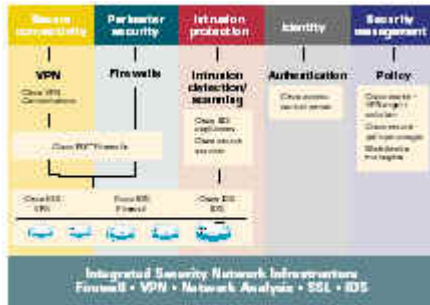


# 用于网中之网的集成化安全保护

## 应用和服务集成



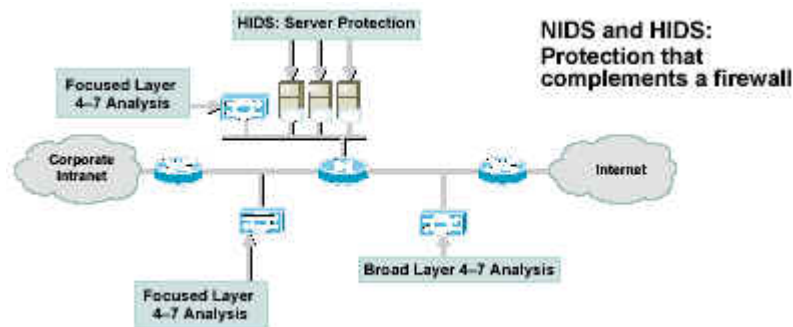
安全连接	周边安全	入侵防范	身份辨识	安全管理
VPN	防火墙	入侵检测/扫描	身份识别	策略
思科 VPN 集中器	Cisco PIX 防火墙	Cisco IOS 设备 思科安全扫描工具	思科访问控制服务器	Ciscoworks - VPN 管理解决方案 思科安全策略管理器 Web 管理管理器
Cisco IOS VPN	Cisco IOS 防火墙	Cisco IOS IDS		
集成化安全网络基础设施				
防火墙 VPN 网络分析 SSL IDS				

## 入侵防范

入侵检测系统的作用类似于现实生活中的监视摄像机。它们可以不间断地扫描网络流量，查找可疑的数据分组。利用一个跟踪特征数据库，它们可以记录任何不正常的情况，并采取相应的措施：发出警报，重置攻击者的 TCP 连接，或者禁止攻击者的 IP 地址再次登录网络。

网络 IDS（NIDS）检测器通常可以利用一个不可寻址的混和接口卡监听某个子网上的所有流量，并通过另外一个更加可靠的接口发送任何警报和记录的流量。

入侵防范是 NIDS 的后续技术。它不仅可以检测到穿过外围安全设施的攻击，还可以将基于主机的 IDS（HIDS）的强大的网络管理解决方案整合到一起，提供一种保护服务。



<p>HIDS：服务器保护</p> <p>集中的第四到第七层分析</p> <p>企业内联网</p> <p>集中的第四到第七层分析</p>	<p>NIDS 和 HIDS：可以补充防火墙的保护技术</p> <p>互联网</p> <p>广泛的第四到第七层分析</p>
--	---

除了检测攻击以外,该解决方案还可以采取一些措施来最大限度减小这样的攻击对网络可能造成的损害。在现实生活中与入侵防范类似的是警卫利用多种工具,包括监视摄像机,防止入侵者撬锁、毁坏财产和窃取重要物品。

NIDS 检测器主要依赖于检测和纠正措施来保护整个网段。基于交换机的检测器可以同时保护多个网段,因而可以补充独立的检测器。

HIDS 检测器可以利用多种工具来保护关键性的服务器,这些工具可以防止潜在的攻击者进行未经授权的系统调用(导致缓存溢出),对某些文件进行未经授权的改动(篡改网页),或者代替管理工具(可以远程控制的特洛伊木马程序)。

### 为什么选择 Cisco IDS ?

#### 先进的特征架构

很多 IDS 厂商依靠一种简单的模式匹配机制来检测攻击。思科则利用分组处理和攻击特征的组合来检测攻击。有些处理涉及到协议分析、碎片整理和状态识别。利用思科特有的先进方法(14 项已经受理和正在申报的专利技术),思科大幅度地降低了所需特征的数量。由于特征的数目不需要随着可能发生的攻击类型的增加而增加,思科的 IDS 产品可以保持其在性能和维护上的优势。

