Check Point
SOFTWARE TECHNOLOGIES LTD.

2018 年 1 月 2 日

R80.10

版本说明

Check Point
SOFTWARE TECHNOLOGIES LTD
INFINITY

重要信息

最新软件

我们建议您安装最新软件版本，以获得最新的功能改善、更好的稳定性、更高的安全级别，并防止不断变化的新攻击入侵。

Check Point R80.10

有关此版本的更多信息，请参见 R80.10 主页
http://supportcontent.checkpoint.com/solutions?id=sk111841

本文档的最新版本

下载本文档的最新版本
http://supportcontent.checkpoint.com/documentation_download?ID=54802

反馈

Check Point 致力于不断改进自己的文档。

请发送您的意见给我们，以帮助我们不断改进
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on R80.10 版本说明。

在多个 PDF 中搜索

要在所有 R80.10 PDF 文档中搜索文本，请下载并解压完整的 R80.10 文档包
http://downloads.checkpoint.com/dc/download.htm?ID=54846。
在 Adobe Reader 或 Foxit reader 中按 **Shift-Control-F** 键。

修订历史

日期	说明
2017 年 7 月 2 日	完成简体中文翻译
2017 年 10 月 19 日	更新了行为变化 (页码 8)部分
2017 年 9 月 27 日	更新了 Check Point 设备 (页码 11)部分
2017 年 7 月 19 日	在向后兼容网关 (页码 13)中添加了针对 UTM-1 Edge N 的支持
2017 年 7 月 2 日	在支持平台 (页码 13)中添加了 Hyper-V 支持。 在 Check Point 设备 (页码 11)中添加了 Smart-1 405 和 410 支持。
2017 年 6 月 1 日	在开放式服务器硬件要求 (页码 12)中更新了安全管理服务器/独立部署的要求。
2017 年 5 月 16 日	本文档第一次发布

Contents

重要信息 3
引言 5
重要链接 5
全新功能 5
安全策略新架构 5
重大改进和新增功能 6
管理增强功能 7
行为变化 8
许可 9
支持的升级路径 9
需要的磁盘空间 10
Check Point 设备 11
硬件状态监控 12
开放式服务器硬件要求 12
支持平台 13
平台支持的最大接口数量 13
向后兼容网关 13
日志记录要求 14
日志容量 14
安全事件控制台 要求 14
管理控制台 15
控制台硬件要求 15
Windows 平台控制台 15
Gaia Web 配置界面 15
版本号 16
威胁仿真 16
移动访问 要求 16
身份识别 要求 17
Endpoint Security 要求 18
最大网关群集成员数量 18
Check Point 客户端支持 18
多用户登录选项支持 18
各 Windows 平台客户端 19
各 Mac 平台客户端 20
DLP Exchange 代理 20

引言

感谢您安装面向未来的网络安全平台 Check Point R80.10。该版本集成了 R80 管理功能，可提供全新的安全网关功能以及增强功能。

重要链接

如需详细了解 R80.10 并下载该软件，请参见 R80.10 主页：sk111841
http://supportcontent.checkpoint.com/solutions?id=sk111841

- 在升级之前，请先了解主页上的最新升级工具。
- 了解已知限制：sk110519 http://supportcontent.checkpoint.com/solutions?id=sk110519
- 查看该版本中解决的问题：sk110518
  http://supportcontent.checkpoint.com/solutions?id=sk110518

访问 Check Point Checkmates 社区 https://community.checkpoint.com/

- 开始讨论
- 获取专家答案
- 加入 API 社区，获取代码示例并分享您自己的代码

访问 http://www.checkpoint.com/architecture/infinity/以详细了解 Infinity R80.10。

全新功能

R80.10 在 Check Point 安全网关 方面实现了突破，这与 R80 安全管理创新技术相得益彰。

R80.10 是 **Check Point Infinity** 的一部分，而后者是一个跨网络、云端和移动环境的整合性网络安全架构。该架构可针对已知和未知目标性攻击提供最高级别的威胁防护，为您的现在和将来提供安全保护。|

