puresecurity

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point IPS-1

用于企业网络的专业入侵防御体系

目录

概述

尽管安全管理者已经开始关注保护企业网络了，但是新的威胁仍然不断地出现。今天，企业面临防止新一轮攻击的挑战，这一轮攻击更复杂，能力更强。防止这些不断出现的威胁很有挑战性，原因有以下几个方面：

第一，现在许多攻击都使用先进的自我繁殖技术来更快更有效地进行感染。这说明零日（Zero Day）攻击比以前更普遍、更难以解决。

第二，攻击者利用许多常见协议（HTTP、SMTP）作为进入企业的攻击通道，这样就可以绕开传统的防火墙策略。许多这样的攻击都是有效负载的一部分，通常在应用级展开。检测这些攻击需要具备像深度信息包检测和协议分析这样的能力。

最后，随着大量新应用程序部署到企业，安全管理者要保持同步通常就显得非常艰难了。实际上，用户通常非正式、无限制地使用许多新应用程序——例如即时消息（IM）或语音电话（VoIP），这样安全小组就更难以防止潜在威胁。许多应用程序与多种攻击传播媒介结合，这说明实际上防止攻击（而不仅仅是检测攻击）变得至关重要。

所以，保护企业安全具有挑战性，也非常复杂。传统的防火墙、虚拟个人网络（VPN）和防病毒软件是所有安全基础的重要部分，但在处理今天面临的安全挑战时，它们还不够。入侵防御系统（IPS）对于公司安全结构而言，不但至关重要，而且必不可少。本白皮书描述了Check Point IPS-1™入侵防御解决方案在处理企业网络安全时的优势和产品性能。

IPS-1的优点

Check Point IPS-1是专用于企业级入侵防御的最主要解决方案。在保护企业网络方面，它有如下优点：

- 高级检测——IPS-1通过核心的混合检测引擎（Hybrid Detection Engine™）提供高级检测功能，该核心检测引擎能以低误判率进行精准检测。
- 从边界到核心的在线防御——IPS-1提供最广泛的防御，在线部署的吞吐率范围是从50Mbps到2Gbps。2007年计划推出10Gbps产品。
- 企业级的入侵防御——IPS-1管理仪表板（IPS-1 Management Dashboard）对企业威胁情况提供了多种视角界面功能。它同时提供企业管理性能，例如透明的远程安装/更新，以及自动签名更新，确保低负担且易管理。而且，IPS-1为远程/分支办事处及大型企业部署提供可扩展性和可靠性。
- 动态屏蔽体系结构（Dynamic Shielding Architecture™）——通过核心的动态屏蔽体系结构，IPS-1接收端

点漏洞信息，进行分析，动态激活与当前网络状况相关的行为。

- IPv6准备就绪——IPS-1完全支持IPv6网络。这意味着将来可以无缝迁移到下一代Internet协议，它也可以确保检测和防御当前通过IPv6通道进行的所有攻击。

