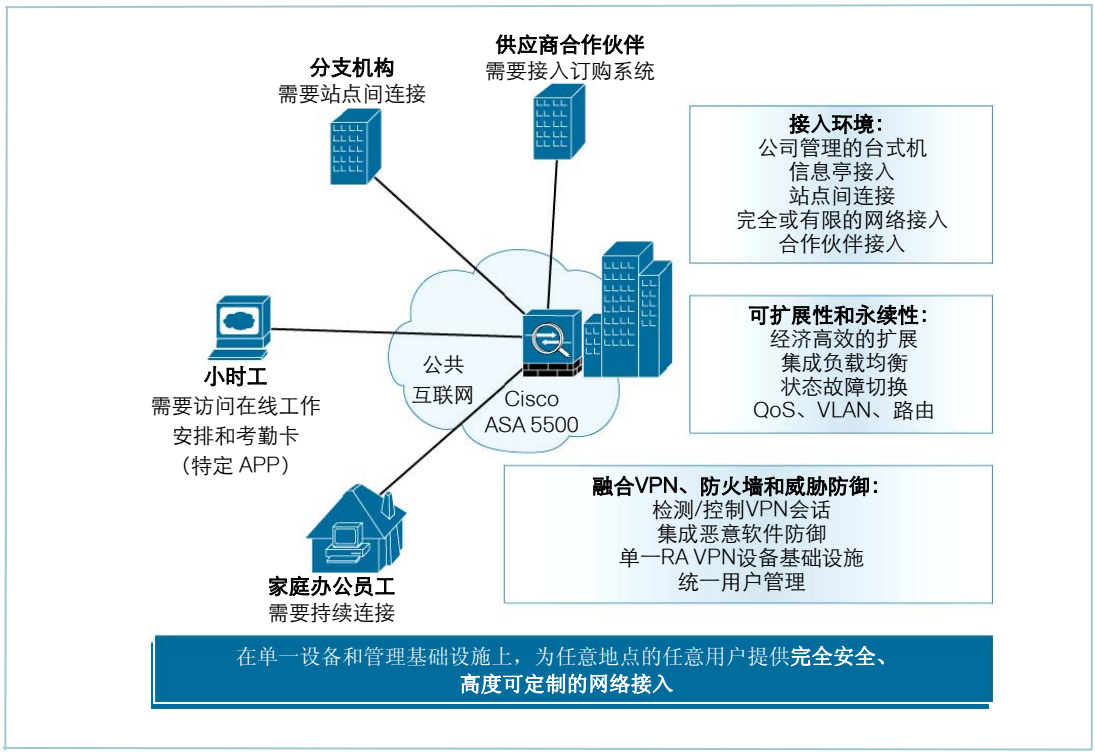
思科安全远程接入解决方案
(Cisco ASA 5500系列SSL/IPsec VPN版本)

Cisco® ASA 5500系列自适应安全设备是一款专用平台，集最佳安全和VPN访问于一身，是中小企业(SMB)和大型企业应用的最佳选择。Cisco ASA 5500系列产品支持针对具体部署环境和选项进行定制，并提供有特别产品版本以支持实现安全远程接入(SSL/IPsec VPN)、防火墙、Anti-X和入侵防御功能。

Cisco ASA 5500系列SSL/IPsec VPN版本（也称为思科安全远程接入解决方案）可支持企业在不影响企业安全策略完整性的情况下，建立互联网连接，并实现互联网传输的成本优势。通过将安全套接层(SSL)和IP安全(IPsec)VPN服务与全面的威胁防御技术相融合，Cisco ASA 5500系列产品可提供高度可定制的网络接入，满足各种部署环境的要求，同时带来先进的端点和网络级安全性（参见图1）。

图1. 适用于任意部署场景的可定制VPN服务



Cisco ASA 5500系列产品安全远程接入解决方案

思科安全远程接入解决方案提供了灵活的VPN技术，适用于任意连接环境，具有出色的可扩展性，每设备最高能支持10,000个并发用户。它通过SSL、传输层数据包安全协议(DTLS)、IPsec VPN客户端技术、先进的免客户端SSL VPN功能，以及网络感知型站点间VPN连接，提供了易于管理的全隧道网络接