安全策略新架构

- **策略层和子策略 -** 实现对安全策略行为的灵活控制。
  - 构建具有多层的规则库，每层都有一组安全规则。按照定义的顺序对各层进行检测，以对规则库流和安全功能的优先级别进行控制。如果在某层中完成“接受”动作，则在下一层中继续进行检测。
  - 子策略（内联层）是指附加到特定规则的规则集。如果相应规则匹配，则在该规则随附的子策略中继续进行检测。 如果相应规则不匹配，则跳过子策略。
    例如，一个子策略可以管理一个网段或分支机构。
  - 根据特定管理员的权限配置情况，其可管理不同策略层和子策略，轻松在团队内实现责任划分。
- **统一安全策略：**
  - 访问控制策略可统一防火墙、应用程序控制与 URL 过滤、数据识别 和移动访问软件刀片策略。
  - 威胁防护策略可统一 IPS、防病毒、防僵尸网络、威胁提取和威胁仿真软件刀片策略。

访问控制策略

- 全新的 数据识别 软件刀片借助基于内容、文件类型和传输方向的数据类型检测，增加了对网络流量中数据传输的可见性和控制。
- 应用程序控制增强功能：
  - 为应用程序新增推荐的服务，可更加方便对统一策略进行配置。
  - 应用程序可与推荐的服务、定制的服务集或任何服务匹配。
  - 为服务对象增加全新的协议签名，以增强策略匹配安全和精细度。
- 可以在主要的统一访问控制策略中定义移动访问策略规则：
  - 统一的规则可定义从不同客户端类型到同一资源的访问。
  - 明确的规则可以阻止指定的移动访问流量。
  - 可以定义仅从指定客户端类型访问资源。
- 安全区域：针对新来源和目标定义将网关接口分组到安全区域。
- 完全限定域名 (FQDN)：域对象的附加模式，将完全限定域名与正向 DNS 查找相匹配。
- 对域对象、动态对象和时间对象进行加速。
- 统一规则库中的新追踪选项。
- 缩短了策略安装所需的时间。

威胁防护策略

- 为每个安全网关提供多个配置文件，以执行精确的威胁防护策略。
- 加快威胁防护策略的安装速度。
- 将 IPS 集成到威胁防护策略规则库和策略安装中。
- 威胁防护配置文件支持基于属性标签来激活 IPS 防护。

重大改进和新增功能

- 全新 **Check Point Labs** 可让您体验新增功能并向 Check Point 发送反馈。首个 Check Point Labs 功能可让您在发布前查看会话更改信息。
- **VPN 和移动访问增强功能**
  - VPN 多核性能扩展功能，针对由下一代防火墙、下一代威胁防护和下一代威胁提取软件刀片检测的 VPN 流量提供 CoreXL 多核可扩展性。
  - 针对站点到站点 VPN 的 NAT-T 支持。
  - 针对移动访问和门户的 TLS 1.2 支持。
  - 为不同客户端和门户的用户提供多因素身份验证方案的多用户登录选项。请参见多用户登录选项支持 (页码 18)。
  - 移动访问透明反向代理允许外部用户在不经过移动访问门户的情况下访问内部资源。
- **身份识别增强功能**
  - 每个网关可最多支持 200,000 个身份会话。
  - 安全网关支持通过 REST API 对第三方或者用户系统进行身份管理。
  - 身份收集器 - 收集来自不同来源（AD 和 ISE）身份信息的新代理，以实现大环境可扩展性。
  - 新增 RADIUS 记帐属性解析功能和 IPv6 支持。
  - 使用 LDAPv3 增强了对 AD LDAP 嵌套用户组的处理能力。

