产品简介

思科集成多业务路由器上的网络安全特性

本文将简要介绍Cisco® 800、1800、2800 和 3800 系列集成多业务路由器上的网络安全特性。

产品概述

目前，思科系统®公司正在用能够提供安全的数据、语音和视频服务的新型集成多业务路由器重新定义最佳路由功能。凭借思科 20 多年来的领先地位和创新传统，模块化的Cisco® 1800 系列、2800 系列、3800 系列和固定配置的Cisco® 800 系列、1800 系列集成多业务路由器不但能提供业界最全面的安全服务，还能智能地在平台中嵌入数据、安全、语音和无线技术，以可扩展的快速方式提供关键业务应用。Cisco 800、1800、2800 和 3800 系列适用于小企业和大型企业的分支机构，提供了一种功能丰富的集成解决方案，便于连接远程办公机构、移动用户、合作伙伴外部网或电信运营商管理的客户端设备（CPE）。

思科的集成多业务路由器能够透明地与Cisco 7200 系列、7301 和 7600 系列高端安全路由器互操作。不仅如此，Cisco 7200 系列和 7301 汇聚路由器还能与集成多业务路由器一样，使用相同的 Cisco IOS® 软件创新、全面的高级安全特性，因而使客户能够建立真正有效的集成式智能网络。

通过将成熟的 Cisco IOS 软件功能与业界领先的 LAN/WAN 连接与世界级网络安全特性相结合，集成化路由器安全解决方案能够为客户提供以下优势：

- **“充分利用已有设施”**——充分利用现有网络基础设施，无需添置硬件，就能通过 Cisco IOS 软件在路由器上实施新安全特性；
- **“将安全功能部署到最需要的地点”**——灵活地将防火墙、入侵防御系统（IPS）和 VPN 等安全功能应用到网络的任意位置，以提高安全保护能力；
- **“保护网关”**——可在网络的所有入口处部署最佳安全功能；
- **“节省资金和时间”**——减少设备数量，从而降低了培训和管理成本；
- **“保护网络基础设施”**——保护路由器，防御直接针对网络基础设施的攻击，例如分布式拒绝服务（DDoS）攻击。

目录

思科自防御网络.....3

Cisco 800、1800、2800 和 3800 集成多业务路由器的安全特性和优点.....4

- Cisco IPSec VPN.....5
- Cisco IOS防火墙和内部入侵防御（IPS）.....5
- 网络基础保护（NFP）.....6
- 网络控制和抑制.....6
- 其他安全特性.....6

Cisco 800、1800、2800 和 3800 系列路由器的硬件安全特性.....16

嵌入式服务管理：思科路由器和安全设备管理器（SDM）.....17

认证.....18

订购信息.....18

服务与支持.....20

更多信息.....21

思科自防御网络

Cisco 800、1800、2800、3800 系列集成多业务路由器与 Cisco 7200 系列和 7301 头端路由器是思科自防御网络（SDN）的有机组成部分，SDN 是一种可帮助机构识别、预防和应对网络安全威胁的战略。利用基于 Cisco IOS 软件的 VPN、防火墙和 IPS，以及可选的增强型 VPN 加速、入侵检测系统（IDS）和内部引擎网络模块（适用于 Cisco 2800 和 3800 系列），思科集成多业务路由器不但能为分支机构提供业界功能最强大的自适应安全解决方案，还能利用 Cisco 7000 平台在头端高端提供补充支持。

思科自防御网络构建的基础是集成化安全、协作式安全系统和自适应威胁防御，而网络基础保护则为它们提供了底层支持结构。

SDN 集成化安全使每个网络元素都成为防御点，这其中包括路由器、交换机、设备和终端，从而为网络安全带来了革命性的改变。集成化安全使路由器成为了保护网络的关键设备，其核心因素包括：安全连接、威胁防御，以及信任和身份识别。

- **安全连接**——提供便于扩展、可传输多种流量的安全网络连接。例如 VPN、动态多点 VPN（DMVPN）、多虚拟路径转发（VRF）和多协议标签交换（MPLS）安全环境、语音和视频型 VPN（V3PN）以及高度安全语音等。
- **威胁防御**——利用网络服务预防网络攻击和威胁并对其作出相应。包括 Cisco IOS IPS 和 Cisco IOS 防火墙。
- **信任和身份识别**——使网络能够利用验证、授权和记帐（AAA），公共交换密钥（PKI）及 802.1x 等技术，智能地保护终端。

凭借 SDN 协作安全系统，安全成为了一个全网系统，包括终端、网络和策略。例如网络准入控制（NAC）等解决方案，其中多项服务和设备相互协作，通过主动管理而防御攻击。

SDN 自适应威胁防御（ATD）可动态防御多个层次的威胁，更为紧密地控制网络流量、终端、用户和应用，从而进一步降低了安全风险。ATD 将服务整合到少数几个设备上，从而简化了架构设计并降低了运营成本。这种创新方式在高性能解决方案中将安全、多层智能、应用保护，以及网络级控制和威胁抑制进行了出色的结合。ATD 的主要组件包括 Anti-X 防御、应用安全，以及网络控制和抑制，实现了经过更出色协调的威胁防御。随着 12.3(14)T 软件版本的面世，思科将继续实施自防御网络安全战略的下一阶段，具体信息如下所述。

- Anti-X 防御－通过创新的、面向流量和内容的安全服务，防御和应对网络威胁。核心安全增强技术包括防火墙、入侵防御系统（IPS）和异常事件检测，它们可与应用检测服务，如网络防病毒、防间谍软件、防垃圾邮件、分布式拒绝服务（DDoS）防御和 URL 过滤等相结合。这为重要的网络安全实施点提供了精确的流量检测服务，因此可在恶意流量在网络中广泛传播前抑制它们。

例如: 通过高级应用检测和控制来保护 Web 服务器免遭损害－HTTP 和电子邮件检测引擎可阻止用户在 Web 服务器上书写或放置内容。

- 应用安全－通过应用级访问控制、应用检测，以及正确的应用使用策略、Web 应用控制和交易保密性等的实施，提供了先进的业务应用保护。

例如: 通过内部入侵防御来抵御网络边缘处的蠕虫－特征定制和字符串引擎支持可在边缘抵御蠕虫的攻击（防间谍软件、防恶意件等）。

- 网络控制和抑制－网络智能和安全技术的虚拟化提供了先进的审查和关联功能，可通过主动

管理和防御功能，控制和保护 IP 语音（VoIP）等网络组件或服务。
例如：通过支持 VRF 的防火墙在保持业务连续性的同时实现最高安全性－针对每个环境的防火墙策略使用户可按部门定制安全策略，而不会干扰工作流程。

网络基础保护（NFP）是思科自防御网络的一个不可缺少的常用组件，可保护网络基础设施免遭攻击和安全漏洞的影响，尤其在网络级，这一功能尤为明显。实例包括控制平面监管、基于网络的应用识别（NBAR）和 AutoSecure 等。

Cisco 800、1800、2800 和 3800 **集成多业务路由器的安全特性和优点**
集成多业务路由器专为提供安全服务而设计，提供了硬件和软件安全特性的独特组合。为支持 Cisco 800、1800、2800 和 3800 系列路由器上的网络安全特性，Cisco IOS 软件提供以下特性集：

- 高级企业服务
- 高级 IP 服务
- 高级安全

如果想详细了解相应特性集的选择方法，请访问：
http://www.cisco.com/en/US/products/sw/iosswrel/ps5460/prod_bulletin09186a00801af451.html。

