思科集成防火墙解决方案

Cisco® ASA 5500 系列自适应安全设备、Cisco PIX®安全设备、思科集成业务路由器和 Cisco ASR 1000 系列汇聚业务路由器中的 Cisco IOS®防火墙、以及用于 Cisco Catalyst® 6500 系列交换机和 Cisco 7600 系列路由器的防火墙业务模块（FWSM）。

现在，网络对于企业的成功比以往任何时候都更加重要。它们支持着关键应用和流程，并为融合的数据、语音和视频服务提供了一个通用基础设施。思科非常了解企业目前面临的安全挑战，并通过为客户提供业界一流的安全解决方案，帮助他们安全地开展业务。与只提供具有基本安全性的单点产品不同，思科致力于将安全性嵌入到整个网络之中，在其所有产品中集成安全服务。这不仅可以加强安全保障，还能使其成为业务基础设施的一个透明、可扩展、可管理的组成部分。

Cisco ASA 5500 系列自适应安全设备、Cisco PIX 安全设备、思科集成业务路由器和 Cisco ASR 1000 系列汇聚业务路由器中的 Cisco IOS 高级安全特性集，以及用于 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器的 FWSM，构成了集成的安全解决方案，完美地诠释了思科安全理念。其中每一款产品都经济高效地集成了全面的防火墙、入侵防御和 VPN 技术。实施这些集成解决方案的客户将可以加强安全性、降低拥有成本和减少运营开支——所有这些优势都得益于单一平台中集成安全服务带来的增强智能共享功能。

满足各种需求的集成防火墙解决方案

Cisco ASA 5500 系列、Cisco PIX 安全设备、Cisco IOS 防火墙，以及用于 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器的 FWSM，构成了思科灵活的集成防火墙解决方案。在模块化、可扩展的平台基础之上，每个产品都设计有一个独特的特性集，可以更好地保护不同的网络环境。您既可以单独地部署这些解决方案，以保护网络基础设施中的特定区域，也可以遵循思科 SAFE 蓝图中所介绍的设计最佳实践，将它们整合到一起，构建出一种分层的深层防御系统。

为了进一步丰富这些集成防火墙解决方案，思科还提供了全面的安全管理产品系列——从思科安全设备、Cisco IOS 软件安全特性和嵌入式设备管理器，到独立的管理应用，以确保您能够有效管理思科安全基础设施。

Cisco ASA 5500系列

Cisco ASA 5500 系列自适应安全设备将经过市场验证的、业界最佳的安全和 VPN 服务，与一个创新的、自适应架构结合在一起。这为客户带来了一个强大的多功能网络安全设备，能够为中小型企业（SMB）、大型企业和数据中心网络提供全面保护，同时降低达到这一全新安全等级所需的总体部署和运营成本。

Cisco ASA 5500 系列采用了专门为 Cisco PIX 500 系列安全设备、Cisco IPS 4200 系列传感器和 Cisco VPN 3000 系列集中器开发的技术。这些技术在 Cisco ASA 5500 系列上无缝融合在一起，提供了一个能

够阻止最广泛威胁的平台。Cisco ASA 5500 系列在其产品系列（如图 1 所示）中，可确保应用和内容的安全，并带来不含威胁的 VPN 连接。这一广泛的安全功能可以保护任何网段，包括最常见的威胁攻击渠道，例如远程站点、局域网连接的内部用户和远程接入 VPN 等。

图 1. Cisco ASA 5500 系列设备产品系列

Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580
小型办公室	**中型分支机构**	**大型企业**	**企业边缘**	**企业边缘或总部**	**数据中心**
					

注： 图 1 提供了一般性指导方针。您应当根据自己的需求部署您的网络。

Cisco ASA 5500 系列通过智能的、可感知应用的检测引擎，提供了强大的应用安全性，能够对四到七层的网络流进行检查。这将可以为客户带来更加安全的网络，包括 Web、语音和第三代（3G）移动无线服务等。

为了保护网络避免遭受应用层攻击，帮助企业更有效地控制在其环境中使用的应用和协议，这些检测引擎还集合了广泛的应用与协议知识，并采用了多项安全执行技术，如协议异常检测、应用和协议状态跟踪等。此外，它们还采用了攻击检测和消除技术，例如应用和协议命令过滤、内容验证及 URL 反混淆技术等。

这些检测引擎还提供了对即时消息、对等文件共享和隧道应用的控制，来支持您的企业执行使用策略，并释放网络带宽用于关键业务应用。

在加强网络安全的同时，Cisco ASA 5500 系列还能降低部署和运营成本。凭借广泛的 VPN 和安全服务特性，其成为一款能够用于多种用途的设备，进而实现了平台标准化。您可以在中央地点将其部署为一个融合的威胁防御设备，以使用其访问控制、应用检测，以及蠕虫、病毒和其他恶意软件防范技术。您还可以将其作为专用的远程接入设备，充分利用其 VPN 功能。它在网络内部也同样能够发挥重要作用，包括提供部门间的访问控制，以及防御内部用户在无意间引入到网络中的蠕虫、病毒和其他恶意代码。