#### 防范和检测

一旦 NIDS 检测器检测到了一个攻击,它会采取一系列措施来防止网络继续遭受损失。HIDS 检测器在这个领域的功能尤其强大,因为它们可以阻止未经授权的系统调用,对注册表和日志文件的修改,以及对文件系统的某些部分的访问。另外,它们还可以防止网页被覆盖,阻止来自于 http 输入缓存的攻击。

#### 特征升级

思科是唯一拥有主要由具有安全背景的退役军事人员和退休政府职员组成的特征研究团队

的 IDS 厂商。思科会不断地进行改进特征列表，并且会以至少每四周一次的频率通过一个可扩展的自动升级服务机制提供特征升级。即使需要升级数百个检测器，整个升级过程也几乎不需要人为干预。

Cisco NIDS 检测器				
如下表所示，Catalyst 6000 系列中有三个 NIDS 设备和一个交换机检测器。除了这些检测器以外，PIX 防火墙系列和 Cisco IOS 防火墙功能集也含有超过 50 个 IDS 特征，可以在某些不一定有一个独立的检测器的地方提供内嵌保护。				
<b>优点</b>				
<ul style="list-style-type: none"> <li>● 市场中速度最快的产品</li> <li>● 高度的可靠性</li> <li>● 整体运营成本（TCO）和新的入侵检测管理（IDM）、IDS 事件查看器（IEV）</li> <li>● 支持质量</li> <li>● 集成到整个安全解决方案中</li> <li>● 能够采取纠正措施</li> <li>● 可以通过我们新推出的“SILVER”语言进行定制</li> </ul>				
	IDS 4210	IDS 4235	IDS 4250	Catalyst 6000 入侵检测系统模块（IDSM）
应用	中小型企业（SMB）	大型企业	大型企业	大型企业
类型	设备	设备	设备	交换机
性能	45 Mbps	200 Mbps	500 Mbps	120 Mbps
接口	FE	FE	FE/GE	内部
尺寸	1RU	1RU	1RU	1 插槽
处理器（MHz）	566（C）	1.3GHz	双 1.3GHz	定制
RAM（MB）	256	1000	2000	不定
性能（Mbps）	45	150-200	300-600	260
反应	重置/规避	重置/规避	重置/规避	否（规避 v3.0）
特征范围	全部	全部	全部	全部
思科 HIDS 代理				
主机 IDS 代理可以支持操作系统（OS）平台和 OS 附带的 Web 应用。一个网络必须通过一个 HIDS 控制器（包括一个代理）来配置和控制其他代理。HIDS 控制台可以单独购买，也可以作为 VMS 的一部分购买。				
<b>优点</b>				
<ul style="list-style-type: none"> <li>● 基于行为的规则——防范已知的和未知的攻击</li> <li>● 在主机中建立多个防护层</li> <li>● 支持质量</li> <li>● 集成到整个安全集成方案中</li> <li>● 可扩展性</li> </ul>				
代理	操作系统版本		OS + 服务器版本	
类型	Windows NT 4.0		Microsoft IIS v4.0 和 v5.0	

	Windows 2000	Apache 1.3.6 和更高版本
	Solaris 2.6 , 2.7 , 2.8	iPlanet Netscape 3.6

## 思科入侵防范的管理

IDS 技术涉及到两项重要的管理功能：配置和监控。配置包括设定操作参数和调整检测器，以消除错误的响应和错误的警报。错误的响应是指由网络上的普通流量触发的特征。错误警报是那些指向错误配置的网络安全部署而不是任何真实的威胁的特征触发事件。

Cisco IDS 产品提供了很多配置选项，每种配置都可以使用一种保密的协议：SSH、SSL、IPSec 或者 SCP。NIDS 检测器可以通过命令行配置，也可以利用免费的 IDS 设备管理器（IDM）通过 Web 浏览器配置，或者可以利用思科安全策略管理器，将其作为整个安全策略的一部分。HIDS 代理则需要通过特殊的控制台代理进行配置和监控。

