

## 思科集成多业务路由器：为中小企业提供集成安全体验

网络现已从封闭的基础设施发展成为集成的系统，通过业务流程和应用的连接和自动化使企业与其全球员工、合作伙伴、客户及供应商更密切地联系在了一起。应用上网大幅度提高了生产率和盈利，但同时也加剧了攻击风险。

安全威胁来自多个方面，包括公司内部的联网 PC 和服务器。新出现的蠕虫和病毒将目标锁定在网络终端，对于缺乏足够的 IT 资源来应对威胁的中小企业影响尤为严重。思科系统公司®能帮助中小企业构建自防御网络，大幅度提高识别、防御和阻断威胁的能力，从而为应对威胁做好准备。新一代思科集成多业务路由器是思科®安全网络基础 (Cisco Secure Network Foundation) 和思科自防御网络的核心组件，能够开拓性地为中小企业以及大型企业的分支机构提供安全的线速数据、语音、视频和其他高级服务。

本《白皮书》将重点介绍不断变化的安全形势以及 Cisco 800、1800、2800 和 3800 系列集成多业务路由器的固有安全特性。市场趋势分析显示，小企业对集成服务的需求与日俱增；本文将简要介绍路由器中集成安全的价值，并阐述思科智能商业规划以及独特的系统方法如何帮助您有效解决现在和将来遇到的安全问题。

本《白皮书》不是技术部署指南，而是解释了思科如何将最佳网络安全技术与 20 多年的路由经验结合在一起，以便重新定义网络安全并为客户提供端到端的网络保护。

## 前所未有的网络安全挑战

无论来自何处，早期的网络安全威胁都具有传播速度缓慢且易于遏制的特征。20世纪80年代出现的第一代安全威胁 – 影响单个电脑和网络的引导区病毒 – 需要几周的传播时间。到了20世纪90年代，第二代安全威胁，包括宏病毒、电子邮件病毒、拒绝服务(DoS)攻击和次数设有上限的非法访问企图等，传播时间缩短至几天。

现在，网络安全威胁和破坏性攻击的传播速度和手段不断提升。互联网病毒、蠕虫、病毒和特洛伊木马的混合威胁只需几分钟便可跨越整个世界蔓延到多个地区网络，造成大幅度的感染和惨重的损失。

## 网络安全威胁和攻击代价高昂

每个安全威胁的平均损失：

- 保密信息盗用：US\$30,933,000
- 病毒导致故障停机和损失：US\$42,787,767
- 内部人员滥用：US\$6,856,450
- 外部人员侵入系统：US\$841,400
- 拒绝服务：US\$7,310,725
- 非法访问：US\$31,233,100

来源：CSI FBI Computer Crime and Security Survey 2005

## 按照法律要求加大安全防范力度

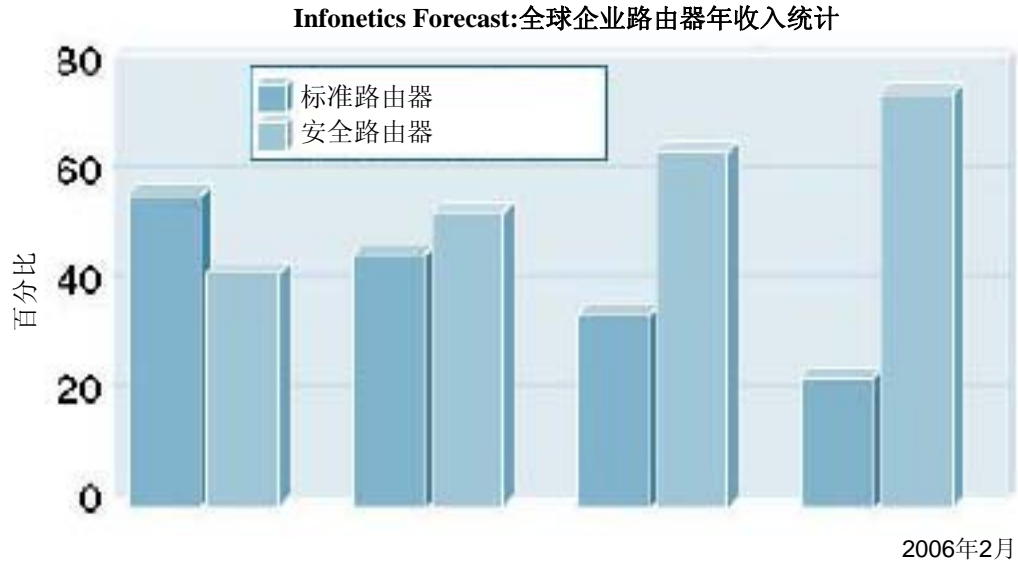
越来越多的政府规定和标准注重增强客户保密性、国家安全和上市公司的责任，成为推动公司提高网络安全的另一个驱动力。例如，美国适用于医疗保健行业的健康保险便携性和责任法案(HIPAA)、适用于金融服务业的 Gramm Leach Bliley Act (GLBA) 以及适用于会计行业的 Sarbanes-Oxley 法案。欧盟的保密法案‘数据保护条例’要求只能将个人数据传输给保密性达标的非欧盟国家。

