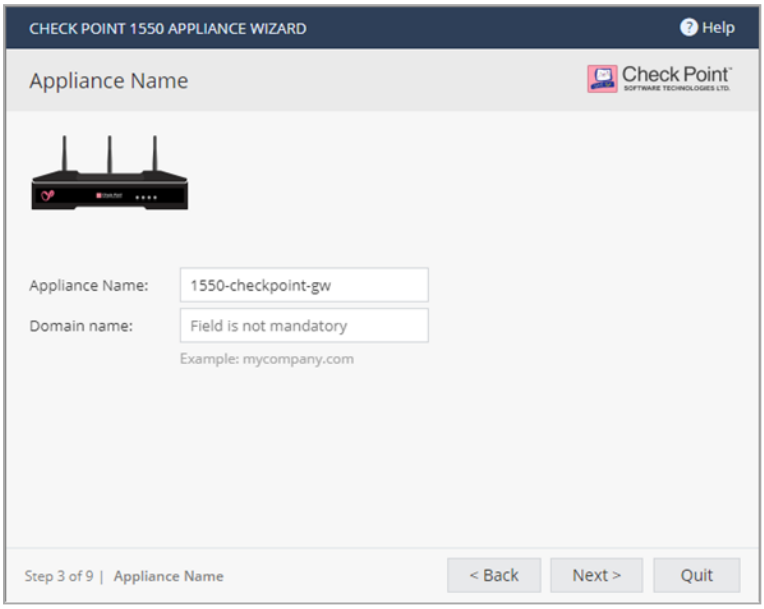
- **Date** - 默认显示主机日期。如需要，请设置一个不同的日期。
- **Time** - 默认显示主机时间。如需要，请设置一个不同的时间。
- **Time Zone** - 默认显示主机时区。如需要，请选择一个时区设置，以准确显示您所在的位置。
- **Primary NTP server** - 主NTP服务器的IP或主机名称。默认服务器为`ntp.checkpoint.com`
- **Secondary NTP server** - 辅助NTP服务器的IP或主机名称。默认服务器为`ntp2.checkpoint.com`



设备名称

在**Appliance Name**页面，输入一个名称以识别设备，然后输入域名(可选)。

当网关针对指定对象名称执行DNS解析时，会将域名附加到对象名称中。如此一来，网络中的主机便可以根据主机的内部名称查找主机。

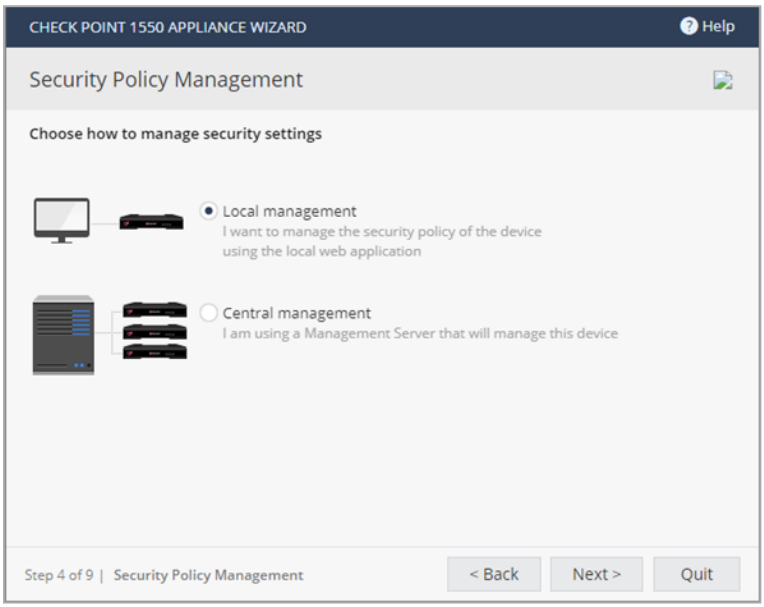


安全策略管理

在**Security Policy Management**页面，选择如何管理安全设置：

- **Central management** - 远程安全管理服务器使用网络对象和安全策略，管理SmartDashboard中的安全网关。
- **Local management** - 设备使用Web应用程序管理安全策略。在您使用首次配置向导配置设备之后，系统将自动执行默认安全策略。利用WebUI，您可以配置您激活的软件刀片，并微调您的安全策略。

本入门指南介绍了如何配置本地和集中托管的部署。



互联网连接

在**Internet Connection**页面，配置您的互联网连接详情，或者选择**Configure Internet connection later**。