入，可支持通过公共网络安全连接到移动用户、远程站点、承包商和业务合作伙伴。由于无需部署辅助设备来扩展和保护VPN，该解决方案能有效降低部署和运行VPN的成本。

思科安全远程接入解决方案的优势包括：

- **基于SSL、DTLS和IPsec的全面网络接入**——全面网络接入使网络层远程用户能够连接几乎任意应用或网络资源，同时这一接入能力还经常被用来向用户提供接入公司笔记本电脑等可管理的计算机。连接通过能够自动下载的Cisco AnyConnect VPN客户端、Cisco IPsec VPN客户端，以及Microsoft和Mac OS X L2TP/IPsec VPN客户端实现。Cisco AnyConnect VPN客户端将根据网络状况，自动将其隧道协议调整为最高效的方式，是第一款使用DTLS协议为延迟敏感型流量提供优化连接的VPN产品，如IP语音（VoIP）流量或基于TCP的应用接入等。通过支持基于SSL、DTLS和IPsec的远程接入VPN技术，Cisco ASA 5500系列提供了无与伦比的灵活性，能满足最为多样化的部署场景要求。
- **出色的免客户端网络接入**——免客户端远程接入支持从任意地点接入网络应用和资源，无需部署台式机VPN客户端软件。通过使用互联网浏览器中普遍存在的SSL加密，Cisco ASA 5500系列产品支持免客户端接入任意基于Web的应用或资源，诸如Citrix、经过优化的Microsoft Outlook Web Access和Lotus iNotes等终端服务应用，以及电子邮件、日历、即时消息、FTP、Telnet和SSH应用等通用厚客户端应用。此外，Cisco ASA 5500系列还提供了出色的内容重写功能，有助于确保可靠交付带有Java、JavaScript、ActiveX、Flash和其他高级内容的复杂网页。
- **网络感知型站点间VPN**——多个办公地点间将可以实现安全、高速的通信。VPN上对于服务质量(QoS)和路由的支持能确保以出色业务质量、可靠地提供延迟敏感型应用，如语音、视频和终端服务等。
- **威胁防御VPN**——VPN是恶意软件入侵网络的主要途径。恶意软件包括蠕虫、病毒、间谍软件、键盘记录器、特洛伊木马和rootkit等。Cisco ASA 5500系列产品具备广泛、深入的入侵防御、防病毒、应用感知防火墙和VPN端点安全功能，能够最大限度地降低VPN连接变成安全威胁途径的风险。
- **更为经济高效的VPN部署和运营**——扩展和保护VPN常常需要增加负载均衡和安全设备，从而会增加设备和运行成本。Cisco ASA 5500系列集成了所有这些功能，在当今可用的VPN产品中提供了前所未有的出色网络和安全集成水平。另外，通过在单一平台上支持灵活的隧道选项，Cisco ASA 5500系列产品还为客户部署并行VPN基础设施提供了经济高效的替代选择。
- **可扩展性和永续性**——Cisco ASA 5500系列产品每个设备最多能支持10,000个同步用户会话，同时通过集成集群和负载均衡功能，还能进行扩展以支持数万个同步用户会话。此外，状态故障切换特性提供了高度可用的服务，可最大限度地延长正常运行时间。
- **OpenSSL技术**——采用了OpenSSL Project开发的、用于OpenSSL工具包的软件(http://www.openssl.org)。

可定制的远程接入VPN特性

全面网络接入

Cisco ASA 5500系列SSL/IPsec VPN版本通过Cisco AnyConnect VPN客户端（如表1所示）或Cisco IPsec VPN客户端的网络隧道特性，提供了广泛的应用和网络资源接入功能。