  - 在访问角色中强制使用远程访问客户端类型。
  - 在每个访问控制策略层使用 X-Forward-For 标头精细级别检测位于 HTTP 代理后的用户。
- **威胁防护增强功能**
  - 在 VSX 中支持威胁仿真 MTA（邮件传输代理）。您可以为每个 VS 实例运行 MTA。
  - 支持针对 VSX 网关的威胁提取功能。
  - 可从 安全控制台 导入 Snort 规则。
  - 支持通过 安全控制台 导入自定义指标 (IoC)。
- **NAT 增强功能**
  - 提高了在高端多核网关上隐藏 NAT 的可扩展性，通过将可用端口动态分配给内核，最大限度提高可用隐藏端口的利用率。请参见 sk103656 http://supportcontent.checkpoint.com/solutions?id=sk103656。
  - IP 池 NAT 性能增强 - 针对 IP 池 NAT 连接的 CoreXL 多核可扩展性。
- **Gaia 增强功能**
  - 针对 IPFIX 的 Netflow 支持（具有 NAT 和 IPv6 流记录）。
  - 支持 ClusterXL 的 IPv6 DHCP 中继（安全网关和 VSX 模式）。
- **动态路由增强功能**
  - 支持 VRRPv2 的 RIPng。
  - SNMP 路由增强功能。
  - BGP 4 字节 AS 和本地 AS。
- **VSX 增强功能**
  - 针对 VSX 网关的 64 位支持，增加了并发连接容量。
  - 针对 VSX 网关的内容识别功能。
- **ClusterXL 增强功能**
  - MAC Magic 值可自动获取，且可向后兼容早期版本中手动配置的网关。
  - 对于负载共享环境 (VSLS) 中的 VSX 群集，除活动成员和待机成员外，备用成员也可与外部网络通信并接收更新。
  - 连接更新现在支持动态路由的同步。

管理增强功能

这些增强功能是首次在 R80 中引入。

- **多域安全管理**
  - 用于进行安全管理和多域安全管理的统一架构与管理控制台。
  - 用于域管理和全局分配的改进新视图。
- **基于角色的并发管理** - 多个管理员可在同一安全策略上并行工作，并可为每个管理员提供精细且灵活的权限委派。
  - 新的高级锁定机制可确保管理员不会覆盖彼此的工作。
  - 针对每个管理员确切权限的强大管理员配置文件，这些权限包括管理特定策略或网络分段、查看特定日志以及执行安全操作（如安装策略）等。
- **安全自动化和协调** - 通过用于安全管理的 CLI 和 API，可实现与第三方系统的完全集成以及日常操作的自动化。可基于相同的权限配置文件执行自动化和 SmartConsole 管理操作。
- **更快的日常操作**

  - 集成式日志记录功能，可在同一屏幕上查看与某个规则相关的所有日志。
  - 详细的规则信息，包括规则的创建者、创建时间、命中率以及用户定义数据（如响应单号）。
  - 增强的搜索功能，可快速找到系统中的任何规则或对象。
  - 增强的管理高可用性仅同步服务器之间的变更，可显著提高效率。
- **下一代日志、事件和报告**
  - 每天通过针对特定要求而定制的图形化视图和报告，分析数以亿计的日志。
  - 日志记录、监控和报告等功能也可通过基于 Web 的界面提供。
  - 日志和事件的自由文本搜索，具有自动提示和收藏功能，可在几秒钟内提供结果。
- **新增和增强的修订管理功能**
  - 内置自动策略修订功能。
  - 安装特定版本的策略。
  - 更改至特定版本的 IPS 包。
- **云演示 -** 在任何计算机上体验 R80.10 管理方案。sk103431 http://supportcontent.checkpoint.com/solutions?id=sk103431
- **vSEC 控制器 -** 可与领先的私有云和公有云平台自然集成：VMware vCenter 和 NSX、CISCO ACI、Amazon Web Services (AWS)、Microsoft Azure 以及 OpenStack。
  vSEC 控制器提供动态安全策略和可见性，能够自动适应云环境中的改变。这样可通过单个统一管理解决方案，跨物理、虚拟和云环境轻松提供自动安全保护。

