思科 Catalyst 6500 系列防火墙服务模块

图 1
Cisco Catalyst 6500 系列防火墙服务模块

用于Cisco Catalyst 6500系列和Cisco 7600系列的Cisco Catalyst 6500 系列防火墙服务模块

用于 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器的 Cisco Catalyst 6500 系列防火墙服务模块（FWSM）是一种高速的、集成化的防火墙服务模块，可以提供 5.5Gb 的吞吐量，每秒 10 万个连接，以及一百万个并发连接。每个设备最高可以提供 20Gb 的吞吐量。作为世界领先的 Cisco PIX 安全产品系列的一部分，FWSM 可以为大型企业和服务供应商提供无以伦比的安全性、可靠性和性能。

FWSM 采用了 Cisco PIX 技术，并且运行 Cisco PIX 操作系统（OS）——一种实时的、牢固的嵌入式系统，可以消除安全漏洞，防止各种可能导致性能降低的损耗。这个系统的核心是一种基于自适应安全算法（ASA）的保护机制，它可以提供面向连接的状态化防火墙功能。

FWSM 还具有很多高级功能，例如可以在路由等级和桥接模式方面提供多种安全环境，因而有助于降低成本和运营复杂度，同时能够从同一个管理平台管理多个防火墙，FWSM 的虚拟化功能可以加强 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器所提供的投资保护，提供一个强大的深入防御解决方案。利用资源管理器等特殊功能，企业可以随时限制为任何一个安全环境分配的资源，这有助于确保不同的安全环境之间不会互相干扰。

利用透明防火墙功能，可将FWSM 设置为一个第二层桥接防火墙，最大限度地减少对网络拓扑的改动。透明防火墙的使用有助于缩短配置和部署时间——这对于任何IT资源有限的企业来说都具有重要的意义。除了管理接口以外不需要 IP 地址；透明防火墙不需要子网或者配置升级。

FWSM 服务管理、增强资源管理和限制功能可以更加有效地配置和监控安全服务，即使在多个虚拟环境之间。这包括等级创建、资源限制，针对每个用户的、基于思科安全访问服务器（ACS）的访问控制列表（ACL），针对每个ACL 的系统日志，系统日志等级配置，地址解析协议（ARP）检测，以及直通式组播支持。

增强过滤功能提供了更加广泛的保护和应用支持，例如语音应用。它还包括：基于策略的网络地址协议（NAT），双向 NAT，双向ACL，增强IP语音（VoIP），支持Skinny的端口地址解析（PAT），会话发起协议（SIP），媒体网关控制协议（MGCP），H.323 v3 和 v4，多协议标签交换（MPLS）和防火墙集成，结合 WebSense 和 N2H2 的 URL 过滤，以及屏蔽和阻塞攻击。

防火墙服务模块的主要优点

防火墙的传统角色已经发生了变化。今天的防火墙的作用已经不再只是防止企业网络遭受未经授权的外部访问的攻击。除了防止企业网络的周边遭受威胁以外，防火墙还可以防止未经授权的用户进入企业网络的子网、工作组和LAN。如果不建设一个层次化的深度防御系统，企业可能会遭受极为惨重的损失。企业网络需要一个可靠的、集成化的解决方案来防止它们的企业资产受到这些日益增加的攻击的威胁。

集成化模块

FWSM 安装在 Cisco Catalyst 6500 系列交换机或者 Cisco 7600 系列路由器的内部，让这些设备的任何端口都可以充当防火墙端口，并且在网络基础设施中集成了状态化防火墙安全性。对于那些机架空间非常有限的系统来说，这种功能非常重要。

适应未来需要

FWSM 最高可以支持 5.5Gb 的吞吐量，因而可以提供无以伦比的性能，让用户无须对系统进行彻底的升级，就可以满足未来的要求。在 Cisco Catalyst 6500 系列中最多可以添加 3 个 FWSM（即总共 4 个模块），以满足用户不断发展的需求。

可靠性和高可用性

FWSM 建立在 Cisco PIX 技术的基础之上，并使用了久经考验的 Cisco PIX 操作系统——一个安全的、实时的操作系统。FWSM 可以利用行之有效的 Cisco PIX 技术检测分组，从而可以在同一个平台上提供性能和安全的独特组合。在永续性方面，FWSM 支持在单个 6500 或者 7600 设备内部的不同模块之间，以及不同设备的模块之间进行高速故障切换。对于设备内和设备间故障切换的支持让客户在防火墙部署方面可以获得全面的灵活性。

易用性

Cisco PIX 设备管理器的直观图形化用户界面（GUI）可以用于管理和配置 FWSM 的各项功能。Cisco PIX 设备管理器可以在系统和设备级别——以及更加具体的安全环境等级——简化 FWSM 的管理和监控。

客户还可以利用可扩展的 CiscoWorks VPN/ 安全管理解决方案（VMS），从一个集中控制台管理 FWSM。CiscoWorks VMS 为在一个思科网络中管理和监控安全解决方案提供了一种模块化，集成化的、可扩展的管理中心可以支持多种解决方案，包括 VPN、路由器、交换机、防火墙和思科安全代理。CiscoWorks 管理中心能够以一种统一的方式，集中地、全面地管理网络中的 FWSM、Cisco PIX 安全设备和基于 Cisco IOS 路由器的防火墙，从而加快大型安全系统的部署速度。