企业可以选择两种方式来监控警报：利用最多可以同时监控三个设备的、免费的 IDS 事件查看器（IEV），或者利用非常便于扩展的警报监控中心——VPN 和安全管理系统（VMS）的组成部分。

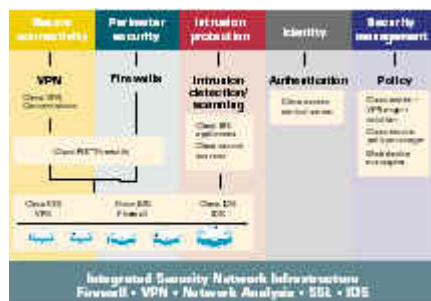
监控中心具有很多特性，其中包括显示警报和报告功能等，这些功能可以为大型企业提供多种符合它们各自安全运营模式的监控方式。IEV 具有这些特性中的一部分显示功能。

思科系统公司在下列国家和地区设有 200 多个分支机构。它们的地址、电话和传真详见思科网站，网址是 [www.cisco.com/go/offices](http://www.cisco.com/go/offices)。

©思科系统公司2002年版权所有。Catalyst ,Cisco ,Cisco IOS , Cisco Systems和Cisco Systems 标志都是Cisco Systems公司和/或它的子公司在美国和其他国家的注册商标。本文或者网页中涉及的所有其他品牌、名称或者商标都是它们各自所属企业的资产。“合作伙伴”一词的使用并不表示Cisco与任何其他公司之间建立了伙伴关系。（0110R）

# 用于网中之网的集成化安全

## 应用和服务集成



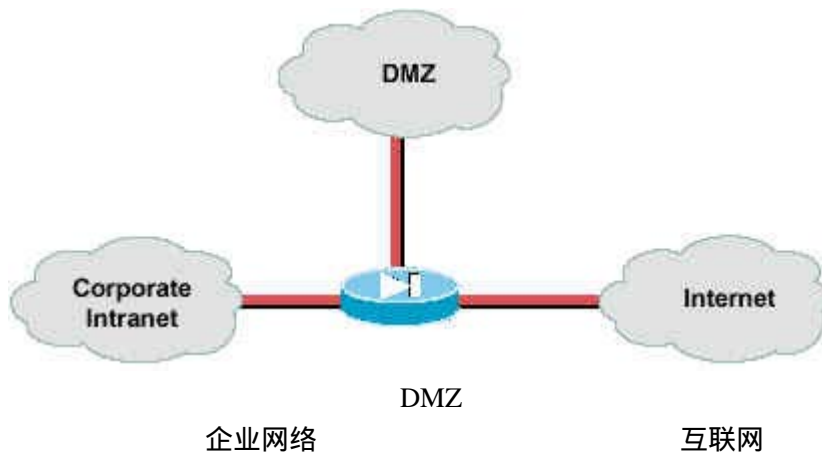
安全连接	周边安全	入侵防范	身份辨识	安全管理
VPN	防火墙	入侵检测/扫描	身份识别	策略
思科 VPN 集中器	Cisco PIX 防火墙	Cisco IOS 设备 思科安全扫描工具	思科访问控制服务器	Ciscoworks - VPN 管理解决方案 思科安全策略管理器 Web 管理管理器
Cisco IOS VPN	Cisco IOS 防火墙	Cisco IOS IDS		
集成化安全网络基础设施				
防火墙 VPN 网络分析 SSL IDS				

## 周边安全

周边安全可以控制对关键性应用、服务和数据的访问，使得只有合法的用户和信息才能从一个网络（信任域）进入另外一个网络。过去，防火墙就等同于互联网（不可靠网络）和 DMZ（可靠的公共网络）和/或内部企业网（可靠的专用网络）之间的周边安全。但是现在，周边安全的更加宽泛的定义还包括访问控制列表（ACL）和一些辅助性的工具，例如杀毒软件和内容过滤工具。在这里我们主要讨论防火墙。