行为变化

- **管理**
  - 管理 API 命令和基于网页的 SmartView 界面代替了**管理门户**。您可以使用 API 命令安装策略以及显示网关及服务器列表。可以使用 SmartView 查看日志。
  - 新的对象标签取代了对象**颜色**的重命名。可以根据颜色命名标签。使用标签后，在 安全控制台 中管理对象将更加简单。
  - 全新及经过改进的管理功能取代了数据库修订功能。要了解 R80 及更高版本中的增强版本管理，请参见 sk113615 http://supportcontent.checkpoint.com/solutions?id=sk113615。
  - 多域服务器 上的 `mdsstop` 和 `mdsstart` 命令是实现**启动和停止域管理服务器**功能的唯一方式。大多数域管理服务器组件都是在一个流程中进行处理，这可以减少内存消耗和 CPU 使用率。
  - 改善了安装策略时的规则库验证流程。因此，升级之前可通过验证流程的安全策略有可能会在升级之后无法通过。如果您在升级之后收到验证错误消息，请手动修复规则。

    注：您可以使用 R80.10 升级验证和环境仿真服务 http://supportcontent.checkpoint.com/solutions?id=sk110267 进行升级仿真。该服务会告知您可能的策略验证失败。
- **日志、事件和报告**
  - 安全控制台 日志与监控视图的“日志”选项卡取代了 **高级日志查询控制台** 和 **实时日志控制台**。通过“日志”选项卡，您可以轻松快速地在所有日志内容中进行搜索。系统可快速得到搜索结果并迅速显示日志记录。
  - 安全事件控制台 取代了 报表控制台 和 SmartEvent Intro。
  - 将计划的报告整合到 SmartConsole 中，不再从旧版 SmartEvent GUI 提供。

- **威胁防护和 IPS**
  - 进行了 IPS 优化的全新配置文件具有出色的安全性和提升的网关性能，取代了推荐的配置文件。当使用推荐的配置文件进行升级时，我们建议您改用优化的配置文件。
  - 威胁防护权限配置文件的精确程度提高 - 可设置 IPS 更新权限。
  - 用户中心身份验证与管理服务器同步，无需明确登录到用户中心即可进行 IPS 和威胁防护更新。 这只适用于有权运行更新的用户。
  - 默认情况下，新的 IPS 保护标记为“阶段性”保护。您可以从**威胁防护配置文件 > IPS** 中对“阶段性”配置进行更改。您可以在**保护**视图中搜索和过滤“阶段性”保护，也可查看相应的日志。这取代了跟进标记。
- **软件刀片**
  - **会话身份验证**和 **UserAuthority** 由“身份识别”取代。
  - “概述”在 R77 版本中是“威胁防护”和“应用程序控制”选项卡的一部分，现在显示在**日志记录和监控**视图中。这需要 SmartEvent 激活和许可。
  - VPN 传统模式由 VPN 简化模式取代。

许可

有关许可的任何问题，请联系客户服务部 mailto:accountservices@checkpoint.com?subject=Licensing Issues。

支持的升级路径

您可以通过数据库迁移将安全管理服务器和多域服务器版本升级至 R80.10：
R75.40、R75.45、R75.46、R75.47、R75.40VS、R76、R77、R77.10、R77.20 和 R77.30。

对于有插件的 R77.20 或 R77.30：

- 无需卸载插件。
- 您必须删除下列不受支持的功能，否则将无法升级至 R80（数据库导出将失败）。
- R80 不支持这些功能：
  - 威胁净化软件刀片。
  - 导入自订指标到威胁防护策略。
  - 应用程序控制软件刀片 Modbus 支持。
  - 运营商解决方案（LTE 套件）支持，例如 NAT64、GTP、SCTP、CGNAT。
  - Web 单点登录"SAML"云连接器。

