IBM ISAM

Web 安全保护解决方案建议书

目 录

摘要

我们对您的目标的理解

企业的兼并、发展、壮大和合规的考核，使企业面临对用户身份和访问的整合、管理、审计问题。如何规范企业用户、账号管理流程；如何集中管理系统资源和应用系统的账号，包括授权；如何解决单点登录问题；如何对特权用户的操作行为进行控制和审计；如何防御针对 Web 应用的攻击行为……

IBM 解决方案

- **ISAM 硬件设备+ ISIM 许可**
- 以 IBM Security 商业软件针对网络、主机、应用等基础平台提供**帐号管理和单点登录**；
- **强认证：**能整合多种认证方式，实现多种方式的强认证，增强企业信息平台的安全性；
- **特权账号管理：**针对网络设备、主机及数据库系统的特权账号实现全面的申请、授权、监控、收回等管理；
- **多纬度授权模式：**符合企业内分级管理，分级授权的管理模式
- **集中审计：**生成用户审计报表，帮助企业实现合规要求；
- **Web 应用的入侵防御模块：**入侵防御、人员控管多角度提高 web 应用安全性；
- **灵活的 API：**定制用户自己的管理平台，符合国内用户灵活性的需求；
- **易于整合：**能整合其它网络和安全管控平台，保持用户体验的一致性和规划的完整性。

为什么选择 IBM

与竞争对手相比，IBM 能够提供：

- 更简单的配置和更好的扩展性和高可用性；
- 原厂的负载均衡和 Web 入侵防御系统；
- X-Fore 支持；

第1章　我们对您的目标的理解

当前，为业务关键型应用程序提供安全访问变得空前复杂，因为今天的 IT 环境已然包括合作伙伴、客户、社交媒体网站、云计算部署和移动终端等多种元素。同时，保护敏感信息和商业资产变得越来越重要。先进的网络威胁和持续增加的网络欺诈发生率迫使企业设法保护用户访问和 web 应用的安全。企业必须寻求有效的解决方案防御先进的网络威胁以及与移动、社交和云的访问相关的风险，同时保证安全合规。他们还需要极其安全的访问管理，使员工、客户和合作伙伴能够安全地访问网络资源。

在这复杂的、基于 web 的世界，防御先进的网络威胁和持续增加的网络欺诈行为、保护 web 安全成为首要任务和挑战。

我们已经确定了以下关键转变，推动今天的现实。

- 越来越多的业务是通过互联网进行，并使用基于 web 的应用程序。
- IT 环境越来越复杂，必须适应合作伙伴、客户、社会媒体网站、云计算部署和移动终端。
- 伴随访问需求的增加，来自黑客和恶意软件的威胁花样繁多，而任何一次成功的攻击都可以对其目标造成破坏性影响。
- 部署安全解决方案的复杂性正在增长。
- 越来越多的组织正在应对业务关键型应用程序，以及在扩展的企业环境中不断蔓延的数据。
- 政府颁布了比以往更多的信息安全法规。

这一新的现实带来了新的挑战。

- 更多移动、云计算和 web 访问会导致更先进的网络威胁和更多的网络欺诈发生。有一支世界性的黑客队伍在伺机发掘与 web 应用程序相关的漏洞。
- 企业需要保护和授权合法用户访问 web 应用程序。
- 企业需要防御先进的网络威胁和与移动、社交和云的访问相关的风险，同时保证安全合规。

- 企业需要快速、轻松地部署可以保护其资产和业务安全的解决方案，同时减少 web 安全管理的复杂性和成本。

因为这些变化和挑战，企业需要以不同的方式来思考和工作。

- **他们需要不同的计划方式。**

基于 web 的应用程序使用的增长，将继续为简化业务和增加受众提供机会，但它也为黑客和恶意软件提供了可攻击的漏洞。IT 组织必须做出长期的 IT 计划，旨在帮助防御先进的网络威胁和欺诈。这些计划应该包括保护和授权合法的用户访问 web 应用程序。