IPS-1产品概述

- IPS-1产品通过多层结构适用于企业级入侵防御，这种多层结构具有独一无二的可扩展性和可靠性。产品结构如图1所示。

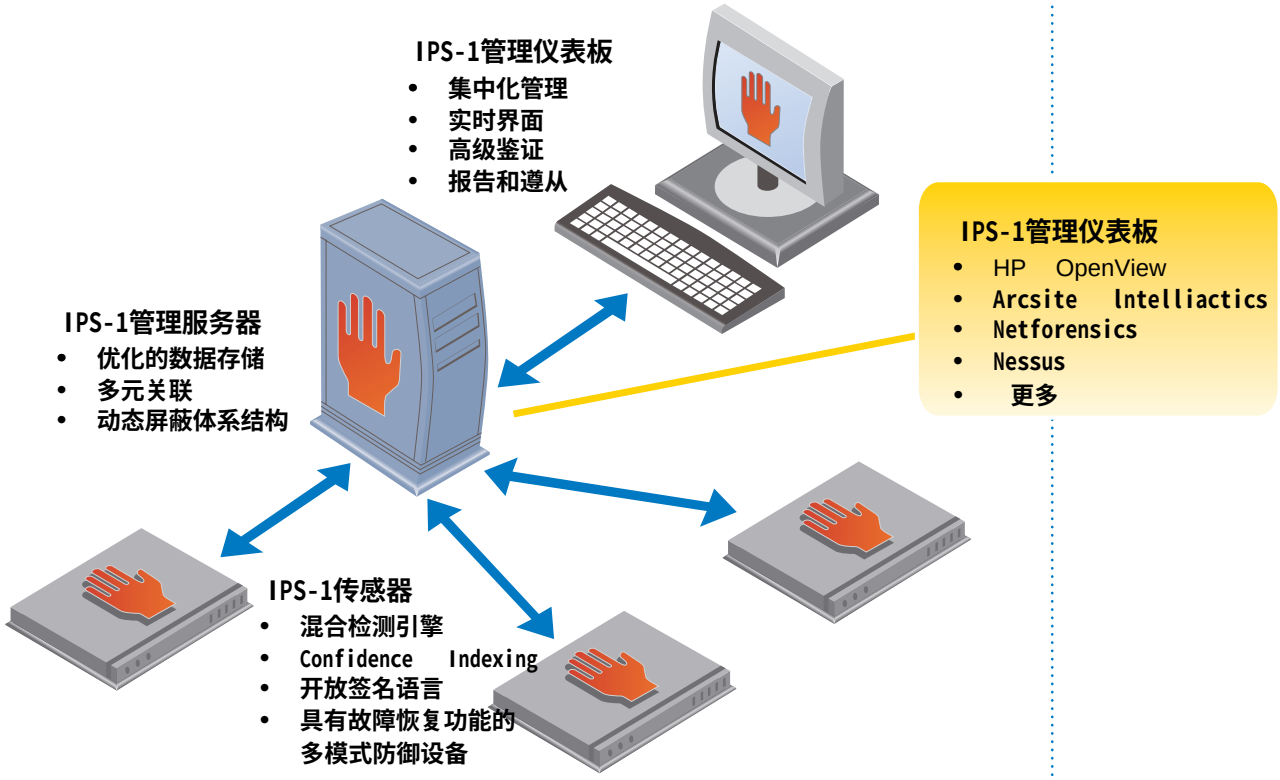

图1 IPS-1产品结构

IPS-1产品结构主要由3部分组成：

- IPS-1传感器
- IPS-1管理服务器
- IPS-1管理仪表板

通过多层产品结构，IPS-1对于企业入侵防御具有真正的可扩展性。IPS-1传感器与IPS-1管理服务器之间是多对一的关系（例如，几个IPS-1传感器可以连接到一个IPS-1管理服务器）。同样，IPS-1管理服务器与单个IPS-1管理仪表板之间也是多对一的关系（例如，几个IPS-1管理服务器可以连接到一个IPS-1管理仪表板）。

IPS-1结构也具有故障恢复功能的特点，可以确保组件所有不可预知的故障不会阻碍网络和安全运行。例如，可以给主要服务器配置多个辅助IPS-1管理服务器。在主IPS-1管理服务器发生故障的情况下，传感器会转换到辅助服务器。同时，所有传感器都有内置的故障恢复模式，如果传感器发生故障，它会自动转发网络信息。

IPS-1 传感器

IPS-1传感器提供网络数据的深度信息包检测功能，并将线速度性能与精确检测结合起来。 IPS-1提供完整的IDS/IPS传感器，以满足从低端到高端多千兆速率的性能需要。

IPS-1 Sensor 模型	数据率 IPS/IDS	PS/IDS 网络
IPS-1 Sensor 50C	50/75Mbps	用于1 IPS或3IDS的全部3个端口
IPS-1 Sensor 200C/F	200/250Mbps	用于1 IPS或3IDS的全部3个端口
IPS-1 Sensor 500C/F	500Mbps/1Gbps	用于2 IPS或4 IDS的全部4个端口
IPS-1 Power Sensor 1000C/F	1/2Gbps	用于4 IPS或8IDS的全部8个端口
IPS-1 Power Sensor 2000C/F	2/4Gbps	用于4 IPS或8IDS的全部8个端口

下一节将描述IPS-1传感器的主要安全特征。

具有故障恢复功能的多模式部署设备

IPS-1可以用3种不同的模式部署——被动入侵检测模式（Passive Intrusion Detection Mode）、在线桥模式（Inline Bridge Mode，也称为学习模式Learning Mode）和全在线防御模式（Inline Prevention Mode）。

