思科 IronPort 上网行为管理安全网关技术建议书

IronPort Systems

2009 年 7 月

目　录

1． 公司简介

IronPort 系统有限公司是业界领先的互联网信息安全产品提供商，为全球超过 3 亿用户提供邮件安全和 Web 安全保护，其客户不但包括众多中小型企业，还包括许多位列全球 2000 强的大型企业。IronPort 为那些面临着管理、保护和发展其至关重要的邮件系统等艰巨任务的企业提供高性能的、易于使用的和技术创新的全球领先高科技产品。

- 成立于 2000 年
- 总部在美国加州 San Bruno
- 季度间营业额增长超过 50%
- 全球大客户超过 1500
- 产品已经有 51 个国家采用
- 保护超过 3 亿的邮箱
- 全球前 100 大企业的总部有 38 家是客户
- 全球 15 大 ISP 中有 12 个采用了 IronPort 产品
- 全球 10 大银行中有 5 个采用了 IronPort 产品
- 在 22 个国家设有分公司/办事处
- 全球有 51 个国家的用户正在使用我们的产品

思科公司（Cisco System）于 2007 年 1 月 4 日发布了收购 IronPort 公司的最终协议，思科公司承诺保留两个公司的合作关系，并且共同寻求两个公司发展的市场策略。目前 IronPort 团队和全部产品线将作为思科安全技术团队（Cisco Security Technology Group）中的一个独立业务部门来运作。

IronPort 的技术专注于邮件安全和 WEB 安全，主要的产品是 C-Series 邮件安全网关和 S-Series 的 WEB 安全网关。

IronPort S 系列 Web 安全网关设备为企业提供的是业界最完善的网络周边防

护，能够有效防御各种间谍软件和基于 Web 的恶意软件。IronPort S 系列设备结合了高性能的安全平台 AsyncOS 和 IronPort 独有的 Web 名誉技术，以及 IronPort 突破性的动态导向和流线引擎(Dynamic Vectoring and Streaming engine, DVS)。DVS 是一种崭新的扫描技术，它能够同时支持多个第三方厂商的基于特征码的间谍软件过滤引擎。S 系列设备强大的管理和报表工具不但简化了系统管理，而且能为管理员提供关于安全威胁活动的完整视图。

2． Web 安全现状

对于广大的 Internet 用户来说，现在越来越多的受到来自 Web 的安全威胁，包括各种木马程序（Trojan），间谍软件（Spyware），广告软件（Adware），网络钓鱼（Phishing）在内的这些恶意软件（malware）问题，已经迅速发展成为企业所必须要面对的几个主要安全问题之一

根据 IDC 的统计，80%的企业用户电脑受到恶意软件的威胁，从 2000 年到现在，恶意软件的增长达到了 400%。而部署了网络周边间谍软件防御系统的企业却不到 10%。由于间谍软件和基于 Web 的恶意软件具有强大的变种能力和飞快的传播速度，其危害性日益严重，因此对企业来说，拥有一个强健的能够保护企业网络周边免受这些安全威胁侵害的安全平台就显得极为重要。

2006 年 11 月，CNNIC 正式公布了“恶意软件定义”，具有下列特征之一的软件可以被认为是恶意软件：

1）强制安装：指未明确提示用户或未经用户许可，在用户计算机或其他终端上安装软件的行为。

2）难以卸载：指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍然有活动程序的行为。

3）浏览器劫持：指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。

4）广告弹出：指未明确提示用户或未经用户许可，利用安装在用户计算机或其他终端上的软件弹出广告的行为。

5）恶意收集用户信息：指未明确提示用户或未经用户许可，恶意收集用户信息的行为。

6）恶意卸载：指未明确提示用户、未经用户许可，或误导、欺骗用户卸载其他软件的行为。

7）恶意捆绑：指在软件中捆绑已被认定为恶意软件的行为。

8）其它侵害用户软件安装、使用和卸载知情权、选择权的恶意行为。

3． 传统技术的缺陷

➢ 防火墙/IDS/IPS 设备

这些设备是企业用户普遍使用的网络安全设备，但是这些设备都是工作在网络层，而来自 Web 的恶意软件主要工作在应用层，仅仅通过分析 TCP 数据包是无法检测到恶意软件。