- **他们需要不同的购买方式。**

今天的购买决策必须考虑许多因素。企业除了需要 web 安全保护，还需要易于部署和可以帮助降低 IT 管理成本的解决方案。

- **他们需要不同的部署方式。**

为提供可以使用户能够安全地访问云、移动和企业门户资源的安全的访问管理，企业需要部署结合了用户访问和 web 应用保护的解决方案。同时，为主动的保护 web 安全、准确地防御最新的威胁，该方案还必须可以简化安全管理、降低运营成本、保证安全合规，并且在未来数年可以抵御最新的威胁。

第2章　ISAM Web 安全保护解决方案介绍

2.1 方案概述

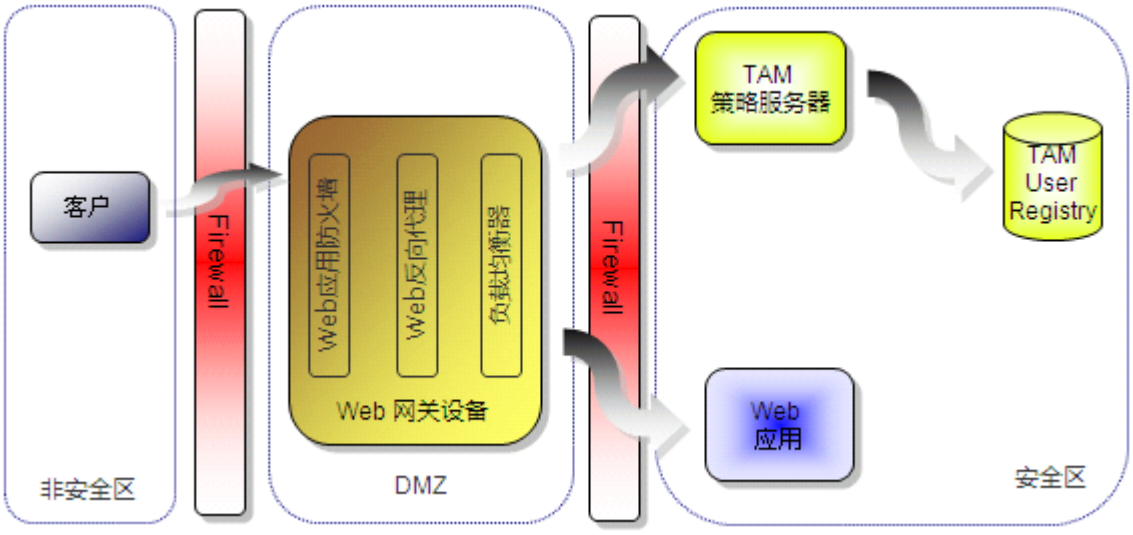
IBM Security Access Manager（ISAM）可以帮助您管理增长和复杂性、控制不断增加的管理成本并处理涵盖广泛的 Web 和应用资源安全策略实施上的困难。它的工作原理是通过集中管理安全性和可前置的 Web 应用程序代理的审计策略执行点，或通过授权和身份验证插件直接进入一个 Web 服务器或应用程序服务器环境。通过 ISAM，任何访问 Web 应用程序的用户都受益于网络的单点登录，以及高可用性和在线应用程序的安全访问。

ISAM 为您提供：

- 企业内部和（配合 Federated Identity Manager Business Gateway（联合身份管理器企业网关））跨业务单位支持的安全会话管理能力。
- 支持强大的身份验证，一旦实施，无需逐个应用程序的进行身份验证。
- 可直接使用，为业务应用程序打造的以策略为基础的安全保护，如客户关系管理（CRM），企业对企业（B2B），企业对客户（B2C），和员工门户网站。
- 可扩展性，高可用性和高性能，在一个单一系统实施里支持多达百万计的用户。
- 为业务单位和联营公司打造灵活的基于 Web 的分布式管理和多级委托功能。
- 一个可完全利用的、可扩展十亿的用户的注册表，也可以根据客户的标准替换成其他主要注册表

2.2 方案架构

如下图所示，ISAM 方案将 WebSEAL 反向代理功能与前端负载均衡设备、Web 应用防火墙组合，提供抵御 Web 访问威胁的访问控制和防护。



图：ISAM 架构

2.3 方案产品

ISAM 方案的产品包括硬件和软件及虚拟设备：

- IBM Security Access Manager for Web V7 （软件和虚拟设备）—— **保证用户访问、web 应用和数据安全**
- IBM Security Web Gateway AMP 5100 Appliance V7 （硬件）——**集成 Web 应用安全防护的新一代的 Web 访问管理解决方案**