表1. Cisco AnyConnect VPN客户端特性

特性	说明
优化的网络接入	• Cisco AnyConnect VPN客户端能根据网络限制条件，自动将其隧道协议调整为最高效的方式。DTLS协议能自动用于为远程敏感型流量，如VoIP流量或基于TCP的应用接入等提供优化连接。HTTP over SSL能通过锁定的环境，包括使用Web代理服务器的环境，确保网络连接的可用性 • 可使用数据压缩来减少数据传输量
广泛的操作系统支持	• Windows 2000 • XP 32位(x86)和64位(x64) • Windows Vista 32位(x86)和64位(x64)，包括Service Pack 1和2 (SP1和SP2) • Windows 7 (x86)和64位(x64)测试版 • Mac OS X Power PC以及Intel 10.4和10.5 • Linux Intel（2.6.x内核） • Cisco AnyConnect Mobile（需额外许可） • Windows Mobile 5.0、6.0和6.1（Professional和Classic）
广泛的部署和连接选项	部署选项： • 预部署，包括Microsoft Installer • 通过ActiveX (仅限Windows)和Java自动前端部署（初始安装时需要管理员权限） 连接模式： • 通过系统图标独立连接 • 通过浏览器启动连接(Weblaunch) • 通过免客户端门户启动连接 • 通过命令行接口(CLI)启动连接 • API
简便的客户端管理	• Cisco AnyConnect VPN客户端使管理员能自动从前端安全设备发布软件和策略更新，从而简化VPN客户端软件升级所需的管理工作
一致的用户体验	• 全隧道客户端模式适用于要求获得像局域网一样一致用户体验的远程接入用户 • 多种交付方法和较小的下载体积，确保了广泛的兼容性和Cisco AnyConnect VPN客户端的迅速下载
先进的IP网络连接	• 能够接入内部IPv4和IPv6网络资源 • 集中拆分隧道控制帮助优化网络接入 IP地址分配机制： • 静态 • 内部池 • DHCP • RADIUS/LDAP

表2. AnyConnect许可选项

许可选项	说明
平台许可	
AnyConnect Essentials	• 提供AnyConnect隧道，不含免客户端SSL VPN和Cisco Secure Desktop功能 • 针对企业应用的全隧道接入 • 每种设备类型单一许可
AnyConnect Premium	• 包含免客户端SSL VPN和Cisco Secure Desktop功能（包括主机扫描）。可选提供针对企业应用的全隧道接入 • 许可基于同步用户数目，分为单设备许可和共享许可
可选特性许可	
AnyConnect Mobile	• 支持移动操作系统平台兼容性 • 除Essentials或Premium许可之外，每设备还要配备此许可
高级端点评估	• 支持高级端点评估功能（如自动修补等） • 除Premium许可之外，每设备还要配备此许可 • 不能与AnyConnect Essentials许可共用

免客户端网络接入

免客户端SSL VPN接入的特性如表3所示，可支持从互联网信息亭、共享交换机、外部网合作伙伴、员工自己的台式机以及公司为员工配备的台式机，精确控制基于Web的特定网络资源和应用访问。

表3. Cisco ASA 5500系列产品基于Web的免客户端接入

特性	说明
广泛、可靠的兼容性	高级转换功能有助于确保支持包含复杂内容的网页，如HTML、Java、ActiveX、JavaScript和Flash等。
集成免客户端应用优化	针对Microsoft Outlook Web Access和Lotus iNotes等资源密集型应用的集成性能优化，提供了出色的响应速度和低延迟，可带来高质量SSL VPN最终用户体验。
可定制的用户体验	增强的免客户端门户采用基于群组的定制特性，可提供精确接入、易用性和可定制的用户体验： • 支持多语言免客户端用户门户 • 用户可定制的资源书签 • 发布基于RSS的信息资源，自动更新重要实时内容
全面免客户端Citrix接入	无需外部帮助应用，即能通过免客户端SSL VPN接入Citrix，有助于确保应用快速启动，降低桌面软件冲突的风险。
集成客户端/服务器应用支持	无需预部署远程客户端，即能访问通用客户端/服务器应用，确保迅速接入Telnet、SSH、RDP和虚拟网络计算(VNC)资源。
支持通用厚客户端应用	端口转发通过一个小型Java应用小程序，支持免客户端接入常用厚客户端应用，如POP、SMTP、IMAP、电子邮件、在线日历、即时消息、Telnet、SSH和其他客户端启动的TCP应用。 智能隧道使Microsoft Windows用户无需管理员权限就能访问TCP应用，并使VPN管理员能保证只有授权应用能访问内部资源。

表3. Cisco ASA 5500系列产品基于Web的免客户端接入（续）

特性	说明
广泛的浏览器支持	支持多种浏览器，包括Microsoft Internet Explorer、Firefox、Opera、Safari和PIE，有助于确保任意地点的广泛连接兼容性。
高级IP网络连接	可访问内部IPv4和IPv6网络资源。

