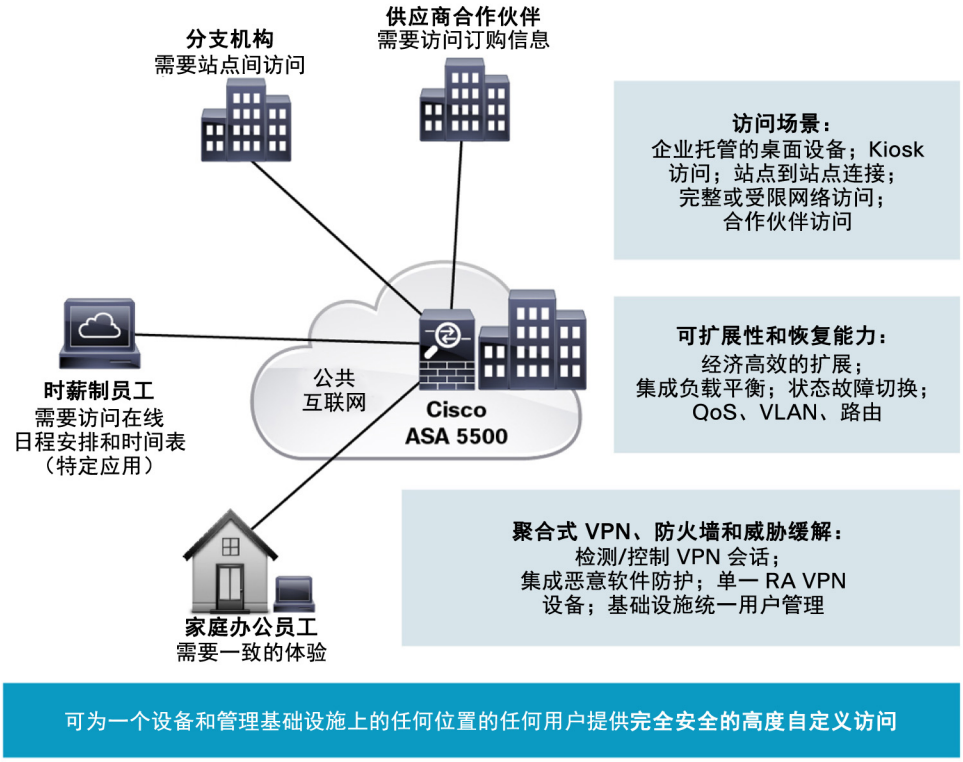
Cisco AnyConnect 安全移动解决方案：Cisco AnyConnect 安全移动客户端和 Cisco ASA 5500 系列（SSL/IPsec VPN 版）

Cisco® ASA 5500 系列自适应安全设备 (ASA) 是专为中小企业 (SMB) 和企业应用设计的平台，结合了一流的安全性和 VPN 服务。Cisco ASA 5500 系列有助于实现面向特定部署环境和选项的定制化，为远程访问 (SSL/IPsec VPN)、站点到站点 VPN、防火墙、内容安全和入侵防御提供专门的产品版本。

Cisco AnyConnect 安全移动解决方案为组织带来互联网传输的连通性和成本优势，同时不影响组织安全策略的完整性。通过将安全套接字层 (SSL) 和 IP 安全 (IPsec) VPN 服务与全面的威胁防御技术相结合，Cisco ASA 5500 系列可提供高度可定制的网络访问，满足各种部署环境的要求，同时提供高级终端和网络层面的安全性（图 1）。

图 1. 适合任意部署方案的可定制 VPN 服务



Cisco ASA 5500 系列 SSL/IPsec VPN 版

该版本可针对任何连接场景提供灵活的 VPN 技术，并可将每台设备的并发用户数量扩展至最多 10,000 位。它通过以下各项实现易于管理、全隧道式的网络访问：

- SSL（DTLS 和 TLS）
- IPsec VPN 客户端技术
- Cisco AnyConnect 安全移动解决方案针对思科网络安全进行了优化
- 高级无客户端 SSL VPN 功能
- 网络感知站点到站点 VPN 连接