2.4 方案部署模式

通过混搭，我们为本方案提供高度可配置的三种部署模式：

1) 独立设备模式

2) 分布式设备模式

3) ISAM for Web software

图：ISAM 的部署模式

2.5 方案产品（ISAM 7.0 和 Web Gateway AMP 5100）介绍

2.5.1 ISAM 7.0 的新功能

ISAM 7.0 版是 IBM Tivoli Access Manager e-business 6.1.1 版的后续版本。V7 更新了许多现有的功能，并引入了新的功能和反向代理（WebSEAL）组成部分的虚拟和物理设备。

ISAM V7.0 更新了现有功能：

- 支持 64 位（将不再支持 32 位）
- 增强的 Web 应用程序集成
  - Microsoft Outlook Web Access（与 HTTP 相较，支持 Microsoft RPC）
  - 供跨浏览器和非浏览器 MS Office 客户的共享 WebSEAL 会话
  - 增强了对 Web 2.0/AJAX 应用的支持
- HTTP 反向代理（WebSEAL）的改善
  - 自定义本地响应重定向域名
  - HTTP 转换规则（HTTP headers、URI 和方法的修改）
  - 简单的 SSO 跨虚拟主机，能够跨多个虚拟结点共享会话
  - 单点关闭退出
- 符合 NIST 标准 - SHA256 与 TLS1.2 支持
- 易于部署

- WebSEAL 配置文件跨 WebSEAL 集群间的自动传播（WebSEALs 具有同样的高可用性或负载平衡）
- 用于 Access Manager Policy Server（pre-reqs Tivoli System Automation Manager 产品）的增强的高可用性选项
- 允许多个授权服务器在同一台机器上
- Java 运行时间的灵活配置

❖ 可维修性改善

- 用于会话管理服务器的、更精细的跟踪粒度
- 用于 WebSEAL 的、增强的启动错误消息
- 用于策略服务器的动态跟踪控制
- 在 WebSEAL 内的跟踪响应时间的能力

通过设备，ISAM 也提供了新的功能。这个设备以虚拟和实体的形式提供。

2.5.2 IBM Security Web Gateway Appliance

IBM Security Web Gateway Appliance (产品型号 = AMP 5100, 产品编号 = 5122-81K)

设备概述

Access Management Proxy（AMP5100）是为 Web 应用程序提供访问、认证和会话管理及保护应用程序免受外在威胁而设计的。 AMP5100 设备提供了一个基于代理的解决方案，它位于用户和 Web /应用程序的服务器之间。AMP5100 具有高可扩展性和可配置性，支持多种应用环境。

设备优势

以下是设备部署相较于运行作为标准软件安装的 WebSEAL 的主要的优势。

设备包装和维护简化了部署，并降低生命周期管理成本

- 预装包被作为包括操作系统和所有的固件的必备软件提供。这意味着你不需要单独管理操作系统和必备补丁（例如 GSKit, Access Manager’s cryto toolkit）
- 该产品为自动更新服务和威胁定义提供支持。
- 快照功能捕捉你的配置，并支持备份您的图片。
- 回滚至以前版本的固件，可以快速恢复以往的配置。
- 支持文件可以简单的用设备创建，捕获关键日志及跟踪需要解决支持问题。
- 具有合并一定数量的、现有的部署反向代理服务器的能力。

Web 图形化用户界面

新的 Web 图形化用户界面提供了一个可以显示连接到设备的工作量和响应时间的整体健康（从性能和可用性透视图）状况的仪表板。

Web 应用程序保护

AMP5100 设备包含 IBM Security Intrusion Protection 原始记录分析模块。由 X-Force 提供动力，该模块可配置用于扫描针对 Web 应用威胁的传入和传出 HTTP 请求。定期更新以防范 X-Force 团队发现的新威胁。结合安全访问管理器代理和该模块，所有 HTTP 流量都可以被扫描并阻止任何检测到的威胁，防止这些威胁访问应用程序服务器。