需要的磁盘空间

在安装或升级之前，系统与补丁升级 会确认是否有足够的可用磁盘空间。如果可用空间不足，系统会显示一条消息，指明需要的空间。

下表显示了一些软件包需要的磁盘空间。

<table>
<tr><th>安装或升级类型</th><th>管理服务器或独立部署</th><th>安全网关</th></tr>
<tr><td>R80.10 全新安装</td><td colspan="2" rowspan="2">需要的最低未分区磁盘空间是以下当中的最大值：
• 当前根分区的大小。
• 当前根分区中已用的空间加上 3 GB。
• 如果已用的空间超过根分区大小的 90%，则为当前根分区大小的 110%。</td></tr>
<tr><td>R80.10 重大升级（从 R80 之前版本升级）</td></tr>
<tr><td>R80.10 小幅升级（从 R80 升级）</td><td>根分区中 3.3GB，日志分区中 2.2GB</td><td>不相关</td></tr>
</table>

如果没有足够的磁盘空间，可以使用逻辑卷管理器 (LVM) 在 Gaia 上增加逻辑卷磁盘空间。这些空间取自未分配的磁盘空间，通常用于快照和升级目的。请参见 sk95566 http://supportcontent.checkpoint.com/solutions?id=sk95566。

多域安全管理 需要的磁盘空间：

在 多域服务器 上运行 R80.10 全新安装之前，请确保根分区中至少有 **10 GB** 的可用磁盘空间。对于具有许多 域管理服务器 的环境，通常需要超过 10 GB 的可用磁盘空间。

Check Point 设备

默认情况下，当进行全新安装或升级至 R80.10 时，独立部署设备和管理服务器会以 64 位启动。

注：如果您从 R80.10 升级中复原，相应设备仍将以 64 位启动，即使该设备原来是 32 位。

管理服务器

组件	Smart-1 25b、205、210、225、405、410	Smart-1 50、150、3050、3150
安全管理	✓	✓
日志服务器	✓	✓
SmartEvent 服务器	✓	✓
多域安全管理		✓
多域日志服务器		✓

* 具有默认内存的 Smart-1 25b、205 和 210 设备可以运行安全管理*或*日志服务器*或* 安全事件控制台。

** 我们建议您在升级至 R80.10 时，将 Smart-1 205 的内存升级至 16GB。

*** 内存扩展至 16GB 的 Smart-1 210 可运行安全管理和/或 日志服务器 和/或 安全事件控制台。

安全网关 和独立部署（网关 + 管理）

下表中的型号适用于支持 R80.10 的设备系列。

设备系列	安全网关	独立部署（网关 + 管理）
2200	✓	
3000	✓	✓
4000	✓	*
5000	✓	✓
12000	✓	12600*
13000	✓	✓
15000	✓	✓
21000	✓	✓
23000	✓	✓

***** 4200 设备不支持独立部署。
以下设备型号在默认 RAM (4GB) 条件下不支持独立部署：4400、4600、4800、12200 和 12400。这些型号至少需升级至 8GB RAM 才能支持独立部署。

硬件状态监控

R80.10 支持针对 Gaia Check Point 设备进行以下硬件状况监控功能：

- **RAID 状况：**使用 SNMP 监控 RAID 阵列中磁盘的状态，获得有关卷和磁盘状态的通知。
- **硬件传感器：**使用 WebUI 或 SNMP 监控风扇转速、主板电压、电源状况和温度。另外可通过 IPMI 接口卡支持某些开放式服务器，此时需要 IPMI 卡。

Check Point 设备	Smart-1
SNMP 硬件传感器监控（轮询和陷阱）	✓
WebUI 硬件传感器监控	✓
使用 SNMP 进行 RAID 监控	✓