## 安全路由器需求旺盛

随着对安全和保密性的关注继续升温，市场对创新安全解决方案的需求也在不断增长。据《Business Communication Review》称，虽然许多人一直抱着浓厚的兴趣在观望安全产品市场，但他们往往忽略了部署路由器和交换机实际上能够提供哪个级别的安全<sup>1</sup>。文章还指出，虽然分布式互联网连接以及公司的网络保护需求推动了多项安全技术向单一产品中的集成，但这些因素同时还推动网络产品制造商将安全集成到路由器和交换机中。这篇文章中引用的 Infonetics 调查报告指出，被调查人中，计划部署安全产品和安全路由器的大约各占一半。

如图 1 所示，Infonetics Research 的调查数据为安全路由器市场的快速增长提供了依据。在近期发表的文章中，Infonetics Research 称无论是从销售量还是从销售收入的角度，安全路由器都呈现正增长趋势。安全路由器收入的年增长率高达121%，2005 年为 8.03 亿美元；销售量几乎翻了三番<sup>2</sup>。

图1. 安全路由器购买趋势分析



### 思科始终致力于提供创新的安全解决方案

安全解决方案通过不断发展满足了动态的安全要求。思科始终在通过最佳的安全解决方案引领整个市场。现在，思科将网络安全嵌入到了每个集成多业务路由器的硬件中，并通过 Cisco IOS<sup>®</sup> 软件的特性集提供端到端的安全保护。思科集成多业务路由器与 Cisco 7200 系列和 Cisco 7301 汇聚路由器互操作，均提供 Cisco IOS 软件全面的高级安全特性集。

<sup>1</sup> “Enemy at the Gates: The Evolution of Network Security,” Business Communication Review, 12/ 2004, Jeff Wilson

<sup>2</sup> “Secure Router Market More Than Doubled in 2005” (internetnews.com, 02/ 2006), Matthias Machowinski

## 通过路由器提供集成安全解决方案的价值

集成安全是思科自防御网络的基本组件。基于路由器的思科集成安全解决方案使用市场领先的思科防火墙和入侵防御技术，同时提供 Cisco IOS 软件的功能、广域网和局域网连接以及世界一流的安全性。

将 Cisco IOS 软件的安全特性直接集成到路由器中可提供许多优势。它使用现有的网络基础设施，允许在路由器上部署全新的安全特性，无需安装其他硬件。这将减少网络设备的数量，从而降低培训和管理成本，藉此降低总体拥有成本(TCO)。现有路由器的思科 SMARTnet® 维护合同也适用于路由器网络模块，从而进一步简化了管理。

集成提供了灵活性，允许在网络中的任何位置执行防火墙、内部入侵防御和 VPN 等安全功能，以确保针对安全威胁提供最佳防御。基于路由器、交换机和安全产品的功能结合在一起，能为整个网络提供端到端的保护。将安全直接集成到路由器中还能保护网络网关，使路由器成为网络入口处的第一道防线。这使您能够在所有的网络入口处部署最佳的安全功能，为网络提供妥善的保护。

路由器安全不仅能够网络入口处提供第一道保护，而且还允许您将路由器作为“可信处理器”，利用这种智能性来处理流量，以便集成更高级的安全、服务质量(QoS)和路由特性。路由器允许共享安全信息并且快速准确地响应威胁，从而帮助确保网络的高可用性。集成安全在保护路由器本身的同时，还能针对分布式 DoS (DDoS) 攻击等直接针对网络基础设施的威胁设立坚固的防线。

许多第三方的点安全产品都只能保护特定的网络段，但极少能够像思科安全产品那样保护所有的网络入口，从而无法保护整个基础设施的安全。

## 思科系统方法的价值

### 帮助小型机构实现高可用性

思科提供了强大的功能集来满足高可用性要求。思科端到端的构想设计能提供可持续访问的网络，允许 IT机构更轻松部署可维护的自防御网络架构。集成多业务路由器提供了可并行使用的更多接口和特性，同时提高了多项安全、管理和集成服务的性能，从而进一步增强了这种方法。

思科集成多业务路由器提供了全面的高可用性解决方案，能最大限度地减少网络中断并确保不中断地访问大多数的关键业务应用。思科注重将全新的基础设施服务与性能集成在一起，允许公司在现在和将来创建更智能、更具永续性、更可靠的网络。

关于思科面向小型机构的高可用性解决方案的更多信息，请登录<http://www.cisco.com/go/isr>，阅读白皮书“Maximizing Availability in the Branch with the Integrated Services Router”。

## 性能

利用系统方法，思科集成多业务路由器能提供适当的广域网线速性能。这意味着如果客户添加语音或安全等更多服务，性能不会低于相应的广域网接口速度。集成多业务路由器能通过合理的 CPU 耗用运行并行服务，并能将 VPN 等 CPU 密集型服务卸载到专用加速器。