如要立即配置互联网连接：

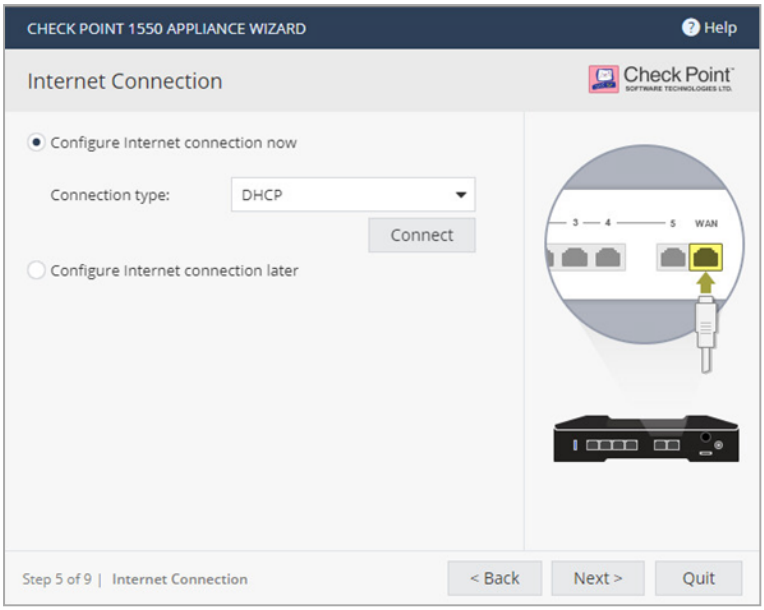
1. 请选择**Configure Internet connection now**。
2. 从**Connection type**下拉列表，选择用于连接至互联网的协议。
3. 输入所选连接协议的字段。对于各项协议，您必须输入不同的信息。您可以从互联网服务提供商(ISP)处获取此类信息。
    - **Static IP** - 固定(非动态) IP地址。
    - **DHCP** - 动态主机配置协议(DHCP)会自动将指定范围内的IP地址发布给网络上的设备。通过电缆调制解调器连接时，这是一个常用选项。
    - **PPPoE** - 一种将点对点协议(PPP)帧封装在以太网帧中的网络协议，主要用于DSL服务，供个人用户通过以太网和城域以太网网络连接至DSL调制解调器。输入**ISP login user name**和**ISP login password**。**注** - 首次配置向导中仅支持动态IP。
    - **PPTP** - 点对点隧道协议(PPTP)是实现虚拟专用网络的一种方式。PPTP使用TCP上的控制信道和GRE隧道操作来封装PPP数据包。
    - **L2TP** - 第二层隧道协议(L2TP)是一种用于支持虚拟专用网络(VPN)的隧道协议，不提供任何加密或保密性，依靠其在隧道内传递的加密协议来提供保密性。
    - **Analog Modem** - 通过USB端口，使用模拟调制解调器连接至互联网。在WebUI应用程序中，您可以进行配置，以通过串行端口使用模拟调制解调器。
    - **Bridge** - 在数据链路层(第二层)连接多个网段。
    - **DNS Server**(静态IP和网桥连接) - 在相关字段输入DNS服务器地址信息。对于DHCP、PPPoE、PPTP、L2TP，DNS设置由您的服务提供商提供。您可以稍后在WebUI应用程序中覆盖这些设置，位于**Device** > **DNS**下方。

我们建议您配置DNS，因为设备需要对不同的功能执行DNS解析。例如，在许可证激活期间或者在启用应用程序控制、网络筛选、防病毒或反垃圾邮件服务时连接至Check Point用户中心。

如要测试您的ISP连接状态：

单击**连接**。

设备将连接至您的ISP。页面底部会显示成功或失败。

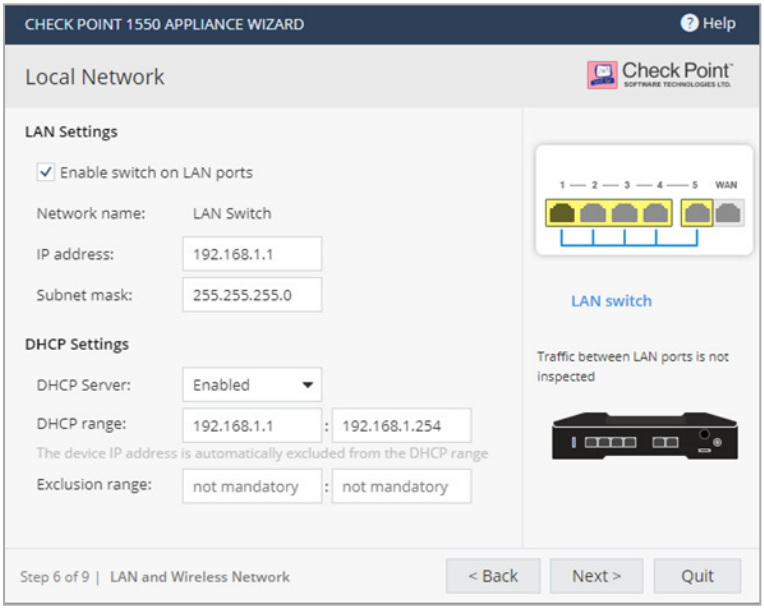

CHECK POINT 1550 APPLIANCE WIZARD
Help
Internet Connection
Check Point
Configure Internet connection now
Connection type:
DHCP
Connect
Configure Internet connection later
3
4
5
WAN
Step 5 of 9 | Internet Connection
< Back
Next >
Quit

本地网络

在**Local Network**页面，选择启用或禁用LAN端口上的交换机，并配置您的网络设置。默认情况下，为启用状态。您可以更改IP地址并保持连接，因为设备的原始IP将作为别名IP保存，直到您首次启动设备。

我想了解更多关于这些字段的信息...