下图显示了用于三种最常见的信任域之间的传统的三接口防火墙。

防火墙不仅可以用在互联网和企业网络的交叉点；它们实际上可以用在网络的各个地方。它们可以用于保护关键性的服务器，例如 IP 电话服务器或者公共 DMZ 上的外联网服务器，还可以用于划分具有不同的信任等级的域；例如来自当前使用网络的段外网络管理域。防火墙还可以防护远程用户，防止他们在利用虚拟专用网（VPN）进行连接时，不会受到未经授权的访问。



## PIX 防火墙管理

思科的防火墙产品可以通过多种方式进行管理,从而让企业可以选择最符合他们的需要的管理解决方案。

PIX 防火墙可以通过一个标准的 Web 浏览器界面进行单独的配置和监控。PIX 设备管理器 (PDM) 是一个 JavaScript 服务器应用,它让管理人员可以控制某个防火墙,并查看它的各种安全特性的使用报告。

拥有多个 PIX 防火墙的企业可以利用防火墙管理中心和自动升级服务器从一个中心位置配置和维护数百个防火墙——即使在这些防火墙没有固定的 IP 地址时也可以。

最后,对于那些需要通过一个策略服务器来管理他们的安全系统的企业来说,可以使用思科安全策略管理器 (CSPM)。CSPM 可以集中管理各种用于支持思科安全产品 (例如思科安全 PIX 防火墙和运行 Cisco IOS 防火墙的思科路由器) 的配置的策略。利用策略管理器,网络安全人员可以在一些用于相关的网络设备的配置文件中定义适当的策略,并将这些配置安全地发送到安全设备。

## 为什么选择思科周边安全产品?

### 高可用性

Cisco PIX 防火墙系列可以为不受限制的 (UR) 515E、525 和 535 产品提供经济有效的、高可用性的功能。您可以利用 UR 设备的四分之一投资再购买一个设备——故障恢复设备 (FO) 设备。FO 设备让网络设计人员可以消除单点故障,提供一个可以满足企业需要的、强大的、安全的网络设计方案。只需一根 LAN 电缆,FO 设备就可以保持与 UR 设备相同的动态状态表——因此当某个设备发生故障时,不会有任何会话发生中断,也不会意外打开任何安全漏洞。

### 安全的周边

PIX 系列的任何成员都为它们的应用提供了相同的增值安全特性。内置的入侵检测检测器

(IDS) 可以针对不可靠网络上的一些常见的小型攻击提供内嵌的防范。内置的 VPN 功能可以帮助企业保障它们在不可靠网络上传输的数据的安全性。

### 可伸缩性和可延展性

从 PIX 501 到 PIX 535 ,Cisco PIX 系列防火墙能够以不同的性能价格比提供相同的企业安全功能集。此外 ,PIX 515E 还可以扩展到六个 FE 接口 ,PIX 525 可以扩展到八个接口 ,而 PIX 535 可以扩展到十个接口 ,其中有两个可以是 GE 接口。

