

Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列互联网路由器的防火墙服务模块

Q. 什么是防火墙服务模块?

A. 防火墙服务模块 (FWSM) 是一个 Catalyst 6500 系列多千兆位防火墙模块。FWSM 是一种支持交换矩阵的模块, 可以与总线和交换矩阵进行交互。FWSM 可以在 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列互联网路由器中提供状态防火墙功能。

Q. FWSM 主要具有哪些特性?

- A. FWSM 的主要特性包括:
- 高性能, OC-48 或者 5 Gbps 吞吐量, 全双工防火墙功能
 - 具有整个 PIX 6.0 软件功能集和 PIX 6.2 的下列特性:
 - ◆ 命令授权
 - ◆ 对象组合
 - ◆ ILS/NetMeeting 修正
 - ◆ URL 过滤改进
 - 3M pps 吞吐量
 - 支持 100 个 VLAN
 - 一百万个并发连接
 - LAN 故障恢复: 主从备份模式, 设备内部/设备之间
 - 利用 OSPF/RIP 进行动态路由
 - 每个机箱支持多个模块

Q. 防火墙服务模块 (FWSM) 和 Cisco PIX 防火墙之间有何不同?

A. FWSM 是 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列互联网路由器的一种集成模块——与独立的 Cisco PIX 防火墙不同。FWSM 建立在 Cisco PIX 技术的基础之上。

Q. FWSM 运行的是什么操作系统?

A. FWSM 和 Cisco PIX 防火墙运行的操作系统都是实时操作系统 Finesse。Finesse 是一种真正的微核系统, 能够提供可重复使用的软件、便于移植的源代码, 并可以提高产品质量, 减少测试次数, 缩短产品上市时间, 提高投资回报。

Q. FWSM 用什么机制检测流量?

A. FWSM 使用与 Cisco PIX 防火墙相同的检测算法: 自适应安全算法 (ASA)。ASA 是一种状态检测引擎, 可以检测流量的完整性。ASA 可以使用源和目的地的地址和端口、TCP 序列号, 以及其他 TCP 标志, 散列 IP 报头信息。散列的作用相当于指纹, 即创建一个独特的代码, 表明建立输入或者输出连接的客户端的身份。

如需查看更多的 ASA 文档，请接入：

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/config/intro.htm

Q. Cisco PIX 防火墙和 FWSM 的特性有何区别？

A. FWSM 支持 Cisco PIX 防火墙 6.0 版本的所有功能和 6.2 版本的某些功能。下表列出了它们的主要区别。如需查看这些区别的详细说明，请参阅“Cisco PIX 与防火墙模块的区别”文档。[提供该文档的 URL]应当链接到防火墙网页]

特性	FSM	Cisco PIX
性能	5 Gb	1.7 Gb
VLAN 标签	有	无
路由	动态	静态
故障恢复使用许可	不需要	需要
VPN 功能	无	有
IDS 签名	无	有
最大接口数	100	10
输入控制列表 (ACL) 支持	128000	2M

Q. FWSM 的性能如何？

A. 总性能约为 5Gbps。FWSM 可以每秒支持一百万个并发连接，并且每秒可以建立超过 10 万个连接。

Q. 装有 FWSM 的 Catalyst 6500 主要部署在什么地方？

A. 装有 FWSM 的 Cisco Catalyst 6500 系列可以提供目前性能最高的防火墙功能——它能够让企业将多种关键任务型防火墙功能整合到一个设备之中，从而减少分散的防火墙的个数，简化对多个防火墙的管理。FWSM 主要部署在企业园区的边缘和分布点。

Q. FWSM 所能支持的最低的软件版本是多少？

A. 最低的 IOS 软件版本是 12.1(13)E，而综合 CatOS 的最低版本是 7.5(1)。

Q. FWSM 支持交换矩阵吗？

A. 是的，FWSM 支持交换矩阵。它具有一条与总线的连接和一条与交换矩阵的连接。

Q. FWSM 是否利用热备份路由协议 (HSRP) 实现冗余？

A. 不是。主 FWSM 和冗余 FWSM 都使用与 Cisco PIX 防火墙相同的协议交换逻辑更新和状态信息。

Q. 怎样将流量发送给 FWSM？该模块是否具有外部端口？

A. FWSM 上没有外部端口。系统会给 FWSM 分配一些传输流量的 VLAN，这些 VLAN 上的流量将获得防火墙的保护。

Q. FWSM 是否支持冗余？

A. FCS 可以提供状态防火墙故障恢复。FWSM 采用了独特的设计，可以结合 PIX 状态故障恢复功能。FWSM 模块可以安装在同一个或者另外一个 Catalyst 6500 系列交换机中。

Q. FWSM 是否支持路由协议？

A. 是的，它支持开放最短路径优先 (OSPF) 和路由信息协议 (RIP)。

Q. 在订购 FWSM 时，我应当使用什么产品编号？

A. FWSM 的产品编号为：

产品编号	说明
WS-SVC-FWM-1-K9	用于 Cisco Catalyst 6500 的防火墙服务模块
WS-SVC-FWM-1-K9=	用于 Cisco Catalyst 6500 的防火墙服务模块 (备件)
SC-SVC-FWM-1.1-K9	用于 Catalyst 6500 的防火墙模块软件
SC-SVC-FWM-1.1-K9=	用于 Catalyst 6500 的防火墙模块软件 (备件)