- **Enable switch on LAN ports** - 聚合交换机的所有LAN端口，充当一个具备一个IP地址的交换机。如果禁用此选项(清除复选框)，则本地网络仅可定义为LAN1。
- **Network name** - 输入网络名称。
- **IP address** - 您可以修改IP地址并保持连接。设备的原始IP将作为别名IP保存以保持连接，直到您完成向导。
- **Subnet mask** - 输入子网掩码。
- **DHCP server and range fields** - 默认启用具有默认网络范围的DHCP。确保设置适合的范围，不要在网络中加入预定义静态IP。
- **Exclusion range** - 针对DHCP服务器未定义的IP地址设置排除范围。已在网络中分配IP地址时，定义DHCP排除的IP地址的范围。设备的IP地址将自动从该范围中排除。例如，如果设备IP是1.1.1.1，则范围也从1.1.1.1开始，但会排除自身的IP地址。



重要信息 - 如果您选择禁用LAN端口上的交换机(清除复选框)，请确保已在LAN1端口中插入网络电缆。否则，当您单击**Next**时，连接会断开。

无线网络

仅限WiFi型号：

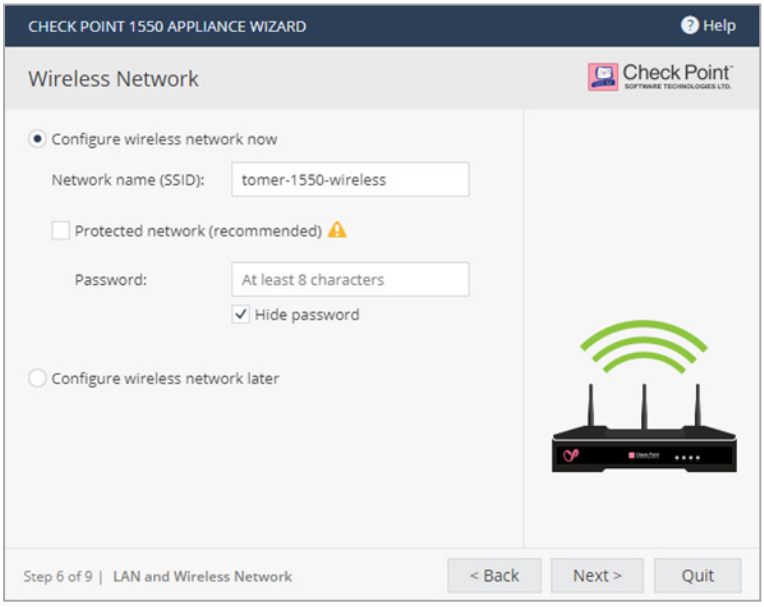
在Wireless Network(无线网络) 页面，配置无线连接详情。

配置无线网络时，须定义网络名称(SSID)。SSID(服务集标识符) 是一个唯一字符串，用于向尝试利用它打开无线连接的客户端标识WLAN网络。

我们建议您使用密码保护无线网络。否则，无线客户端无需身份验证即可连接到网络。

如要立即配置无线网络：

1. 选择**Configure wireless network now**。
2. 在**Network name (SSID)**字段输入名称。此名称便是向在传输区域寻找接入点的客户端显示的名称。
3. 如果无线网络使用密码保护，请选择**Protected network (recommended)**。
4. 输入**Password**。
5. 默认选择**Hide**密码选项。
6. 默认选择**Allow access from this network to the local network**。这意味着，无线网络将被视为可信网络，并且允许从该网络访问本地网络。
7. 无线电波段
   - 2.4GHz：2414-2462 MHz
   - 5GHz：5180-5240、5260-5320、5500-5720、5745- 5825MHz



管理员访问

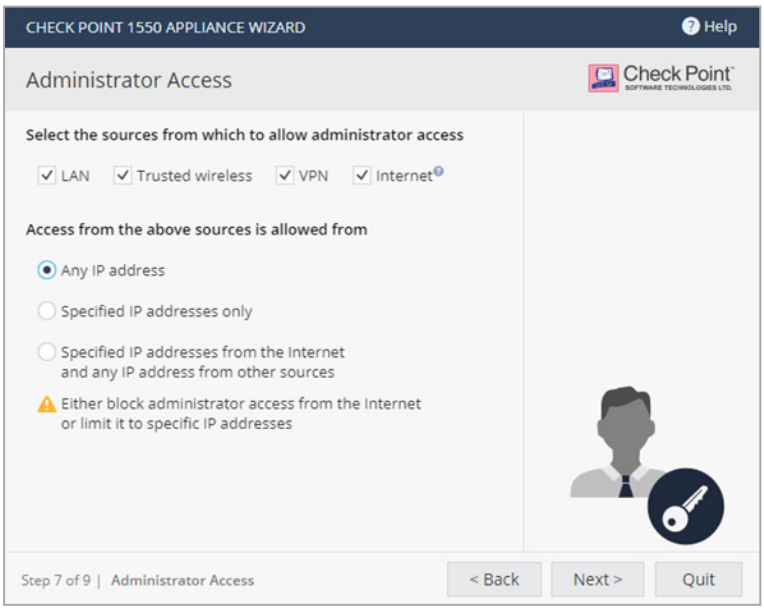
在**Administrator Access**页面，配置管理员是否可以使用来自特定IP地址或任意IP地址的设备。

如需配置管理员访问：

1. 选择允许管理员从其中访问的来源：
   - **LAN** - 所有内部物理端口。
   - **Trusted wireless** - 已知无线网络。
   - **VPN** - 通过VPN隧道从远程站点使用加密流量，或者使用远程访问客户端。
   - **Internet** - 清除来自互联网的流量(不推荐)。
2. 选择管理员可以从其中访问设备的IP地址:
   - **Any IP address**。
   - **Specified IP addresses only** - 选择此选项以允许管理员从指定IP地址或网络访问设备。单击**New**以配置IP地址信息。
   - **Specified IP addresses from the Internet and any IP address from other sources** - 选择此选项以允许管理员仅从互联网的特定IP地址进行访问，以及从其他选定来源的任何IP地址进行访问。此选项为默认设置。