在小型企业和分支机构环境中，Cisco ASA 5500 系列可以充当一个“多功能一体”的设备，提供全面的威胁防御和 VPN 服务，同时满足此类部署的预算和运营模式要求。这种自适应的“单一设备，多种用途”方法减少了您需要部署和管理的平台数量，同时在所有部署中提供了一个通用的运营与管理环境。这一方法将可以简化配置、监控、故障排除和安全人员培训工作。为了最大限度地降低运营成本，Cisco ASA 5500 系列还具有很高的网络感知能力，可以在不中断合法流量和应用的情况下，无缝地部署到网络之中。

Cisco ASA 5500 系列防火墙性能

- Cisco ASA 5505: 150 Mbps
- Cisco ASA 5510: 300 Mbps
- Cisco ASA 5520: 450 Mbps
- Cisco ASA 5540: 650 Mbps
- Cisco ASA 5550: 1.2 Gbps
- Cisco ASA 5580-20: 6.5 Gbps
- Cisco ASA 5580-40: 14 Gbps

Cisco PIX安全设备

市场领先的 Cisco PIX 系列安全设备通过经济高效、易于部署的解决方案，提供了强大的用户和应用策略执行，多矢量攻击防范和加密连接服务。这些设备提供了多种集成的安全和网络服务，包括先进的应用感知防火墙服务、市场领先的 IP 语音（VoIP）和多媒体安全、稳定的站点间和远程接入 IP 安全（IPSec）VPN 连接、屡获殊荣的永续性、智能网络服务，以及灵活的管理解决方案等。

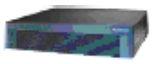
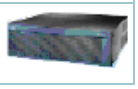
Cisco PIX 系列包括多种产品——从面向小型和家庭办公室的、外型小巧、便于使用的桌面设备，到面向大型企业和服务供应商环境、具有出色投资保护能力的模块化千兆位设备。Cisco PIX 安全设备能够为各种规模的网络环境带来稳定的安全保护、性能和可靠性。

Cisco PIX 安全设备集成了广泛的高级防火墙服务，以防止企业在互联网和企业网络环境中受到威胁的持续攻击（如图 2 所示）。这些设备能够提供丰富的状态检测防火墙服务，跟踪所有网络通信的状态，以及阻止未经授权的网络访问。

它们还通过智能的、可感知应用的检测引擎，提供了强大的应用层安全功能，能够对四到七层的网络流进行检查。为了保护网络免受应用层攻击，帮助企业更有效地控制在其环境中使用的应用和协议，这些检测引擎集合了广泛的应用和协议知识，并采用了安全执行技术，其中包括协议异常检测、应用和协议状态跟踪，网络地址转换（NAT）服务，以及攻击检测和消除技术，如应用和协议命令过滤、内容验证及 URL 反混淆技术等。

这些检测引擎还能帮助您的企业控制即时消息、对等文件共享和隧道应用，支持您执行使用策略，并释放网络带宽用于合法的业务应用。

图 2 Cisco PIX 安全设备产品系列

Cisco PIX 501	Cisco PIX 506E	Cisco PIX 515E	Cisco PIX 525	Cisco PIX 525	Cisco PIX 535
远程办公人员或 SOHO（1-20 名用户）	**小型分支机构（20-99 名用户）**	**中型分支机构（100-999 名用户）**	**大型企业分支机构（100-999 名用户）**	**企业边缘**	**企业总部数据中心**
					

注：图 2 提供的是一般性应用指导方针。您应根据自己的应用需求，而不仅仅是根据网络的规模，选择合适的产品。

Cisco PIX 安全设备建立在一个可以提供多种安全服务的加固操作系统基础之上，能够提供最高级别的安全性。它已经通过了多项业界评估和认证，包括针对防火墙的通用标准评估保障（EAL）四级和 IPSec 认证。Cisco PIX 安全设备能够为多种 VoIP 和其他多媒体标准提供市场领先的安全保护，包括 H.232 版本 4、会话创建协议（SIP）、思科瘦客户端控制协议（SCCP）、实时流协议（RTSP）和媒体网关控制协议（MGCP）等，以帮助企业安全地部署多种现有的和下一代 VoIP 和多媒体应用。

Cisco PIX 安全设备能够提供多种配置、监控和故障排除选项，让您的企业可以灵活地使用最符合自身需要的方法。在管理解决方案方面，既有基于策略的集中管理工具，也有基于 Web 的集成管理，并支持远程监控协议，如简单网络管理协议（SNMP）和系统日志等。集成的思科自适应安全设备管理器（ASDM）提供了一个基于 Web 的世界一流管理界面，能够显著简化单一 Cisco PIX 安全设备的部署、后续配置和监控工作，且无需在管理员的计算机上安装任何软件（除了标准 Web 浏览器和 Java 插件以外）。

管理员还能利用一个命令行接口（CLI），远程配置、监控和排除 Cisco PIX 安全设备故障。安全 CLI 访问可通过多种方法实现，包括 Secure Shell 版本 2（SSHv2）协议、基于 IPSec 的 Telnet，以及通过控制台端口进行带外访问。Cisco PIX 安全设备还具有强大的自动更新功能，以及一组革命性的安全远程管理服务，可确保防火墙配置和软件映像始终保持最新状态。此外，Cisco PIX 安全设备还支持使用多种由思科技术开发合作伙伴提供的配置和监控工具。

