

Cisco集成多业务路由器的安全特性 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/242/2021\\_2022\\_Cisco\\_E9\\_9B\\_86\\_E6\\_88\\_c101\\_242574.htm](https://www.100test.com/kao_ti2020/242/2021_2022_Cisco_E9_9B_86_E6_88_c101_242574.htm) 产品概述 思科系统公司推出了一个全新的集成多业务路由器系列模块化Cisco 1800、2800和3800集成多业务路由器作为思科自防御网络的关键部件，思科集成多业务路由器使客户实现了路由和安全策略的同步，并降低了运营成本，提高了整个网络的安全水平。凭借基于Cisco IOS 软件的VPN、防火墙和IPS，以及可选增强VPN加速、入侵检测系统（IDS）和内容引擎网络模块（Cisco 2800和3800系列），思科为分支机构路由器提供了业界最强大、可适应的安全解决方案。通过将成熟的Cisco IOS功能和业界领先的LAN/WAN连接与世界一流的安全特性相结合，集成化安全解决方案为客户提供了下列优势：“利用现有设施”利用现有网络基础设施，在路由器上通过Cisco IOS支持全新安全特性，无需部署额外的硬件“在最需要的地方部署安全特性”为在网络任意地点采用防火墙、IPS和VPN等安全功能提供了灵活性，从而最大限度地发挥了安全优势“保护您的网关”在网络所有的入点部署最佳安全功能“节省时间和资金”减少了设备数量，降低了培训和管理成本“保护您的基础设施”保护了路由器，可以防御直接针对网络基础设施的攻击，如DDoS 思科自防御网络 Cisco 1800、2800和3800路由器支持作为属于思科自防御网络的内容广泛的安全特性，这种安全策略使公司可识别、防止和适应安全威胁。思科自防御网络拥有四类适用于路由器的保护措施：安全连接 提供了安全、可扩展的网络连接，容纳了多种流量类型

，如VPN、动态多点VPN（DMVPN）、多VRF和MPLS安全环境、话音和视频型VPN（V3PN），以及安全话音。威胁防御 利用网络服务可以预防和响应网络攻击和威胁。包括网络入侵防御系统（IPS）和Cisco IOS防火墙。信任和身份 允许网络利用网络准入控制（NAC）、身份服务和AAA等技术智能地保护终端。网络基础设施保护 保护网络免受攻击和漏洞的影响，尤其在网络级别。包括控制面板监管、基于网络的应用识别（NBAR）和AutoSecure。集成多业务路由器特性为有助于实现Cisco 1800、2800和3800系列上的安全特性，配备了下列Cisco IOS软件特性集：Advanced Enterprise Service（高级企业服务）Advanced IP Services（高级IP服务）Advanced Security（高级安全特性）内嵌服务管理：思科路由器和安全设备管理器（SDM）思科路由器和安全设备管理器（SDM）每台Cisco 1800、2800和3800都带有在工厂中安装的思科路由器和安全设备管理器（SDM）。Cisco SDM是一种直观的、基于Web的设备管理器（GUI），用于思科路由器的部署和管理（Cisco SDM 2.0将路由和安全服务管理与使用方便的智能向导和深入排障功能相结合，为将服务集成到路由器之上、以从中获益而提供了支持工具。目前，客户可以在整个网络内将路由和安全策略同步化，拥有更全面的路由器服务状态浏览能力，并降低了运营成本。Cisco SDM 2.0的全新关键特性包括：嵌入的IPS，可更新特征和定制特征基于角色的路由器接入 Easy VPN服务器和AAA用于IPSec VPN的数字证书 VPN和WAN连接排障 QoS策略配置和基于NBAR的应用流量监控 100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)