要指定IP地址：

1. 单击**New**。
2. 在IP Address Configuration(IP地址配置)窗口，选择一个选项：
   - **Specific IP address** - 输入**IP address**或单击**Get IP from my computer**。
   - **Specific network** - 输入**Network IP**地址和**Subnet mask**。
3. 单击**Apply**。



设备注册

设备可通过其凭证连接到Check Point用户中心，提取许可证信息并激活设备。

如果您已配置互联网连接：

单击**Activate License**。

系统会通知您已成功激活设备，并向您显示每个刀片的许可证状态。

如果您在配置设备时离线操作：

1. 在具有Check Point用户中心的授权访问权限的计算机上，执行程序a或b：
   a. **使用您的用户中心帐户：**
      - 登录您的用户中心帐户。
      - 选择您的设备的指定容器。
      - 从**Product Information**选项卡，单击**License** > **Activate**。
        显示如下消息："Licenses were generated successfully(已成功生成许可证) "。
      - 单击**Get Activation File**，并将文件保存在本地。

   b. **注册您的设备：**
      - 请前往：https://smbregistration.checkpoint.com
      - 输入您的设备详情，并单击**Activate**。
        显示如下消息："Licenses were generated successfully(已成功生成许可证) "。
      - 单击**Get Activation File**，并将文件保存在本地。
2. 在First Time Configuration Wizard(首次配置向导) 的Appliance Activation(设备激活) 页面，单击**Offline**。
   Import from File(从文件导入) 窗口将打开
3. 浏览您下载的激活文件，并单击Import(导入) 。激活过程将开始。
   系统会通知您已成功激活设备，并向您显示每个刀片的许可证状态。

如果设备和互联网之间设有代理，则您必须先配置代理详情，然后才能激活许可证。

如需配置代理详情：

1. 单击**Set proxy**。
2. 选择**Use proxy server**，然后输入代理服务器**Address**和**Port**。
3. 单击**Apply**。
4. 单击**Activate License**。

系统会通知您已成功激活设备，并向您显示每个刀片的许可证状态。

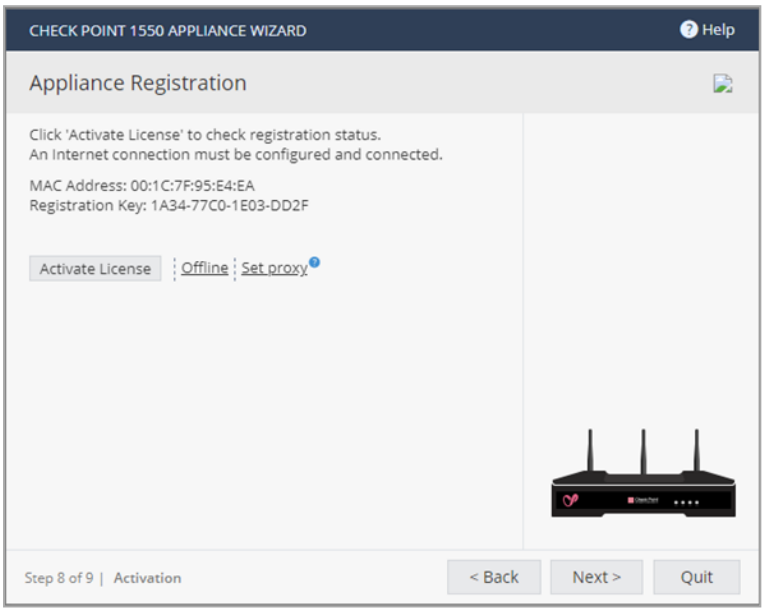
如要推迟设备注册并获得30天试用许可证：

1. 单击**Next**。

   将显示License activation was not complete(许可证激活未完成) 通知消息。

2. 单击**确定**。

   设备可以使用适用于所有刀片的30天试用许可证。您可以稍后从WebUI Device(WebUI设备) > **License**页面注册设备。



如果您的设备未与用户中心帐户配对，则您必须创建一个帐户，或者请求您的公司管理员为您创建一个帐户。

如需新建一个用户中心帐户 (仅限本地托管) ：

1. 单击**Activate License**。

   Appliance Registration(设备注册) 窗口将打开。

2. 选择**Create a new User Center account**，并单击**Next**。
3. 在新窗口中，输入：
   - **First name**
   - **Last Name**
   - **Email**。您必须再次输入此信息以确认。
   - **Company** - 这是与设备配对的帐户名称。
4. 单击**Next**。