Mier Communications, Inc. (Miercom) 对全新思科集成多业务路由器的配置、运行和性能进行了独立验证。经 Miercom 证实，在繁忙的分支机构同时运行多项重要的高级网络服务时，包括 Cisco IOS 状态防火墙和网络地址转换(NAT)、入侵防御、IP语音 (VoIP) 和模拟电话服务等，虽然数据传输量极大，但这些系统仍可保持卓越性能。测试还证明，系统在高负荷情况下能够确保语音服务的质量。具体地说，经测试，Cisco 3845 集成多业务路由器能够加载 T3 IP-WAN 链路并在完全使用 T3 链路传输数据的情况下通过 IP 安全 (IPsec) VPN 满足高级加密标准(AES)的要求。Miercom 还对 Cisco 2851, 2811, 2801, 1841 和 1812 无线集成多业务路由器以及基于 Web 的思科路由器和 Security Device Manager (SDM) 应用进行了测试。

如想阅读全篇 Miercom 总结报告，请访问：<http://www.miercom.com>。

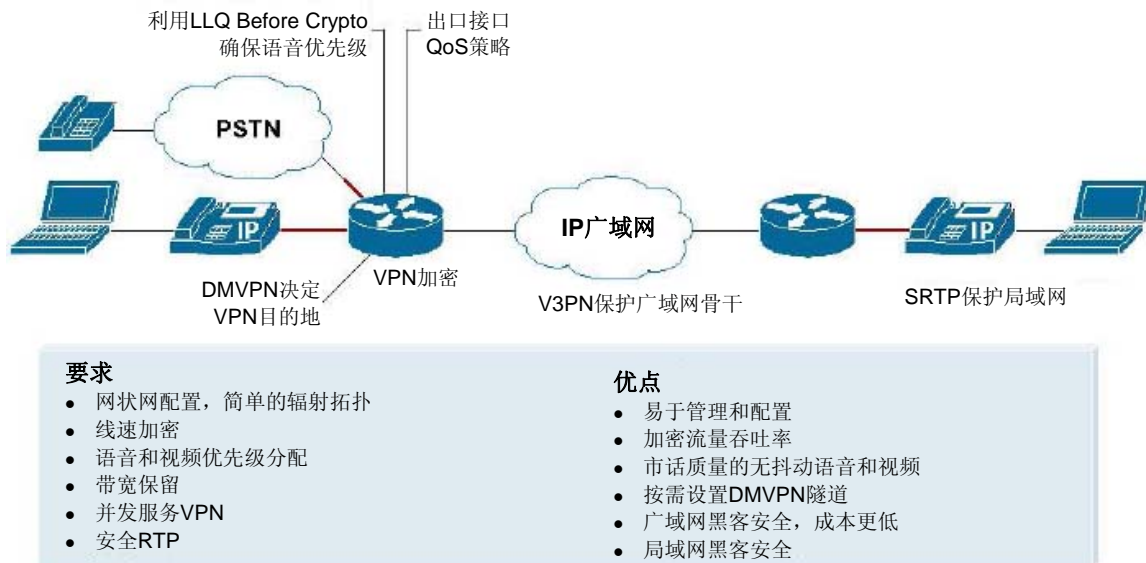
**“我们的测试证明，Cisco 3845 能够通过 T3 广域网链路同时全速运行多个应用。产品内嵌的加密处理器能够轻松处理128位 AES 和 IPsec VPN，同时以最高的广域网链路速度提供防火墙、入侵防御、QoS 和数据路由。此外，Cisco 3845 惊人的 72 路语音流量处理功能，包括代码转换、语音留言、自动值守、传真和远程电话应急呼叫，并未造成性能降级。”**

—Ed Mier, Mier Communications, Inc. 总裁

## 智能

系统方法首先应用于思科集成多业务路由器等单一永续性平台，但必须扩展到“单一设备”方法的范围之外，将智能服务打包在内。协作时，智能服务能提供动态多点VPN (DMVPN) 等显著优势，以实现动态隧道或基于语音和视频的 VPN (V3PN)，如图 2 所示。

图2. 使用 DMVPN, V3PN 实现安全、市话质量的 IP 电话



系统方法将语音、安全、路由和应用服务结合在一起，能提高流程的自动化和智能水平，从而使安全功能普遍应用到网络和应用中，改进了面向数据、语音和视频流量的服务质量，提高了工作效率并允许更好地使用网络资源。

### 通过战略方法实现增长

中小企业需要保护并按自己的步伐充分利用网络投资和有限的支持资源。思科安全网络基础（Cisco Secure Network Foundation）为实施各级安全性和高级应用提供了可扩展的灵活方式。思科安全网络基础是思科智能商业规划中的核心步骤，提供了精心策划的结构化演进路径，旨在帮助企业把握现在的商机并实现长期技术投资回报的最大化。利用思科智能商业规划，企业可与思科及思科合作伙伴建立更密切的合作关系，以便为将来的增长做好规划、简化技术部署流程、缩短部署时间并降低总成本。