- 被动入侵检测模式——作为传统的入侵检测模式，被动入侵检测模式接收一段时间内端口信息，镜像端口或者TAP设备的网络流量。在这种模式下，IPS-1不在线但接收攻击检测分析信息的副本，并相应提高报警级别。
- 在线桥模式——用在线桥模式（也称为学习模式Learning Mode）部署时，IPS部署为在线，但检测到攻击信息时它实际上不阻止这些信息。相反，它允许所有信息通过，但提高报警级别，就像在被动检测模式中一样。这种模式激活从检测到防御的转换步骤，这里用户可能观察IPS-1运行在线、检测攻击，但实际上不阻止检测到的攻击信息的效力。这种模式也有利于网络管理团队评估放置于在线防御模式下的设备的弹性。
- 在线防御模式——当部署为完全在线防御模式时，IPS-1就是具有完全功能的入侵防御系统。它阻止检测到的恶意信息。

另外，IPS-1传感器有在线故障回复功能。通过简单的指示和点击，安全管理者就可以确定传感器在断电或其他灾难性故障情况下是不做故障回复还是进行故障。故障切换模式说明，当传感器失效时，网络信息会继续传递，确保网络的完整性和公司运转。这种典型的默认模式可以确保网络连续运行，同时不会产生故障或信息丢失。不进行故障转换模式就不会转发网络信息。使用这种模式强化了一种策略，那就是安全比数据流更重要。

混合检测引擎

因为有效的入侵防御建立在精确检测的基础之上，所以IPS-1传感器最重要的特征就是混合检测引擎，它利用多种检测和分析技术检测和防御潜在威胁。一些主要分析和检测技术有：

- 基于攻击的签名——通过提供与特定攻击特征相匹配的签名，来检测已知威胁。
- 漏洞签名——提供与漏洞特征相这样可以有效防止零日（Zero Day）攻击。
- 基于策略的签名——检测违反安全策略的情况，包括误用和异常。
- 协议确认——通过检测协议规则和用法的异常来防止零日（Zero Day）攻击。
- 被动操作系统指纹识别——确定目标主机的操作系统（OS）来激活称为智能重组的特殊特征，智能重组依据目标主机的OS自动重新组装IP信息包。由于每个操作系统重新组装片断的方式不同，攻击者可以利用这些差异发动片断攻击，这些攻击可以绕过典型的检测方法。IPS-1使用指纹识别来检测这种隐藏的攻击。
- 多要素相关——从拓扑结构上检测其他熟悉的离散事件，将它们上升为较高的相关性报警程序。例如，发生在地理上分布式网络中的多扫描和攻击企图，依据策略，来自相同源IP地址的所有攻击都会被检测、报警、列入黑名单。
- 动态蠕虫抑制——利用统计报警行为来确定和自动检测快速自我繁殖的零日（Zero Day）蠕虫。

精确检测不只是检测攻击。也包括减少或排除误报。如前面所述，IPS-1有在线的OS指纹识别。启用这一功能后，就可以将误报减少到最低。当IPS-1检测到来自特定主机的潜在攻击时，它互相参照主机状况，以确定该主机是否真的容易受到攻击。例如，如果在Linux机器上检测到了基于Window的攻击，可以配置IPS-1，让它不会发生实际的报警。降低误报，管理员就没有必要分析对潜在目标没有重要影响的攻击。

报警溢出抑制是另一种IPS-1工具，它可以让安全团队更有效率，更有效果。如果发生大范围攻击，安全管理者通常会被本质相同的报警淹没。这让安全管理者很难（并非不可能）在合理时间内查看所有报警。报警溢出抑制可以抑制指定时间窗口内相同来源/目标地址的类似报警，将信息结合成综合报警，减少报警溢出。

Confidence Indexing

IPS-1的独特性能之一是称为Confidence Indexing™的专利未决特

征，它依据“信用分”控制防御级别，这样在在线防御部署时对于降低误报非常有用。

通过Confidence Indexing，IPS-1将信用分与每个检测到的事件联系起来。此分数表示检测到的事件是合法攻击这一保证的级别。在明确签名匹配的情况下，指派的分数可能是90%或更多，它表示高级别的恶意信息信用。有潜在协议违背或误用的地方，信用分就越低，表示协议违背可能是善意的，并不是攻击的标志。

依据组织的风险限度，管理员可以将IPS-1设置为阻止所有发现的攻击，这些攻击的信用分为90%或更高。这样可以在在线防御模式中最小化误报的风险，同时允许用户控制与组织风险状况相适应的防御级别。