表 1 列出了 Cisco 800、1800、2800 和 3800 系列集成多业务路由器的某些硬件安全特性。

表1 Cisco 800、1800、2800和3800系列集成多业务路由器的硬件安全特性

特性	**Cisco 3800**	**Cisco 2800**	**Cisco 1800**	**Cisco 800**
内部 VPN 加密加速（IPSec DES、3DES 和 AES 128、192 和 256）	每种型号的标准配置。需 Cisco IOS 软件高级安全或更高特性集支持。	每种型号的标准配置。需 Cisco IOS 软件高级安全或更高特性集支持。	每种型号的标准配置。需 Cisco IOS 软件高级安全或更高特性集支持。	每种型号的标准配置。需 Cisco IOS 软件高级安全或更高特性集支持。
高级 VPN 加密加速利用 IPPCP 执行硬件辅助压缩	可通过增强模块提高性能和隧道扩展能力。（产品编号：Cisco 3825: AIM-VPN/EPII-PLUS Cisco 3845: AIM-VPN/HPII-PLUS）	可通过增强模块提高性能和隧道扩展能力。（产品编号：AIM-VPN/EPII-PLUS）	可在模块化的 Cisco 1800 上通过增强模块提高性能和隧道扩展能力。（产品编号：AIM-VPN/BPII-PLUS）	—
IDS 网络模块*	可通过（产品编号 NM-CIDS）增强性能	可通过（产品编号 NM-CIDS*）增强性能	—	—
用于提高内	可利用思科内容	可利用思科内容引擎	—	—

特性	Cisco 3800	Cisco 2800	Cisco 1800	Cisco 800
容安全性的内容引擎网络模块	引擎网络模块增强性能（产品编号 CE-NM）	网络模块增强性能（产品编号 CE-NM*）		

表 2 提供了 Cisco 800、1800、2800 和 3800 系列的集成化安全特性和优点。补充型 Cisco 7000 头端路由器也提供其中许多特性。对于列出的大多数特性，本文中还包含连接到更多信息的超级链接。

表 2 Cisco 800、1800、2800 和 3800 系列路由器的主要集成化安全特性和优点

特性	优点
Cisco IPSec VPN	
MPLS VPN 支持	专为分支机构而优化的客户边缘（CE）功能，通过多 VRF 感知型防火墙和 IPSec，将客户 MPLS-VPN 网络扩展到了 CE。
DMVPN	提供了一种在分支机构间建立虚拟全网格 IPSec 隧道的灵活、可扩展方式。添加新分支时无需在中心进行任何配置。
Cisco Easy VPN Remote 和 Server 支持	该特性可从单一终端主动将新的安全策略分发给远程地点，从而简化了点对点 VPN 的管理。
V3PN	通过 VPN，经济有效地向任意地点提供集成的语音、视频和数据。
虚拟隧道接口（VTI）	简化了 VPN 配置和设计。
多 VRF 和 MPLS 安全环境	支持位于分支机构的多个独立环境（编址、路由和接口），以便隔离部门、分支或客户。所有环境可共享一条到核心的上行链路（例如 IPSec VPN 或帧中继/ATM），且仍能保持它们之间的安全隔离。
安全配置/数字证书	在安全网络基础设施中注册新远程地点设备的一种简单、强大的机制。
Cisco IOS 防火墙和内部入侵防御（IPS）	
Cisco IOS 防火墙	一个理想的单设备安全和路由解决方案，可保护广域网入点。现在支持 IPv6。
透明防火墙	无需更改地址，即可将现有网络部署划分为安全信任区！支持子接口和 VLAN 中继。同时支持透明防火墙和第三层防火墙。
高级应用检测和控制	使用检测引擎来确保符合协议，防止恶意或未授权行为，如端口 80 隧道或电子邮件连接误用。
VRF 感知型防火墙	该防火墙已纳入单环境级服务列表，可用于执行 VRF 部署。
H.323	
内部入侵防御（IPS）	一种内部深层分组检测解决方案，可与 Cisco IOS 软件共用，有效抵御网络攻击。IPS 可以丢弃流量，发送警报，进行隔离，或者重新建立连接，使路由器立即对安全威胁作出响应，保护网络的安全。
透明 IPS	
URL 过滤（设备外）	帮助 Cisco IOS 防火墙与 Websense 或 N2H2 URL 过滤软件交互，可根据公司安全策略防止用户访问某些网站。

网络基础保护（NFP）	
控制平面监管	监管发往控制平面的流量速率，以降低 DoS 攻击的成功概率。即使遭受了攻击，也能保持网络可靠性。
AutoSecure	简化路由器的安全配置，降低配置错误风险。
NBAR	Cisco IOS 软件中的这种分类引擎可以识别各类应用。进行应用识别后，网络可以为该应用激活特定服务，并根据需要提供适当的控制级别。
CPU/内存阈值设定	通过保留 CPU 和内存，这个特性能够保证路由器在高负载下正常操作，例如遇到攻击时。
SSHv2	
SNMPv3	
基于角色的 CLI 访问	提供基于视图的 CLI 命令访问，安全执行 NetOps、SecOps 和最终用户之间高度安全的逻辑隔离。
网络控制和抑制	
NAC	只允许符合预定访问和安全策略的信任设备接入网络，防止病毒和蠕虫传播。
其他安全特性	
AAA	使管理员能够为每条线路（每个用户）或每种服务（例如 IP、IPX 或 VPDN）动态配置验证和授权类型。
为集成交换提供标准 802.1x 支持	标准 802.1x 应用要求使用合法访问证书，以便使对于受保护信息资源的未授权访问和部署不安全的无线接入点变得更加困难。
Cisco IOS 证书服务器和客户端	使路由器可作为网络上的证书授权设备。
管理	
利用思科 SDM 执行安全管理	利用 HTTPS 和 SSH，可以远程访问这个嵌入在 Cisco IOS 软件接入路由器中、易于使用的 Web 型直观管理工具。
企业安全管理	可以利用以下两个工具执行企业安全部署： • CiscoWorks VMS 是一种适合大中型 VPN 部署的全面管理工具；它可以配置 IPSec 隧道和防火墙规则。 • Cisco IP Solution Center（ISC）3.0 是一种适合电信运营商使用的 MPLS IPSec 管理工具。

Cisco IPSec VPN：VPN 隧道和加密、DMVPN、Easy VPN、V3PN、虚拟隧道接口（VTI），多 VRF 环境和安全配置/数字证书

VPN 隧道和加密

VPN 一直是发展最快的一种网络连接方式，思科通过将 VPN 硬件嵌入到集成多业务路由器中，使其达到了新标准。Cisco 800、1800、2800 和 3800 系列路由器采用了内部硬件加密加速，使主处理器无需处理互联网协议安全（IPSec）、高级加密标准（AES）、数据加密标准（DES）和三重 DES（3DES）加密和 VPN 流程，在尽量不影响路由器 CPU 的情况下提高了 VPN 的吞吐率。如果还需要提高 VPN 吞吐率或扩展能力，可以选择在模块化 Cisco 1800、2800 和 3800 系列上添加 VPN 加密高级集成模块（AIM）。利用这种方式，可以提高 VPN 的性能——比以前的型号加快四倍，且降低路由器 CPU 总体使用率。与以前的型号相比，可选 AIM 能够将加密性能和隧道