通过将最佳软件和应用结合到一个平台中，客户能够：

- 更快速地部署基础和高级服务
- 使用通用的工具和接口来管理这些服务，从而简化运营
- 通过最大限度地减少需要保护的单个产品的数量来提高网络安全性
- 利用现有的和将来的接口和网络模块来加速数据交付，用现有硬件支持新应用
- 加快排障速度，更轻松地获得“备件”并快速培训员工，以降低运营成本
- 利用捆绑包装和服务合同来降低前期成本

## 全新的思科集成多业务路由器具有与众不同的安全特性

Cisco 800, 1800, 2800 和 3800 系列集成多业务路由器都提供了业界最全面的安全服务，并且以智能的方式将数据、安全和语音嵌入到一个具有永续性的系统中，以便通过可扩展的方法快速交付关键任务的商业应用。思科将基于硬件的加密作为标准特性提供，从而将安全嵌入到所有的集成服务中。这种基于硬件的固有的加密加速机制可卸载 VPN 处理任务，以便提高 VPN 的吞吐率，同时确保对路由器 CPU 的影响最小化。如果需要提高 VPN 的吞吐率或可扩展性(例如 VPN 隧道数量)，您可使用可选的 VPN 加密高级集成模块 (AIM)。

思科自防御网络为新型路由器提供四种保护：信任和身份验证、网络基础设施保护、安全的连接、威胁防御 (图3)。

图3. 思科集成多业务路由器和自防御网络



## 设备管理

### 思科路由器和 Security Device Manager (SDM)

所有的 Cisco 800, 1800, 2800 和 3800 系列; Cisco 7200 系列和 Cisco 7301 路由器都配备有 Cisco SDM。SDM是基于 Web 的图形化设备管理器(GUI), 用于思科路由器的部署与管理。Cisco SDM 提供了安装向导, 用于快速的路由器部署和路由器“锁定”, 从而简化了路由器的配置和监控流程。SDM 提供的智能向导能支持安全性和路由特性、经过思科技术支持中心 (TAC) 验证的路由器配置以及与主题相关的培训内容。

### 信任和身份验证

信任和身份验证服务允许网络使用网络准入控制(NAC)、身份识别以及验证、授权和记账等(AAA) 技术来智能地保护端点。

### 网络准入控制

NAC 是由思科领导, 整个业界共同努力的结晶, 旨在确保授予访问权限之前每个端点都遵守网络安全策略。在允许产品访问网络之前, NAC 将对其进行盘查, 以查看是否遵从公司最新的防病毒和操作系统补丁策略, 从而限制病毒和蠕虫造成的损失。NAC 将隔离存在安全漏洞的主机和违规主机并限制它们访问网络, 直到安装了补丁并得到保护为止, 从而防止它们成为蠕虫和病毒的传播源或目标。

Cisco 800, 1800, 2800 和 3800 系列、Cisco 7200 系列以及 Cisco 7301 路由器都可提供 NAC 和其他集成安全服务以及 Cisco IOS 软件的高级安全、高级 IP 服务或高级企业服务特性集。

### 认证、授权和计费

思科 AAA 网络安全服务为您在路由器或接入服务器上设置访问控制策略提供了主要的框架。通过 AAA, 管理员可使用应用于特定服务或接口的方法列表来逐线路(逐用户)、逐服务(IP、Novell Internetwork Packet Exchange [IPX]或逐个虚拟专用拨号网络[VPDN])地动态配置验证和授权类型。

### 802.1x

标准的 802.1x 应用要求访问者在访问网络时提交有效的访问证书, 从而进一步阻止了对受保护信息资源的非法访问。通过部署 802.1x 应用, 网络管理员还能有效避免用户部署不安全的无线接入点, 帮助解决了易于部署的无线局域网(WLAN) 设备带来的最棘手的一个问题。

### USB 端口/可转移的证书

思科集成多业务路由器提供了集成的板载 USB 1.1 端口, 能支持重要的安全和存储功能。通过这些功能, 路由器能进行安全的用户验证、保存可转移的证书以便建立安全的 VPN 连接、安全地分配配置文件并为文件和配置提供大容量的闪速存储支持。

## 网络基础保护

网络基础保护能防止网络因安全漏洞而受到攻击，包括控制层面监管、AutoSecure以及基于网络的应用识别 (NBAR)等。

### 控制层面监管

即便是最强韧的软件和硬件架构也有可能遭遇 DoS 攻击，致使恶意流量淹没整个网络基础设施，造成网络瘫痪。为了阻止这类威胁和伪装成特定类型控制数据包的攻击直捣网络核心，Cisco IOS 软件提供了监管功能，对目的地为控制层面处理器的流量进行限速。这个名为控制层面监管的特性能识别特定类型的流量，然后按规定的门限值限制这些流量或者完全禁止其穿过网络。