➢ 网站地址变化频繁

在 Web 域名飞速增长和频繁变化的今天，单纯的依靠域名过滤，难以完全解决来自 Web 的各种恶意软件，对于那些来自新申请域名的网站，难以及时和准确的发现那些带有恶意代码的 URL。

4． IronPort Web 网关系统架构

IronPort S 系列设备的设计集成了多种先进技术，其中包括四层(L4)流量监控和支持 HTTP、HTTPS 和 FTP 等多种协议的安全应用代理，以及一个先进的扫描和

导向引擎，为企业提供的是强大的具有最优性能和效用的 Web 安全平台。

4.1 专用操作系统

IronPort S 系列设备结合了多种先进技术，其中包括针对 Web 数据流的安全应用代理、一个第四层(L4)数据流监视器，以及 IronPort 动态导向和流线引擎™ (Dynamic Vectoring and Streaming engine™, DVS)，它帮助企业确保 Web 数据流的安全和控制 Web 数据流风险。DVS 引擎是一种为克服扫描 Web 事务和对象时遇到的独特挑战而全新设计的先进扫描和导向引擎。所有这一切为企业提供了一个强大的具有最优性能和功效的 Web 安全平台。

IronPort 通过硬件/软件的高度整合，设计开发了专用的 Web 安全系统平台：AsyncOS 操作系统。这个系统是基于 FreeBSD 的内核，针对 Web 业务的特点，专门开发了多项安全技术，大大提高了系统的高性能，高可靠性和安全性。

4.2 四层流量监控

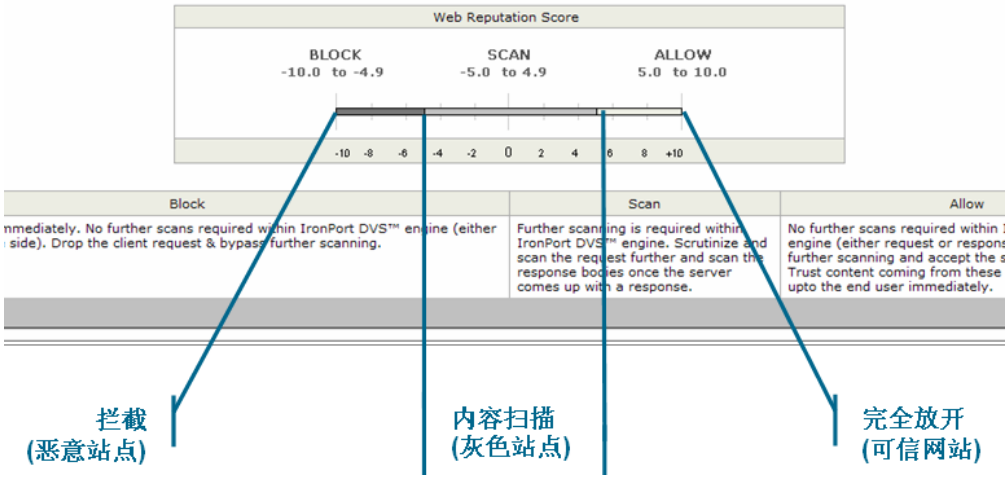
除了监控 http（80 端口）和 https（443 端口）外，IronPort Web 网关还可以监控 0-65535 的所有的应用端口，以检测和拦截恶意软件的“回连行为”（Phone Home）。通过配置交换机端口 Span 的方式，将所有客户端访问互联网的流量转发到 IronPort Web 网关上。Web 网关对这些流量进行扫描和分析，可以有效阻挡所有试图绕过“端

口 80”的恶意软件，并且还能够防止 P2P 和 IRC 的欺骗行为。

4.3 网站信誉过滤

IronPort S-Series Web 安全网关通过对网站 URL 的信誉评分，保护用户不受恶意 URL 网站的威胁。IronPort 利用独有的 SenderBase Network 数据库信息，通过对 URL 超过 50 个参数的分析，能够准确的给出 URL 的信誉得分，成为 Web Reputation Score（WBRS），从-10 到+10 用以标识网站 URL 的信誉度，并根据不同的信誉评分，设置不同的访问策略。