扩展能力提高 10 倍。内部 VPN 加速器和基于 AIM 的 VPN 加速器的主要特性包括：

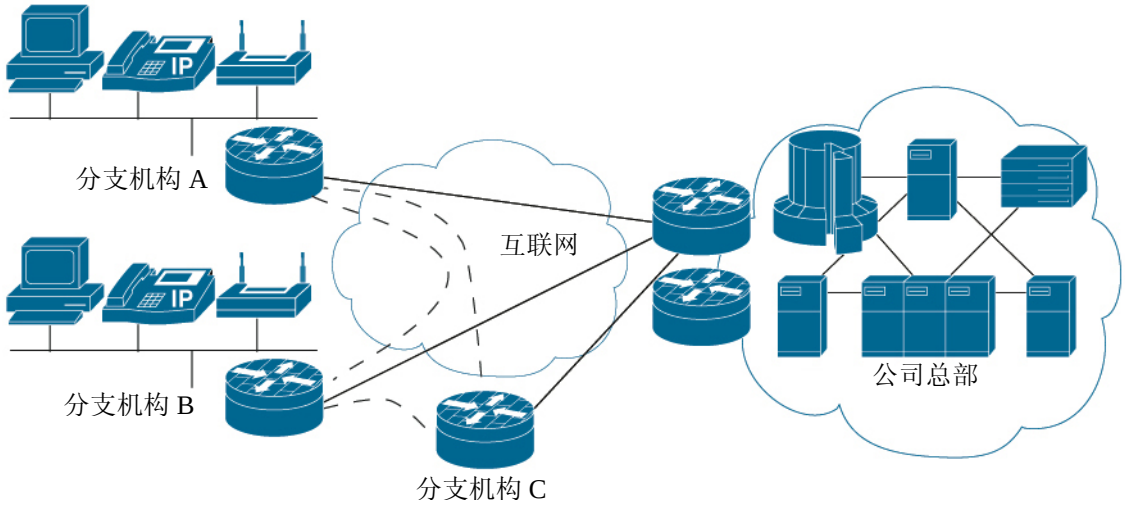
- 能够以数倍于全双工 T3/E3 的速度对 IPSec 加速；
- 能够为所有模块（内部 VPN 和基于 AIM 的 VPN）提供硬件 DES、3DES 和 AES（128、192 和 256）加密算法加速；
- 支持 Rivest、Shamir、Aldeman（RSA）算法和 Diffie-Hellman 验证；
- 利用安全散列算法 1（SHA-1）或消息摘要算法 5（MD5）散列算法保证数据完整性；
- 添加了 VPN 加密模块，在硬件中支持第三层（IP 负载压缩协议[IPPCP]）压缩。

除通用 IPSec 外，集成多业务路由器还可使用能够将 IPSec 和通用路由封装（GRE）协议相结合的另一种隧道技术。采用了 GRE 隧道技术的 IPSec 是思科独家开发的解决方案，由于能够通过 VPN 传输动态路由协议，此隧道技术提供了高于纯 IPSec 解决方案的网络永续性。除提供故障恢复机制外，GRE 隧道能加密组播和广播分组及非 IP 协议。利用支持 IPSec 的 GRE，思科集成多业务路由器不但支持 AppleTalk 和 Novell 互联网分组交换（IPX）等协议，还支持视频等组播和广播应用。

动态多点 VPN（DMVPN）

思科率先推出了第一台具有 DMVPN 功能的路由器。利用 DMVPN，可以扩展的按需全网状 VPN 不但能缩短延迟，保留带宽，还能简化 VPN 部署（见图 1）。DMVPN 特性建立在思科 IPSec 和路由特性的基础之上，可以动态配置 GRE 隧道、IPSec 加密、NHRP、OSPF 和 EIGRP。这种 VPN 隧道的动态配置与服务质量（QoS）和 IP 组播等技术相结合，能够优化语音和视频等对延迟敏感的应用。另外，DMVPN 还能减轻管理负担，因为添加新分支或设置分支间的连接时，不需要对中心进行任何配置。

图 1 DMVPN 实例



Easy VPN

Easy VPN 是一种 IPSec 解决方案，能以最小的开销建立星形 VPN 拓扑，同时提供高扩展能力。Easy VPN 能够简化思科 PIX 防火墙、Cisco VPN 3000 系列集中器和各类思科路由器 VPN 解决

方案的供应和管理。Easy VPN 已经成功地运用到了数千个客户环境中，它不但能利用“策略推行”技术简化配置，还能提供丰富的特性和策略控制功能。

Easy VPN 具有以下优点：

- Easy VPN 能够利用同一台中央路由器同时支持硬件（接入路由器）CPE 和软件远程接入客户端。Cisco VPN Client 软件可以安装在 PC、Mac 和 UNIX 系统上，以便为基于路由器的 VPN 免费添加远程接入连接。由于为硬件 CPE 和软件客户端采用的是同一种技术（Easy VPN），因而简化并统一了配置、监控和 AAA 服务，最终降低了总拥有成本。
- Easy VPN 同时为 CPE 路由器和单个用户提供基于路由器的本地验证，以及集中 RADIUS 和 AAA 验证方式。另外，还可以利用基于 802.1x 的验证核查每个 CPE 处的主机。
- Easy VPN 提供数字证书，提高了预共享密钥的安全性。
- 为中央 Easy VPN 集中器提供负载平衡，即自动将负载分布到多台 Easy VPN 服务器上。由于各公司能够将备份集中器信息的策略分发部署到 CPE 上，因而无需重新配置 CPE 就能扩展解决方案。
- 通过虚拟化 Easy VPN Server，电信运营商能够利用一个平台向多个客户提供 VPN 服务。
- Easy VPN 提供全部特性集成，包括动态 QoS 策略分配、防火墙和 IPS、隧道拆分以及用于监控性能的思科服务保证代理和 NetFlow。
- 利用思科路由器和安全设备管理器（SDM），可以通过向导快速部署 Easy VPN 与 AAA 和防火墙的集成，以及提供远程 Easy VPN 客户端的实时图形监控。
- Cisco IOS 软件、Cisco PIX 防火墙和 Cisco VPN 3000 系列集中器等所有思科 VPN 服务产品系列都支持 Easy VPN。

语音和视频型 IPSec（V3PN）

Cisco 800、1800、2800 和 3800 系列以及 Cisco 7000 高端解决方案均支持 V3PN。V3PN 提供的 VPN 基础设施能够在支持 QoS、高度安全的 IPSec 网络上实现数据、语音和视频的收敛，使利用 IP 传输网络的客户能够获得与 WAN 链路同等的语音和视频应用传输安全性和有效性。与市场上的许多其它 VPN 设备不同，思科集成多业务路由器能够满足各种网络拓扑和流量要求，因而能支持多服务 IPSec VPN。V3PN 的端到端网络架构充分利用了思科安全路由器和 Cisco IOS 软件的强大功能来保护语音流量。

要通过 IPSec VPN 提供高质量语音和视频传输，不仅需要对流量加密，还需要采用各种多服务和 IPSec VPN 技术。支持思科 V3PN 的 Cisco IOS 软件技术包括以多服务为中心的 QoS、对各种流量类型的支持、对多服务网络拓扑的支持以及增强型网络故障恢复功能。