每款 Cisco PIX 安全设备产品的防火墙性能如下：

Cisco PIX 安全设备防火墙性能：

- Cisco PIX 501: 60 Mbps
- Cisco PIX 506E: 100 Mbps
- Cisco PIX 515E: 190 Mbps
- Cisco PIX 525: 330 Mbps
- Cisco PIX 535: 1.7 Gbps

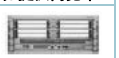
Cisco IOS防火墙

Cisco IOS 防火墙是一种状态检测防火墙选件，适用于 Cisco 1800、2800 和 3800 系列集成业务路由器；Cisco 800 和 7200 系列路由器；Cisco ASR 1000 系列汇聚业务路由器；以及 Cisco 7301 路由器。所有配有 Cisco IOS 软件高级安全或更高特性集的集成业务路由器，都支持 Cisco IOS 防火墙。Cisco ASR 1000 系列汇聚业务路由器还能为企业网络的广域网和互联网边缘，以及电信运营商网络中的宽带用户，提供基于区域的多千兆位速率 Cisco IOS 防火墙。

Cisco IOS 防火墙是一款理想的一体化安全与路由解决方案，可为 WAN 到网络的接入点提供有效保护。其主要特性包括：具有拒绝服务（DoS）防护功能的状态检测防火墙；增强的应用、流量和用户感知能力，有利于发现、检查和控制应用；针对语音、视频和其他应用的先进的协议检查功能；针对每个用户、每个接口或者子接口的安全策略；紧密集成的身份识别服务，针对每个用户提供身份验证和授权；以及方便的管理。基于角色的精细访问，可支持在网络运营和安全运营人员之间，安全合理地区分路由器管理权限。

Cisco IOS 防火墙不仅能够帮助在网络周边实现单点保护，还能将安全策略的实施变成网络自身的一个固有组成部分。Cisco IOS 防火墙可以运行在多种基于 Cisco IOS 软件的路由器上（如图 3 所示）。它为那些既希望利用网络基础设施保障安全，又想要继续利用 Cisco IOS 软件功能的客户（无论办公场所的规模多大）提供了最佳选择。这些软件功能包括服务质量（QoS）、多协议、组播和先进路由支持等。

图 3. Cisco IOS 防火墙产品系列

Cisco 871	Cisco 1841	Cisco 2801	Cisco 2811	Cisco 2821	Cisco 2851	Cisco 3825	Cisco 3845	Cisco ASR 1000 系列
SOHO 企业级远程办公人员（ECT）	**小型分支机构**	**中型分支机构**	**中型分支机构**	**中型分支机构**	**中型分支机构**	**大型企业分支机构**	**大型企业分支机构**	**大型企业广域网边缘和高速分支机构，服务提供商宽带**
								

注：图 3 提供了一般性指导方针。您应当根据自己的应用需求，而不仅仅是根据网络的规模，选择合适的产品。

集成 Cisco IOS 防火墙采用了一种先进的防火墙引擎，能够根据应用信息动态控制流量，从而为复杂的应用提供增强的安全保护。它还针对 HTTP 和电子邮件消息提供了先进的应用检查和控制功能。Cisco IOS 防火墙 HTTP 检查引擎可以确保协议一致性，防范恶意的或者未经授权的行为（例如端口 80 隧道、畸形数据包和特洛伊木马等）侵入网络。HTTP 检查引擎为 Cisco IOS 防火墙提供的信息不仅能够拦截非 HTTP 流量，还可以确保被假定为 HTTP 的流量源自于合法的 Web 浏览，而不是即时消息或者其他试图穿越防火墙的流量。在此基础之上，网络管理员将能够更加有效地控制穿越防火墙的应用。

思科集成业务路由器还包含充分利用了思科 IPS 技术的入侵防御系统（IPS）。Cisco IOS IPS 是一款基于深层数据包检查的内嵌解决方案，能够帮助思科路由器有效遏制网络攻击。由于 Cisco IOS IPS 嵌入在网络之中，因而它可以丢弃流量，使路由器能够立即应对安全威胁，保障网络的安全。

Cisco IOS 防火墙的其他功能包括：语音穿越支持；IPv6 支持；透明防火墙；URL 过滤；对虚拟路由转发（VRF）环境中各个防火墙上下文的支持；思科网络准入控制（NAC）支持；故障切换支持；网络地址转换（NAT）；基于时间的访问列表；Java Applet 拦截；对等路由器身份验证；实时告警；审计追踪；以及事件日志等。Cisco IOS 防火墙通过了 CC EAL4 认证；Cisco IOS IPSec 通过了 FIPS 140-2 认证。

您可以利用多种方法，通过一个便捷的 CLI 管理 Cisco IOS 防火墙。这些方法包括 Telnet、SSH，或通过一个控制台端口进行带外管理。或者，您也可以利用思科路由器和 Cisco Configuration Professional（CCP）配置和监控 Cisco IOS 防火墙。CCP 是一款基于 Web 的直观、安全的设备管理工具，内嵌于 Cisco IOS 防火墙之中。思科 SDM 能够通过智能向导简化设备和安全配置，让客户无需深入了解 Cisco IOS CLI，即可快速、方便地部署、配置和监控 Cisco IOS 防火墙。