- WBRS [-10 ~ -5.0]：拦截
- WBRS [-4.9 ~ +4.9]：允许但扫描网页内容
- WBRS [+5.0 ~ +10]：完全放开



4.4 URL 网站地址过滤

随着互联网提供了越来越多的资源，方便了通信并提供了巨大的信息资源。互联网的访问在产生巨大生产力的同时，也带来了极大的法律风险。据 IDC 估计，企业中互联网访问流量的近 40%与业务无关，这对员工的生产率和网络资源造成了极

大的浪费和损失。此外，据估计，目前互联网的网页数量高达 100 亿（以每年近 30%的速度增长），无节制的浏览不可避免的会违反企业 IT 管理策略，有可能使公司承担严重的法律责任。

IronPort 的 URL 分类数据库，是目前最大最广泛最精确的数据库，数据库中包含了超过 52 个分类，2100 万网站和 35 亿个页面信息，并且能够提供 7*24 小时的维护和更新。在 S-Series 网关上，可以根据网站的类别，分别设置允许或者禁止的访问策略，并且能够根据企业的实际要求，设置例外的域名 URL 地址。

4.5 恶意软件拦截

IronPort S-Series 通过 DVS 引擎，提供了集成不同厂商提供的多种类型的特征码判定引擎的解决方案。目前 IronPort 网关提供了包括 Webroot 和 McAfee 的特征码判定引擎，能够及时发现对来自网站的各种恶意软件和病毒，并对其实施监控或拦截。所有引擎的判定都是自动进行，同时自动更新恶意软件代码库。

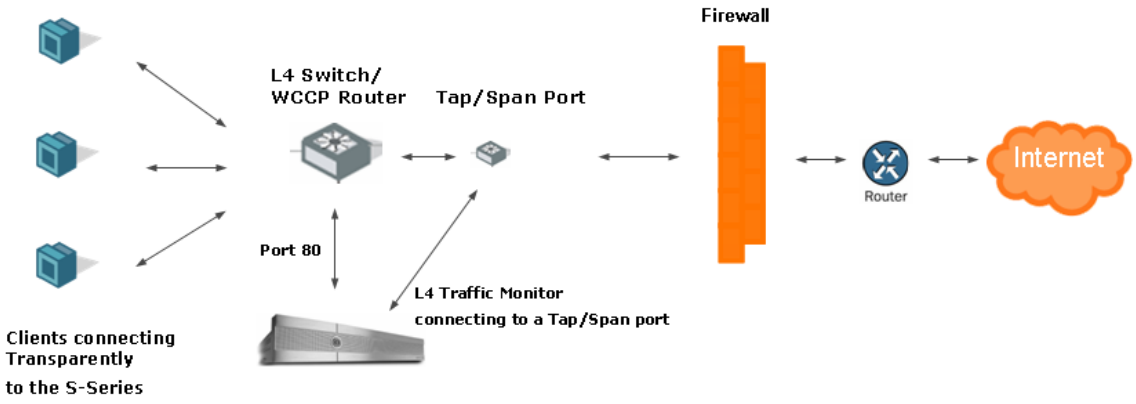
IronPort S-Series 的防恶意软件模块，能够扫描存在 HTTP 或 HTTPS 页面中的可执行代码，判断其属于病毒还是恶意软件，最终拦截下来所有的病毒和恶意软件，而正常的页面内容则返回给客户端。