全面的身份认证和授权选项

Cisco ASA 5500系列提供了全面的用户身份认证和授权选项，如表4所示。

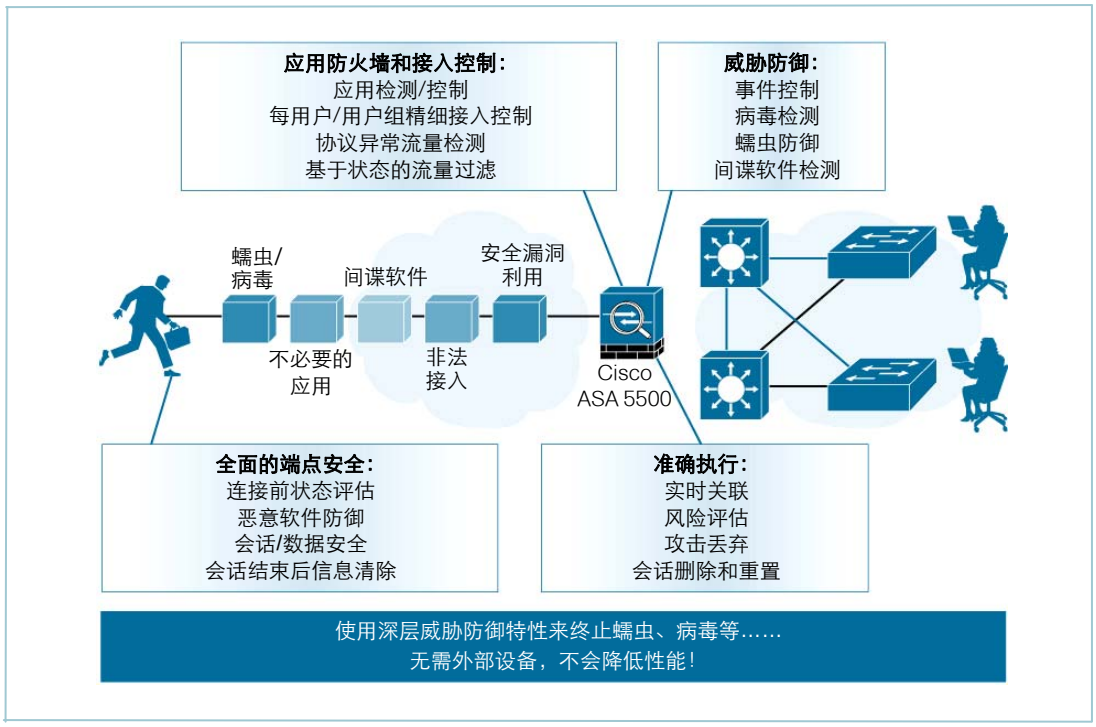
表4. Cisco ASA 5500系列身份认证和授权选项

特性	说明
身份认证选项	• RADIUS • RADIUS，带针对NT局域网管理器(NTLM)的密码过期功能(MSCHAPv2) • RADIUS一次性密码(OTP)支持（状态/回复消息属性） • RSA SecurID • 双重身份认证 • Active Directory/Kerberos • CA • 数字证书/智能卡（包括AnyConnect机器证书） • LDAP，带密码过期和老化功能 • 通用LDAP支持 • 证书和用户名/密码多因素综合身份认证 • 内部域密码提示，实现简单的单次登录(SSO) • SSL VPN虚拟键盘验证，为防御击键记录器提供额外保护
先进的授权	• RADIUS和LDAP策略映射 • 动态接入策略直接利用域成员和状态来创建用户策略
针对免客户端SSL VPN用户的单次登录 (SSO)	• Computer Associates Siteminder • RSA Access Manager (ClearTrust) • SAML • 基本/NTLM身份认证直通 • 基于表单的身份认证直通

威胁防御VPN特性

Cisco ASA 5500系列安全远程接入解决方案通过集成网络和端点安全技术，为VPN部署提供了先进安全性。确保VPN的安全对于防御蠕虫、病毒、间谍软件、键盘记录器、特洛伊木马、rootkit或黑客入侵等网络攻击有着重要意义。详细的应用和接入控制策略有助于确保单个用户和群组用户仅能访问他们有权访问的应用和网络服务（参见图2）。