这为移动用户、远程站点、承包商和业务合作伙伴提供了高度安全的公共网络连接。无需辅助设备即可轻松扩展 VPN 和保证其安全，从而降低 VPN 部署和运营相关的成本。

Cisco AnyConnect 安全移动解决方案的优势包括：

- **SSL（TLS 和 DTLS）和基于 IPsec 的全网络访问：**全网络访问可以为几乎所有的应用或网络资源提供网络层远程用户连接，而且通常用于将访问扩展至受管计算机，如属于公司的笔记本电脑。可以通过自动下载的 Cisco AnyConnect 安全移动客户端、Microsoft 第二层隧道协议 (L2TP)/IPsec VPN 客户端和 Apple iPhone/Mac OS X 10.6+IPsec VPN 客户端获得连接。

  Cisco AnyConnect 安全移动客户端将根据网络限制，自动将其隧道协议调整为最有效的方法，并且该客户端是第一个使用 DTLS 协议的 VPN 产品，可为延迟敏感型流量（如 IP 语音 [VoIP] 流量或基于 TCP 的应用访问）提供优化的连接。Cisco ASA 5500 系列支持 SSL（TLS 和 DTLS）和基于 IPsec 的远程访问 VPN 技术，具有卓越的灵活性，可满足大多数部署方案的需求。
- **高品质的无客户端网络访问：**通过互联网浏览器中普遍使用的 SSL 加密，AnyConnect 安全移动解决方案可实现无客户端远程访问。这可实现对网络应用和资源不受地点限制的访问，且无需桌面 VPN 客户端软件。

  该解决方案针对任何基于网络的应用或资源、诸如 Citrix 等终端服务应用以及优化的 Microsoft Outlook Web Access 和 Lotus iNotes 等提供无客户端访问。同时针对诸如邮件、日历、即时通信、FTP、Telnet 和 SSH 应用等常用胖客户端应用提供访问。此外，Cisco ASA 5500 系列的高级内容重写功能有助于确保可靠渲染含有 Java、JavaScript、ActiveX、Flash 和其他复杂内容的复杂网页。
- **Cisco AnyConnect 安全移动解决方案：**在每次交易中强制实施安全策略，无论用户身在何处、无论所用的是企业、“内部”应用还是软件即服务 (SaaS) 应用。安全移动功能让管理员可以通过安全策略要求客户端始终开启 VPN 安全网络连接，以便在 VPN 网络无法连接时允许或拒绝网络连接。这些服务经过优化用于思科网络安全，并要求 AnyConnect Premium 许可证或安全移动许可证。
- **网络感知型站点到站点 VPN：**在多个办公地点之间实现高度安全的高速通信。支持服务质量 (QoS) 和跨 VPN 路由，有助于确保以商业质量可靠地提供延迟敏感型应用，如音频、视频和终端服务等。
- **威胁保护型远程访问 VPN：**VPN 是恶意软件入侵网络的主要来源。恶意软件包括蠕虫、病毒、间谍软件、按键记录器、特洛伊木马和 rootkit。在 Cisco ASA 5500 系列中，入侵预防、抗病毒、应用感知型防火墙和 VPN 终端安全功能的深度和广度最大限度地降低了 VPN 连接将成为安全威胁通道的风险。
- **具成本效益的 VPN 部署和运营：**通常情况下，扩展和保护 VPN 需要额外的负载平衡和安全设备，这将增加设备和运营成本。Cisco ASA 5500 系列集成了这些功能，从而在当今现有的 VPN 产品中提供了前所未有的网络和安全集成水平，为您节省成本。Cisco ASA 5500 系列支持单一平台上的灵活隧道选项，可为客户提供具有成本效益的选择来部署并行 VPN 基础设施。
- **可扩展性和恢复能力 -** Cisco ASA 5500 系列每台设备可支持多达 10,000 个并发用户会话，通过集成的集群和负载平衡功能可以扩展至成千上万个并发用户会话。状态故障切换功能可提供畅通性高的服务，从而确保无与伦比的正常运行时间。
- **OpenSSL 技术 -** Cisco AnyConnect 安全移动客户端包括由 OpenSSL Project 开发用于 OpenSSL 工具包的软件 (http://www.openssl.org)。