开放式服务器：

硬件传感器：使用 WebUI 或 SNMP 监控风扇转速、主板电压、电源状况和温度。另外可通过 IPMI 接口卡支持某些开放式服务器，此时需要 IPMI 卡。

注：IPMI 是一个开放标准。我们不能保证在所有系统和配置上都具有良好的硬件状态监控效果。

开放式服务器硬件要求

R80.10 服务器旨在高效利用可用的硬件资源，最大限度提高性能和可扩展性。我们建议您利用此优势，并充分发挥硬件潜力以获得最佳性能。

组件	安全网关	VSX 网关	安全管理服务器/独立部署	多域服务器
处理器	英特尔奔腾 IV，2 Ghz 或同等处理器	英特尔奔腾 IV，2 Ghz 或同等处理器	英特尔奔腾 IV，2.6 GHz 或同等处理器	双插槽 2x 至强 E5-2609v2 4 核，2.5 GHz 或同等处理器
总核数	2	2	2	8
内存	4 GB RAM	4 GB RAM	6 GB RAM	32 GB RAM
可用磁盘空间	15 GB	12 GB + 1 GB（每 VS）	500 GB（安装中包含操作系统）	1 TB（安装中包含操作系统）

支持平台

组件	Red Hat Enterprise Linux*	VMware ESXi	Microsoft Hyper-V
安全管理	5.5、6.8、7.3	5.x、6.x	Windows 2012 R2
多域安全管理	5.5、6.8、7.3	5.x、6.x	Windows 2012 R2
安全网关	不支持	5.x、6.x	未认证**

***** 要在 Linux 上安装 R80.10，请联系 Check Point 支持人员。

** 有关 Microsoft Hyper-V 的最新信息，请参见硬件兼容性列表 https://www.checkpoint.com/support-services/hcl/的*虚拟机* 部分。

平台支持的最大接口数量

下表显示了各平台支持的最大接口数量（物理和虚拟）。

平台	最大接口数量	备注
Gaia	1024	
Virtual System	256	包括 VLAN 和 Warp 接口
VSX Gateway	4096	包括 VLAN 和 Warp 接口

向后兼容网关

R80.10 管理服务器可以管理以下版本的网关：

网关类型	发布版本
安全网关	R75.20、R75.30、R75.40、R75.45、R75.40VS、R75.46、R75.47、 R76 R77、R77.10、R77.20、R77.30
VSX	R75.40 VS 或更高版本

R80.10 管理服务器可以管理以下版本的设备安全网关：

设备	发布版本
Security Gateway 80	R75.20.x
UTM-1 Edge N	8.1 或更高版本
1100 设备	R75.20.x、R77.20.x

设备	发布版本
1200R 设备	R77.20.x
1400 设备	R77.20.x
60000/40000 安全平台	适用于 61000/41000 的 R76SP、R76SP.10、R76SP.20、R76SP.30、R76SP.40 适用于 61000/41000 和 64000/44000 的 R76SP.50

日志记录要求

日志可存储在以下位置：

- 从 安全网关 收集日志的 安全管理服务器。这是系统默认设置。
- 专用计算机上的 日志服务器。建议日志生成量大的组织采用此位置。

与具有激活的日志记录服务的 安全管理服务器 相比，专用日志服务器的容量更大，性能更高。在专用的日志服务器上，日志服务器 的版本必须与管理服务器相同。

日志容量

Check Point 设备	**Smart-1 205**	**Smart-1 210**	**Smart-1 225**	**Smart-1 3050**	**Smart-1 3150**
每秒的索引日志数	1,000	2,000	4,000	7,000	9,000

注

- 日志记录速率基于高峰通信数据。我们假设常规运营时间的流量约是该数据的一半。公布的数据专用于日志服务器。对于集成式日志和管理服务器，该数据将更小。
  如需更多有关日志功能的信息，请参见 *R80 日志和监控指南*。
- 将于 2016 年调整和优化大规模部署的性能和容量。将于今年年底公布更详细的规格说明。

安全事件控制台 要求

您可以将 安全事件控制台 Server 安装在 安全管理服务器 或其他专用服务器上。安全事件控制台 R80.10 可连接至其他版本的日志服务器，如 R77.xx 或更低版本。

安全事件控制台 和相关单元通常安装在同一服务器上。您也可以将其安装在不同的服务器上，以便平衡大量日志环境中的负载。相关单元的版本必须与 安全事件控制台 相同。

要部署 安全事件控制台 并生成报告，需要有效的许可证或合约。

管理控制台

控制台硬件要求

下表显示控制台应用程序的最低硬件要求：

组件	Windows
CPU	英特尔奔腾处理器 E2140 或 2 GHz 同等处理器
内存	4 GB
可用磁盘空间	2 GB
视频适配器	最低分辨率：1024 x 768