虚拟隧道接口（VTI）

目前，VPN 正在逐渐成为建立安全 WAN 连接的主流解决方案。它将取代或增强使用租用线路、帧中继或 ATM 的专用网络，更加经济、有效、灵活地将远程和分支机构与中央站点相连。但是，这种趋势要求 VPN 设备不断提高性能，同时支持 LAN 和 WAN 接口，并提供高网络可靠性。思科 IPSec 虚拟隧道接口（VTI）是一种全新的工具，利用它，客户可以在各地点的设备之间配置基于 IPSec 的 VPN。IPSec VTI 隧道能够在公共 WAN 上建立一条专用路径，然后用新的分组报头封装流量，以保证将其传输到特定的目的地。由于流量只能在某个端点进入通道，因而网络是专用的。另外，IPSec 还能提供真正的保密性（与加密效果相同），而且可以传输加密流量。

利用思科开发的 IPSec VTI，企业不但可以充分利用经济有效的 VPN，而且不需要牺牲质量和可

靠性就可以为其数据网络添加语音和视频。Cisco IPSec VTI 不仅为站点间 VPN 提供高度安全的连接，还可以与思科 AVVID（集成语音、视频和数据架构）相结合，通过 IP 网络提供收敛的语音、视频和数据。

为电信运营商提供多 VRF 和 MPLS 安全环境

多 VRF 也称为 VRF-Lite，能够在同一台物理路由器中配置和维护多份路由和转发表。多 VRF 与以太网 VLAN 技术和帧中继等 WAN VPN 技术相结合，即可在一个物理网中提供多种逻辑服务，从而将保密性和安全性扩展到分支机构 LAN。

带多 VRF 的思科路由器能以重叠的 IP 地址支持多家公司，且能保持数据、路由和物理接口的隔离。如果想详细了解多 VRF，请参考产品公告。

安全配置和数字证书

安全设备配置（SDP）提供了一种简单、强大的机制，可在安全的网络基础设施中推出新远程机构设备。相对不太了解技术的远程机构管理员可在配置基本互联网连接后，从 SDM 启动 SDP Web 界面。只需使用他们自己的用户名、密码和 SDP 注册 URL，远程用户就可全面配置其站点的路由器，使用任意 Cisco IOS 支持的 IPsec 选项，他们也可采用一个基本引导程序配置，将路由器应用于更为复杂的服务供应基础设施。SDP 利用 Cisco IOS 的集成证书授权服务器，来向 IPsec 网络设备发放安全、可扩展的数字证书。这些解决方案的组合使 Cisco IOS 成为了集成网络安全领域的业界领先产品。

Cisco IOS 防火墙内部入侵防御

Cisco IOS 防火墙

Cisco IOS 防火墙是为思科路由器提供的状态化检测防火墙选项，它以市场领先的 PIX 防火墙技术为基础，安装了 Cisco IOS 软件高级安全或更高版本特性集的所有集成多业务路由器都支持这个组件。Cisco IOS 防火墙是一个理想的独立安全和路由解决方案，能够保护广域网入口。虽然网络中心是设置防火墙和检查恶意流量、以防御攻击的常用位置，但并不是部署网络安全功能的惟一位置，分支机构也是网络中设置防火墙和检查恶意流量的重要位置。

Cisco IOS 防火墙的主要特性包括：

- 状态化防火墙，包括 DoS 保护；
- 提高对应用、流量和用户的感知，以便识别、检测和控制应用；
- 对语音、视频及其它应用执行高级协议检测；
- 对每个用户、接口或子接口制订安全策略；
- 提供紧密集成的身份识别服务，可对每个用户执行验证和授权；
- 利用能够在 NetOps、SecOps 和最终用户之间安全地逻辑划分路由器的、基于角色的 CLI 访问视图，以及思科 SDM 中的防火墙策略视图，来简化管理。

Cisco IOS 防火墙不但能在网络周边建立单保护点，还能将安全策略实施作为网络本身的有机组成部分。利用专用策略实施和集成策略实施的灵活性、经济性和有效性，可以为分支或远程机构的外部网和内部网周边及互联网连接提供安全可靠的解决方案。Cisco IOS 防火墙通过 Cisco IOS 软件集成到网络中，使客户能够在同一台路由器中使用高级 QoS 特性。

Cisco IOS 软件支持 IPv6 防火墙，并可在 IPv4 和 IPv6 混合环境中部署。Cisco IOS IPv6 防火墙不但能对 IPv6 流量执行状态化协议检测（异常检测），还能抵御 IPv6 DoS 攻击。

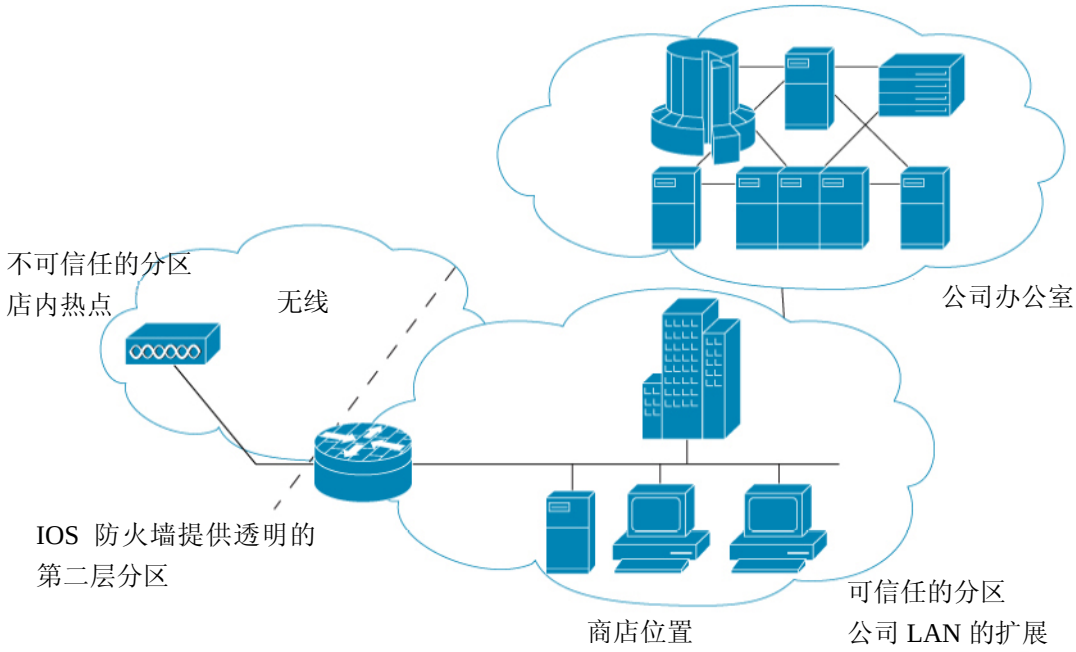
透明防火墙

除第三层状态化防火墙外，Cisco 800、1800、2800 和 3800 系列集成多业务路由器和 Cisco 7000 高端解决方案还支持透明防火墙设置，以便为第二层连接提供第三层防火墙功能。透明防火墙的优点包括：

- 无需对 IP 子网重编号就能方便地为现有网络添加防火墙；
- 支持子接口和 VLAN 中继；
- 支持生成树协议——能够针对 802.1d 正确地处理 BPDU 分组，而不只是“通过或丢弃”；
- 在同一台机器上支持第二层和第三层防火墙的混合；
- 不需要为接口分配 IP 地址；
- 支持 DHCP 直通，可在相反的接口（双向）上分配 DHCP 地址。

