



SmartCenter

统一安全管理的最智能化的选择

您遇到的挑战

在过去,为您的边界安装防火墙并且为您的台式机安装防病毒软件被认为是最先进的安全防范措施。但现在,情况已经发生变化。随着互联网蠕虫的出现和复杂的攻击手段不断增多,如今的网络安全情况远比过去复杂得多。这样的新环境,以及新的安全规定和为远程用户以及商业合作伙伴提供远程访问的需要,都要求一个更全面彻底的安全实施。多层次的保护将从带防火墙的网络边界开始并逐渐深入到网络内部,从而保护敏感的部门、服务器、应用程序,甚至用户的个人电脑和笔记本。但不幸的是,这样的多层安全防范又导致了管理上的复杂。对于资源有限的IT部门而言,在多个站点和多个平台上确保其安全防范措施能保持更新就成了一项艰巨的任务。

如果没有有效的管理,即便是最复杂的安全部署,其所能提供的安全保障也只将受限于自身最弱的环节。安全管理解决方案必须让企业能跟踪自己安全部署的效率,为安全法律调查提供详细的信息,支持在整个企业执行一致的安全策略和主动式升级。

我们的解决方案

SmartCenter™ 以 Check Point 公司统一的安全架构为基础,它支持企业集中定义边界、内部、Web 和终端的安全策略;关联并对安全事件进行优先级划分;实施高级的监视和报告功能——这一切都通过一个控制台来实现。使所有网关分配安全策略升级变得很简单,从而确保一致的策略实施并提高运营效率。这样,企业能保护对业务关键的资产并实现它们在安全方面投资的最大化。

综合的安全管理

Check Point 公司通过 SmartCenter UTM™ 和 SmartCenter Power™ 提供各种水平的管理功能,从而提供集成的、可节约成本的解决方案,以支持通过单个管理控制台来实现最高级的控制和安全。



NGX 平台为 Check Point 的边界、内部和 Web 安全提供一个统一的安全架构

产品描述

SmartCenter™ 解决方案提供了功能强大的软件工具来集中配置、管理和监视多个 Check Point 网关和执行点。

产品特点

- 集成的边界、内部、Web 和终端安全管理
- 实现安全策略可视化
- 策略和软件自动化分配
- 通过 Web 门户或者管理控制台访问策略
- 高可用性和可扩展性

产品优点

- 实现运营效率的最大化
- 实现对整个网络的策略执行和控制保持一致
- 对规则遵循提供更简单的展示

NGX 亮点

- 通过互联网访问 SmartCenter
- 集成的网络、VPN、Web、终端和最终用户日志记录、监视和报表功能
- 全局安全防范升级,抵御最新威胁



Check Point 保护您网络的每个部分:边界,内部和 Web,使得您的信息资源安全,可访问且易于管理

SmartCenter UTM 为所有 Check Point 应用程序提供集中的管理。它包括以下组件

- SmartDashboard™ 是一种能支持管理员集中定义安全和 VPN 策略的界面。
- SmartView Tracker™ 可以对所有有日志记录的连接和管理员活动提供实时的可视化跟踪。