此外，从 Cisco IOS Software Release 12.3 开始，Cisco IOS 防火墙将集成 Cisco AutoSecure 功能。这项功能支持通过自动配置安全特性和移除在默认情况下启用的不安全特性，极大降低保护路由器安全的复杂性。该功能可以简化安全流程，帮助客户快速实施安全策略和步骤，从而确保网络服务的安全。您还可以思科技术开发合作伙伴提供的工具，配置和监控 Cisco IOS 防火墙。

Cisco ASR 1000系列: 一种面向广域网边缘的、功能强大的新产品

全新 Cisco ASR 1000 系列汇聚业务路由器采用了思科 QuantumFlow 处理器来提供诸如防火墙、深层数据包检查和日志服务等高性能集成威胁控制服务，同时进行广域网和互联网边缘路由。QuantumFlow 处理器是业界首款大规模并行处理器硬件和软件架构。

Cisco ASR 1000 系列路由器采用独特设计，将攻击识别和防御能力完美集成到企业广域网和互联网边缘路由器中：

- Cisco IOS 防火墙服务可以扩展到 5、10 和 20Gbps。您可以对所有 Cisco ASR 1000 系列路由器接口应用基于分区的防火墙策略。
- 采用了基于网络的应用识别（NBAR）和灵活分组匹配（FPM）技术的深层分组检查，能够以多千兆位速度运行，并可以利用 Cisco NetFlow v9 进行高速日志记录（每秒 40,000 个会话）。

所有采用了 Cisco IOS XE ASR 1000 系列路由处理器 1（RP1）和路由处理器 2（RP2）高级 IP 服务软件及高级企业服务映像选件（包括没有加密功能的选件）的 Cisco ASR 1000 系列汇聚业务路由器，都支持 Cisco IOS 防火墙。

Cisco ASR 1000 系列防火墙能够在一个运营商级广域网中提供高达 20 Gbps 的性能。其定位介于 Cisco 7200 系列与用于 Cisco 7600 系列和 Cisco Catalyst 6500 系列的防火墙服务模块之间。

如需了解关于 Cisco ASR 1000 系列的更多信息，请访问：http://www.cisco.com/go/asr1000。

下表列出了不同 Cisco IOS 路由器平台在运行 Cisco IOS 防火墙时的性能。这些性能数据反映了在对包含 64-KB 对象的 HTTP 流量进行状态检查时的测试结果。

Cisco IOS 防火墙的性能

- Cisco 870: 32 Mbps
- Cisco 1812: 40 Mbps
- Cisco 1841: 42 Mbps
- Cisco 2801: 45 Mbps
- Cisco 2811: 51 Mbps
- Cisco 2821: 208 Mbps
- Cisco 2851: 264 Mbps
- Cisco 3825: 287 Mbps
- Cisco 3845: 405 Mbps
- Cisco ASR 1000 系列：5、10 或 20 Gbps

用于Cisco Catalyst 6500系列交换机和Cisco 7600系列路由器的 Cisco FWSM

Cisco FWSM 是一款用于 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器的高速集成防火墙模块。该模块能够提供业界领先的数据速率：5Gbps 的吞吐率；每秒 100,000 个连接（cps）；以及 100 万个并发连接。

您可以在同一个机箱中安装多达 4 个 Cisco FWSM，从而使每个机箱达到无与伦比的 20 Gbps 的防火墙容量。此外，您还可以将 Cisco FWSM 与其他思科安全服务模块结合到一起，例如入侵检测服务模块（IDSM-2）、IPSec VPN 服务模块（VPNSM）和网络分析模块（NAM-1 和 NAM-2）等。这种模块化方式使您可以充分利用现有的交换和路由基础设施，并获得业界最高的性能，同时无需进行昂贵的升级。FWSM 是面向企业和电信运营商数据中心、以及企业园区各分发点的最佳解决方案。

Cisco FWSM（如图 4 所示）安装在 Cisco Catalyst 6500 系列交换机或 Cisco 7600 系列路由器之中，允许设备上的任何端口充当防火墙端口，并将状态检测防火墙安全集成到网络基础设施之中。这一特性在机架空间非常昂贵的环境中极为重要。Cisco Catalyst 6500 系列是那些需要多种智能服务的客户的首选 IP 服务交换机。这些服务包括防火墙服务、入侵检测、VPN 服务，以及多层 LAN、WAN 和 MAN 交换功能等。

图 4 用于 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器的 Cisco FWSM

Cisco FWSM 构建于 Cisco PIX 技术的基础之上，使用了经过实践检验的相同 Cisco PIX 操作系统——一种安全的实时操作系统。利用业经验证的 Cisco PIX 技术来检查数据包，Cisco FWSM 可在同一平台上提供独特的性能与安全性。

Cisco FWSM 可用于面向 Cisco Catalyst 6500 系列交换机的 CiscoView Device Manager 中。它在初始安装之后，可为所有服务提供图形化的 VLAN 虚拟化功能。您也可以从 CiscoView Device Manager 启用 Cisco PIX Device Manager，这是一款具有高级配置、监控和故障排除功能的嵌入式管理器。另外，Cisco FWSM 还得到了思科技术开发合作伙伴的支持，利用他们提供的工作进行配置、监控和报告工作。