透明防火墙的应用如图 2 所示。

图 2 在不修改地址的前提下将现有网络分成多个安全信任区，Cisco IOS 防火墙负责提供透明的第二层分区。



高级应用检测和控制

Cisco IOS 防火墙添加了包含 HTTP 和若干电子邮件检测引擎的高级应用检测和控制功能。公司有时希望根据具体情况允许某些常见应用，例如 Web 浏览，通过其防火墙。而不幸的是，这种访问可能会使某些 HTTP 应用，例如即时消息（IM），趁机非法盗用该防火墙后面的主机。传统的防火墙是根据源地址和目标地址、协议和端口号来阻挡流量的，而 Cisco IOS 防火墙 HTTP 检测引擎则能够保证遵守协议要求，防止恶意或非法流量通过，例如端口 80 隧道、恶意分组和特洛伊木马等。HTTP 检测引擎能够为 Cisco IOS 防火墙提供智能特性，不但能阻挡非 HTTP 流量，还能保证 HTTP 流量等合法 Web 浏览流量顺利通过防火墙，而 IM 或类似流量不能通过防火墙，以便网络管理员能够更加精确地控制穿越防火墙的应用。其优点包括：

- 能够为端口 80 制订和执行安全策略；
- 能够防止将流量送入 HTTP 的恶意应用冒用端口 80，或者利用端口 80 逃避检查；
- 执行协议异常检测服务；
- HTTP 检测引擎
  - 检测 HTTP/Web 连接误用
  - 防止协议伪装
  - 严格执行 RFC 标准
  - RFC 命令控制（例如 get 或 put）
  - 执行 URL 或报头长度策略
  - 支持实时警报和审计跟踪消息
  - MIME 型过滤和内容校验
- 电子邮件检测引擎
  - SMTP/ESMTP/POP3/IMAP

- 检测电子邮件连接误用
- 防止协议伪装
- 严格执行 RFC 标准

VRF 感知型防火墙

目前，Cisco IOS 防火墙已包含在单环境级服务列表中，可用于 VRF 部署。利用 VRF 感知型防火墙，客户能够充分利用思科 VRF 技术的强大功能：

- 为每个网络提供可感知 VRF 的防火墙解决方案
- 以 VRF 为单位支持当前全局参数
- 用 VRF 信息标记系统记录
- 能够限制每个 VRF 的防火墙连接数量

H.323 支持

Cisco IOS 防火墙支持 H.323 第 1 版本和第 2 版本检测。H.323 V2 提供的选项多于 H.323 V1，包括“快速启动”选项。快速启动选项能够缩短用户进行的数据连接和接收（语音、视频）之间的延迟。H.323 V2 检测与 H.323 V1 兼容。

利用 H.323 V1，能够在客户端和服务器间建立了 TCP 连接（H.225 通道）之后，为介质控制打开一条独立通道（H.245 通道），然后利用这条通道进一步协商音频和视频的多媒体通道。

H.323 V2 客户端可与正在端口 1720 上接收信息的服务器建立连接。客户端与服务器之间的数据通信可利用任何高 UDP 端口（1024～65536）动态协商。

防火墙利用这些端口信息以及客户端提供的连接信息在防火墙中建立动态 ACL 项。当 TCP 或 UDP 连接中断后，防火墙将从相应的 ACL 中删除这些动态项。

入侵防御系统（IPS）

思科率先在路由器中提供了 IPS 功能。Cisco IOS IPS 是一种内部深层分组检测解决方案，可与 Cisco IOS 软件共用，有效抵御网络攻击。Cisco IOS IPS 可用于入侵防御和事件通知，并能够充分利用思科 IDS 系列中采用的技术，包括 Cisco IDS 4200 系列传感器、Cisco Catalyst 6500 系列 IDS 服务模块和网络模块硬件 IDS 设备。由于 Cisco IOS 软件 IPS 安装在内部，它可以丢弃流量，因而使路由器能够快速对安全威胁作出响应，有效保护网络安全。

一般情况下，部署 IPS 系统的目的是检查头端处的恶意流量，但是，保护分支机构也很重要，因为这样才能在最接近网络入口的地方终止恶意流量的传输。如果在分支机构利用 Cisco IOS IPS，与分支机构相连的路由器就可以丢弃流量，发送警报，进行隔离，或者重新建立连接，将攻击流量阻挡在发源地，或者尽快从网络中删除。这些操作能以特征为单位配置。虽然 IT 专家都赞同这些防御方法，但在每个接入点都部署 IPS 系统是非常昂贵的。而现在，将 IPS 解决方案集成到现有接入路由器中之后，只需支付路由器的费用就可以在整个网络中实施这些最佳实践。

其优点包括：

- 能够像思科 IDS 传感器设备那样加载和支持选定的 IPS 特征；
- 可供选择的特征数量不断增加，目前，思科 IDS 传感器平台支持的特征总数已经超过了 1200 个；

- 用户可以修改现有特征，也可以创建新特征，以便抵御新型威胁（对每个特征的操作可以独立执行）；
- 利用思科 AVVID 合作伙伴 Trend Micro 提供的全球病毒检测服务。

利用 Cisco IOS IPS，希望进一步增强入侵保护的用户还可以选择易于使用、包含“最有可能出现的”蠕虫和攻击特征的特征文件。与这些高度确定的蠕虫和攻击特征相匹配的流量将被立即丢弃。思科 SDM 提供的直观用户界面可以提供这些特征，包括从 Cisco.com 上载新特征，而且不需要修改软件镜像，随后思科 SDM 可根据这些特征对路由器作相应的配置。

透明 IPS

从 12.4(第一版)T 开始，除支持第三层 IPS 外，Cisco 800、1800、2800 和 3800 系列集成多业务路由器和 Cisco 7000 头端解决方案将支持透明 IPS，它能为第二层连接提供第三层 IPS。透明 IPS 的优点包括：

- 无需对 IP 子网重编号，即可方便地向现有网络添加 IPS
- 支持子接口和 VLAN 中继
- 生成树协议支持－正确地处理每 802.1d 的 BPDU 分组，而不只是“通过或丢弃”
- 支持同一路由器上的第二层和第三层 IPS 混合
- 不需要为接口分配 IP 地址
- 支持 DHCP 直通，可在相反的接口（双向）上分配 DHCP 地址

URL 过滤

思科提供的 URL 过滤（设备内或设备外）能够支持 Cisco IOS 防火墙，使客户能够将 Websense 或 N2H2 URL 过滤产品与思科路由器共用。Websense URL 过滤特性能够帮助 Cisco IOS 防火墙与独立服务器上运行的 Websense 或 N2H2 URL 过滤软件交互，以便根据安全策略防止用户防止某些网站。Cisco IOS 防火墙与 Websense 和 N2H2 服务器配合，能够批准或拒绝（阻止）某 URL。如果想了解设备内 URL 过滤和内容安全的更多信息，请参考 Cisco 2800 和 3800 系列上用于执行 URL 过滤功能的内容引擎网络模块。

网络基础保护（NFP）（Cisco IOS 软件，包括在 IP Base 和更高版本中）：控制平面监管、AutoSecure、NBAR、CPU/内存阈值设定、SSHv2、SNMP 和基于角色的 CLI 访问