Software Blades Activation(软件刀片激活) 页面将打开。

安全管理服务器身份验证

仅限集中托管设备：

当您选择集中管理作为安全策略管理方法时，将打开**Security Management Server Authentication**页面。

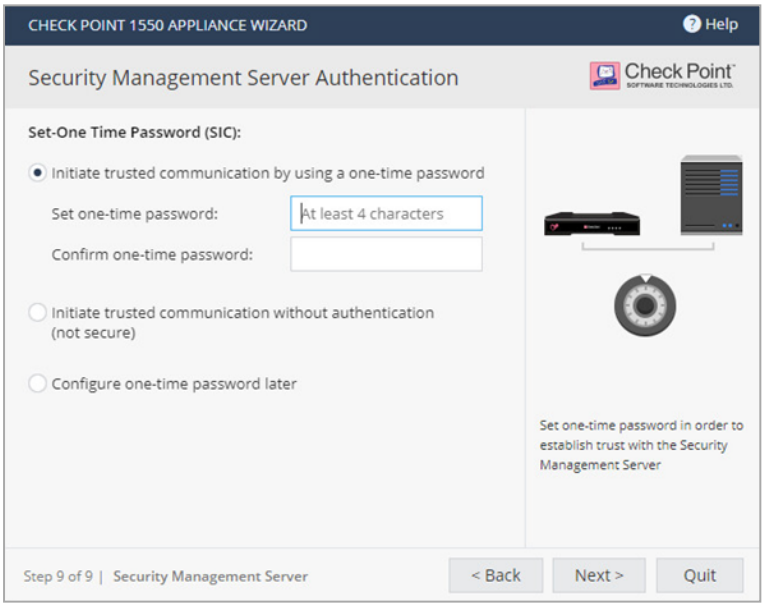
选择一个选项，以验证与安全管理服务器的可信通信：

- **Initiate trusted communication securely by using a one-time password** - 一次性密码用于安全地验证设备和安全管理服务器之间的通信。

  输入**one-time password**并确认。此密码仅用于建立初始信任。建立后，信任将基于安全证书。

  重要信息 - 此密码必须与为安全管理服务器SmartConsole中的设备对象配置的安全通信身份验证一次性密码相同。

- **Initiate trusted communication without authentication (not secure)** - 仅在没有恶意行为风险的情况下使用此选项(例如在实验室环境中) 。
- **Configure one-time password later** - 在其他时间使用WebUI应用程序设置一次性密码。



安全管理服务器连接

仅限集中托管设备：

在您为安全管理服务器和设备设置一次性密码之后，您可以连接至安全管理服务器，在安全管理服务器和设备之间建立信任。

如要连接至安全管理服务器，请选择以下其中一个选项：

- **Connect to the Security Management Server now**。
- **Connect to the Security Management Server later**。

如果您选择立即连接，请在以下字段输入数据：

- **Management address** - 输入安全管理服务器的IP地址或主机名称。
- **Connect** - 成功连接到安全管理服务器后，将自动提取并安装安全策略。
- 如果在第三方设备之后部署安全管理服务器，请选择**Always use the above address to connect to the Security Management Server**。手动输入设备的IP地址或主机名称，以连接至安全管理服务器。

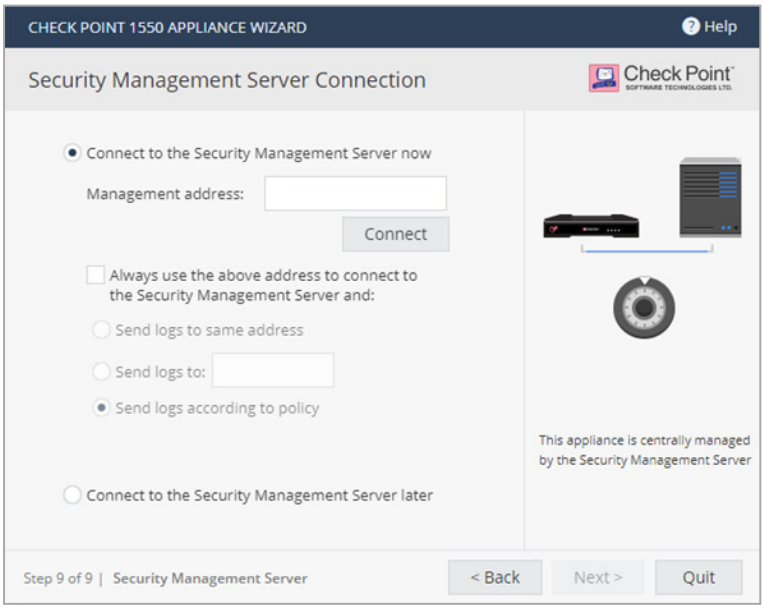
  如果您输入IP地址，则该IP地址将覆盖为每台设备确定可路由的安全管理服务器IP地址的自动机制。

  如果您输入主机名称，则该主机名称将保存，安全网关将重新解析IP地址更改的名称。此配置可稍后在WebUI的**Home** > **Security Management**页面编辑。

  如果您未选择此复选框，并且使用主机名称来提取策略，则在提取策略后，安全管理服务器IP将设置为策略中的IP地址。

  选择将日志发送到哪一位置：

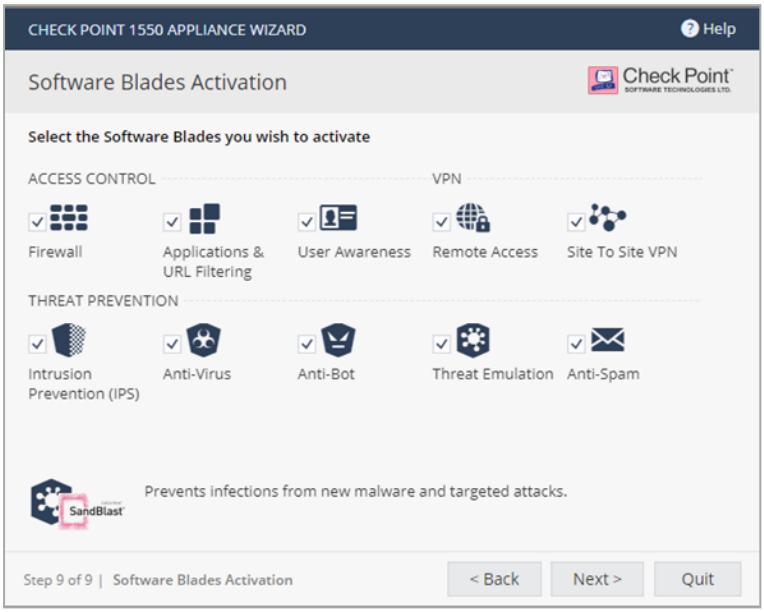
  - **Send logs to same address** - 将日志发送到本页面上输入的安全管理服务器的IP地址。
  - **Send logs to** - 输入日志服务器的IP地址。
  - **Send logs according to policy** - 根据策略中指定的日志服务器定义发送日志。