IronPort DVS 引擎，即动态导向和流向引擎（Dynamic Vectoring and Streaming Engine），其主要技术特点包括：

- 快速的对象定位与分析
- Stream 流扫描技术
- 动态分析快速识别
- 基于信誉评分的定位扫描

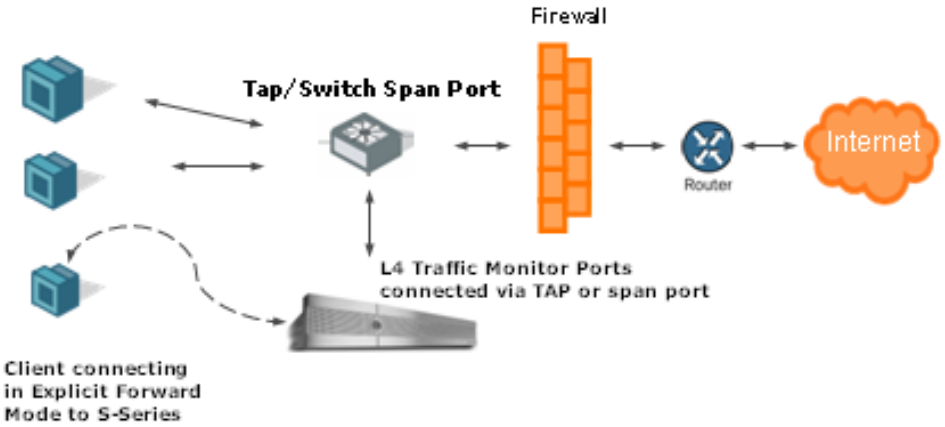
5． 部署模式

5.1 透明代理方式



IronPort Web 安全网关部署在 L4 交换机或者 WCCP Router 的前端。用户端浏览器不做任何修改。所有从客户端发出的 HTTP 请求，经过 L4 交换机或 WCCP 路由器后，直接将其转发给 S-Series 网关，再由网关向 Web 服务器发出 HTTP 的请求。

5.2 客户端代理方式



在这种模式下，所有的客户端浏览器都要配置 Proxy 服务器。配置的方式包括：

- 自动 proxy 配置；
- 手工 proxy 配置；
- Proxy 脚本配置；

6． Web 安全网关的功能特点

IronPort S 系列设备是业界开创先河的，同时将传统的 URL 过滤，Web 网站信誉过滤和恶意软件过滤等功能集中在一台设备上实现。通过同时应用这些技术，IronPort S 系列设备能够帮助企业在 Web 访问管理以及控制 Web 访问风险方面，应对日益严峻的挑战。

多种先进技术相结合的产物，其中包括四层(L4)流量监控和支持 HTTP、HTTPS 和 FTP 等多种协议的安全应用代理，以及一个先进的扫描和导向引擎，为企业提供的是强大的具有最优性能和效用的 Web 安全平台。

6.1 高速代理

能够进行深入的内容分析，而这对于要想准确地检测出那些不断进化和变异的基于 Web 的恶意软件来说是至关重要的。由于其幕后的支撑力量是 IronPort 专有的 AsyncOS 操作系统，因此该代理可以轻松地同时支持多达 10 万个 TCP 连接，这足以确保即使是最大型的企业网络也始终能够拥有最高的性能和吞吐能力。

AsyncOS 的主要性能参数包括：

- TCP 并发连接数支持 100000 个
- HTTP 每小时事务数达到 500~700 万（满负荷状态）

- 平均延迟时间 5~15 毫秒

6.2 用户访问安全策略

（1）集成用户认证

IronPort S-Series 能够和系统中现有的用户数据库集成，要求用户必须通过身份验证后，才被允许访问互连网。集成的用户认证方式包括：

- 基于 LDAP 的身份验证，如 Active Directory 等。
- 基于 NTLM 的身份验证

（2）分组策略管理

IronPort S-Series 能够按照 LDAP 的用户属性和 IP 地址进行分组，针对不同的组别，可以设置不同的访问策略，这些策略包括应用程序访问管理，URL 过滤，防恶意软件系统等。

