

Cisco Catalyst 6500 系列入侵检测系统 (IDSM-2) 服务模块

思科的集成化网络安全解决方案让机构可以保护生产率成果和降低运营成本

Cisco IDSM-2 是思科入侵检测系统的组成部分。它可以与其他组件合作，有效地保护您的数据基础设施。随着安全威胁的复杂性的日益提高，实施有效的网络入侵安全解决方案对于确保高水平的安全保障至关重要。高水平的安全保障可以确保业务连续性，最大限度地避免入侵可能造成的巨额损失。

如需了解关于整个思科入侵检测系统的信息，请访问：www.cisco.com/go/ids。

思科的集成化网络安全解决方案让机构可以防止他们的联网业务资产受到威胁，提高入侵防范的效率。这些解决方案中包括第二代思科入侵检测系统 (IDS) 模块，即 IDSM-2，它可以用在广泛部署的 Cisco Catalyst 系列设备上。Catalyst 系列设备的装机量已经达到数十万台，它是包括防火墙、虚拟专用网 (VPN) 和入侵检测系统 (IDS) 服务在内的附加服务的理想平台。由于认识到这种方式的价值，思科推出了这个第二代模块，以便为那些寻求 IDS 攻击防范的客户提提供独特的优势。

图 1 Cisco IDSM-2



特性和优点

Cisco IDSM-2 可以提供下列特性和优点：

- 思科是唯一可以提供一个交换机内置 IDS 解决方案的厂商，这种解决方案可以通过 VLAN 访问控制列表 (VACL) 获取功能来提供对数据流的访问权限。VACL 可以支持无限个 VLAN。



- 通过被动的、综合的操作提供透明的操作。这种操作方式可以通过 VACL 获取功能和交换机端口分析工具/远程 SPAN (RSPAN/SPAN) 检测分组的复本，而且如果设备需要维护，因为它并不位于交换机转发路径上，因而它不会导致网络性能降低或者中断。
- 体积只占一个机架单元，在 Cisco Catalyst 设备中只占用一个插槽，从而使它成为能够有效地支持所有 Catalyst 设备（从有三个插槽的 Catalyst 6503 到这个系列中最大的设备）的平台，并让用户可以根据自己的需要，同时安装多个模块，为更多的 VLAN 和流量提供保护
- 每秒 500Mb (Mbps) 的 IDS 检测能力可以提供高速的分组检查功能，让用户可以为各种类型的网络和流量提供更多的保护
- 多种用于获取和响应的技术，包括 SPAN/RSPAN 和 VACL 获取功能，以及屏蔽和 TCP 重置功能，从而让用户可以监控不同的网段和流量，同时让产品可以采取及时的措施，以消除威胁
- 使用与曾获大奖的 Cisco IDS 网络设备相同的程序代码，让用户可以将单一的管理技术作为标准，并让安装、培训、操作和支持变得更加便捷，同时可以利用 Cisco IDS 的全面的攻击识别能力和特征库
- 重要的管理技术（例如 Cisco VMS 2.1 安全产品包提供的支持，以及内置的 Cisco IDS 设备管理器 (IDM)、IDS 事件浏览器 (IEV) 本地管理功能和 CLI 支持）让 IDSM-2 更加便于管理，更加善于检测和响应威胁，同时就潜在的攻击向管理人员发出警报。此外，这个新的产品还让管理人员可以更加方便地在范围广泛、多样化的网络上管理多个设备

技术规格

Cisco IDSM-2 编号

WS-SVC-IDS2-BUN-K9

Cisco IDSM-2 服务编号

CON-xxxx-WS-IDSM2-K9

编号中的“xxxx”表示：

- SNT=8×5×下一个工作日
- SNTE=8×5×4 小时服务
- SNTP=24×7×4 小时服务
- OS=8×5×下一个工作日
- OSE=8×5×4 小时现场服务
- OSP=24×7×4 小时现场服务



机型

单机架单元模块，占用 Cisco Catalyst 6500 机箱中的一个插槽

LED 和开关

单一指示器（LED）

- 关闭—没有上电
- 黄色—启动/待机
- 绿色—应用正在运行
- 红色—已经确定模块故障的位置

在从机箱中卸载该模块之前，必须使用关机开关。

热插拔需求

在卸载之前需要关闭该模块。

插/拔模块不会对 Cisco Catalyst 交换机造成任何影响。

处理器

主板上装有 Pentium 1.13 GHz 处理器，加速器上装有 IXP 处理器

操作系统

Red Hat Linux 6.2

每个机箱最多可以安装的模块数量

每个机箱可以安装无限多个模块

流量获取方式

VACL 获取

SPAN

RSPAN



最低的软件版本

4.0 版

特性:

- TCP 重置
- IP 记录
- SME (Signature Micro Engine)
- IDM
- NTP 同步
- 本地 CLI (命令行接口)
- 性能提升

Catalyst Supervisor 软件需求

Catalyst OS 7.5(1) (最低)

自带 Cisco IOS 软件版本 12.1(19)E

装有 IDSM-2 的 Catalyst Supervisor 硬件选项

采用 Catalyst OS 7.5(1): Supervisor Engine 1A

- Supervisor Engine 1A/PFC2
- Supervisor Engine 1A/MSFC1
- Supervisor Engine 1A/MSFC2
- Supervisor Engine 2
- Supervisor Engine 2/MSFC2

采用自带 Cisco IOS 软件版本 12.1(19)E:

- Supervisor Engine 2/MSFC2

性能指标

- 对 450 字节的分组的处理能力为 600Mbps
- 每秒最多可以支持 5000 个 TCP 连接 (新到达)
- 最多可以支持 50 万个并发连接
- 100% 警报率
- 在 Cisco Catalyst 机箱中添加 VLAN 或者设备不会对 Catalyst 的性能造成任何影响
- 支持矩阵



VLAN 最大数量（802.1q 标签）

无限

故障切换保护

IDS-2 是一个被动设备，在发生故障时不会对 Cisco Catalyst 设备造成任何破坏性影响。

管理

IDS-2 中内置 Cisco IDM 和 IEV。

- Cisco IEV 的基于 PC 的配置管理器（3 个设备）
- Cisco IDM 内置 Web 浏览器（1 个设备）
- 带有安全监视器的 Cisco VMS 2.1 和 IDS 管理中心 v1.1（至少 20 个设备）

物理尺寸

在 Catalyst 6000 机箱中占用一个插槽，用户可以根据需要添加任意数量的 IDS-2 模块

高度：3.0 厘米（1.2 英寸）

宽度：35.6 厘米（14.4 英寸）

长度：40.6 厘米（16 英寸）

重量：2.27 公斤（5 磅）

工作环境

工作温度：0 到 40°C（32 到 104.5°F）

非工作温度：-40 到 70°C（-40 到 158°F）

工作相对湿度：10%到 90%（非冷凝）

非工作相对湿度：5%到 95%（非冷凝）

工作和非工作高度：海拔 3050 米（10000 英尺）



认证机构

电磁辐射性

FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS/NZS 3548 Class A, VCCI Class A with UTP cables, EN55022 Class B, CISPR22 Class B, AS/NZS 3548 Class B, VCCI Class B with FTP cables

安全性

CE marking according to UL 1950, CSA 22.2 No. 950, EN 60950, IEC 60950, TS 001, AS/NZS 3260

出口限制

Cisco IDSM-2 属于“高度加密”产品，受到出口限制。如需了解相关细节，请访问：

<http://www.cisco.com/wwl/export/crypto/tool/>

其他信息

如需了解更多关于 Cisco Catalyst 6500 交换机的信息，请访问：

<http://www.cisco.com/go/6000>

如需了解更多关于思科安全入侵检测系统的信息，请访问：

<http://www.cisco.com/go/ids/>

思科在你身边 世界由此改变



思科系统 (中国) 网络技术有限公司

北京

北京市东城区东长安街一
号东方广场东一办公楼
19-21层

邮政编码: 100738

电话: (8610) 65267777

传真: (8610) 85181881

广州

广州市天河北路 233 号中信
广场 43 楼

邮政编码: 510620

电话: (8620) 87007000

传真: (8620) 38770077

上海

上海市淮海中路 222 号力宝
广场 32-33 层

邮政编码: 200021

电话: (8621) 33104777

传真: (8621) 53966750

成都

成都市顺城大街 308 号冠城
广场 23 层

邮政编码: 610017

电话: (8628) 86758000

传真: (8628) 6528999

如需了解思科公司的更多信息, 请浏览 <http://www.cisco.com>

2002 年思科系统 (中国) 网络技术有限公司北京印刷, 版权所有。

2002©思科系统公司版权所有。该版权和/或其它所有权利均由思科系统公司拥有并保留。Cisco, Cisco IOS, Cisco IOS 标识, Cisco Systems, Cisco Systems 标识, Cisco Systems Cisco Press 标识等均为思科系统公司或其在美国和其他国家的附属机构的注册商标。这份文档中所提到的所有其它品牌、名称或商标均为其各自所有人的财产。合作伙伴一词的使用并不意味着在思科和任何其他公司之间存在合伙经营的关系。