软件刀片激活

选择要在此设备上激活的软件刀片。

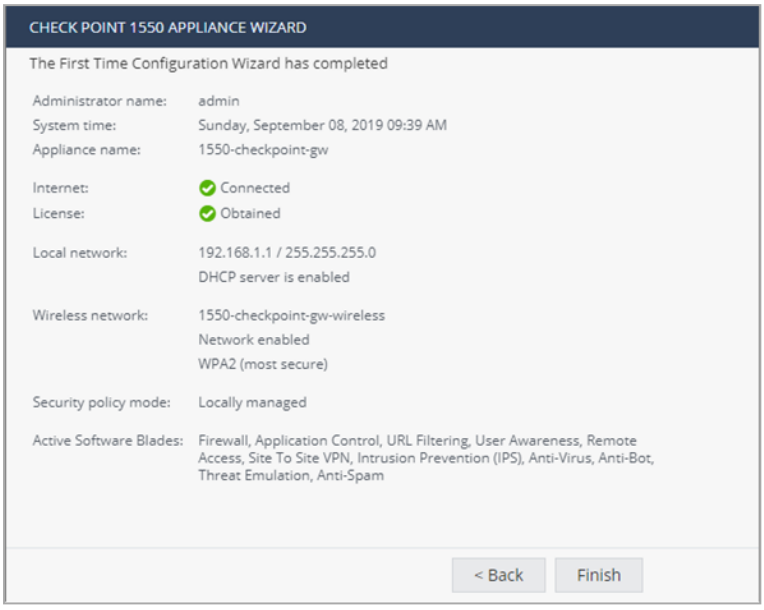
仅可在完成首次配置向导后，从WebUI激活QoS(带宽控制) 。



摘要

Summary页面显示使用首次配置向导配置的元素的详情。

单击**Finish**，完成首次配置向导。



WebUI将在**Home** > **System**页面上打开。

如要在WebUI中备份系统配置：

前往**Device** > **System Operations** > **Backup**。

Zero Touch云服务

借助Zero Touch云服务，您可以轻松管理Zero Touch portal(Zero Touch门户)中网关的初始部署。

借助Zero Touch，网关可以在首次连接至互联网后，自动从云端提取设置。

注 - 如果您已使用首次配置向导配置您的设备，则无法使用Zero Touch云服务。如果您在安装Zero Touch设置期间，开始首次配置向导，则安装过程将终止。

如果网关通过DHCP连接到互联网，则无需额外操作即可提取Zero Touch设置。如果没有可用的DHCP服务，则您必须运行首次配置向导，配置Internet Connection(互联网连接) 设置，然后从Zero Touch服务器提取设置。

如要从首次配置向导连接至Zero Touch服务器：

1. 在首次配置向导的**Welcome**页面，单击**Fetch Settings from the cloud**。
2. 在打开的窗口中，单击**Yes**，以确认您想要继续。
3. 首次配置向导的**Internet connection**页面将打开。配置您的互联网连接，并单击**Connect**。

   设置会自动下载并安装。

   新的窗口将打开并显示安装状态。安装完成可能需要几分钟的时间。

在您重新连接至WebUI，或者单击**Refresh**时，您可能看到以下项目之一：

- **Login**页面 - 这表示，过程已成功终止，且您的设置已安装。
- 首次配置向导的**Welcome**页面 - 过程仍在运行。设置正在安装，或者未存在于云端。

  注 - 如果您单击**Welcome**页面上的**Next**，Zero Touch设置安装过程将终止
- **Page not found** - 设备本地IP地址可能已被云设置安装所更改。尝试访问 `http://my.firewall`，或者咨询您的管理员，获取新的本地IP地址。

网关下载并成功应用设置后，将不会再次连接到Zero Touch服务器。

有关如何使用Zero Touch的更多信息，请查看sk116375和R80.20 Zero Touch Web门户管理指南。

重试机制：

在云激活期间，有时会出现一些临时问题，阻止网关激活云服务。请参见*"前面板"在本页13*部分中关于管理LED的说明。

U盘

U盘让您无需使用首次配置向导，即可快速部署配置文件，或安装映像。相较于使用首次配置向导，使用配置文件可以配置更多的设置和参数

在以下情况下，您可以部署配置文件：

- 设备具有默认设置，但尚未经过配置。
- 设备已有现有配置。

Check Point设备将启动，并自动装载U盘，并在根目录中搜索配置文件。

注 - U盘必须为FAT32格式。

健康与安全信息

请在设置或使用设备前阅读以下警告。

警告-不要阻塞通风口。要求保留至少1/2英寸的空隙。

警告 - 此设备不包含任何用户可维修的零件。请勿拆除任何盖子或试图访问产品内部。以任何方式打开或修改设备都有人身伤害的风险，并且会导致您的保修无效。以下说明仅适用于经过培训的维修人员。