除了提供 SmartCenter 的所有功能，SmartCenter Power 还可以为最复杂的环境提供以下增加的管理功能：

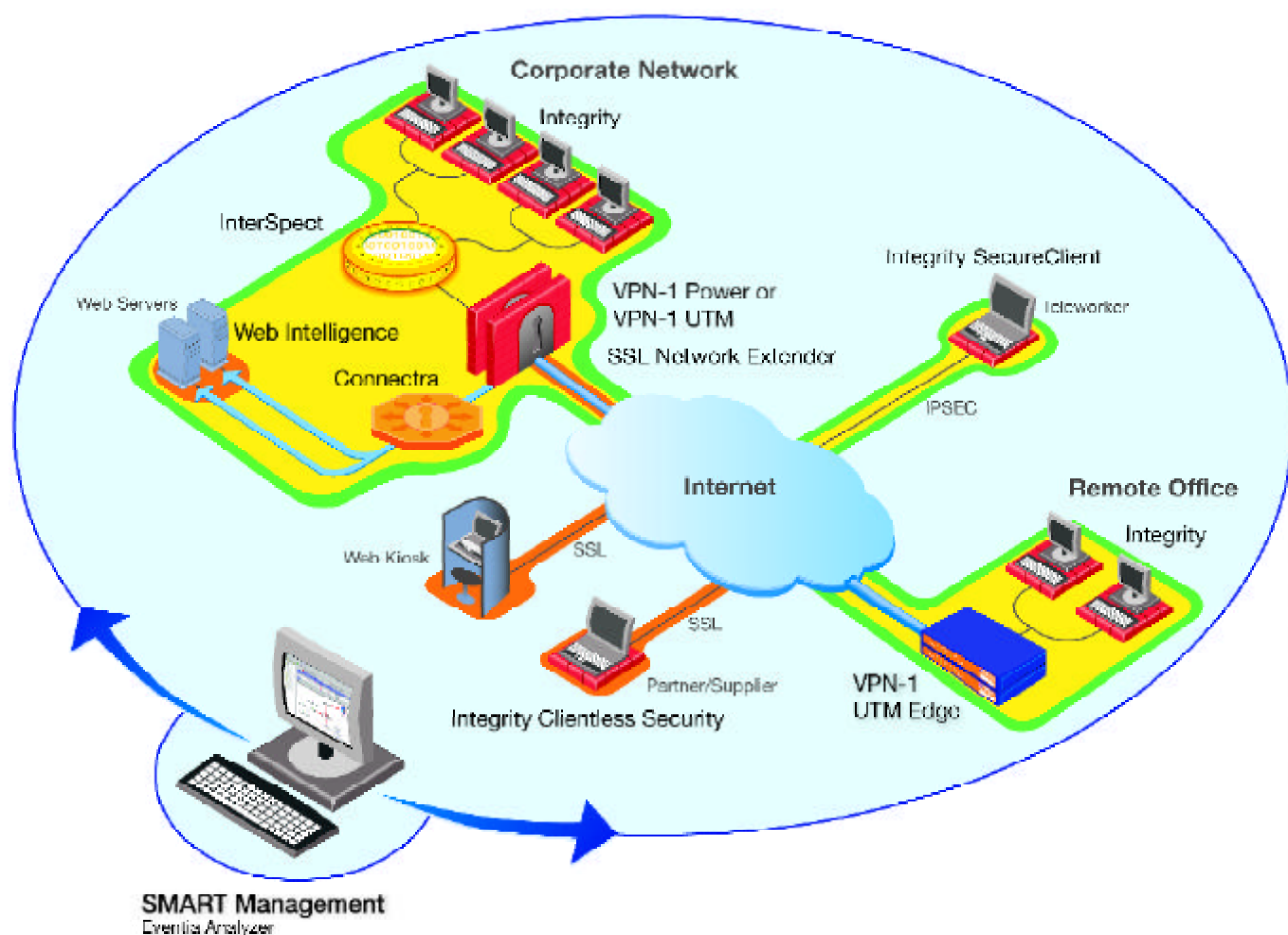
- SmartPortal™ 为 SmartCenter 增添了基于浏览器的访问功能。
- SmartMap™ 支持对安全策略的可视化管理。
- SmartView Monitor 支持对网络、VPN 和用户进行实时监视。
- SmartUpdate™ 对相关软件和证书进行集中分配和存储。
- SmartLSM™ 支持对远程 VPN-1 UTM™ Edge™ 设备进行大规模管理。
- SmartDirectory 提供对基于 LDAP 的目录的集成。

- Management High Availability (管理高可用性) 为所有管理操作提供容错功能。

除此以外，Eventia Reporter™ 能提供综合、易于理解的图形化报表，而 Eventia Analyzer™ 能对来自 Check Point 网关以及多个安全和网络设备的日志数据进行实时事件关联。Eventia Reporter 和 Eventia Analyzer 是 SmartCenter 的附加软件。

基于策略的VPN/防火墙管理

作为 SmartCenter 的一部分，SmartDashboard 虽然复杂，但在使用上仍然很方便。管理员可以集中定义一个安全策略的各个方面：VPN、网络地址转换(NAT)、服务质量(QoS)、Web 访问以及台式机和终端的安全、防病毒保护、SmartDefense™ 升级。被定义为安全策略一部分的“对象”，比如网络、主机、用户、服务、资源和活动，都可以在 SmartDashboard 中被图形化显示并能被直接处理。比如，对象可以被包含到 SmartGroup 中，或者网络对象可以被轻松克隆以简化对策略的定义。



集中的SMART管理统一了对Check Point公司边界、内部、Web和终端安全解决方案的管理。

因为统一安全架构的组件紧密集成，相同的对象可以在执行点和应用程序间被共享，从而节省管理时间并确保整个网络策略配置的一致性。

除了集中的仪表盘工具，SmartCenter 解决方案还提供了很多种策略管理工具来改进策略的创建。预定义的全局策略支持利用各种服务来在执行点之间进行恰当的连接。SmartCenter 可以管理策略的多种版本，允许管理员还原到策略的老版本。