何时部署各款思科集成防火墙解决方案

Cisco ASA 5500 系列、Cisco PIX 安全设备、Cisco IOS 防火墙和 Cisco FWSM 都采用了先进的防火墙技术，具有很多共同的特性和优势。但是，每款解决方案都是针对特定环境而设计的。表 1 – 4 列出了这些解决方案的相似之处和区别，并提供了一般性指导方针，帮助网络设计人员决定在何时应当部署各款解决方案，以及如何充分发挥它们各自的优势。

表 1. Cisco ASA 5500 系列、Cisco PIX 安全设备、Cisco IOS 防火墙和 Cisco FWSM 共有的特性和优势

特性	优势
状态检查防火墙	通过执行由管理员定义的访问控制策略，以及执行深层数据包检测和跟踪所有网络通信的状态，提供强大的网络和应用安全
应用和协议检测与控制	通过使用能够在第四到第七层检查数据流的专用检测引擎，提供增强的应用和协议安全
针对每个用户的动态身份验证和授权	通过采用高性能的直通式代理机制，并集成采用了 RADIUS 和 TACACS+ 协议的思科安全访问控制服务器（ACS），提供灵活的用户身份验证和授权。该特性允许与多种用户数据库进行集成，包括微软活动目录、Microsoft Windows NT 域、轻型目录访问协议（LDAP）目录和一次性密码系统等
动态和静态的 NAT 与端口地址转换（PAT）	提供广泛的 NAT 应用和协议支持，并能防止内部网络地址受到外部影响，提供了一个额外的保护层
内容过滤	通过集成领先的第三方 URL 过滤解决方案，提高员工的工作效率；同时它还支持 URL 过滤，可以拦截恶意的 Java Applet
远程管理	为开展配置、监控和故障排除工作提供了多种远程管理方法。管理解决方案中既有高度可扩展的中央管理工具，也有基于 Web 的集成管理方案，能够支持诸如 SNMP 和系统日志等各种远程监控协议

表 1. Cisco ASA 5500 系列、Cisco PIX 安全设备、Cisco IOS 防火墙和 Cisco FWSM 共有的特性和优势（续）

特性	优势
基于身份验证、授权和记账（AAA）的管理权限控制	支持基于 TACACS+和 RADIUS 协议所提供的 AAA 服务，对管理权限进行精细控制，支持管理员应用访问策略来控制每一个管理用户或者管理组可以使用的服务和命令
多 DMZ 支持	支持额外的物理或者虚拟网络接口，可以在共享网络（DMZ）上为服务器提供受保护的访问权限（例如 Web、电子邮件、FTP 或者域名系统 [DNS]）
广泛的多媒体支持，包括流视频、流音频和语音应用	为多种 VoIP 标准和其他多媒体标准提供了丰富的状态检查防火墙服务，让企业可以安全地利用融合数据、语音和视频网络能够带来的多种优势，例如生产率和竞争优势的增强等
DoS 攻击防护	为拦截和阻止 DoS 攻击提供了多种机制，如 TCP 拦截、TCP SYN cookie、DNS 防护、Flood Guard、邮件保护和单播反向路径转发（URPF）
安全的动态路由	为路由信息协议（RIP）和开放最短路径优先（OSPF）提供了基于消息摘要算法 5（MD5）和明文的路由身份验证，放置路由伪装和各种基于路由的 DoS 攻击
防火墙虚拟化	允许将设备划分为多个虚拟防火墙或者安全环境。企业可以单独管理每个虚拟防火墙，并能在同一个物理基础设施上划分业务单元或者其他功能领域。同样，电信运营商可以利用防火墙虚拟化，在同一个物理设备上支持和划分多个客户

表 2. 何时应用 Cisco ASA 5500 自适应安全设备

客户要求	Cisco ASA 5500 安全设备优势
专门设计的业界一流“融合”安全设备	Cisco ASA 5500 系列设备能够提供目前最先进的集成网络安全服务，包括状态检查防火墙、IPS、VPN，蠕虫和恶意软件防护，网络防病毒，VPN 集群服务，以及一个模块化的安全服务插槽。Cisco ASA 5500 系列设备完全兼容 Cisco PIX 设备。您可以利用来自于这两个系列的设备，来满足客户的需求
可以在前端和分支机构用于多种用途的单个安全设备	您可以在中心地点，将 Cisco ASA 5500 系列设备用作融合和威胁防御设备，以利用它们的访问控制、应用检测，以及蠕虫、病毒和恶意软件防护技术。您还可以将它们部署为远程访问设备，使用其 IPSec 和 SSL VPN 功能。您可以在网络内部，用它们来实施部门间访问控制，防范内部用户可能在无意之间引入网络的蠕虫、病毒和其他恶意代码。在所有这些情况下，Cisco ASA 设备都堪称功能最丰富的思科解决方案
可以降低运营成本的融合设备	“单个设备，多种用途”的方式有助于减少您所需要部署和管理的平台数量，为所有部署提供一个通用的操作和管理环境。这种方式有助于简化配置、监控、故障排除和安全人员的培训工作
高可用性	在配置为故障切换对时，Cisco ASA 5500 系列设备能够通过同步的连接状态和设备配置数据，提供全状态故障切换能力，从而确保网络会话可以自动地在设备之间切换，并且对用户完全透明