### AutoSecure

作为 Cisco IOS 软件的一个特性，AutoSecure能简化路由器安全的配置工作并降低配置出错的风险。适用于老练用户的互动模式将提示用户定制安全设置和路由器服务，从而加大对路由器安全功能的控制力度。非互动模式能基于思科的默认设置或国际计算机安全协会(ICSA)的推荐设置自动开启路由器安全功能。您只需执行一个命令便可即时配置路由器的安全状态并关闭不必要的系统程序和服务，避免潜在的网络安全威胁。

### 基于网络的应用识别

NBAR 是 Cisco IOS 软件中的分类引擎，它使用深层和状态数据包检测技术来识别大量的应用，包括基于 Web 的应用和其他难以分类的协议。当在安全上下文中使用时，NBAR能基于有效负荷签名检测出蠕虫的存在。当NBAR 识别出应用并对应用进行分类时，网络可调用适用于特定应用的服务。Cisco SDM 为 NBAR 提供了易用的向导，同时还提供了应用流量的图形视图。

## 安全的连接

思科集成多业务路由器提供了安全、可扩展的网络连接，能传输多类流量，例如 VPN 隧道和加密、DMVPN、Easy VPN、V3PN、虚拟隧道接口(VTI)、多虚拟路由转发(VRF)、多协议标签交换(MPLS)和安全的上下文等。

### VPN 隧道和加密

VPN 是快速增长的网络连接方式。所有的思科集成多业务路由器都带有基于硬件的内置 VPN 加密加速工具，以便通过卸载 IPsec 加密和 VPN 处理任务来提高 VPN 吞吐率，同时确保只对路由器 CPU 产生最低的影响。这个特性支持 IPsec、AES、数字加密标准(DES)和三重 DES (3DES) 加密，不占用 AIM 插槽。

可选的 VPN 加密 AIM 适用于需要提高 VPN 吞吐率或可扩展性的企业。这些 AIM 可帮助提高 VPN 性能，同时将路由器 CPU 的总体利用率保持在较低水平。与原来的机型相比，每个 AIM 能提供 10 倍的加密性能以及隧道可扩展性。思科集成多业务路由器还可使用结合了 IPsec 和通用路由封装(GRE)协议的其他隧道技术。IPsec -GRE 技术是独特的思科解决方案，能通过 VPN 发送动态路由协议，从而提供优于纯 IPsec 解决方案的网络永续性。除提供故障切换机制外，GRE 隧道还能加密组播和广播数据包以及不基于互联网的协议。

### **Cisco IOS Web VPN**

安全套接字层 (SSL) VPN 对最终用户是透明的且易于管理，因此是极具吸引力的远程接入安全解决方案。通过思科集成多业务路由器上部署的 Cisco IOS Web VPN，客户可将安全企业网络扩展到基于互联网的任何位置，包括家用电脑、互联网信息台和无线热点等，从而提高员工生产率并保护公司数据，同时允许合作伙伴及顾问访问公司网络。

### **动态多点 VPN**

DMVPN 支持按需应变的、可扩展的全网状网 VPN，以便缩短时延、保留带宽并简化部署。DMVPN 以 Cisco IPsec 和路由技术为依托，支持GRE隧道动态配置、IPsec 加密、下一跳解析协议(NHRP)、开放最短路径优先(OSPF)和增强型内部网关路由协议(EIGRP)。如果与 QoS 和 IP 组播等技术结合使用，DMVPN 还能优化语音和视频等时延敏感型应用。此外，DMVPN 还能简化管理工作，在添加分支设备或设置分支间的连接时，无需在中枢位置进行配置。

### **安全的语音**

思科集成多业务路由器提供的媒体验证和加密特性能确保端接在时分多工 (TDM) 或模拟语音网关端口的语音通话免遭窃听。这些可扩展的可靠特性为局域网或广域网上的IP 通信提供了安全的环境。

安全的实时传输协议(SRTP)能加密语音通话，使进入语音域的内外部黑客无法解读。作为 IETF RFC 3711 标准，SRTP 专为语音数据包而设计，支持 AES 算法。相对 IPsec 来说，使用 SRTP 的媒体加密的带宽利用率更高。

### **Easy VPN**

Cisco Easy VPN 是一种 IPsec 解决方案，能轻而易举地支持集中星形 VPN 拓扑，同时确保高可扩展性。Cisco Easy VPN 能简化 Cisco PIX® 安全产品、Cisco VPN 3000 客户机以及各种路由器之间的 VPN 解决方案的设置和管理工作。经数千名客户实践验证，Cisco Easy VPN 能使用“策略推广”技术来简化配置，同时保持特性的丰富性和策略控制。

## 基于语音和视频的 VPN

Cisco 800, 1800, 2800和3800系列、Cisco 7200系列和Cisco 7301路由器都支持 V3PN，能够为客户提供适当的基础设施，以便将数据、语音和视频融合到一个基于QoS的安全的IPsec网络上。客户在 IP 传输路径上能获得与广域网链路完全相同的语音和视频应用性能 – 安全且高效。不同于目前在销的许多其他 VPN 产品，这些思科路由器能适应多业务IPsec VPN的不同网络拓扑并满足它们的流量要求。V3PN 端到端的网络架构利用安全的思科路由器，通过 Cisco IOS 软件来确保语音流量的安全。