集成的边界、内部和 Web 安全

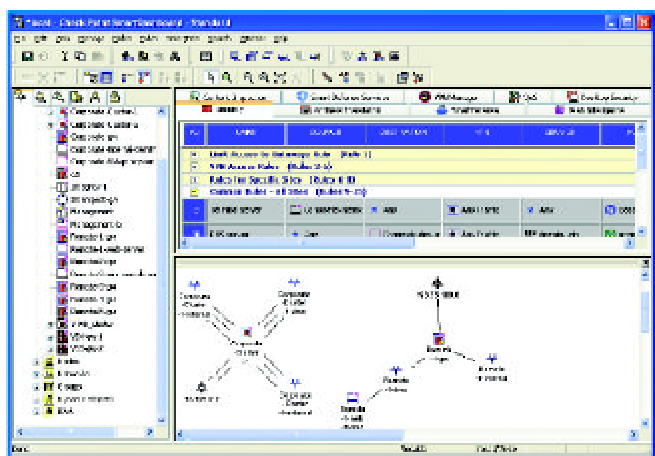
SmartCenter 进行集中管理的对象包括：VPN-1 Power、VPN-1 UTM、VPN-1 UTM Edge、InterSpec™、VPN-1 VSX 网关、SecureClient™ 应用程序。通过 SmartDashboard，管理员可以定义和实施策略、跟踪日志、监视安全和网络活动、查看有关网络和安全活动趋势的报表以及集中分配安全和软件升级。通过这些随手可得的功能，管理员可以提高运营效率，更清楚、直观的了解整个网络的安全状况。

集成的终端安全

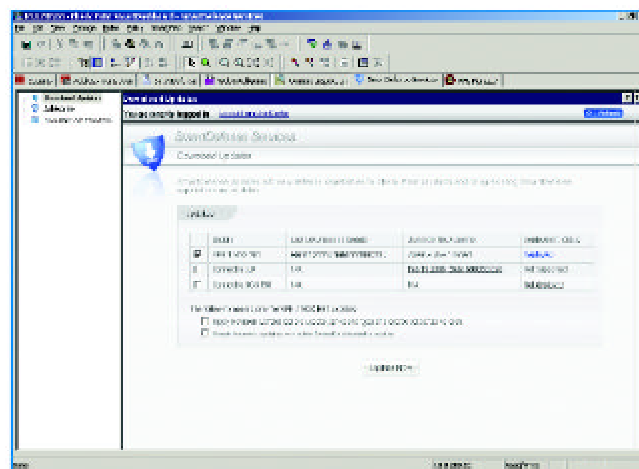
Check Point Integrity™ 可以为终端以及企业终端所连接的网络提供安全保护，抵御最新的蠕虫、间谍软件和入侵企图。Integrity 的主动式防御包括个人防火墙、输出威胁拦截、入侵防范、清除间谍软件、确保只有安全的计算机能被授权进入网络。集成了 SmartCenter 之后，Integrity 可以与 Check Point 公司的其它解决方案一起被集中管理，提高对整个企业范围进行安全管理的效率。

全局安全防范升级

通过 SmartDashboard 中的 SmartDefense 服务控制台，管理员可以从一个统一的界面全局性更新安全配置和保护措施，



通过 SmartDashboard 实现策略集中管理和可视化。



通过 SmartDashboard 实现集中安全配置和防御升级

确保安全系统总是保持最新版本并能抵御新出现的和变化的各种威胁。这些升级可以被实时部署到多个设备中，并且不会中断服务，因此，可以减轻管理负担并减少出错情况的发生。

简单的 VPN 部署

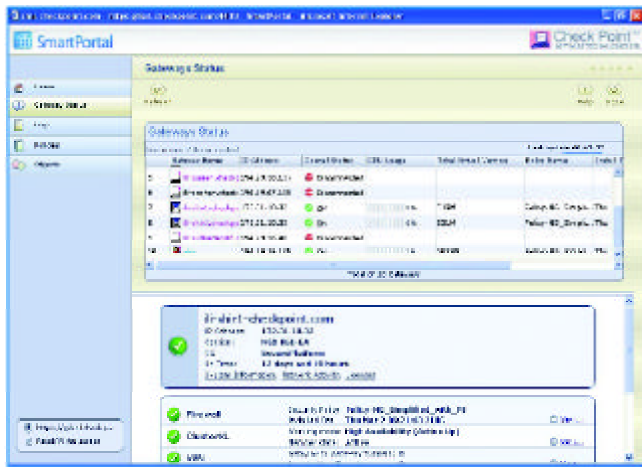
SmartDashboard 支持管理员通过一个简单的操作来定义 VPN 团体，并为整个 VPN 拓扑（包括内网、外网和远程访问部署）设定安全参数。安全管理员只需要将所有 VPN-1 网关组成一个团体，VPN 就能在所有网关间或者远程用户和网关间自动启动。当新站点或者用户被加入团体时，它们能自动继承相应的属性并能立刻与其余的 VPN 团体建立安全会话。安全管理员可以不用再做像设计和定义加密规则之类的重复性工作。SmartCenter 支持各种网络拓扑结构，包括全网状拓扑、星型拓扑、集中星型拓扑和混合拓扑。VPN 对象和团体能被轻松集成到安全规则库中。