Cisco PIX 防火墙系列					
Cisco PIX 防火墙的市场份额和产品性能都处于业界领先地位,从 1996 年以来它就一直是思科在安全领域的旗舰产品。安装到网络中以后,PIX 防火墙可以判断在任何一个方向上传输的流量是否经过授权。如果流量已经获得授权,它才会建立连接,而对网络性能几乎不会产生任何影响。所有未获批准的流量将被完全丢弃。					
<b>特性和优点</b>					
<ul style="list-style-type: none"> <li>● 安全性——思科安全 PIX 防火墙采用了一种加固的操作系统,强调保护设备和受保护网络的安全。其他很多同类防火墙都建立在庞大的、通用的、面向不同的功能的操作系统平台上,因而更容易受到互联网攻击的威胁。</li> <li>● 性能——PIX 防火墙的数据处理能力是其他任何一个竞争性产品的很多倍,因而可以在最大限度地减小对网络性能的影响的前提下,提供坚不可摧的安全性。</li> <li>● 可靠性——因为 PIX 防火墙只用于一个目的——安全性,因而它非常可靠。这是一个在网络中扮演着如此重要的角色的设备的一项基本需求。PIX 防火墙的平均故障间隔时间在六年以上。</li> <li>● 可扩展性——PIX 平台具有多种尺寸,适用于各种规模的企业——从小型企业/分支机构到跨国企业的总部。所有 PIX 平台都使用相同的软件和管理解决方案,可以提供最大程度的可扩展性和集成能力。</li> <li>● 便于安装和维护——作为一个专用设备,思科安全 PIX 防火墙非常便于安全和维护。不需要安装任何软件,也不需要配置任何服务器端口。</li> <li>● 内嵌的、基于标准的 VPN——作为安全功能的一部分,PIX 防火墙还可以提供基于 IPSec 标准的 VPN 功能。除了它的市场领先的防火墙性能以外,PIX 防火墙还具有强大的站点间和远程访问 VPN 功能。</li> </ul>					
<b>优点</b>					
<ul style="list-style-type: none"> <li>● 极低的整体运营成本</li> <li>● 防火墙设备外型</li> <li>● 出色的故障恢复性能</li> <li>● 集成的 IDS 特征 ( 50 )</li> <li>● 支持质量</li> <li>● 集成到整个安全解决方案中</li> <li>● 管理—特殊设备和整个企业</li> <li>● 免费的 VPN 客户端</li> <li>● 最快的防火墙吞吐速度</li> </ul>					
	PIX 501	PIX 506E	PIX 515E-UR	PIX 525-UR , 支持 GIG	PIX 535-UR , 支持 GIG
市场	小型办公室 家庭办公室	远程办公室	中小型分支机 构	大型企业	大型企业 + 服 务供应商
许可用户个数	10 或者 50	无限	无限	无限	无限
VPN 对等端最	5	25	2000	2000	2000

大数量					
尺寸 (RU)	<1	1	1	2	3
处理器 (MHz)	133	300	433	600	1GHz
RAM (MB)	16	32	64	256	1GB
最大接口数	1 个 10BT + 4 个 FE	2 个 10BaseT	6	8	10
明文 (Mbps)	10	20	188	360	1.7GHz
3DES (Mbps)	3	16	63	70	95
接口个数	2 个 10BaseT 4 端口交换机	2 个 10BaseT	2 个 10/100 + 4 个 10/100	2 个 10/100 + 6 个 FE/GE	2 个 10/100 + 8 个 FE/GE
防火墙性能	10Mbps	40Mbps	180Mbps	450Mbps	1.7Gbps
VPN (3DES) 性能	3Mbps	10Mbps	63Mbps	70Mbps	90Mbps
故障恢复	无	无	有, 只限 UR	有, 只限 UR	有, 只限 UR
尺寸	桌面	桌面	1RU	2RU	3RU

#### Cisco IOS 防火墙功能集

Cisco IOS 防火墙可以提供先进的防火墙功能,并结合了其他一些安全技术,例如 VPN 的 IPSec DES 加密、入侵检测和身份认证。该软件是 Cisco IOS 软件的一个附加模块,可以通过多种思科路由器和交换机提供。因此,它可以增强现有的安全功能,并且由于它建立在 Cisco IOS 软件中已有的一些动态安全特性的基础上,因而可以利用您的企业对思科基础设施的投资。

#### 特性和优点

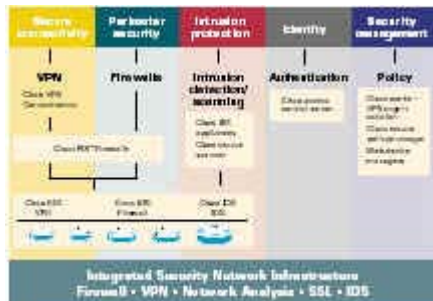
- 为网络增加安全性——通过将这种技术集成到网络操作系统中,思科让网络平台变得更加安全。通过提高您的网络平台的安全性,Cisco IOS 防火墙从根本上改变了网络安全市场的局面,并提供了无与伦比的集成性。
- 灵活性——由于 Cisco IOS 防火墙可以部署在各种思科路由器和交换机上,所以它的先进的安全功能可以部署在网络中的很多节点上。
- 利用现有的基础设施——Cisco IOS 防火墙建立在思科网络设备的基础上,从而让您可以将几乎任何一种思科路由器或者交换机加入到安全平台中。
- 集成化的 IDS——Cisco IOS 防火墙采用了入侵检测系统 (IDS) 技术,可以为网络基础设施提供更高的安全性。