企业级IPS传感器

IPS-1产品提供从50Mbps到2Gbps的吞吐量，它提供的性能适用于各种规模的组织和公司。

如前面所述，所有传感器都有内置在线的故障通讯转发功能，确保如果发生故障，能够保证网络不中断。而且，IPS-1 Power Sensors（所有传感器都有1Gbps以上的在线吞吐量）也利用冗余的主要组件——例如电源、风扇、驱动器、处理器和端口——提供企业功能性。IPS-1 Power Sensor主组件支持热插拔，它们让现场服务简单有效。

专用签名语言

IPS-1的签名和签名语言（称为N-Code）是开放的，客户可用它们来修改或写自己的签名。虽然大多数客户依赖Check Point提供签名，但有些情况下，也需要或期望修改签名以满足组织的特殊要求。而有些情况下，组织可能部署使用特定专用协议的应用程序，这些协议可能需要进行深度信息包检测和协议确认。在这些情况下，选择使用这种强大的脚本签名语言为Check Point的IPS-1设计有效的专用签名非常有价值。

IPS-1管理服务器

IPS-1管理服务器为IPS-1提供数据管理。它由最佳的高性能数据库组成，该数据库中存储着来自传感器的报警。每个IPS-1管理服务器依据数据率、配置状况和网络信息类型，都可以支持多个IPS-1传感器。

动态屏蔽体系结构

IPS-1管理服务器封装动态屏蔽体系结构的核心，它利用成形的主机信息预先保护网络。动态屏蔽体系结构工作流程如下所述：

- 利用像Nessus这样的主动扫描工具或像动态网络防御组

件这样的被动扫描工具，接收主机和网络信息，

- 与IPS-1配置的签名状况互相参照，确定适当的行动。
- 采取行动，这些行动可能是自动更新签名状态，最新研发的版本或隔离有威胁机器的能力。

例如，XYZ Corp.的策略是只能运行加固的Apache Web服务器。这样，用这种假设来配置防御状况：例如，安装了Apache签名。然而，配置后不久，在没有许可的情况下，会计部门安装了流氓Microsoft IIS服务器来运行部门内部互联网。主动网络扫描（目前是Nessus）检测到该流氓服务器之后，动态屏蔽体系结构就会让IPS-1：

1. 显示报警，将网络变化告知安全小组
2. 显示策略违反报警（IIS Web服务器违反了Apache专用HTTP服务器策略）
3. 互相参照签名防御状态，确定当前配置不包括IIS签名后，通过将IIS签名推给传感器来自动更新防御状态。

这些行动会通报给违反安全小组，在安全小组有时间调查服务器部署，确定是谁部署的服务器以及为什么部署之前，对被利用的流氓服务器提供现有的最好防御。

这种预先适应与安全环境改变范围相关的防御状态，可以确保提供比标准的静态IDS/IPS部署更广泛的网络安全。

IPS-1管理仪表板

IPS-1管理仪表板提供用户界面来管理IPS-1部署。IPS-1 管理仪表板与其他入侵防御产品的标准用户界面明显不同。主要差别是IPS-1 Dashboard的如下特征：

威胁状态界面

IPS-1 Dashboard用于监控组织的安全状态，而不仅仅是监控报警。除了与多个IPS仪表板相同的标准报警管理界面之外，IPS-1 Dashboard同时具有多威胁状态界面功能（如图2所示）。不仅仅是关注报警，管理员还可以关注真正重要的信息——他/她所负责组织或网络部分的安全状态。