表 3. 何时应用 Cisco PIX 安全设备

客户要求	Cisco PIX 安全设备优势
专门设计的、业界一流一体化安全设备	Cisco PIX 安全设备能够提供目前最先进的集成网络安全服务，包括状态检查防火墙，协议和应用检测，VPN、内嵌入侵防御，以及富媒体和语音安全服务。Cisco PIX 安全设备完全兼容 Cisco ASA 5500 系列设备；您可以利用来自于这两个系列的设备，来满足客户的需求
适合企业前端和数据中心的专用设备	Cisco PIX 安全设备专为确保安全而设计，采用了一个经过加固的、嵌入式操作系统，从而能够消除通用操作系统的常见安全漏洞，为保障总体安全提供一个出色的系统
分离的安全基础设施	您可以将 Cisco PIX 安全设备部署为专用的安全系统，提供增强的安全功能，并可以有效地将安全基础设施与网络的其余部分隔离
高可用性	与 Cisco ASA 5500 系列设备相同，在配置为故障切换对时，Cisco PIX 安全设备能够通过同步的连接状态和设备配置数据，提供全状态故障切换能力。这有助于确保网络会话可以自动地在设备之间切换，并且对用户完全透明
适用于小型办公室和家庭办公室的安全设备	Cisco PIX 501 安全设备通过一个紧凑的、一体化的安全解决方案，提供了多种集成的安全服务，先进的网络服务，以及强大的远程管理功能。它能够通过一个可靠的、便于部署的专用设备，为小型办公室和远程办公环境带来企业级的安全

表 4. 何时应用 Cisco IOS 防火墙

客户要求	支持的平台	Cisco IOS 防火墙优势
一体化解决方案，集成强大的安全、QoS、多协议路由、集成 WAN 接口和语音应用支持	Cisco 800、1800、2800 和 3800 集成业务路由器，Cisco 7200 路由器，以及 Cisco ASR 1000 系列	Cisco IOS 软件高级安全特性集在单个设备中，提供一个完善的集成安全解决方案，包括状态数据包过滤，入侵检测与防范，针对每个用户的身份验证和授权，VPN 功能，广泛的 QoS 机制，多协议路由，语音应用支持，以及集成 WAN 接口支持等
使用网络基础设施保障安全	Cisco 800、1800、2800 和 3800 系列，Cisco 7200，以及 Cisco ASR 1000 系列	你可以在现有基于 Cisco IOS 软件的路由器上加载 Cisco IOS 防火墙，从而在网络基础设施实现更出色的投资保护。重复使用相同的硬件机箱和组件，不仅能降低拥有成本，还能减少运营开支——您可以使用相同的管理基础设施，而不需要再进行额外的人员培训
在单个设备中提供广泛的 VPN 和防火墙支持	Cisco 800、1800、2800 和 3800 系列，Cisco 7200，以及 Cisco ASR 1000 系列	通过为 Cisco IOS 防火墙部署 Cisco IOS 加密和 QoS VPN 功能，可以在公共网络上实现安全的、低成本的数据传输。Cisco IOS 防火墙提供了最为广泛的 VPN 支持，包括（但不仅限于）动态多点 VPN（DMVPN）、IPSec 全状态故障切换、Easy VPN Remote、Easy VPN Server、站点间 VPN、高级加密标准（AES）、VPN 加速卡，支持语音和视频流的 VPN（V3PN）和 VPN QoS

表 4. 何时应用 Cisco IOS 防火墙（续）

客户要求	支持的平台	Cisco IOS 防火墙优势
高性能、高可用性广域网前端和互联网边缘	Cisco ASR 1000 系列	可以在不影响广域网路由性能的情况下，在 Cisco ASR 1000 系列中启用嵌入式的高性能安全服务。集成的“一体化”路由器方法可简化运营，降低成本，缩短审核、部署和维护 WAN 基础设施所需的时间 **高性能下一代路由器带来速度更快的全新广域网边缘服务** ● 与 Cisco 7200 系列相比，平台性能最高可以提升 20 倍 ● 5、10 和 20Gbps 防火墙，NAT，以及板载的千兆位级 IPSec 加速性能 ● 基于 NBAR 和灵活数据包匹配（FPM）的高速嵌入式深层数据包检测 ● 采用了思科 QuantumFlow 处理器——业界首个大规模并行处理器硬件和软件架构 ● 定位介于 Cisco 7200 系列和 Cisco Catalyst 6500 系列/7600 系列之间 **运营商级设计带来独一无二的广域网可用性** ● 通过分离控制和数据平面，提供最大限度的系统可用性 ● 冗余控制平面支持快速故障切换，实现零数据包丢失 ● 冗余转发引擎支持全状态故障切换，可最大限度地减少数据包丢失 ● 板载的双 Cisco IOS 软件映像提供软件冗余 ● 模块化 Cisco IOS XE 软件带来进程重启、故障管理、以及不间断软件升级（ISSU）功能 **卓越运营** ● 通过改善带宽利用率、整合网络、集成服务和提高能效优化 WAN 成本 ● 在无需叉车式升级的情况下提升容量 ● 可扩展的灵活 QoS 带来最佳应用性能 ● 可扩展的 NetFLow v9
为电信运营商网络建立针对每个用户的防火墙	Cisco ASR 1000 系列	这一特性将 Cisco IOS 基于分区的策略防火墙，与 Cisco ASR 1000 系列丰富的宽带特性集结合到一起，让互联网服务提供商能够为其宽带用户提供防火墙服务 这一解决方案安装在 Cisco ASR 1000 系列上，作为 L2TP 网络服务器（LNS）。所有功能都内嵌于 QuantumFlow 处理器之中，能够在宽带环境中提供千兆位性能的中央防火墙服务