思科系统公司在下列国家和地区设有 200 多个分支机构。它们的地址、电话和传真详见思科网站,网址是 [www.cisco.com/go/offices](http://www.cisco.com/go/offices)。

©思科系统公司2002年版权所有。Catalyst ,Cisco ,Cisco IOS , Cisco Systems和Cisco Systems 标志都是Cisco Systems公司和/或它的子公司在美国和其他国家的注册商标。本文或者网页中涉及的所有其他品牌、名称或者商标都是它们各自所属企业的资产。“合作伙伴”一词的使用并不表示思科与任何其他公司之间建立了伙伴关系。(0110R)

# 用于网中之网的集成化安全保护

## 应用和服务集成



安全连接	周边安全	入侵防范	身份辨识	安全管理
VPN	防火墙	入侵检测/扫描	身份识别	策略
思科 VPN 集中器	Cisco PIX 防火墙	Cisco IOS 设备 思科安全扫描工具	思科访问控制服务器	Ciscoworks - VPN 管理解决方案 思科安全策略管理器 Web 管理管理器
Cisco IOS VPN	Cisco IOS 防火墙	Cisco IOS IDS		
		集成化安全网络基础设施		
		防火墙 VPN 网络分析 SSL IDS		

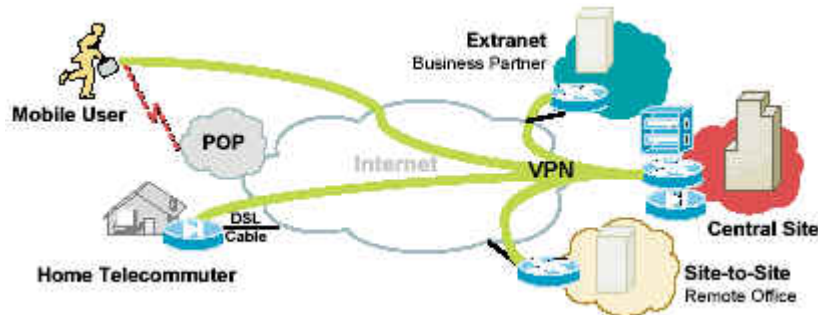
## 安全连接

利用互联网协议安全标准（IPSec）的虚拟专用网（VPN）可以提供信息的安全性、完整性和终端身份认证。目前主要有两种 VPN：站点间 VPN 和远程访问 VPN。站点间 VPN 可以作为一种价格低廉的替代方案，取代那些用于“难以到达”的地点的传统 WLAN 链路，或者作为一种高可用性机制充当某个企业的 WAN 连接的扩展。

在简单的集中星型部署中，如果两个站点需要互相进行身份认证，并且需要对流量进行加密，以确保安全性，就需要使用 IPSec 隧道。在那些需要非 IP 流量、路由协议和弹性的比较复杂的配置中，则需要将 GRE 隧道和 IPSec 隧道结合在一起，提供一个完整的 WAN 解决方案。

远程访问 VPN 的两个关键的需求是：用户配置/维护和隧道数量的可扩展性。一旦用户通过了中央设备的身份认证，就可以从远程的软件 VPN 客户端建立一个 IPSec 隧道。在客户通过身份认证以后，管理人员可以通过让中央设备将安全参数发送到远程客户端，保持网络的安全状况。这些安全参数包括：IPSec 1 段和 2 段参数，企业网络的 DHCP 参数，远程防火墙配置和 VPN 连接期间的网络访问授权。