可定制的远程访问 VPN 功能

全网络访问

通过 Cisco AnyConnect 安全移动客户端（如表 1 所示）或 Cisco IPsec VPN 客户端所提供的网络隧道功能，Cisco ASA 5500 系列 SSL/IPsec VPN 版可提供广泛的应用和网络资源访问。

表 1. Cisco AnyConnect 安全移动客户端功能

功能	优势
广泛的操作系统支持	• Windows 7 32 位 (x86) 和 64 位 (x64) • Windows Vista 32 位 (x86) 和 64 位 (x64)，包括 Service Pack 1 和 2 (SP1/SP2) • XP SP2+ 32 位 (x86) 和 64 位 (x64) • Mac OS X 10.6 和更高版本 • Linux Intel
软件访问	• 在 Cisco.com 提供，主要针对在其自适应安全设备 (ASA) 上具有有效 SMARTnet 合约的客户
优化网络访问 - VPN 协议选择 SSL（TLS 和 DTLS），及 IPsec/IKEv2	• AnyConnect 目前提供多种 VPN 协议，管理员可选择使用最符合其业务需求的协议 • 隧道支持包括 SSL（传输层安全 [TLS] 和数据报传输层安全 [DTLS]）及下一代 IPsec (IKEv2) • 使用 DTLS 可为延迟敏感型流量（如 VoIP 流量或基于 TCP 的应用访问）提供优化连接 • TLS (HTTP over TLS/SSL) 可通过锁定环境（包括使用 Web 代理服务器的环境）确保网络连接的可用性 • IPsec/IKEv2 可在安全策略要求使用 IPsec 的情况下，为延迟敏感型流量提供优化连接
最佳网关选择	• 确定并建立与最佳网络访问点的连接，因此，最终用户无需确定最近的访问位置
便于移动	• 针对移动用户而设计 • 可进行配置，以便在 IP 地址变更、失去连接、休眠或待机状态下，VPN 连接仍保持连接状态 • 值得信赖的网络检测可使 VPN 连接在最终用户处于办公室时自动断开，在用户位于远程位置时自动连接
加密	• 支持强加密，包括 AES-256 和 3DES-168（安全网关设备必须启用强加密许可证）。 • 下一代加密，包括 NSA Suite B 算法、采用 IKEv2 的 ESPv3、4096 位的 RSA 密钥、Diffie-Hellman 第 24 组、增强型 SHA2（SHA-256 和 SHA-384）（仅用于 IPsec IKEv2 连接；需要 Premium ASA 许可证）
多种部署和连接选项	部署选项： • 预部署，包括 Microsoft Installer • 使用 ActiveX（仅限 Windows）和 Java 的自动安全网关部署（初始安装需要管理权限） 连接模式： • 使用系统图标的独立连接 • 浏览器启动 (Weblaunch) • 无客户端门户启动 • 命令行界面 (CLI) 启动 • 应用编程接口 (API) 启动
广泛的身份验证选项	• RADIUS • 具有 Password Expiry (MSCHAPv2) 至 NT LAN Manager (NTLM) 的 RADIUS • RADIUS 一次性密码 (OTP) 支持（状态/回复消息属性） • RSA SecurID（包括 SoftID 集成） • 活动目录/Kerberos • 嵌入式证书授权 (CA) • 自动或用户选择的数字证书/智能卡（包括计算机证书支持） • 带有密码期限和时效的轻量级目录访问协议 (LDAP) • 一般 LDAP 支持 • 结合证书和用户名/密码的多因素身份验证（双重身份验证）
一致的用户体验	• 全隧道客户端模式支持需要一致的类似 LAN 用户体验的远程访问用户 • 多种交付方法有助于确保 Cisco AnyConnect 的广泛兼容性 • 用户可以延迟安装推送的 AnyConnect 更新 • 客户体验反馈选项
集中化策略控制和管理	• 策略可以进行预配置或进行本地配置，并可从 VPN 安全网关自动进行更新 • AnyConnect 的应用编程界面 (API) 可用于通过网页或应用轻松进行部署。 • 不受信证书检查和用户警告 • 可从本地查看和管理证书