控制平面监管

即使是功能最强的软件和硬件架构，也有可能遭受 DoS 攻击。DoS 攻击的形式是伪装成发往控制平面处理器的某种类型的控制分组，向某网络基础设施发送大量垃圾流量，直至使其瘫痪。为阻止这种流量及其它类似针对网络核心的威胁，Cisco IOS 软件在路由器中采用了可编程监管功能，以便限制或“监管”通过控制平面的流量。该特性称为控制平面监管，可以完全限制特定流量类型通过，或者在超过某个阈值之后发现并限制特定流量类型通过。

AutoSecure

AutoSecure 是 Cisco IOS 软件的一个特性，能够简化路由器的安全配置和减小配置错误风险。利用适合经验丰富的用户的交互模式，可以提示用户定制安全设置和路由器服务，从而更加严格地控制路由器的安全功能。如果未经培训的用户希望在无需太多人工干预的情况下快速保护路由器，可以使用 AutoSecure 的非交互模式。该模式可以按照预先设定的默认特性集自动实施路由器安全功能。只需一个命令，就可以配置好路由器的安全设置，并关闭不必要的系统流程和服务，有效消除潜在的网络安全风险。

NBAR

NBAR 是 Cisco IOS 软件中的一个分类引擎，它使用状态化深层分组检测来识别各种应用，包括 Web 协议以及其它使用动态 TCP/UDP 端口分配的许多难以分类的协议。如果在安全环境中使用，NBR 能够根据负载特征检测到蠕虫。NBAR 对应用进行识别和分类之后，网络就可以针对该应用激活特定服务。另外，NBAR 还能与 QoS 特性一起保证网络带宽的高效使用，提供带宽保证、带宽限制、流量整形和分组标记功能。SDM（参见下面介绍的思科路由器和安全设备管理器）配有易于使用的向导，不但支持 NBAR，还能提供应用流量的图形视图。

CPU/内存阈值设定

Cisco IOS 软件不但能设置路由器内存利用率的全局内存阈值，还能在达到阈值时发出通知。通过降低 CPU 和内存使用率，这个特性能够保证路由器在高负载（例如遇到攻击时）情况下仍能正常运行。

Secure Shell 版本 2

Secure Shell 版本 2（SSHv2）提供了强有力的新型验证和加密功能，增加了很多通过加密连接传输各种流量的方法，包括文件复制和电子邮件协议。另外，网络安全也通过新增的验证功能得到了增强，包括数字证书和越来越多的双因素验证选项。

SNMPv3

SNMPv3 是一种用于网络管理的、可互操作的标准协议。SNMPv3 能够在网络上将分组验证和分组加密相结合，提供安全设备访问。SNMPv3 中提供的安全特性包括：

- **消息完整性**——保证信息在传输过程中未被篡改；
- **验证**——确定消息来源是否可靠；
- **加密**——对信息内容加密，防止未授权用户阅读。

SNMPv3 同时提供多种安全模式和多个安全等级。安全模式是为用户和用户所在组制订的验证策略。安全等级是在安全模式中设定的安全级别。安全模式和安全等级相结合，组成了处理 SNMP 分组所使用的安全机制。有三种安全模式：SNMPv1、SNMPv2C 和 SNMPv3。

基于角色的 CLI 访问

利用基于角色的 CLI 访问特性，网络管理员可以定义“视图”，即有选择地或部分地访问 Cisco IOS 软件的一组操作命令和配置功能。视图不但能限制对 Cisco IOS 命令行界面（CLI）和配置信息的访问，还能规定哪些命令可接受，哪些配置信息可见。基于角色的 CLI 访问的应用包括网络管理员允许安全人员访问某些功能等。另外，电信运营商还可以利用这个功能限制对最终客户的访问，以便排除网络故障。思科 SDM 提供厂内管理员默认访问设置、只读设置（对最终用户）、防火墙策略和 Easy VPN Remote 设置。利用基于角色的特定访问方式登录到思科 SDM 的用户只能看到其角色许可范围内的 GUI 屏幕信息。

网络控制和抑制：NAC

网络准入控制（NAC）

网络准入控制（NAC）是由思科系统公司发起的一个行业协作项目，目的是只为符合网络安全策略要求的端点授予网络接入权，以防受到病毒和蠕虫的损害。NAC 控制网络接入的方法是检查与网络相连的设备是否符合网络安全策略要求。

NAC 能够发现薄弱系统，并实施有效的网络准入控制，因为它只允许符合最新企业防病毒和操作系统补丁策略的信任端点设备接入网络。为防止薄弱主机和不符合要求的主机成为蠕虫和病毒传播的发源地或攻击目标，这些主机将被隔离，只能访问网络的某个区域，直到它安装了补丁或得到保护为止。

在采用 Cisco IOS 软件高级安全、高级 IP 服务或高级企业服务特性集的 Cisco 800、1800、2800 和 3800 系列上，支持 NAC。另外， Cisco 7000 头端路由器也提供了 NAC。

NAC 的优点包括：

- **拓宽了控制范围**——能够监控主机与网络相连的各种常用方式，例如路由器 WAN 链路、IPSec 远程接入和拨号接入等。
- **多厂商解决方案**——由思科发起的 NAC，是多家厂商与领先防病毒厂商密切合作的结果，这其中包括 Network Associates、Symantec 和 Trend Micro。
- **延伸了现有技术和标准**——NAC 扩展了现有通信协议和网络安全技术的使用，例如可扩展验证协议（EAP）、802.1x 和 RADIUS 服务。
- **更好地利用现有网络和防病毒投资**——NAC 能够将现有网络基础设施和防病毒技术投资相结合，提供准入控制设施。

其他安全特性

验证、授权和记帐（AAA）

利用 Cisco IOS 软件 AAA 网络安全服务提供的框架，可以在路由器或接入服务器上设置访问控制。利用 AAA，管理员可以使用针对各种服务或接口的方法列表，配置每条线路（每个用户）或每种服务（例如 IP、互联网分组交换[IPX]或虚拟专用拨号网络[VPDN]），以动态配置验证和授权的类型。

802.1x

802.1x 应用要求使用合法访问证书，因而使未授权访问受保护信息资源变得更加困难。部署 802.1x 应用之后，网络管理员还可以有效消除用户部署不安全无线接入点的可能性，便于 WLAN 设备的部署。

Cisco IOS 证书服务器和客户端

Cisco IOS 证书服务器将一个证书服务器嵌入 Cisco IOS 软件中，使路由器可作为网络上的证书授权设备。

思科证书服务器可签发和取消数字证书。过去，随着 VPN 安装范围的扩大，很难生成和管理密码信息。思科证书服务器可通过在支持 IPsec VPN 的相同硬件上构建一个简单、可扩展、易于管理的证书授权机制，而解决上述问题。Cisco IOS 证书服务器为简单对称密钥部署提供了一种重要的方法。

Cisco IOS 还支持内嵌 PKI 客户端功能，可与证书服务器和第三方证书授权机构互操作。PKI 客户端的特性包括：

- 支持机载 ACL，根据证书字段接受/拒绝证书
- 与 AAA 集成，根据用户名和其他属性进行证书授权

- 支持在线证书状态协议（OCSP）
- 支持证书撤销列表和自动重新注册

Cisco 800、1800、2800 和 3800 系列路由器的硬件安全特性

USB 端口/可拆卸证书

Cisco 800、1800、2800 和 3800 系列集成多业务路由器配有集成式板载 USB 1.1 端口，可用于执行重要的安全和存储功能。这些功能可支持安全用户验证；保存可拆卸证书，建立安全 VPN 连接；安全分发配置文件；以及为文件和配置提供大量闪存。