Q. FWSM 是否具有使用许可选项?

A. 没有,该模块没有任何受限的和不受限的使用许可选项。

Q. FWSM 使用的是什么三重数据加密标准 (3DES) 软件?

A. FWSM 上的加密功能只能用于网络管理。您不能用该模块上的 3DES 软件进行远程接入或者站点间隧道端接。

Q. 模块软件是否内置 3DES 软件,我是否需要单独订购该软件?

A. 3DES 与软件镜像捆绑提供。您不需要单独订购该软件。

Q. 机载闪存和 DRAM 内存有多大,我能否升级 DRAM?

A. FWSM 的闪存为 128MB, DRAM 内存为 1GB。内存无法现场升级。

Q. FWSM 获得了什么认证?

A. 我们将在 2002 日历年度的第四季度之前获得 ICSA 认证。

Q. 我是否可以在 FWSM 上连接远程虚拟专用网 (VPN) 用户?

A. 不行, FWSM 不能提供 VPN 功能。

Q. 我是否可以在同一个机箱中安装多个模块?

A. 可以,每个机箱最多可以安装四个模块。

Q. FWSM 是否支持组播功能?

A. 最初的版本不能支持组播功能,但是组播支持将在未来的版本中提供。

Q. 我是否可以在同一个设备中安装和运行 FWSM 和 IPSec VPN 加速模块?

A. 不能。最初版本的 IOS 镜像不能互相兼容,因而不能将这两个模块安装在同一个设备中。

Q. FWSM 是否支持 IDS 入侵检测模块?

A. 防火墙服务模块和 IDS 模块可以共存于同一个设备中。由于 IDS 模块是一个从设备,所以获得防火墙保护的 VLAN 也可以拓展到 IDS 模块,进行入侵检测。

Q. FWSM 是否可以提供拒绝服务 /DDoS 检测和管理功能?

A. 可以。FWSM 可以根据协议或者地址设置阈值、日志和配置。

Q. FWSM 可以发现哪些拒绝服务攻击?

A. 它可以发现下列攻击:

- ◆ ICMP Flood
- ◆ UDP Flood
- ◆ Ping of Death
- ◆ IP Spoofing
- ◆ IP 源路由选项

Q. FWSM 是否支持 IP 源路由过滤功能?

A. IP 源路由过滤功能由 IOS 提供。

Q. FWSM 是否可以支持 URL/HTTP 过滤?

A. 是的,需要通过像 Websense 这样的 Web 过滤工具。

Q. FWSM 缺省的安全设置是什么?

A. FWSM 会拒绝所有方向上的所有分组,包括来自于管理接口的探测流量。

Q. FWSM 是否可以提供高可用性的主/主备份支持?

A. FWSM 目前可以提供主/从备份支持。主/主备份支持目前正在研究之中。

Q. FWSM 的主/从冗余功能是否可以提供无缝的故障恢复?

A. 可以。

Q. FWSM 是否支持流量整形?

A. FWSM 可以通过 Catalyst 6500 线卡支持流量整形,这种线卡可以为 FWSM 提供 VLAN 接口。

Q. FWSM 是否支持 QoS 机制和速率限制?

A. 可以, 它支持 Catalyst 6500 的所有 QoS 功能。

Q. FWSMD 是否支持安全的带外管理?

A. 可以, 通过管理 VLAN 上的 IPsec。

Q. FWSM 是否支持 Traceroute 和 ping?

A. 如果获得明确许可就可以支持。缺省状态下不支持。

Q. 应当用什么应用配置 FWSM 和监控系统日志流量?

A. 在最初的版本中, 用户可以通过 CLI 和 Cisco PIX 设备管理器 (PDM) 管理 FWSM。PDM 可以通过基于向导的菜单帮助用户进行防火墙配置。如需了解更多信息, 请接入:

<http://www.cisco.com/warp/public/cc/pd/nemnsw/vpdvnm/index.shtml>

此外, FWSM 还可以获得 Cisco AVVID 合作伙伴的支持。

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
东方广场东方经贸城东一办公楼 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)86528999

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

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。