电源信息

为减少DC电源潜在安全问题，请仅使用以下配件：

- 设备随附的AC适配器。
- Check Point提供的替换AC适配器。
- 从Check Point购买的AC适配器配件。

为了防止任何系统受到损坏，请务必小心拿取所有零件。以下措施通常足以保护您的设备免受静电放电的影响：

- 不使用通信设备系统板和外围设备，或未将其安装于机架中时，请将其存放于防静电袋中。即使在关闭电源后，系统板上的某些电路仍可以持续运作。
- 切勿让为实时时钟供电的锂电池短路。短路会造成电池发热，并产生灼伤的危险。

  警告-电池更换不当会产生爆炸危险。只能使用制造商推荐的相同或等效类型的电池进行更换。根据制造商说明丢弃使用过的电池。

- 请勿将电池置入火中，或者与家庭垃圾一同处置。
- 请联系您当地的废物处理机构，查询距您最近的电池回收点。
- 连接电缆或断开电缆连接，或是安装或移除任何系统板组件前，请先断开系统板电源连接。未执行此操作会造成人员伤害或设备损坏。
- 避免锂电池短路；这会导致其过热并在触摸时造成灼伤。
- 切勿在没有散热解决方案的情况下运行处理器。这可能会在数秒钟内造成处理器损坏。

重要安全须知：在使用电话设备时，请务必采取基本的安全防护措施，以降低火灾、触电或人员受伤风险，这些措施包括：

- 请勿在近水位置使用本产品，比如浴缸、洗脸盆、厨房水槽或洗衣盆附近，潮湿的地下室或游泳池附近。
- 避免在雷暴天气使用电话(无绳电话除外)。否则雷电可能造成远距离触电风险。
- 当附近发生燃气泄漏时，切勿使用电话报警。
- 仅可使用本手册中指定的电源线和电池。请勿将电池置入火中。否则，电池可能会爆炸。请查阅当地法规，了解可能的特殊处置说明。
- 本设备不适合在有儿童出没的地方使用。
- 务必将电源线连接到接地的插座上。
- 切勿打开设备。出于安全原因，设备应仅可由Check Point授权的合格技术人员打开。

注意：为了降低火灾风险，仅可使用经UL列名或CSA认证的26号AWG或更大号(如24号AWG)通信电线。

加利福尼亚州：

高氯酸盐材料-可申请特殊处理。请参见http://www.dtsc.ca.gov/hazardouswaste/perchlorate

上述注意事项根据《加利福尼亚州规章和行政规则》第33章第4.5节第22条提供。高氯酸盐材料的最佳管理实践。本产品、零件或两者可能包括含有高氯酸盐物质的锂二氧化锰电池电池。

65号提案化学品

加州根据1986年《加州饮用水安全与毒性物质强制执行法》、《加州安全与健康法规》第25249.5节等(“第65号提案”)确定的化学品，其为“加州已知的会导致癌症或生殖毒性”的化学品。请参见http://www.calepa.ca.gov。

警告：

拿取此产品的电源线将接触到铅，这是一种加州已知的会导致癌症以及先天缺陷或其他生殖危害的化学品。拿取后请洗手。

符合性声明

制造商名称：	Check Point Software Technologies Ltd.
制造商地址：	5 Shlomo Kaplan Street, Tel Aviv 67897, Israel
型号：	V-80、*V-80W
产品选项：	1530/1550设备(有线)，1530 / 1550 WiFi
首次申请日期：	2019年8月

我方全权负责以下声明，即产品：符合以下产品规格：

RF/Wi-Fi(标有*的型号)

新认证	Type
CE EN 55032:2015 + AC:2016，B类 CE EN 55032:2012 + AC:2013，B类 CE EN 55024:2010 / A1:2015 CE EN 55024:2010 FCC第15B部分 ICES-003 AS/NZS CISPR32 VCCI，V-3/2015.4，V4/2012.04，B类VCCI CISPR 32:2016 ISO标准8802-3第14部分(10BASE-T) ISO标准8802-3第25部分(100BASE-TX) ISO标准8802-3第40部分(1000BASE-T)第9条 * EN300 328 * EN301 893 * ETSI EN301 489-1 * ETSI EN301 489-1-17 * EN62311:2008 * EN50386:2002、EN50383:2010 * AS/NZS 4268:2017 * FCC第15C+E部分 * RSS-247 * RSS-102 * JP ARIB STD-T66 * JP ARIB STD-T71	EMC，*RF/Wi-Fi
IEC/EN 62368-1 UL 62368-1	安全

物理和环保可靠性	说明
运行条件	振动和冲击符合EN 300 019-2-3
存储条件	温度：(-40)°C ~ 60°C，湿度：95%，非冷凝，振动和冲击符合EN 300 019-2-1
运输条件	温度：(-40)°C ~ 85°C，湿度：95%，非冷凝，振动和冲击符合EN 300 019-2-2

发布日期和地点：2019年8月，以色列特拉维夫

测试实验室

Address: No 9 Harrison Road, Harrison Industrial Building, #05-01

Issued By: Bureau Veritas Consumer Products Services (H.K.) Ltd., Taoyuan Branch Lin Kou Laboratories

Lab Address: No. 47-2, 14th Ling, Chia Pau Vil., Lin Kou Dist., New Taipei City, Taiwan

联邦通信委员会(FCC)声明：

FCC SDOC

符合FCC第15部分

我方，Check Point Software Technologies Ltd.