负载平衡

AMP5100 设备提供前端和后端的负载平衡。前端的负载平衡器在传输层工作（TCP），网络流量可以在多个设备以及跨越多个 WebSEAL（设备）间路由。除了分发负载，还可以为设备提供高可用性。如果其中一组的设备出现故障，流量可以自动路由到其他设备。前端负载均衡器可制作成高度可用的。

后端负载均衡器可以跨后端 Web 和应用服务器分散流量。它和 WebSEAL 会话管理机制同时集成，并能根据用户的会话保持粘性。

管理界面

AMP5100 设备提供了基于 Web 的图形化管理界面，称为本地管理界面（LMI）。此界面提供了配置设备和安全反向代理服务器的能力。Web 界面还提供了一个使管理员能够查看的设备的整体健康状况的仪表板。

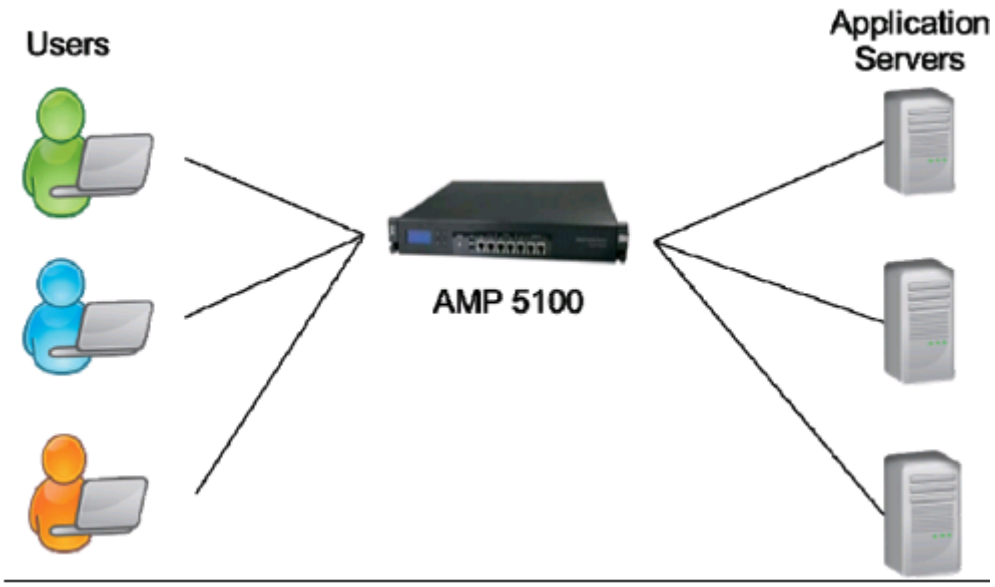
由设备提供 Web 服务界面可使它能够编程交互。

命令行界面可用于执行管理任务的一个子集。

设备部署

AMP5100 设备通常会被部署在 DMZ 中，所有传入和传出的 HTTP 的流量将通过设备路由。该设备可以部署在两种模式下，单机和互联的。

1）**单机模式：**在这种模式下，AMP5100 设备不需要任何一个单独的 IBM Security Access Manager Policy Server 或用户注册表，如有需要，可以使用外部 LDAP 注册表。每个设备都将包含它自己的策略并提供验证和授权，为 Web 应用程序提供单点登录，为用户会话提供会话管理。