FWSM 特性

表 1 特性和说明

主要特性	说明
性能	• 5.5 Gbps，一百万个并发连接，每秒建立和断开 10 万个连接 • 256，000 个 PAT 和 256，000 个 NAT 解析
路由和透明防火墙	防火墙可以运行在下列模式下: • 路由——FWSM 被视为网络中的一个路由器跳 • 透明——FWSM 的作用相当于“线缆内的块”，而不是一个路由器跳。FWSM 可以在它的内部和外部端口上连接同一个网络，这两个端口必须位于一个不同的 VLAN 上
多个安全环境	• 在多环境模式下，最多可以创建 256 个不同的安全环境 – 虚拟防火墙。一个安全环境就是一个拥有自己的安全策略和接口的虚拟防火墙。每个环境在路由模式下可以支持 256 个 VLAN • 多个环境就类似于拥有多个独立的防火墙 • 所有安全环境都必须运行在路由模式或者透明模式中
双向 NAT 和基于策略的 NAT	• 提供动态 / 静态 NAT 和 PAT • 您可以在内部和外部地址上设置 NAT。对于基于策略的 NAT，您可以利用一个扩展 ACL 发现需要解析的地址，这让您可以在确定哪些地址需要解析方面获得更高的控制权

表 1 特性和说明（续）

主要特性	说明
资源管理	• 允许限制每个环境的资源，从而避免由一个环境占用所有资源
直通式代理	• 在每个 VLAN 的基础上实施安全策略
URL 过滤	• 利用 WebSense Enterprise 或者 N2H2 的 HTTP 过滤技术，过滤 HTTP、HTTPS 和 FTP 请求
配置支持	• 控制台到命令行界面(CLI)(从交换机发起的会话) • Telnet 到 FWSM 的内部接口 • 基于 IP 安全（IPSec）的 Telnet 到 FWSM 的外部接口 • 安全套接子层（SSH）到 CLI • 安全套接子层（SSH）到 Cisco PIX 设备管理器 • 用于防火墙的 CiscoWorks VMS 管理中心
AAA 支持	• 通过 TACACS＋和 RADIUS 支持，集成常见的身份认证、授权和记帐服务（AAA）
Cisco PIX 设备管理器(PDM)	• 简便、直观、基于 Web 的 GUI 可以支持远程防火墙管理 • 多种基于实时数据和历史数据的报告可以提供使用趋势、基本性能和安全事件等信息 • Cisco PIX 设备管理器还与 CiscoView 设备管理器——相集成。借助 CiscoView 设备管理器，用户可以通过一个便于使用的 GUI 集中管理 Cisco Catalyst 6500 系列中的模块，例如 FWSM 和 Supervisor 模块
安全网络管理	• 安全的、采用三重数据加密标准 (3DES)加密的网络管理访问
访问控制列表	• 最多支持 80,000 个 ACL 支持下列 ACL 类型: • 扩展 ACL 可以控制一个接口上的 IP 流量 • 对于透明防火墙模式，EtherType ACL 可以控制非 IP 流量 • 用于开放最短路径优先（OSPF）路由重新分配的标准 ACL • 针对每个用户的、基于思科安全 ACS 的 ACL
动态路由协议	在单环境模式下，FWSM 支持下列路由协议: • 路由信息协议（RIP）v1 和 v2（被动模式） • OSPF 透明模式只支持静态路由
命令授权	• 让您可以控制对命令的访问权限，创建与这些优先级对应的用户账号或者登录环境。
对象群组	• 能够为 ACL 组合网络对象（例如主机）和服务（例如 FTP 和 HTTP） 防范拒绝服务（DoS）攻击 • DNS 保护; Flood Defender; Flood Guard; TCP 阻截; 单播反向路径发送（uRPF）; 邮件保护; FragGuard 和虚拟重组; 互联网控制消息协议（ICMP）状态化检测; 用户数据报协议（UDP）速率控制
ARP 检测	• 对于透明防火墙模式，FWSM 会将所有 ARP 分组中的 MAC 地址和 IP 地址与 ARP 表中的静态条目进行对比
动态主机控制协议（DHCP）	• FWSM 充当一个 DHCP 服务器。FWSM 还支持 DHCP 中继功能，可以将 DHCP 请求转发到一台上游路由器
高可用性	• 状态化故障转移－设备内部和设备之间
日志	• 全面的系统日志、FTP、URL 和 ACL 日志
其他协议	• H.323 v3和v4;基于IP的NetBios; RAS 第二版本;实时流协议（RTSP）;基于PAT的SIP; XDMCP; Skinny

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1号东方广场
东方经贸城东一办公楼19～21层
邮编：100738
电话：(8610)65267777
传真：(8610)85181881

上海
上海市淮海中路222号
力宝广场32～33层
邮编：200021
电话：(8621)33104777
传真：(8621)53966750

广州
广州市天河北路233号
中信广场43楼
邮编：510620
电话：(8620)87007000
传真：(8620)38770077

成都
成都市顺城大街308号
冠城广场23层
邮编：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

欢迎下载电子文档，http://www.cisco.com/cn/products/sc/pix_firewall/index.shtml

2004 年 8 月印刷