- 根据单个用户或组设定策略
- 多种动作选择：监控和拦截
- 用户通知页面定制

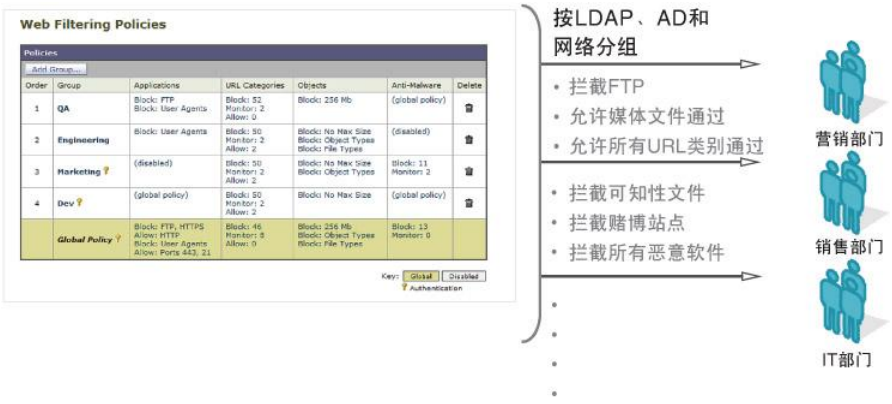
6.3 完善的监控和报表

6.3.1 Web 安全管理器

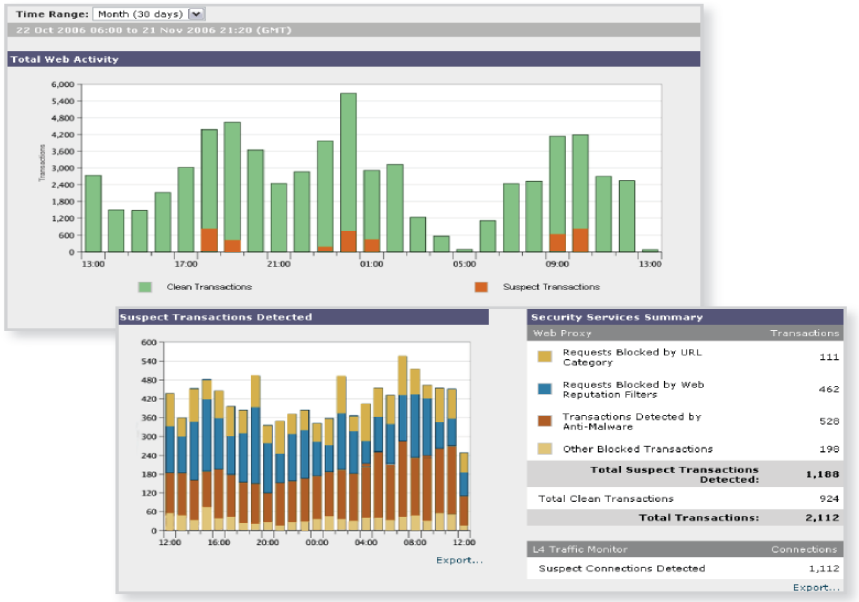
IronPort Web 安全管理器（Web Security Manager）能够为设备上所有的过滤服务提供精确的选项，并按照已验证和未验证用户类别，提供丰富的配置选项。

管理人员可以在 Web 安全管理器完成所有的 Web 访问策略的设置，包括 URL 过滤、Web 信誉过滤和恶意软件过滤。同时，管理员还可根据用户或用户分组来创

建不同的策略。



对企业网络内部的 Web 活动、威胁的识别和预防情况，Web 安全管理器以在线(on-box)或离线(off-box)提供了可以为管理人员设置策略提供依据的信息，以及这些 Web 活动的历史趋势。通过这些报表信息，还可以清楚地看到违反策略管理和安全需求的图表视图。



6.3.2 多种部署模式

支持手工代理和透明代理等多种模式，具备了足够的灵活性。可以以浏览器方

式设置代理，或是以网络的四层交换机或路由器 WCCP 的透明部署方式。在这些代理模式下，IronPort Web 网关既可以独立存在，也可以和其他代理设备共存。

6.3.3 SNMP 企业管理信息库

通过提供 SNMP 的支持，实现对包括硬件、性能和可用性在内的所有关键系统参数实现无人值守的监控。企业级的 SNMP Enterprise MIB 确保了对所有参数的监管，其中包括硬件、安全、性能和可用性。

通过 LDAP（如 Active Directory）实现的用户身份集成认证，加上实施多种认证方案(如 NTLM)的能力，使企业能够无缝地部署 IronPort S 系列设备，并充分利用企业网络中原有的认证和访问控制策略。

6.3.4 详尽的日志

Web 网关提供了详细的日志信息，使企业能够跟踪并记录所有的 Web 数据流，包括与无害或与恶意软件有关的数据流。标准的日志格式包括 Apache、Squid 或 Squid-detailed 等，另外还支持客户自定义日志格式，以便与企业日志政策保持一致。管理员可以根据日志类型来启用或禁用日志订阅功能，或者设置日志订阅，或者设置日志的回滚和尺寸限制等等。

7． 产品优势

7.1 安全集中控制

通过 IronPort S 系列网关单台设备，确保了企业网络安全和控制企业网络所面临的三大 Web 数据流风险，即安全风险、资源风险和合规性风险。

IronPort 为了应对各种基于 Web 的恶意软件带来的威胁，全新设计了 IronPort S 系列设备。这种多层防御体系包括 IronPort URL 过滤器、IronPort Web 声誉过滤器以及 IronPort DVS 引擎中多种类型的恶意软件特征码，从而能够确保其准确率业界领先。