表 4. 何时应用 Cisco IOS 防火墙（续）

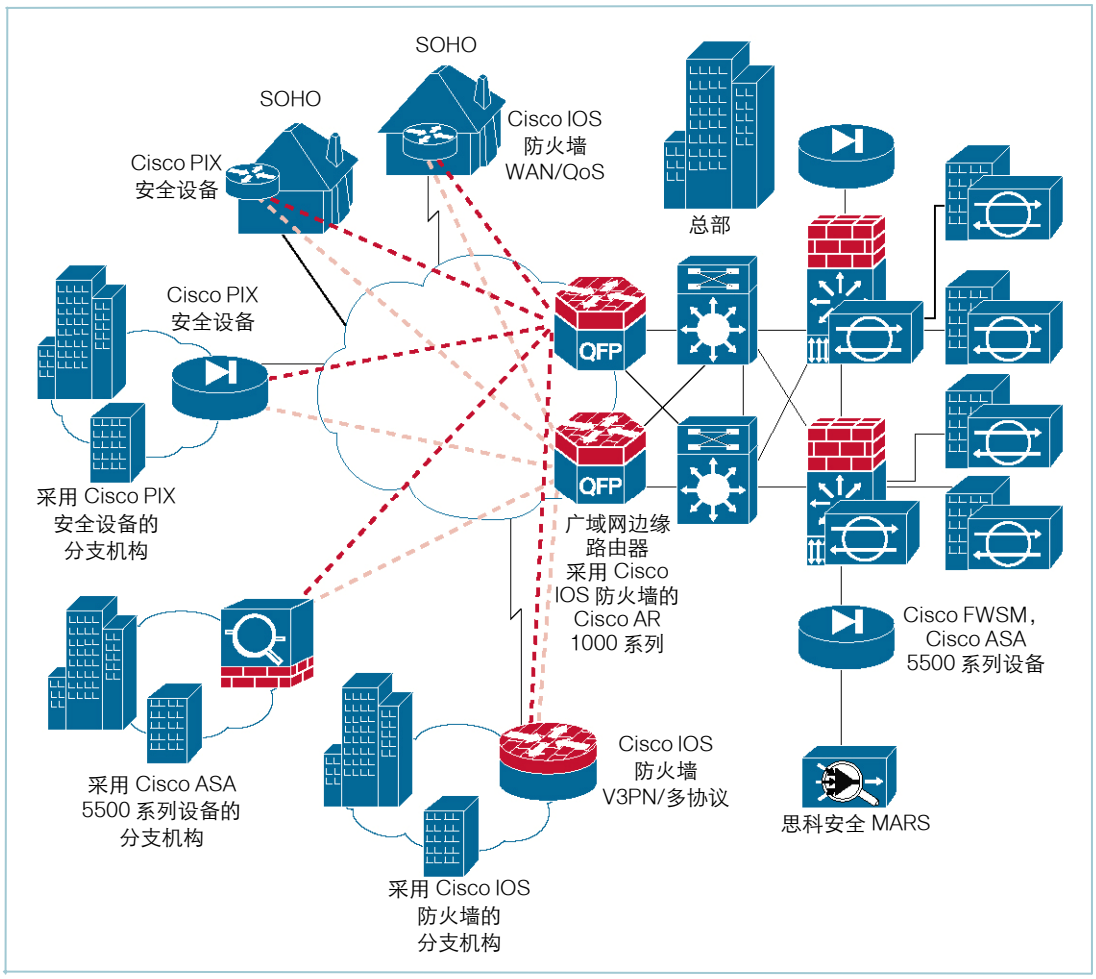
客户要求	支持的平台	Cisco IOS 防火墙优势
为电信运营商网络建立针对每个用户的防火墙（续）	Cisco ASR 1000 系列（续）	**主要特性包括：** • 通过 RADIUS，动态为防火墙分区分配虚拟访问接口 • 以精确到用户点对点协议（PPP）会话的方式，提供应用级监控和状态数据包检测 • 在防火墙丢弃日志消息中包含用户的用户名，跟踪每个用户的数据包丢弃情况 • 能够为匹配的来源和目的地分区设置区域对，以控制用户之间的流量