中央 VPN 集中器设备最多可以同时支持 10000 个用户，并可以为大规模部署提供负载平衡和弹性。



移动用户

外联网 企业合作伙伴

互联网

VPN

中央站点

DSL 有线电缆

站点间远程办公室

家庭办公人员

### VPN 技术的管理

所有 Cisco VPN 设备都内置了一个基于 Web 的设备管理应用，可以通过一个标准的 Web 浏览器访问。IOS 路由器可以通过 VPN 设备管理器（VDM）进行管理，VDM 是 IOS 防火墙功能集的组成部分。在 PIX 系列中，PIX 设备管理器（PDM）2.0 具有功能齐全的 VPN 应用。VPN 3000 集中器拥有一个功能强大的、基于 Java 的管理服务器。这些设备管理器都拥有一个设置向导，有助于降低管理人员的配置难度。

对于大型 VPN 部署来说，思科可以提供一套完整的管理应用，作为 VPN/安全管理系统（VMS）的一部分。除了标准的企业管理工具以外，VMS 还可以提供一些专门针对 VPN 的应用。VPN 管理中心可以帮助管理人员集中配置和维护复杂的大型站点间和远程访问 VPN 网络。VPN 监视应用让管理人员可以监控 VPN 隧道的状态和使用情况。思科安全策略管理器（CSPM）可以提供对 VPN 和安全的集成化策略管理。

### 为什么选择思科 VPN？

#### 适用于所有 VPN 需求的、灵活的解决方案

思科拥有三个 VPN 产品系列，每个系列都拥有全套的产品，可以适应不同客户的需求。VPN 3000 集中器系列主要用于远程访问应用，包括五种不同尺寸的型号——外加一个硬件客户端（3002）。思科将 VPN 功能集成到了大多数的 IOS 平台中，其中还含有针对 1700、2600、3600、7200、7400 路由器系列和 Catalyst 6000 产品系列的硬件加速工具。最后，思科还将 VPN 功能集成到了整个 PIX 系列中，其中 501 和 506E 充当 VPN 客户端，515E、525 和 535 拥有 VPN 加速卡。

#### 利用 EasyVPN 提高 ROI

EasyVPN 让企业能够以与远程客户端相同的方式扩展他们的远程站点的连接能力。思科在很多低端设备中采用了它的远程 VPN 客户端技术，以便于对远程站点进行配置和维护。这

使得拥有多个站点的企业可以享受到 VPN 功能带来的好处——即使他们在这些站点只有很少的本地技术人员。

### 无所不在的 VPN 客户端连接

在购买任何一款 Cisco VPN 集中器或者 VPN 加速卡时,都会获得一个没有限制的 VPN 客户端使用许可。它可以帮助企业灵活地将他们的 VPN 解决方案部署到任何站点。软件客户端还包括一个个人防火墙,它可以确保将企业周边安全正确地扩展到远程用户主机。最后,VPN 客户端支持大多数主流操作系统:MS Windows、Linux、Solaris 和 Macintosh。

Cisco VPN 3000 集中器					
Cisco VPN 3000 集中器系列是一个曾经获得大奖的、非常先进的远程访问 VPN 解决方案。Cisco VPN 3000 集中器系列可以将最先进的高可用性功能和一种独特的、有针对性的架构结合在一起,让企业可以建设高性能的、可扩展的、强大的 VPN 解决方案,以支持他们的关键任务型远程访问应用。					
Cisco VPN 3000 集中器系列包括一个基于标准的、便于使用率的 VPN 客户端和可扩展的 VPN 隧道终端设备,以及一个让您可以方便地安装、配置和监控您的远程访问 VPN 的管理系统。					
它是业界唯一一个可以提供能够现场交换并能由客户进行升级的组件的平台。Cisco VPN 3000 集中器系列提供了七种不同的型号,可以支持各种规模的企业,其中包括曾经被 <i>网络计算</i> 杂志评为“年度最佳硬件产品”的 Cisco VPN 3060 集中器。					
优点					
<ul style="list-style-type: none"> <li>● 设备外型</li> <li>● 支持硬件客户端</li> <li>● 支持非 Windows 的客户端</li> <li>● 投资保护</li> <li>● 支持质量</li> <li>● 集成到整个安全解决方案中</li> <li>● 自动客户端分发</li> <li>● 免费的软件 VPN 客户端</li> <li>● 针对远程访问 VPN 而设计</li> </ul>					
VPN 3005	VPN 3015	VPN 3030	VPN 3060	VPN 3080	
应用	SMB*	SMB*	大型企业	大型企业	大型企业-SP**
用户个数	100	100	1500	5000	10000
VPN (3DES) 性能	4Mbps	4Mbps	50Mbps	100Mbps	100Mbps
VPN H/W	软件	软件	1 SEP	2 SEP	4 SEP
LAN-LAN 个数	100	100	500	1000	1000
用户群组数据库的大小	100	100	500	1000	1000
加密	SW	SW	HW	HW	HW
性能	4MB/s	4MB/s	50MB/s	100MB/s	100MB/s
内存 (MB)	32	64	128	256	256
SEP	0	0	1	2	4
可升级	否	是	是	是	N/A