实时排错

SmartView Tracker 可以对所有有日志记录的连接和管理员活动提供实时的可视化跟踪。管理员可以过滤或者搜寻感兴趣的事件，如果出现攻击事件或者发现可疑活动，他们可以立即禁止或者终止与某个 IP 地址的连接。这些功能大大减少了排除配置错误所需要的时间。

SMARTCENTER POWER——为复杂的环境提供高级的安全管理

SmartCenter 为企业提供了能集中定义和监视其安全策略的功能。SmartCenter Power 和诸如 Eventia Reporter 以及 Eventia Analyzer 等管理附加模块通过一系列高级的集成功能使企业能更好的理解和控制其安全环境。



SmartPortalWeb 管理门户可以支持企业多个用户查看安全信息显示。

通过Web访问SmartCenter

通过 SmartPortal ,安全小组可以让外部团队 ,如技术支持或者审核员访问基于浏览器的 SmartCenter ,但同时又继续保持对策略执行的集中控制。SmartPortal 用户可以查看安全策略和 Check Point 产品的状态 ,以及管理员的审核跟踪 (audit trail)。高级用户可以获得管理员管理权限。这个扩展功能促进了在减少攻击或者排除网络错误和安全问题时的团队合作。SmartPortal 允许安全管理员根据自己的判断将对安全策略的访问扩展到其它小组 ,从而在企业内部提高了对安全的可视化。

安全可视化

大多数企业都有着复杂的拓扑结构 ,包括网关、主机、服务器以及由许多台不同机器组成的网络 ,同时还执行着许多不同的规则和规则库。SmartMap对安全策略进行图形化显示 ,从而使对该策略的理解和排错更轻松。它还支持安全管理器在部署前校验其安全策略的一致性。

实时监控

SmartView Monitor 对安全、网络、VPN通道和用户活动进行实时监控。这个解决方案为管理员提供统计数据的图形化显示 ,比如带宽、数据往返时间以及丢包值和VPN通道状态。在 SmartView Monitor 所提供信息的帮助下 ,管理员

可以实现它们网络性能的最大化并控制住成本。

软件和许可的自动分配

SmartUpdate 向 Check Point 和 OPSEC 认证过的产品自动分配软件应用程序和升级并且管理产品证书。它采用集成的方法来确保整个网络的安全总是保持最新更新。除此以外 ,它减少了其分支机构对 IT 员工的需要。

大规模的VPN和安全管理

SmartLSM 为大规模VPN/安全安装引入了一种新的管理范例。利用 SmartLSM ,管理员可以规定一个单一安全策略——称为配置文件 (Profile) ,并将其应用到成百上千的网关中。除此之外 ,策略安装和升级的自动化过程可以支持快速部署 ,并使管理需求最小化。这减少了为成百上千个网关部署和管理安全所需要的成本和时间。

基于LDAP的用户管理

SmartDirectory简化了安全管理过程 ,特别是大规模部署时的安全管理过程。它支持 Check Point 执行点从 OPSEC 认证过的LDAP目录服务器为网络用户获取身份和安全信息。

管理基础架构冗余

Management High Availability (管理高可用性) 为 Check Point 执行点提供不间断的连接。多台管理服务器可以通过“敏感系统 (nervous system)”和其它设备相连 ,并自动同步客户和管理员数据。这可以消除部署专门的、冗余的硬件和软件的需要。

支持的操作系统

SmartCenter 图形用户界面控制台

Windows 2000/2003/XP操作系统, Solaris 8/9/10操作系统

SmartCenter 服务器

SecurePlatform™, Windows 2000/2003 服务器版操作系统
Solaris 8/9/10 操作系统, Red Hat Linux 企业版 3.0, Nokia IPSO

©2006 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, Eventia Reporter, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMSecure, INSPECT, INSPECT XL, Integrity, InterSpec, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Power, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988 and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

May 12, 2006 P/N 502130

Worldwide Headquarters
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753-4555
Fax: 972-3-575-9256
Email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391/650-628-2000
Fax: 650-654-4233
www.checkpoint.com

 **Check Point**
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.