地址：Shlomo Kaplan St 5, / HaSolelim St 5 Tel Aviv-Yafo # 67897，电话：+972-3-753-4555。

本装置符合FCC规则第15部分的规定。运行应满足下列两个条件：(1)本设备不会造成有害干扰，且(2)本设备必须接受收到的任何干扰，包括可能导致意外运行的干扰。

根据FCC规则第15部分，本设备已经过测试，符合针对B类数字装置的限值。这些限制旨在提供合理保护，避免民用安装中的有害干扰。本设备产生、使用并且可以辐射射频能量，若未根据说明进行安装和使用，可能会对无线电通信造成有害干扰。但是，无法保证特定设施不会受到干扰。如果本设备确实对无线电或电视接收造成了有害干扰，可通过关闭并打开设备进行确定，我们鼓励用户尝试通过下列措施之一纠正干扰情况：

- 重新定向或定位接收天线。
- 增加设备和接收器间的距离。
- 将设备连接至电路插座，该插座不同于接收器所连接的插座。
- 咨询经销商或经验丰富的无线电/TV技术人员以获得帮助。

FCC警告：

- 任何未经合规责任方明确批准的变更或修改可能会导致用户运行本设备的权限无效。
- 本发射机不得与任何其他天线或发射机共同安装或共同运行。
- 5.15-5.25GHz频段的运行仅限室内使用。

辐射暴露声明

本设备符合针对非受控环境规定的FCC射频辐射暴露限制。在安装和操作本设备时，您的身体应与散热器保持至少20厘米的距离。

国家/地区代码选择使用(WLAN设备)

注：国家/地区代码选择仅适用于非美国型号，不适用所有美国型号。根据FCC法规，所有在美国销售的WiFi产品必须固定在美国运行信道。

如果此网关发生故障，有关维修或保修信息，请联系：

Check Point

6330 Commerce Drive Suite 120, Irving, Texas 75063

办公室电话号码：972-444-6612

加拿大工业部合规声明

此无线电广播发射机(根据认证编号确定设备)经加拿大工业部批准，可使用下列标示有最大允许增益的天线类型进行操作。本列表中未包含的天线类型，如果其增益大于该类型的标示最大增益，则严禁与本设备一起使用。

辐射暴露声明：

本设备符合针对非受控环境规定的IC辐射暴露限制。在安装和操作本设备时，您的身体应与散热器应保持至少20厘米的距离。

本设备符合加拿大工业部的许可豁免RSS标准。运行应满足下列两个条件：

1. 本设备不会造成干扰，且
2. 本装置必须接收任何干扰，包括可能导致设备意外运行的干扰。

B类数字装置符合加拿大ICES-003。

除经过测试的内置无线电设备外，本设备及其天线不得与任何其他天线或发射机共同安装或运行。

对于在美国/加拿大销售的产品，已禁用县代码选择功能。

对于WLAN 5 GHz设备：

注意：

1. 在5150-5250 MHz频段运行的设备仅限于室内使用，以减少可能对同信道移动卫星系统造成的有害干扰；
2. 设备在5725-5850 MHz频段所允许的最大天线增益应符合e.i.r.p.关于点对点和非点对点操作的限制规定(如适用)。
3. 应清楚标明要确保符合第6.2.2(3)所述e.i.r.p.截止高度角要求所需的最低倾斜角。(仅适用于配备DFS设备的5G B2)
4. 如适用，应清楚标明要确保符合第6.2.2.3所述e.i.r.p.截止高度角要求所需的天线类型、天线型号和最低倾斜角。
5. 此外，还应告知用户，大功率雷达已被分配为5250-5350 MHz和5650-5850 MHz频段的主要用户(即优先用户)，这些雷达可能会对LE-LAN设备造成干扰和/或损坏。

注意：此终端设备的振铃等效值(REN)是01。分配给每个终端设备的REN指示允许连接到电话接口的终端最大数量。接口上的终端可由任何设备组合组成，但前提是所有设备的振铃等效值之和不得超过5。

日本A类合规性声明：

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

欧盟(EU)电磁兼容指令

兹确认本产品符合关于使各成员国有关电磁兼容性指令的法律趋于一致的理事会指令中规定的要求(2014/30/EU)。本产品经确认符合RED 2014/53/EU要求。

本产品符合低电压指令2014/35/EU，并且符合理事会指令2014/35/EU中有关专为在特定电压限值范围内使用的电气设备的要求，以及修订指令93/68/EEC。

产品处理

产品或其包装上的标志表示，此产品不得与其他生活垃圾一同处理。相反，您有责任将废旧设备交于指定收集点进行处理，以回收利用废旧电气或电子设备。处理时将废旧设备分开收集和回收利用将有利于保护自然资源，并确保其以一种保护人类健康和环境的方式进行回收利用。如需有关丢弃废旧设备以进行回收利用的更多信息，请联系当地的市政办公室或生活垃圾处理服务处。

支持

如需技术援助，请联系Check Point全天候热线：

- +1 972-444-6600(美洲)
- +972 3-611-5100(国际)

联系支持时，请务必提供您的MAC地址。

如需更多技术信息，请访问：http://supportcenter.checkpoint.com

如需进一步了解Check Point互联网安全产品套件和其他安全解决方案，请访问：https://www.checkpoint.com