可利用这些 USB 端口的两个新特性为 USB 电子令牌和 USB 闪存。通过 USB 电子令牌和 USB 闪存，配有内置 USB 端口的思科路由器能够支持电子令牌和 USB 闪存。USB 电子令牌提供安全配置分发，使用户能够保存待部署的 VPN 证书。USB 闪存特性则允许用户利用 USB 闪存，来存储镜像和配置。

安全无线 LAN 服务

模块化的 Cisco 1800、2800、3800 系列，以及固定配置的 Cisco 850、870、1800 系列集成多业务路由器，提供了全套企业级安全无线服务，可提高无线企业分支机构、中小企业、Wi-Fi 热点和远程工作地点的生产率。

优势：

- 整个集成多业务路由器系列都具有集成无线 LAN 接入点选项（802.11b/g 和 802.11a/b/g）
- 扩展无线安全性能，包括 WiFi 受保护接入（WPA）和各种验证类型，以及用于远程地点无线客户端的应急本地验证
- 接入区路由和服务选择网关服务，可在 WiFi 热点提供安全公共接入
- 移动 IP 服务，在无线 LAN 和蜂窝网络中提供移动性
- 通过思科服务选择网关（SSG）和思科用户边缘服务管理器（SESM），为大型企业提供定制访客接入解决方案

高级安全网络模块（Cisco 2800 和 3800 系列）

如果客户需要为 IDS 和内容安全实施专用硬件解决方案，可以采用为 Cisco 2800 和 3800 系列路由器开发的两个网络安全模块。

入侵检测网络模块

在 Cisco 2800 或 3800 系列路由器中添加思科 IDS 网络模块（产品编号 NM-CIDS）之后，能够形成完整的 IDS 系统，作为思科 IDS 传感器系列的一部分。这些 IDS 传感器能够与其它 IDS 组件配合使用，包括思科 IDS 管理控制台、CiscoWorks VPN/安全管理解决方案（VMS）和思科 IDS 设备管理器，以便有效保护客户的数据和信息基础设施。思科 IDS 网络模块为 IDS 配备了专用 CPU，和 20GB 硬盘驱动器，以便记录 1200 多个 IPS 特征。通过与 IPSec VPN 和 GRE 流量的配合，该模块可以在网络的第一个入点对流量进行解密、隧道端接和检测－这是业界的首创特性。这可减少支持系统所需的设备、降低运营和投资开支，并增强安全性能。

内容安全网络模块

作为思科的设备内容安全和 URL 过滤解决方案，为 Cisco 2800 和 3800 系列路由器开发的内容引

擎网络模块（NM-CE）可以作为集成式全功能互联网代理高速缓存，以及 Websense 或 SmartFilter 的 URL 过滤服务器，且不需要添置独立的 Web 过滤服务器，从而大大降低了成本。

嵌入式服务管理：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 800、1800、2800 和 3800 系列路由器都配有工厂预安装的思科路由器和安全设备管理器（SDM），而且这种 SDM 也能够在 Cisco 7000 头端平台上使用。思科 SDM 是一种直观、基于 Web 的设备管理器（GUI），可以部署和管理思科路由器（见图 3）。思科 SDM 能够简化路由器的配置和监控，因为它不但能利用启动向导快速完成部署和路由器锁定，通过智能向导执行安全和路由特性，还提供由思科技术帮助中心（TAC）认可的路由器配置，以及与主题相关的培训内容。

思科 SDM 将路由和安全服务管理功能与易用性、智能向导和深入排障功能有机地结合，平滑地将集成多业务的优点延伸到了路由器上。现在，客户不但能实现整个网络的路由和安全策略的同步，还能更全面地了解路由器服务状态，因而大大降低了运营成本。

思科 SDM 2.1.1 的主要新特性包括：

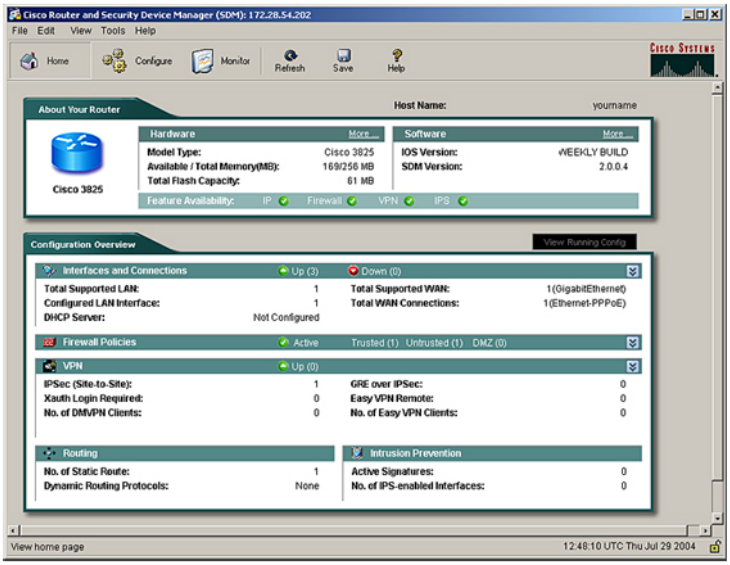
- 固定配置的 Cisco 800 系列和 1800 系列集成多业务路由器
- 集成无线管理
- 快速、方便的路由器部署向导－Express Setup
- 基于 PC 的 SDM（路由器闪存上无需 SDM 文件）
- ATM 点对点协议（PPPoA）配置
- 日文 Windows OS 支持
- 翻译为日文、简体中文、法文、德文、意大利文和西班牙文的 SDM 用户界面（2005 年 6 月面世）

思科 SDM 2.0 的主要优点包括：

- 内部 IPS，具有可升级特征和可以定制的动态特征更新和特征定制（参见 IPS）
- 基于角色的路由器访问
- 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

如果想了解思科SDM的更多信息，请访问：http://www.cisco.com/go/sdm。

图 3 思科路由器和安全设备管理器



用户可以通过CiscoWorks VPN/安全管理解决方案（VMS）管理捆绑，来管理防火墙和VPN特性。如果想详细了解CiscoWorks VMS，请访问：http://www.cisco.com/go/vms。

认证

思科致力于为全球客户提供一个灵活的产品认证和评估计划。Cisco IOS VPN已经通过了FIPS 140-2认证，Cisco IOS防火墙已经通过了ICSA认证，即将通过Common Criteria EAL4+认证。思科认为，这些认证是集成安全战略的重要组成部分，因而会继续FIPS、ICSA和Common Criteria EAL4+认证工作。更多信息，请访问：http://www.cisco.com/go/securitycert。

FIPS

Cisco 800、1800、2800和3800系列能够满足FIPS 140-1的二级安全标准。NIST已经将FIPS 140-1升级为FIPS 140-2。目前，思科的许多路由器都正在申请FIPS 140-2的二级认证。

ICSA

ICSA是一个商业安全认证组织，主要为各种安全产品提供ICSA IPSec和ICSA防火墙认证。思科不但参加了ICSA的IPSec计划，还参加了其防火墙计划。

Common Criteria

Common Criteria是一种用于评估IT安全的国际标准，该标准由多个国家共同开发，旨在取代各国现存的各种安全评估过程，建立国际通用的统一标准。目前，共有14个国家公开承认Common Criteria标准。Cisco IOS软件 IPSec的几个版本和思科路由器目前正在接受澳大利亚信息安全评估计划（AISEP）的评估，评估的标准是ITSEC或Common Criteria。