表 5. 何时应用 Cisco FWSM

客户要求	Cisco FWSM 优势
电信运营商和大型企业的前端和数据中心	Cisco FWSM 具有卓越的性能、可扩展性和虚拟化功能，是电信运营商和大型企业的前端与数据中心的最佳选择。Cisco FWSM 可以提供：5Gbps 的吞吐率；100000 cps；100 万个并发连接。您可以在一个机箱中最多部署 4 个 Cisco FWSM，从而提供总共 20Gbps 的吞吐率。单个 FWSM 最多可以支持 1000 个虚拟接口（每个上下文环境 256 个），单个机箱最多可以扩展到 4000 个 VLAN。您可以将单个 FWSM 划分为最多 100 个虚拟防火墙（安全上下文环境）。利用 Cisco FWSM 资源管理器，您的组织随时可以限制为每个安全上下文环境分配的资源，从而确保每个安全上下文环境不会互相干扰
能够在前端或者数据中心使用网络和交换基础设施	您可以在现有的 Cisco Catalyst 6500 系列交换机或者 Cisco 7600 系列路由器中部署 Cisco FWSM，从而实现更加全面的投资保护，并且集成高速交换和路由能力。此外，您还能够以透明的第二层桥接模式，或者第三层路由器模式，部署 FWSM。透明的第二层防火墙可以简化网络集成，允许流量在不需要进行任何路由的情况下，在同一个子网中对其进行监控
高可用性	您可以成对部署 Cisco FWSM，在机箱内部或者机箱之间提供全状态故障切换服务，为最为关键的环境带来可靠的网络保护能力。配置为故障切换模式的模块能够不断地同步它们的连接状态和设备配置数据；如果发生故障，模块能够以完全透明的方式完成故障切换

图 5 显示了如何部署思科集成防火墙解决方案来保障整个企业网络的安全。

图 5. 思科集成安全解决方案如何保障您企业网络的安全



思科安全管理解决方案

除了思科防火墙解决方案中的嵌入式设备管理器以外，思科还为那些希望管理超过嵌入式管理器的设备数量的客户，提供了集成安全管理应用。

对于那些希望对思科防火墙解决方案进行全面的安全策略管理的客户，思科提供了思科安全管理器。思科安全管理器是一种功能强大、便于使用的解决方案，可以支持完成思科防火墙、VPN 和入侵防御系统（IPS）等的设备配置和安全策略工作。该解决方案既可以管理不超过 10 个设备的小型网络，又能够通过扩展，有效地管理包含数千个设备的大型网络。基于策略的智能管理技术可以帮助客户轻松实现可扩展性，从而简化管理工作。

在集中安全信息管理方面，思科提供了思科安全监控、分析和响应系统（MARS）。思科安全 MARS 是一个高性能、可扩展的威胁消除设备系列，可以巩固网络设备和安全对策。通过整合网络拓扑信息、上下文关联、分析和自动消除功能，思科安全 MARS 可以发现、管理和消除网络攻击，保持法规遵从性。思科安全管理器和思科安全 MARS 可以通过集成，降低运营开支（OpEx），提高防火墙部署的投资回报（ROI）。

例如，您可以通过在思科安全 MARS 中选择一个防火墙系统日志，显示生成该系统日志的思科安全管理

器中的所有访问列表规则，从而加快故障单的解决速度。

针对企业WAN边缘的思科服务

思科和我们的认证合作伙伴致力于通过多种基于成熟方法的服务，帮助您成功地部署企业广域网边缘。我们可以帮助您建立一个安全、可靠的广域网架构，并且成功地将安全、思科统一通信技术和带宽结合到一起，支持视频、协作、分支机构解决方案和业务发展，以实现您的业务目标。

思科生命周期服务方式定义了解决方案生命周期每个阶段的必要活动。出色的规划和设计能力可加快解决方案的采用速度。屡获殊荣的技术支持可以提高运营效率。而优化服务则能够提升性能、永续性、稳定性和可预测性，让您的网络和团队做好充分准备来迎接变化。如需了解更多信息，请访问：http://www.cisco.com/go/services。

其他信息

如需了解更多信息，请访问以下站点：

- Cisco ASA 5500 系列自适应安全设备：http://www.cisco.com/go/asa
- Cisco PIX 安全设备： http://www.cisco.com/go/pix
- Cisco ASR 1000 系列汇聚业务路由器： http://www.cisco.com/go/asr1000
- Cisco IOS 防火墙: http://www.cisco.com/go/firewall
- 思科路由器安全： http://www.cisco.com/go/routersecurity
- 思科防火墙服务模块：http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
- Cisco PIX 设备管理器：http://www.cisco.com/en/US/products/sw/netmgtsw/ps2032/index.html
- 思科安全设备管理器：http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html
- 思科安全管理器：http://www.cisco.com/go/csmanager
- 思科安全 MARS：http://www.cisco.com/go/mars
- 思科 SAFE 蓝图：http://www.cisco.com/go/safe

北京
北京市朝阳区建国门外
大街 2 号北京银泰中心
银泰写字楼 C 座 7-12 层
邮编：100022
电话：(8610) 85155000
传真：(8610) 85155960

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
成都市滨江东路 9 号 B 座
香格里拉中心办公楼 12 层
邮编：610021
电话：(8628) 86961000
传真：(8628) 86961003

如需了解思科公司的更多信息，请浏览 http：//www.cisco.com /cn