要想通过 IPsec VPN 提供市话质量的语音和视频，您不仅需要加密流量，而且还需要混合部署多项高级的多业务和 IPsec VPN 技术。帮助实现 Cisco V3PN 的主要 Cisco IOS 软件技术包括：以多业务为中心的 QoS、对多种流量的支持、对多业务网络拓扑的支持以及增强型网络故障切换功能等。

## 虚拟隧道接口

Cisco IPsec VTI 是帮助客户在站点间的设备之间配置基于 IPsec 的 VPN 的新工具。IPsec VTI 隧道在共享广域网上提供指定的路径并可通过全新的数据包报头来封装流量，从而帮助确保将流量传输到指定目的地。鉴于流量只能进入端点位置的隧道，因此，这个网络是专用网络。此外，IPsec 还提供真正的保密性(如同加密一样)并能传输加密后的流量。

## 面向电信运营商的 Multi-VRF 和 MPLS 安全环境

Multi-VRF 是站点间 IPsec VPN 的扩展，能在公司流量穿过电信运营商网络时帮助确保安全性和保密性。然而，Multi-VRF 使在传统的局域网上合理分割流量变得更加复杂，尤其是在为多个分支机构部署 Multi-VRF 时。Multi-VRF 专门用于以合理的价格在网络段之间确保流量的私密性。

## 威胁防御

威胁防御服务能使用网络服务来响应并抵御网络攻击和威胁，例如 Cisco IOS 防火墙和 Cisco IOS IPS。

## Cisco IOS 防火墙

Cisco IOS 防火墙是用于思科路由器的状态检测防火墙。Cisco IOS 防火墙与思科安全产品使用完全相同的状态防火墙技术，能安装在所有的集成多业务路由器上，提供高级安全性或更高级的 Cisco IOS 软件特性集。Cisco IOS 防火墙是理想的单一设备安全和路由解决方案，用于保护网络的广域网入口。虽然总部通常是安装防火墙和检测流量攻击的位置，但您在部署安全系统时，也应仔细考虑远程机构。

Cisco IOS 防火墙还通过其他特性来提供更高级别的安全性和执行能力。应用防火墙为 Cisco IOS 防火墙提供了智能，使其不仅能够阻断非 HTTP 流量，而且还能确保 HTTP 流量是合法的 Web 浏览流量，不是试图穿过防火墙的即时消息或类似流量。基于分区的策略配置机制提供了清晰的界面，

用于配置与传统安全策略相一致的防火墙策略。Cisco IOS 软件支持 IPv6 防火墙并允许 IPv4 与 IPv6 共存。Cisco IOS 防火墙的 IPv6 特性能够对 IPv6 数据包进行状态协议检测 (发现异常协议) 并遏制 IPv6 DoS 攻击。这些特性都支持网管对穿过防火墙的应用进行更严格的控制。

Cisco IOS 防火墙不仅允许在网络外围提供单点保护,而且还使安全策略成为固有的网络组件。专用和集成的策略执行工具都具有灵活性和经济高效性,能够改进面向外联网和内联网外围的安全解决方案以及面向分支或远程机构的互联网安全解决方案。此外,Cisco IOS 防火墙还允许客户在相同的路由器中使用高级的 QoS 特性。

### 透明防火墙

除 L3 状态防火墙外,Cisco 800, 1800, 2800 和 3800 系列、Cisco 7200 系列以及 Cisco 7301 路由器还支持透明防火墙,以便为相同路由器上的 L2 连接提供 L3 防火墙支持。透明防火墙支持子接口和 WLAN 中继线、生成树协议、所有的标准管理工具、以及动态主机配置协议(DHCP)直通功能,以便在对面的接口上(双向)分配 DHCP 地址。透明防火墙无需对接口上的 IP 子网和 IP 地址进行重新编号,因此可轻松添加到现有网络中。

### 内部入侵防御

思科开发出了第一款提供内部入侵防御功能的路由器。Cisco IOS IPS 是基于深层数据包检测的内部防御解决方案,能帮助 Cisco IOS 软件有效遏制网络攻击。Cisco IOS IPS 用于入侵防御和事件通知,利用思科入侵检测与防御系统 (IDS/IPS) 提供的技术,包括 Cisco IPS 4200 系列传感器产品、Cisco Catalyst® 6500 系列 IDS 服务模块以及网络模块 IDS 产品等。

由于是内部防御产品,Cisco IOS IPS 能够丢弃流量、发送警报或重新设置连接,从而帮助路由器即刻响应安全威胁。通过与 IPsec VPN、GRE 和 Cisco IOS 防火墙协作,Cisco IOS IPS 成为允许在第一个网络入口处(分支机构或总部)实施解密、隧道端接、防火墙和流量检测的业界第一款产品。Cisco IOS IPS 能帮助客户尽量靠近攻击源阻断攻击流量。