订购信息

如需订购，请访问思科订购首页。Cisco 800、1800、2800和3800系列路由器安全捆绑的订购信息如表3所示。如果想了解思科的访问和头端安全捆绑的更多信息，请访问：http://www.cisco.com/go/securitybundles。

表3 Cisco 800、1800、2800和3800系列路由器的订购信息

产品名称	产品编号
Cisco 851安全以太网路由器	CISCO851-K9
Cisco 876安全捆绑，带Plus ISDN特性集	CISCO876-SEC-I-K9
Cisco 876安全捆绑，带Plus特性集	CISCO876-SEC-K9
Cisco 877安全捆绑，带Plus特性集	CISCO877-SEC-K9
Cisco 878安全捆绑，带Plus特性集	CISCO878-SEC-K9
Cisco 871安全以太网路由器	CISCO871-K9
双以太网安全路由器，带V.92调制解调器备份	CISCO1811/K9
双以太网安全路由器，带ISDN S/T备份	CISCO1812/K9
Cisco 1841 安全捆绑，带高级安全 Cisco IOS软件	CISCO1841-SEC/K9
Cisco 2801 安全捆绑，带高级安全 Cisco IOS软件	CISCO2801-SEC/K9
Cisco 2811 安全捆绑，带高级安全 Cisco IOS软件	CISCO2811-SEC/K9
Cisco 2821 安全捆绑，带高级安全 Cisco IOS软件	CISCO2821-SEC/K9
Cisco 2851 安全捆绑，带高级安全 Cisco IOS软件	CISCO2851-SEC/K9
Cisco 3825 安全捆绑，带高级安全 Cisco IOS软件	CISCO3825-SEC/K9
Cisco 3845 安全捆绑，带高级安全 Cisco IOS软件	CISCO3845-SEC/K9
Cisco 1841 增强安全捆绑，带 AIM-VPN BPII-PLUS，高级 IP Cisco IOS软件	CISCO1841-HSEC/K9
Cisco 2801 增强安全捆绑，带 AIM-VPN EPII-PLUS，高级IP Cisco IOS软件	CISCO2801-HSEC/K9
Cisco 2811 增强安全捆绑，带 AIM-VPN EPII-PLUS，高级IP Cisco IOS软件	CISCO2811-HSEC/K9
Cisco 2821 增强安全捆绑，带 AIM-VPN EPII-PLUS，高级IP Cisco IOS软件	CISCO2821-HSEC/K9
Cisco 2851 增强安全捆绑，带 AIM-VPN EPII-PLUS，高级IP Cisco IOS软件	CISCO2851-HSEC/K9
Cisco 3825 增强安全捆绑，带 AIM-VPN EPII-PLUS，高级IP Cisco IOS软件	CISCO3825-HSEC/K9
Cisco 3845 增强安全捆绑，带 AIM-VPN HPII-PLUS，高级IP Cisco IOS软件	CISCO3845-HSEC/K9
Cisco 2801 V3PN 捆绑，带 AIM-VPN EPII-PLUS，PVDM2-8，高级 IP Cisco IOS软件，64 MB闪存，256 DRAM	CISCO2801-V3PN/K9
Cisco 2811 V3PN 捆绑，带 AIM-VPN EPII-PLUS，PVDM2-16，高级 IP Cisco IOS软	CISCO2811-V3PN/K9

产品名称	产品编号
件，FL-SRST-36，64 MB闪存，256 DRAM	
Cisco 2821 V3PN 捆绑，带 AIM-VPN EPII-PLUS，PVDM2-32，高级 IP Cisco IOS软件，FL-SRST-48，64 MB闪存，256 DRAM	CISCO2821-V3PN/K9
Cisco 2851 V3PN 捆绑，带 AIM-VPN EPII-PLUS，PVDM2-48，高级 IP Cisco IOS软件，FL-SRST-72，64 MB闪存，256 DRAM	CISCO2851-V3PN/K9
Cisco 3825 V3PN 捆绑，带 AIM-VPN HPII-PLUS，PVDM2-64，FL-SRST-168，高级 IP Cisco IOS软件，64 MB闪存，256 DRAM	CISCO3825-V3PN/K9
Cisco 3845 V3PN 捆绑，带 AIM-VPN HPII-PLUS，PVDM2-64，FL-SRST-240，高级 IP Cisco IOS软件，64 MB 闪存，256 DRAM	CISCO3845-V3PN/K9
用于Cisco 1800的增强性能DES、3DES和 AES VPN 加密和压缩	AIM-VPN/BPII-PLUS
用于Cisco 2800的增强性能DES、3DES和 AES VPN 加密和压缩	AIM-VPN/EPII-PLUS
用于Cisco 3800的增强性能DES、3DES和 AES VPN 加密和压缩	AIM-VPN/HPII-PLUS
Cisco 1841 高级安全 （Cisco IOS软件）	c184x-advsecurityk9
Cisco 2801 高级安全 （Cisco IOS软件）	S28NASK9
Cisco 2800 高级安全 （Cisco IOS软件）	S28NASK9
Cisco 3825 高级安全 （Cisco IOS软件）	S382ASK9
Cisco 3845 高级安全 （Cisco IOS软件）	S384ASK9
Cisco 1841 高级IP服务 （Cisco IOS软件）	c184x-advipservicesk9-mz
Cisco 2801 高级IP服务 （Cisco IOS软件）	S28AISK9
Cisco 2800 高级IP服务 （Cisco IOS软件）	S28AISK9
Cisco 3825 高级IP服务 （Cisco IOS软件）	S382AISK9
Cisco 3845 高级IP服务 （Cisco IOS软件）	S384AISK9
Cisco 1841 高级企业服务 （Cisco IOS软件）	c184x-adventerprisek9-mz
Cisco 2801 高级企业服务 （Cisco IOS软件）	S28AESK9
Cisco 2800 高级企业服务 （Cisco IOS软件）	S28NAESK9
Cisco 3825 高级企业服务 （Cisco IOS软件）	S382AESK9
Cisco 3845 高级IP服务（Cisco IOS软件）	S384AESK9
入侵检测系统网络模块	NM-CIDS-K9
内容引擎网络模块-基本性能-20 GB	NM-CE-BP-20G-K9
内容引擎网络模块-基本性能-40 GB	NM-CE-BP-40G-K9
内容引擎网络模块-基本性能-80 GB	NM-CE-BP-80G-K9

服务与支持

思科提供了广泛的服务项目来促使客户的成功。这些创新的服务项目通过一个由人员、流程、工具和合作伙伴构成的独特网络提供，来实现高的客户满意度。思科服务可以帮助您保护您的网络

投资，优化网络运营，让您的网络为新的应用做好充分的准备，从而拓展网络智能并增强您的业务优势。如需了解更多关于思科服务的信息，请访问思科技术支持服务或者思科高级服务。

更多信息

如果想了解Cisco 800、1800、2800和3800系列集成多业务路由器和补充型Cisco 7000高端安全解决方案的更多信息，请访问：http://www.cisco.com/go/routersecurity，或者与当地的思科客户代表联系。

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

邮政编码：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

邮政编码：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

邮政编码：510620
电话：(8620) 85193000
传真：(8620) 38770077

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) 86961000
传真：(8628) 86528999