支持双 PS	否	是	是	是	是
--------	---	---	---	---	---

#### Cisco PIX VPN 防火墙

所有 PIX 防火墙都具有 VPN 功能。它主要适用于那些安全策略要求必须将 VPN 技术作为防火墙系统的一部分的企业。它可以满足站点间和远程访问应用的要求，并能够连接到 VPN 客户端和任何一个 VPN 路由器。

	PIX 501	PIX 506E	PIX 515E	PIX 525-E	PIX 535
应用	SOHO***	ROBO****	SMB*	大型企业	大型企业-SP
VPN 隧道的个数	5	50	500	1000	2000
VPN ( 3DES ) 性能	3Mbps	10Mbps	63Mbps	70Mbps	90Mbps
VPN H/W	软件	软件	VAC	VAC	VAC
许可用户个数	10 或者 50	无限	无限	无限	无限
VPN 对等端最大数量	5	25	2000	2000	2000
尺寸 ( RU )	<1	1	1	2	3
处理器 ( MHz )	133	300	433	600	1GHz
RAM ( MB )	16	32	64	256	1GB
最大接口数	1 个 10BT + 4 个 FE	2 个 10BaseT	6	8	10
故障恢复	否	否	是	是	是
明文 ( Mbps )	10	20	188	360	1.7GHz
3DES ( Mbps )	3	16	63	70	95

#### Cisco IOS VPN 路由器/服务模块

很多 Cisco IOS 平台都拥有 VPN 硬件加速模块，它们可以提高 IOS 中的软件 VPN 功能的性能。在 IOS 平台中，VPN 设计可以保持与传统的站点间 WAN 设计相同的功能。这些包括用于传输对延时非常敏感流量——例如语音和视频——的服务质量 ( QoS ) 功能、高可用性和非 IP 流量的路由。下表列出了具有硬件加速模块的 IOS 平台。

	IOS 1700	IOS 2600	IOS 3600	IOS 7000	IPSec VPN 服务模块 ( Catalyst 6500 和 7600 )
应用	SOHO***	SMB*	大型企业	大型企业	大型企业-SP**
VPN 隧道个数	100	300-800	800-1300	2000-5000	8000
VPN ( 3DES ) 性能	4Mbps	8-12Mbps	16-40Mbps	90-140Mbps	2000Mbps
VPN H/W	AIM	AIM	NP-VM	VAM	VISM

\* 中小型企业    \*\* 服务供应商    \*\*\* 小型办公室家庭办公室    \*\*\*\* 远程办公室分支机构

思科系统公司在下列国家和地区设有 200 多个分支机构。它们的地址、电话和传真详见思科

网站，网址是 [www.cisco.com/go/offices](http://www.cisco.com/go/offices)。

©思科系统公司2002年版权所有。Catalyst ,Cisco ,Cisco IOS , Cisco Systems和Cisco Systems标志都是Cisco Systems公司和/或它的子公司在美国和其他国家的注册商标。本文或者网页中涉及的所有其他品牌、名称或者商标都是它们各自所属企业的资产。“合作伙伴”一词的使用并不表示Cisco与任何其他公司之间建立了伙伴关系。( 0110R )