当与思科集成多业务路由器结合使用时,Cisco IOS IPS 能通过与 Cisco IPS 传感器产品相同的方式加载并支持选定的 IPS 特征码,从而允许客户从 Cisco IDS/IPS 平台支持的 1200 多种特征码中进行选择。公司可修改现有特征码或创建新特征码来应对新发现的威胁。为了提供最佳保护,客户可选择使用包含“类似”蠕虫和攻击特征码的易用的特征码文件;并通过配置系统来丢弃与这些“类似”蠕虫和攻击签名相匹配的流量。Cisco SDM 提供了直观用户界面来设置这些特征码,包括从 Cisco.com 加载新的特征码,无需更改软件版本。Cisco SDM 能够为这些签名配置适当的路由器。

### URL 过滤(设备外和设备内选项)

思科的 URL 过滤工具支持 Cisco IOS 防火墙,允许客户将思科安全路由器与 Websense 或 N2H2 URL 过滤产品一起使用。Websense URL 过滤特性允许客户使用的 Cisco IOS 防火墙与 Websense

或 N2H2 URL 过滤软件互动，以防用户无视安全策略访问特定网站。Cisco IOS 防火墙可与 Websense 和 N2H2 服务器协作，决定允许还是拒绝(阻断)特殊的 URL。

### **高级安全网络模块(面向 Cisco 2800 和 3800 系列)**

希望部署基于硬件的专用 IDS/IPS 和内容安全解决方案的机构，可选择向 Cisco 2800 或 3800 系列路由器中添加两个安全网络模块。

Cisco IDS 网络模块可帮助实现完整的 IDS/IPS 系统，以便与其他 IDS/IPS 组件一起高效保护数据和信息基础设施的安全。Cisco IDS 网络模块为 IDS 提供专用的 CPU 并提供 20GB 的硬盘驱动器，用于记录 1000 多个受支持的 IPS 签名。

思科内容引擎网络模块提供了路由器集成内容分发系统和内容安全特性。除智能缓存和内容路由外，该模块还能用作 URL 过滤 (Websense, SmartFilter) 应用服务器。

### **路由器集成服务引起市场的浓厚兴趣**

思科看到，从小企业到大型企业，路由器集成服务引起了市场的浓厚兴趣。

### **Pep Boys**

Pep Boys 是美国著名的汽车零部件和服务连锁企业，在美国和波多黎各有近 600 家商店。为了连接零售网点并允许客户访问库存、销售点和公司应用，这家汽车零售商决定升级现有基础设施，以确保网络的高永续性和高可用性。Pep Boys 选择了提供集成加密、IPsec VPN、网络准入控制(NAC)和入侵防御功能的思科路由器。这些安全的路由器帮助 Pep Boys 满足了业务需求，包括始终保持强大的安全性等。公司的另一个目标是通过提供运行时间最长的高性能网络来确保 Pep Boys 连锁店为客户提供最佳体验。

### **Fresenius Medical Care (FMCNA)**

FMCNA 是为慢性肾病患者提供产品和服务的最大的综合医疗机构，在北美洲有 1140 家透析门诊部，拥有 28,000 多名员工。公司更换了帧中继网络并实施了医疗级网络。FMCNA 现已能够利用思科路由器内嵌的加密加速、IPsec VPN、防火墙、内部入侵防御和网络准入控制(NAC)等特性来高速访问病人信息和工作流应用。随着门诊部的不断增加，公司还能利用动态多点 VPN (DMVPN) 功能将 VPN 服务轻松扩展到一千多个位置。Cisco IOS 防火墙使公司能够始终恪守安全标准，从而满足了健康保险便携性和责任法案 (HIPAA) 以及 Sarbanes-Oxley 法案的要求。

### **选择专用安全产品还是集成安全路由器？**

部署防火墙的客户可选择思科一流的专用 Cisco ASA 安全产品或提供安全特性的思科集成多业务路由器。路由器集成的安全特性基于为安全产品开发的安全技术，并借鉴了思科 20 多年的路由经

验。思科将继续在其路由器以及专用安全产品中提供一流的内嵌安全性，以便为负责保护网络安全的客户提供多种选择。虽然集成安全与单个产品之间的界限越来越模糊，但客户还是有理由在二者间做出选择或综合使用这两种安全解决方案。

## 集成安全：适用于中小企业

您在选择安全产品时，需要保护的网络在什么位置是一个重要的考虑因素。许多公司都选择将安全集成到他们的边缘汇聚路由器中。然而，规模更大的企业倾向于通过独立的产品来保护总部安全，并通过基于交换机的防火墙服务模块来保护数据中心安全，以满足这些网络区域更高的吞吐率要求。这些企业也可能选择通过向分支机构添加提供集成安全的路由器来保护所有网络点的安全。