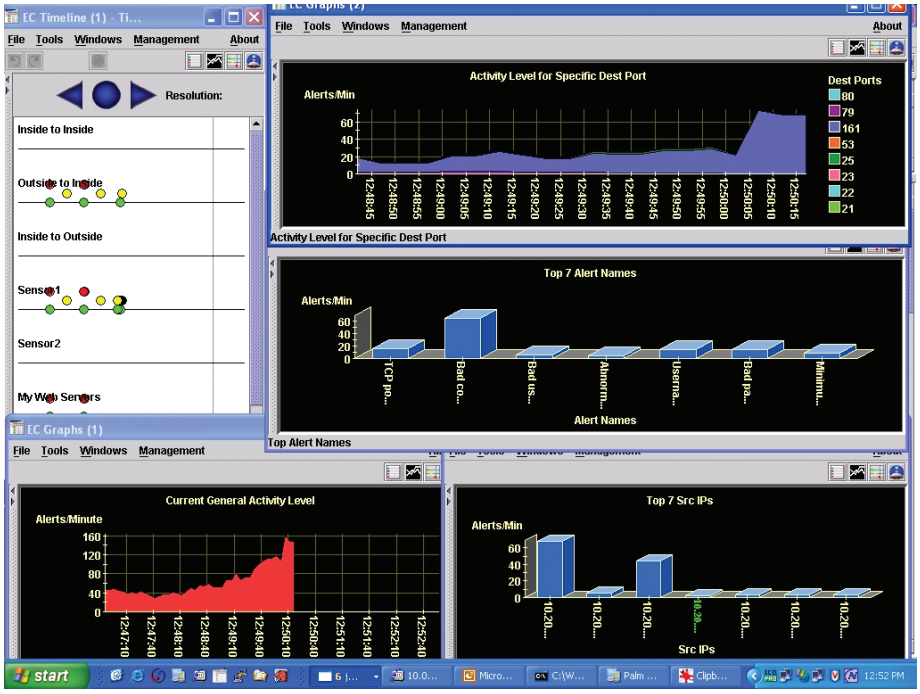

图2 IPS-1 Dashboard威胁状态界面

IPS-1 Dashboard提供的一种特别界面是时间线界面（Timeline view，如图3所示），它将安全相关的活动划分为移动的时间线，可以提供高效的图形威胁监控。另外，时间线界面（Timeline View）让安全管理员能够及时复查威胁活动。

可升级的集中化管理

IPS-1部署的范围从某些配置的传感器一直延伸到全球网络中配置的成百上千台传感器。特别是在较大部署的情况下，管理IPS-1系统的能力就显得极其重要。使用IPS-1 Dashboard，管理员可以管理安装、更新、配置和诊断成百上千台传感器，不管它们在哪里。出于策略管理的目的，IPS-1 Dashboard内的设备提供了这种低负担、可扩展的管理，用来创建虚拟组。例如，通过创建所有这些设备的虚拟组，公司用户可以管理所有分支办事处的IPS-1解决方案。她能够通过虚拟组执行策略管理，而不是单调乏味地为单个设备管理策略。

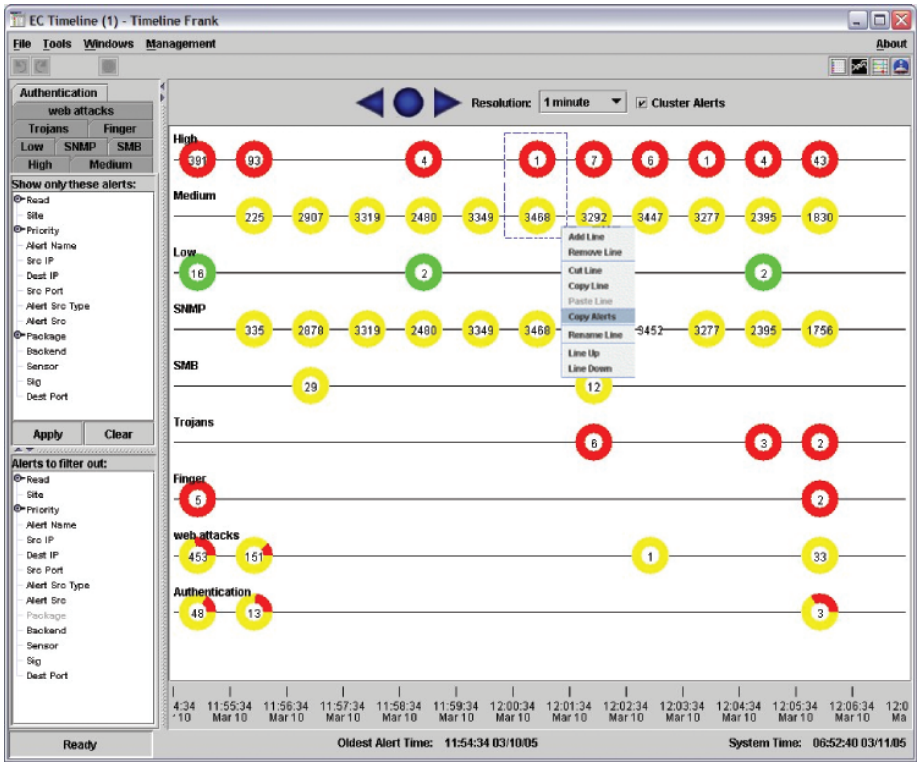

图3 时间线界面（Timeline View）

论证分析

IPS-1具有强大的分析能力，可以帮助管理员快速剖析攻击数据，编辑攻击和事件趋势报告。通过IPS-1管理仪表板，管理员可以获得所有传感器实时的、高级别的图形界面，研究分析和将事件和报警数据分组，以便有效查明攻击来源及其范围。管理员可以定制攻击图和攻击传播媒介时序，形成自己的窗口，监控实时攻击和防御行为。报警数据很容易被分成普通组，它们都是依据用户配置标准定制的。报警可以由任何域——例如源IP、攻击类型和目标漏洞——进行分组。