图2. 威胁防御VPN服务使用板载安全特性来防御VPN威胁



VPN网关的网络安全特性

蠕虫、病毒、应用内嵌攻击和应用滥用是当今网络面临的最大安全挑战。远程接入和远程办公室VPN连接是此类威胁的常见攻击切入点，这主要是因为VPN设备的安全功能有限。VPN在部署时通常不像总部隧道端接点那样提供适当的威胁检测和防御功能，这使得来自远程办公室或用户的恶意软件会入侵网络并进行传播。借助Cisco ASA 5500系列产品的融合威胁防御功能，客户能在恶意软件进入网络内部前检测到它们并终止其运行。对于应用内嵌攻击，例如通过文件共享对等网络传播的间谍软件或广告软件等，Cisco ASA 5500系列产品能深入检测应用流量，以便在危险负载到达其目标并造成损害前发现它们并阻止其内容。表5列出了Cisco ASA 5500系列产品提供了部分VPN网关安全特性。

表5. VPN网关的网络安全特性

特性	说明
广泛恶意软件防御	Cisco ASA 5500系列VPN网关能阻止蠕虫、病毒、键盘记录器、特洛伊木马和rootkit通过，从而可在其进行网络传播前消除威胁。
应用感知型防火墙和接入控制	应用感知型流量检测支持全面用户接入控制，有助于防止滥用不必要的应用，如VPN连接上的对等文件共享等。
入侵防御	Cisco ASA 5500系列产品能预防大量网络安全漏洞利用事件。
接入限制	根据灵活的配置策略和当前状态，允许或拒绝对保密资源的访问。
虚拟局域网(VLAN) 映射	根据所配置的VLAN，实施基于用户或用户群组的流量访问限制。

面向SSL VPN的全面端点安全性

SSL VPN部署支持来自安全端点和企业管理范围以外端点的通用访问，并能将网络资源提供给不同用户社区使用。在此网络扩展情况下，潜在网络安全攻击点也相应增加。无论用户是通过公司管理的PC、个

人网络接入设备还是公共终端接入网络，Cisco Secure Desktop都能最大限度地消除SSL VPN会话终止后留下的cookie、浏览器历史记录、临时文件和下载的内容等数据。通过集成Cisco NAC设备和Cisco NAC框架，Cisco Secure Desktop还为全面接入网络的用户提供了端点状态检查功能。表6列出了重要的Cisco Secure Desktop特性。

表6. Cisco Secure Desktop可确保从网络到端点的全面信息安全

特性	说明
连接前状态评估	主机完整性认证检查首先检测在端点系统上是否存在防病毒软件、个人防火墙软件以及Windows服务包，再授权接入网络。 通过此机制，现在已经建立了一个庞大的应用和版本列表。该列表定期更新，以支持新产品版本。 管理员还能选择根据运行的流程，设置定制状态检查。
连接前资产评估	Cisco Secure Desktop能检测出远程系统上的水印。水印能用于识别资产是否为公司所有，并藉此提供不同的接入权限。水印检查功能包括系统注册表值、与所需CRC32检查和匹配的文件、IP地址范围匹配，以及颁发/匹配的证书等。
全面的会话保护	Cisco Secure Desktop为所有与会话相关的数据，包括密码、文件下载、历史记录、cookie和高速缓存文件等提供额外保护。会话数据将被加密，并在Cisco Secure Desktop安全库中存储。
会话终止后数据清除	在会话终止后，安全库中的数据将被覆盖。
击键记录器检测	Cisco Secure Desktop在会话开始时进行初始检查，查看是否存在某些基于软件的击键记录软件。如果在会话启动后，一个异常程序开始在安全库中运行，就会提示用户终止此可疑活动。
支持访客权限	从远程机器接入网络的用户可能不具备所有系统的管理员权限。Cisco Secure Desktop通常可在仅有访客权限的情况下安装，从而确保能够在所有系统上交付和安装。
高级端点评估许可	Cisco Secure Desktop提供一个先进的端点评估选项，能够自动执行流程来修复不符合安全策略的应用。

网络感知型站点间VPN特性

通过使用Cisco ASA 5500系列SSL/IPsec VPN版本所提供的网络感知型IPsec站点间VPN功能，企业能安全地通过低成本互联网连接将网络扩展到业务合作伙伴和全球远程及卫星办事处（参见表7）。

表7. Cisco ASA 5500系列SSL/IPsec VPN版本站点间VPN连接

特性	说明
支持QoS	支持延迟敏感型应用，如语音、视频和终端服务。
网络感知路由	隧道邻接点间支持开放最短路径优先(OSPF)协议，能够感知网络拓扑结构，从而简化网络集成。