功能	优势
高级 IP 网络连接	• 进/出 IPv4 和 IPv6 网络的公共连接 • 通过 SSL 访问内部 IPv4 和 IPv6 网络资源（IPv6 内部访问需要 TLS/DTLS） • 管理员控制的分离/全隧道网络访问策略 • 访问控制策略 IP 地址分配机制： • 静态 • 内部池 • 动态主机配置协议 (DHCP) • RADIUS/LDAP
预连接状况评估（需要 Premium 许可证）	• 结合思科安全桌面，Host Scan 验证检查在允许进行网络访问之前，会检测终端系统中是否有防病毒软件、个人防火墙软件和 Windows 服务包 • 管理员还可以根据是否存在运行的流程来定义自定义状况检查 • 思科安全桌面可检测远程系统上是否存在水印，水印可用于识别属企业所有的资产并提供差异化访问；水印检测功能包括： ◦ 系统注册表项值 ◦ 已存在的文件数与所需的 CRC32 校验和相匹配 ◦ IP 地址范围匹配 ◦ 发布自/至的证书匹配 • 高级终端评估选项可以用于自动修复不合规应用
客户端防火墙策略	• 增加了对分离隧道配置的保护 • 与思科安全移动结合使用，允许存在本地访问例外（例如，打印、系留设备支持等） • 支持 IPv4 的基于端口规则以及 IPv6 的网络/IP 访问控制列表 (ACL) • 可供 Windows XP SP2、Vista、Windows 7 和 Mac OS X 使用
本地化	除英语外，还提供以下语言的翻译版本： • 捷克语 (cs-cz) • 德语 (de-de) • 拉丁美洲西班牙语 (es-co) • 加拿大法语 (fr-ca) • 日语 (ja-jp) • 韩语 (ko-kr) • 波兰语 (pl-pl) • 简体中文 (zh-cn)
轻松的客户端管理	• 管理员可以通过前端安全设备自动发布软件和策略更新，从而消除与客户端软件更新有关的管理工作 • 管理员可以确定提供哪些功能用于最终用户配置 • 当域登录脚本无法使用时，管理员可以在连接/断开时触发终端脚本 • 管理员可以完全定制和本地化最终用户的可视消息
AnyConnect 配置文件编辑器	• AnyConnect 策略可以从思科自适应安全设备管理器 (ASDM) 直接定制
诊断	• 设备上的统计数据和登录信息 • 查看设备上的日志 • 可轻松将日志通过邮件发送至思科或管理员进行分析
联邦信息处理标准 (FIPS)	• FIPS 140-2 Level 2 兼容（平台、功能和版本限制适用）
轻松的客户端管理	• Cisco AnyConnect 安全移动客户端允许管理员从安全网关自动分配软件和策略更新，从而消除与客户端软件更新相关的管理 • 管理员可以确定提供哪些功能用于最终用户配置 • 当域登录脚本无法使用时，管理员可以在连接/断开时触发终端脚本 • 管理员可以完全定制和/或本地化最终用户的可视消息
一致的用户体验	• 全隧道客户端模式支持需要一致的类似 LAN 用户体验的远程访问用户 • 多种交付方法和小的下载大小有助于确保 Cisco AnyConnect 安全移动客户端的广泛兼容性和快速下载