该设备为管理员身份的定义提供本地目录。这个设备也可以被连接到一个远程 LDAP 服务器。

管理员可以用标准的 pdadmin 命令行界面定义访问管理策略。策略定义包括服务器任务命令（如：结点管理），用户管理命令和策略管理（ACL/ POP）。

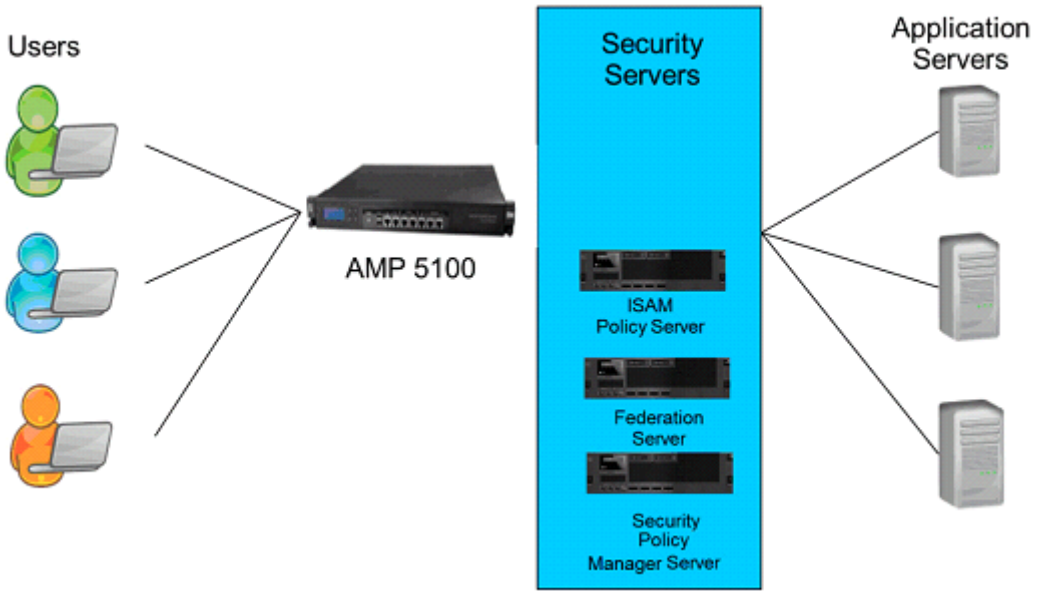
这些功能是在设备上的，并且不需要一个单独的服务器。

2）**互联模式：**在该模式下，AMP5100 设备可以连接到外部安全服务器，并提供额外的功能。

A. IBM Security Access Manager Policy Server 可以为如联合单点登录，基于风险的访问，细粒度访问控制和权限管理的额外访问管理功能提供支持。

B. IBM Federated Identity Manager 提供跨多个应用程序的、至终端用户的 Web 和 Federated 单点登录（SSO）。基于浏览器的集成和开放标准，它可以快速提升用户的工作效率、用户体验以及减少管理成本。Federated Identity Manager 也提供基于内容和风险的访问控制，使设备属性和用户访问属性能够在访问策略中被考虑到。多因素验证可以被调用来确保最终用户正确的身份验证，尤其是在移动和云的部署。

C. IBM Security Policy Manager 集中安全策略管理和应用程序、数据库、门户网站及服务的细粒数据访问控制。Security Policy Manager 可以提供中央策略的管理和定义，包括风险为基础的策略。



2.6 IBM 方案价值

- 软硬一体的单点登录设备(ISAM)：
  - 开箱即用，快速部署
  - 高性能减少性能瓶颈
  - 易于安装配置和运行维护
- 用户帐号的全生命周期管理，帮助企业实现合规要求
- 特权账号管理避免特权账号滥用，减少敏感数据泄漏风险

第3章　为什么选择 IBM

IBM 拥有世界上规模最大的安全研发和交付机构，每天监控 130 多个国家超过 130 亿个安全事件，并持有 3,000 多项安全专利。IBM Security 可提供最先进的集成式企业安全产品和服务组合之一。该组合由世界知名的 IBM X-Force® 研发团队提供支持，提供充足的安全智能，以身份和访问管理、数据库安全、应用程序开发、风险管理、端点管理、网络安全及其他各方面的解决方案，帮助企业全面保障其人员、基础架构、数据和应用程序的安全。这些解决方案可帮助企业有效管理风险，并针对移动设备、云平台、社交媒体及其他企业业务架构实施集成式安全解决方案。

ISAM Web 安全解决方案与竞争对手的方案相比，IBM 能够提供：

- 更简单的配置和更好的扩展性和高可用性；
- 原厂的负载均衡和 Web 入侵防御系统；
- X-Fore 支持；

同时 IBM，IBM 在该领域保持着领先地位：

- **Leader (2012 - #1 in Identity and Access segment)** IDC Analyze the Future
- **Access Mgr. 2011 Gartner MQ “Leader”** Gartner

此外，IBM Global Financing 可以帮助您以最经济高效和最具策略性的方式获得您企业所需的软件功能。 我们将与符合信用要求的客户合作以定制最适合其业务与发展目标的融资解决方案，实现高效的现金管理，并降低其总拥有成本。 IBM Global Financing 可为您的重要 IT 投资筹措资金并推动业务向前迈进。