通过平台集成实现VPN经济高效性

Cisco ASA 5500系列产品集成了大量功能，如安全和负载均衡等，能减少扩展和保护VPN所需的设备数目，从而降低设备成本、架构复杂度和运营成本（参见表8）。

表8. 有效补充VPN部署的集成功能

特性	说明
网络和端点安全	板载恶意软件防御、IPS和防火墙功能可提高VPN安全性，并减少所需部署的设备数量。
负载均衡	集成负载均衡特性支持多机箱集群，无需昂贵的负载均衡设备。

Cisco ASA 5500系列平台概述

Cisco ASA 5500系列平台通过以下七个型号，提供了从小型办公室到企业总部的站点特定可扩展性，其中包括：5505、5510、5520、5540、5550、5580-20和5580-40（参见图3）。型号5510到5550共享一个通用机箱，内置了支持并发服务可扩展性、投资保护和未来技术可扩展性的平台。表9列出了Cisco ASA 5500系列各型号的规格。

图3. Cisco ASA 5500系列产品系列

表9. Cisco ASA 5500系列自适应安全设备各型号的规格

平台	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
最大VPN吞吐率	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps
最大并发SSL VPN会话数量[1]	25	250	750	2500	5000	10,000	10,000
最大并发IPsec VPN会话数量[1]	25	250	750	5000	5000	10,000	10,000
接口	8个10/100铜线以太网端口，带动态端口分组功能。包括2个以太网供电(PoE)端口，3个USB端口	3个10/100/1000铜线以太网端口，1个带外管理端口，2个USB端口	4个10/100/1000铜线以太网端口，1个带外管理端口，2个USB端口	4个10/100/1000铜线以太网端口，1个带外管理端口，2个USB端口	8个千兆以太网端口，4个小封装可热插拔(SFP)光纤端口，1个快速以太网端口	2个USB端口，2个RJ-45管理端口，2个千兆以太网管理端口 配备接口扩展卡： ● 多达12个万兆以太网(10GE)端口 ● 多达24个千兆以太网端口 ● 多达24个10/100/1000以太网端口	2个USB端口，2个RJ-45管理端口，2个千兆以太网管理端口 配备接口扩展卡： ● 多达12个10GE端口 ● 多达24个千兆以太网端口 ● 多达24个10/100/1000以太网端口

表9. Cisco ASA 5500系列自适应安全设备各型号的规格（续）

平台	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
外形	台式	1-RU	1-RU	1-RU	1-RU	4-RU	4-RU
状态故障切换	不支持	许可特性[2]	支持	支持	支持	支持	支持
VPN 负载均衡	不支持	许可特性[2]	支持	支持	支持	支持	支持
共享 VPN 许可选项	不支持	支持	支持	支持	支持	支持	支持

思科服务

思科及其合作伙伴提供了多项服务来帮助您部署和管理安全解决方案。思科采用了生命周期服务方法，能够满足您部署和运行思科自适应安全设备和其他思科安全技术的所有需要。这一方法能帮助您优化网络安全状态，提高网络的可用性和可靠性，为支持新应用做好准备，同时降低您的网络成本，并在日常运行中保持网络健康状态。如需了解更多有关思科安全服务的信息，请访问：http://www.cisco.com/go/services/security。

了解更多信息

- Cisco ASA 5500系列产品：http://www.cisco.com/go/asa
- 思科安全远程接入解决方案：VPN许可概述文件**[[编辑注释：这是新文件，请提供链接]]。**
- Cisco AnyConnect VPN客户端：**[[编辑注释：这是新文件，请提供链接]]。**
- 思科自适应安全设备管理器：http://www.cisco.com/go/asdm
- 思科产品证书：http://www.cisco.com/go/securitycert
- 思科安全服务：http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

[1] 设备包括一个支持两名SSL VPN用户的许可，用于评估和远程管理用途。并发IPsec和SSL（免客户端和基于隧道）VPN会话总数不能超过表中所示的并发IPsec会话总数。SSL VPN会话数也不能超过设备上许可的会话数量。ASA 5580支持的同步用户数多于ASA 5550，而总SSL VPN吞吐率与ASA 5550相当。在您进行容量规划时，应该考虑这些因素。

[2] Cisco ASA 5510 Security Plus许可支持此升级。

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