漏洞管理

IPS-1也具有在线到IPS-1 管理仪表板的漏洞管理功能。这种特征（称为IPS-1 Vulnerability Browser，如图4所示）利用主动扫描接收的数据，可以从单个仪表板进行漏洞浏览和管理。Vulnerability Browser将IPS-1功能与Nessus漏洞扫描（一种流行的开源网络扫描工具，由Tenable Networks发起，全球75,000多个组织都在使用）结合起来，让安全管理员能够快速确定高风险安全问题，详细分析网络中的特定漏洞，了解当前哪些漏洞和服务受到了攻击。同时，通过IPS-1动态屏蔽体系结构，IPS-1预先防御了当前曝露的漏洞，确保网络中的当前漏洞完全不被利用。

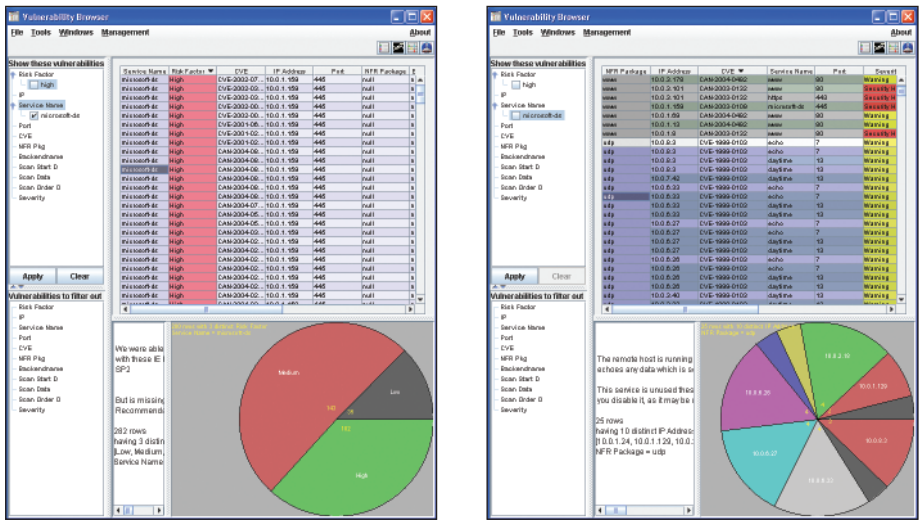

图4 Vulnerability Browser

报告和相关性

IPS-1包含40多份报告，这些报告为用户提供了组织安全状态的观点，因此可以提供最好的安全报告（如图5所示）。它既可以提供实时的分析报告，也可以提供历史的分析报告。

图5 报告

IPS-1 Dashboard也提供了与许多传统的IPS仪表板不同的相关性功能。它允许创建实时图表，这些图表是建立在用户定义的条件规则基础之上的数据集合。这些规则由通过图形界面的指示和点击（不是脚本）定义，这样非编程人员也可以使用这种功能性。

结论

当今广泛存在的威胁需要多层防御，这些防御包括周边及公司网络内的信任点数。入侵防御系统要能够精确检测和防御对IT系统的攻击，同时兼顾不断变化的环境中的多个传播媒介。

这种动态改变的IT环境要求今天的入侵防御系统不只是简单的检测和防御，而且要提供功能性1）通过细粒度和自定义检测机制，极大地降低误报；2）将应用主机漏洞信息来智能应用正确防御行为；3）在攻击情况下，提供细粒度论证来确定原因和相关性行为；4）随着企业不同而不同——是意味着适合新的应用程序、系统更新还是日益增长的网络性能要求。今天的入侵防御系统需要提供所有这些功能，同时最小化管理系统所需的管理费用。

Check Point IPS-1给IT组织提供了强大的入侵防御系统，该系统不仅能够满足今天的要求，而且具有在线适应性和可扩展性，可以随着环境或企业要求的改变而发展变化。

March 8, 2007 P/N 502462