中小型机构与大型企业总部面临相同的安全问题，但他们通常缺少/或根本没有本地 IT 资源来管理安全解决方案。在 IT 资源有限的情况下，部署和管理多个产品将与支持模式发生冲突。将多个产品集成到一个集中管理的平台中可简化这些小型机构的排障和维护工作，从而降低 TCO。

思科集成多业务路由器适用于小型企业，它为连接远程机构、移动用户、合作伙伴外联网或电信运营商管理的客户端设备(CPE)提供了丰富的集成解决方案。通过基于 Cisco IOS 软件的 VPN、防火墙和 IPS 功能以及可选的增强型 VPN 加速、IDS 和内容引擎网络模块，思科为中小型机构提供了业界最强韧、适应能力最强的安全解决方案。

## 公司偏好

选择集成安全解决方案还是专用的网络安全解决方案还受客户喜好的影响：是希望利用现有的基础设施、部署和运行架构；还是对某些特性有特殊需求。某些公司倾向于“让路由器和交换机各自开展本职工作”，或者从管理的角度看，因为设立了专门的安全和 VPN 管理部门，因此，公司希望将安全和 VPN 基础设施与联网基础设施相分离。

## 未来成本评估

利用现有的路由器或交换机来确保安全性 – 添加 Cisco IOS 软件的安全版本和 VPN 模块 – 是延长基础设施寿命的经济高效的方法，能最大限度地提高最初投资的回报率并大幅度降低与更换早期产品相关的长期成本和业务中断。评估长期成本时，计划中和意外停机成本是最重要的考虑因素。

集成服务能力的提高允许网络支持将来的多媒体汇聚部署，从而大幅度提高了网络的灵活性和可用性。此外，这些功能还使企业能够加快响应速度以避免错失良机、缩短新服务的部署时间、避免不必要的短期产品升级、并通过提高可扩展性来降低 TCO。

## 特性区别

由于思科将 Cisco ASA 安全产品技术集成到了 Cisco IOS 防火墙中，因此，两个安全解决方案的特

性集越来越相似。也就是说，思科将继续使用安全产品来改进并验证新技术，然后再将它们应用到集成多业务路由器中。如果企业需要最先进的创新安全特性，Cisco ASA 安全产品通常可先于 Cisco IOS 防火墙提供全新的安全特性。

## 总结

IT 经理一直都高度重视网络安全。随着安全要求的提高，企业需要更集成的安全解决方案来保护所有的网络入口。思科始终致力于通过不断增强其安全产品来大幅度提高网络识别、抵御和响应威胁的能力。

思科集成多业务路由器采用内嵌的安全硬件加速技术，集成了 Cisco IOS VPN、防火墙和内部 IPS 服务，提供了业界最全面的自适应安全解决方案。集成多业务路由器尤其适用于满足小型企业和远程机构的要求，为他们提供集成安全，以便最大限度地减少操作系统和设备数量，客户 IT 资源短缺问题。

思科集成安全解决方案将强大的 Cisco IOS 软件功能和业界领先的局域网和广域网连接与世界一流的安全功能结合在一起，能帮助公司利用现有网络基础设施并在安全需求最迫切的地方部署安全产品。Cisco IOS 软件允许客户使用路由器上全新的集成安全特性并将这些安全功能应用到网络中的任何位置，无需添加硬件。思科集成多业务路由器能够保护所有的网络入口并阻断直接针对网络基础设施的攻击。通过部署作为思科智能商业规划一部分的思科集成多业务路由器，技术决策人有理由相信他们目前的技术投资能够通过扩展来实现长期网络目标。

## 更多信息

关于模块化 Cisco 800, 1800, 2800 和 3800 系列集成多业务路由器的集成安全特性的更多信息，请参阅以下文献：

### 产品简介

思科集成多业务路由器的安全特性

[http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1650/cdcont\\_0900aecd80169b0a.pdf](http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1650/cdcont_0900aecd80169b0a.pdf)

### Q&A

思科集成多业务路由器的安全特性

[http://www.cisco.com/en/US/products/ps5854/products\\_qanda\\_item0900aecd80169bba.shtml](http://www.cisco.com/en/US/products/ps5854/products_qanda_item0900aecd80169bba.shtml)

### Miercom 实验室测试总结报告

思科集成多业务路由器

<http://www.miercom.com>

## 网络准入控制

[http://www.cisco.com/en/US/netsol/ns466/networking\\_solutions\\_package.html](http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html)

## 网络基础设施保护

[http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_data\\_sheet09186a00801f98de.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_data_sheet09186a00801f98de.html)

## 思科路由器及 Security Device Manager

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

## 技术信息

如需详细了解 WebVPN 及其他安全技术，请访问：

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

## **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) 85155000

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) 23024000

传真: (8621) 23024450

## **广州**

广州市天河区林和西路 161 号中泰国际广场 A 塔 34 层

邮编: 510620

电话: (8620) 85193000

传真: (8620) 85193008

## **成都**

成都市顺城大街 308 号冠城广场 23 层

邮编: 610017

电话: (8628) 86961000

传真: (8628) 86528999

翻译日期: 2007年2月1日