IronPort S 系列多层防护基于对内容应用的深入检查以及网络层的模式检测，既查验进站活动，也查验出站活动。 这些创新使 IronPort S 系列设备防护成为了业界最准确地反恶意软件解决方案。

7.2 降低风险和成本

由于多达 75%的公司电脑感染了恶意软件，因此需要花相当高的成本去管理受感染的电脑，使最终用户的停机时间和信息泄漏的风险降至最低。

利用 IronPort S 系列设备将这些威胁拒之于网络之外，企业可以极大地降低管理成本，阻止恶意软件的“回连”行为（phone-home）通信活动，减少支持呼叫，提高工人的生产力，并且还可以消除伴随这些威胁而来的商业泄密。

7.3 Web 访问安全策略

IronPort Web 网关通过制定用户访问 Web 策略，企业能够监控员工的 Web 行为，而且还能培养对风险的防范意识和强化防范风险的教育。企业可以增加员工从事与职责相关业务活动的时间，从而减少对企业网络和带宽的浪费和误用。

IronPort S 系列设备可以提供实时和历史的安全信息，使管理员能够迅速掌握

Web 数据流的活动情况。实时报告功能让管理员在违反用户访问策略和违反安全要求等问题出现时可以及时发现和追踪，而历史报告功能则有助于管理员分析安全趋势，并得出系统功效和投资回报情况的报告。

7.4 企业级性能

实时 Web 数据流扫描一直以来都存在性能低下和高延迟等问题。因此，以往企业都尽量避免在 HTTP 层上部署基于特征码的保护系统。IronPort S 系列设备能够满足 Web 数据流扫描的独特需要，因此可以确保带给最终用户的体验不会降低。IronPort 的性能（AsyncOS 中的技术创新，包括 TCP 连接管理、基于声誉的缓存和自适应对象存储），确保了它是一个能够满足最大型企业容量要求的平台。

7.5 降低总体成本

传统代理服务器基于 ICAP 的解决方案，通常需要多台设备或者服务器来确保 Web 数据流安全和控制 Web 数据流安全风险、资源风险和合规风险的问题。与其它解决方案不同，IronPort S 系列是一个单一平台，提供全面深入的防护能力和必要的管理工具，因此极大地降低了初始和后续的拥有总成本。

最大限度地降低管理开销是 IronPort S 系列设备的设计初衷。为此，IronPort S 系列设备提供了便捷的利用直观的图形用户界面进行设置和管理的功能，支持自动升级，还提供全面的监视和报警功能。该解决方案可以方便地根据公司具体的政策进行部署和配置。

7.6 总结

在确保企业 Web 数据流安全和控制 Web 数据流风险方面，所面临的挑战日趋严峻而且在不断变化。由于基于 Web 的恶意软件和间谍软件的发展速度十分惊人，直接给大量的企业造成了停机和生产力损失，对企业的 IT 资源也是一个极大的负担。因此，企业网络面临着实实在在的风险，企业必须掌握其员工正在何时、何地和以何种手段使用 Web。另外，如果企业网络遭到恶意软件的入侵，企业也将随时处于违反合规性检查和数据保密规范的风险之下，而这种违规行为一旦造成泄密，其代价将非常高昂。同样，对于那些遭到间谍软件和恶意软件入侵的企业，它们的关键业务数据和知识产权资产也随时可能被不法分子窃取。

要想控制和防范 Web 数据流带来的这些风险，最好在企业网关进行。通过 Web 代理和第四层数据流监视器，将 Web 数据流政策和深入的应用内容检查相结合，能确保企业的网络得到最完善的保护。该解决方案将 IronPort Web 声誉过滤器和 Webroot/McAfee 提供的多种恶意软件特征码集成在 IronPort 的 DVS 引擎和 IronPort URL 过滤器之中，从而在检查可疑 Web 数据流的准确性方面居业界领先。随着面临的威胁日趋复杂，IronPort S 系列为企业提供了业界最全面的 Web 安全解决方案，同时确保实现企业级的性能。