Windows 平台控制台

支持 安全控制台 的平台：

- Windows 10（所有版本）、 Windows 8.1 (Pro) 和 Windows 7 （SP1、旗舰版、专业版和企业版）。
- Windows Server 2016、2012、2008 (SP2) 和 2008 R2 (SP1)。

Gaia Web 配置界面

以下浏览器可支持 Gaia Web 配置界面（也称为 Gaia 门户）：

浏览器	支持的版本
Google Chrome	14 及更高版本
Microsoft Internet Explorer	8 及更高版本 （如果使用 Internet Explorer 8，则通过 Gaia 门户上传的文件不能超过 2 GB。）
Microsoft Edge	任何版本
Mozilla Firefox	6 及更高版本
Safari	5 及更高版本

版本号

软件刀片/产品	版本号	验证版本号
Gaia	421	`show version all`
安全网关	423	`fw ver`
安全管理	187	`fwm ver`
多域服务器	223	`fwm mds ver`
SmartConsole	991310572	菜单 > 关于 Check Point *安全控制台*

威胁仿真

根据仿真位置的不同，威胁仿真 要求会有所不同：

- 威胁云 - Gaia 操作系统（64 位或 32 位）
- 本地或远程仿真 - 安装 Gaia 操作系统（仅 64 位）的 Threat Emulation Private Cloud Appliance

不支持在运行 R80.10 的本地 威胁仿真 设备上进行仿真。

移动访问 要求

操作系统兼容性

终端操作系统兼容性	Windows	Linux	Mac	iOS	Android
移动访问 门户	✓	✓	✓	✓	✓
Web 应用程序的无客户端访问（链接转换）	✓	✓	✓	✓	✓
终端按需安全	✓	✓	✓		
SecureWorkspace	✓				
SSL Network Extender - 网络模式	✓	✓	✓		
SSL Network Extender - 应用程序模式	✓				
从 移动访问 应用程序下载	✓	✓	✓		

终端操作系统兼容性	Windows	Linux	Mac	iOS	Android
无客户端 Citrix	✓	✓	✓		
文件共享 - 基于 Web 的文件查看器 (HTML)	✓	✓	✓	✓	✓
Web 邮件	✓	✓	✓	✓	✓

浏览器兼容性

终端浏览器兼容性	Internet Explorer	Google Chrome	Mozilla Firefox	Macintosh Safari	Opera for Windows
移动访问 门户	✓	✓	✓	✓	✓
Web 应用程序的无客户端访问（链接转换）	✓	✓	✓	✓	✓
终端按需安全	✓	*✓	✓	✓	
SecureWorkspace	✓	*✓	✓		
SSL Network Extender - 网络模式	✓	*✓	✓	✓	
SSL Network Extender - 应用程序模式	✓	*✓	✓		
从 移动访问 应用程序下载	✓	✓	✓	✓	
无客户端 Citrix	✓		✓		
文件共享 - 基于 Web 的文件查看器 (HTML)	✓	✓	✓	✓	有限支持
Web 邮件	✓	✓	✓	✓	✓

***** 需要在最终用户的计算机上安装 32 位 Java JRE，Google Chrome 才能支持 移动访问 门户按需客户端，例如 SSL Network Extender、Secure Workspace 和终端按需安全。

身份识别 要求

身份代理

请参见各 Windows 平台客户端 (页码 19)和各 Mac 平台客户端 (页码 20)，了解以下相关信息：

- 身份代理（精简版和完整版）
- 终端服务器身份代理

AD 查询

以下平台支持 AD 查询的动态目录：
Microsoft Windows Server 2008、2008 R2、2012、2012 R2 和 2016。

Endpoint Security 要求

以下是在 安全管理服务器 上启用终端策略管理的最低要求：

组件	所有支持的操作系统上都必须达到的要求
内核数	4
内存	8GB RAM
磁盘空间	100GB

- 终端安全管理服务器 可部署在仅用于管理目的的计算机或设备上。不支持独立（安全网关 + 管理）部署。
- 终端安全管理服务器 不可部署在 RedHat Enterprise Linux 的各种版本上。
- R80.10 终端安全管理服务器 可以管理针对 Windows 系统的 E80.62 和 E80.64 Endpoint Security 客户端以及针对 Mac 系统的 E80.64 Endpoint Security 客户端。
- R80.10 管理不支持以下 Endpoint Security 刀片 ：
  网址过滤、Capsule Docs 和 SandBlast Agent 刀片（防僵尸、Forensics，以及 Threat Extraction 和 威胁仿真）。

有关详细信息，请参见您的版本所对应的《针对 Windows 系统的 Endpoint Security 客户端用户指南》和《R80.10 Endpoint Security 管理指南》
http://downloads.checkpoint.com/dc/download.htm?ID=54801。

最大网关群集成员数量

群集类型	最大支持的群集成员数量
ClusterXL	5
Virtual System 负载共享	13
第三方	8

Check Point 客户端支持

多用户登录选项支持

该版本为不同客户端和 移动访问 门户的用户在各个网关提供了多用户登录选项，支持多因素身份验证方案。例如，可以配置一个选项，以便通过个人证书和密码进行身份验证，或者通过 SMS 或电子邮件发送密码和动态 ID 进行验证。

在连接已启用 IPsec VPN 或 移动访问 的 R80.10 网关 时，可以支持这些功能。

支持的客户端或门户	支持的最低版本
移动访问 门户	R80.10
安全胶囊-工作区（适用于 iOS）	1002.2
安全胶囊-工作区（适用于 Android）	7.1
远程访问客户端 - 独立客户端	E80.65
Endpoint Security 组件的 Remote Access VPN 刀片	E80.65

请参见*《移动访问 管理指南》* http://downloads.checkpoint.com/dc/download.htm?ID=53103 或*《VPN 远程访问管理指南》* http://downloads.checkpoint.com/dc/download.htm?ID=53105 以了解详细信息。

各 Windows 平台客户端

Microsoft Windows

在下表中，Windows 7 支持是指旗舰版、专业版和企业版。Windows 8 支持是指专业版和企业版。所有标记的控制台和客户端都同时支持 32 位和 64 位。

Check Point 产品	Windows 7 (+SP1)	Windows 8.1	Windows 10
远程访问客户端 E80.x	✓	✓（安装 8.1 Update 1）	✓（E80.62 及更高版本）
Capsule VPN 插件		✓	✓
SSL Network Extender	✓	✓	✓
UserCheck 客户端	✓	✓	✓
身份代理（精简版和完整版）	✓	✓	✓
终端服务器身份代理	✓		

Microsoft Windows Server

Check Point 产品	Server 2008 (SP1-2) 32/64	Server 2008R2 (+SP1)	Server 2012	Server 2012 R2 64 位	Server 2016
UserCheck 客户端	✓	✓		✓	✓
终端服务器身份代理	✓	✓	✓	✓	✓

注：XenApp 6 上也支持终端服务器身份代理。

各 Mac 平台客户端

仅支持 64 位。

Check Point 产品	OS X 10.9	OS X 10.10	OS X 10.11	macOS 10.12
身份代理	✓	✓	✓	✓
SSL Network Extender	✓	✓	✓	✓
Endpoint Security VPN E80.x 或更高版本	✓（E80.50.03 及更高版本）	✓（E80.60 及更高版本）	✓（E80.62 及更高版本）	✓（E80.64 及更高版本）

DLP Exchange 代理

以下平台可支持 R80.10 DLP Exchange 代理：

Windows Server	Exchange Server
2012 R2 64 位	2010、2013
2016 64 位	2016

对于更低的服务器版本，请使用 R77.30 DLP Exchange 代理。