功能	优势
高级 IP 网络连接	• 至/自 IPv4 和 IPv6 网络的公共连接 • 通过 SSL 访问内部 IPv4 和 IPv6 网络资源（v6 内部访问需要 TLS/DTLS） • 管理员控制的分离/全隧道网络访问策略 • 访问控制策略 IP 地址分配机制： • 静态 • 内部池 • 动态主机配置协议 (DHCP) • RADIUS/轻量级目录访问协议 (LDAP)
客户端防火墙策略	• 增加了对分离隧道配置的保护。 • 与思科移动用户安全结合使用，允许存在本地访问例外（例如，打印、系留设备支持等） • 支持 IPv4 的基于端口规则以及 IPv6 的网络/IP 访问控制列表 (ACL) • 可供 Windows XP SP2、Vista、Windows 7 和 Mac OS X 使用
Cisco AnyConnect 配置文件编辑器	• AnyConnect 策略可以从思科自适应安全设备管理器 (ASDM) 直接定制

表 2 总结了 Cisco AnyConnect 许可选项。

表 2. Cisco AnyConnect 许可选项

许可证要求 （要求以下每个许可证）	说明
Cisco ASA 平台许可证	**Cisco AnyConnect Essentials**[1] P/N：(L-ASA-AC-E-55**=) 05、10、20、40、50、80、85 • 高安全性远程访问连接 • 每个 ASA 设备型号一个许可证（而不是每个用户一个许可证）；平台上允许最大并发用户数 • 全隧道访问企业级应用
	Cisco AnyConnect Premium[2] P/N：(L-ASA-SSL-***=) 10、25、50、100、250、500、1000、2500、5000、10000 • 还提供对无客户端 SSL VPN 以及桌面 Cisco AnyConnect 平台上的功能的支持，包括思科安全桌面 HostScan 和 Always-On VPN 连接 • 许可证基于并发用户的数量，并且可作为单一设备许可证或共享许可证提供
Cisco AnyConnect 移动证书[5] P/N：(L-ASA-AC-M-55*=) 05、10、20、40、50、80、85	• 确保 Mobile OS 平台兼容性 • 每个 ASA 设备型号需要一个许可证（除 Essentials 或 Premium 许可证以外），而非每个用户都要有一个许可证

无客户端网络访问

Cisco ASA 5500 系列无客户端 SSL VPN 访问（功能如表 3 所示）可对特定网络资源和应用进行基于 Web 的精确控制的访问。这些网络资源和应用可通过互联网服务亭、共享电脑、外网合作伙伴、员工所有的桌面设备、企业所有的员工桌面设备进行访问。

表 3. Cisco ASA 5500 系列基于 Web 的无客户端访问

功能	说明
广泛可靠的兼容性	高级转换功能有助于确保与包含复杂内容（包括 HTML、Java、ActiveX、JavaScript 和 Flash）的网页的兼容性。
集成的无客户端应用优化	资源密集型应用程序（如 Microsoft Outlook Web Access 和 Lotus iNotes）的集成性能优化可以提供良好的响应时间和低延迟，从而提供高质量的 SSL VPN 最终用户体验。
可定制的用户体验	增强型无客户端门户具有基于组的详细访问定制、易于使用且可定制的用户体验等特点： • 支持多语言、无客户端用户门户 • 用户可定制的资源书签 • 发布基于简易信息聚合 (RSS) 的信息资源，实现重要实时内容的自动更新
完全无客户端 Citrix 访问	无客户端 SSL VPN 上的 Citrix 访问无需外部辅助应用，这有助于确保实现快速应用启动时间和降低桌面软件冲突

[1] ** 会替换为相应 ASA 型号的最后两个数字。
[2] *** 会替换为许可证总席位数。

功能	说明
	风险。
集成的客户端服务器应用支持	提供对普通客户端服务器应用的访问，无需预部署的远程客户端，从而授权对 Telnet、SSH、远程桌面协议 (RDP) 和虚拟网络计算 (VNC) 资源的访问。
支持普通胖客户端应用	端口转发可通过以下 Java 小工具，支持对流行的胖客户端应用进行无客户端访问： • 邮局协议 (POP) • 简单邮件传输协议 (SMTP) • 互联网消息访问协议 (IMAP) • 邮件 • 在线日历 • 即时通信 • Telnet • SSH • 其他启用客户端的 TCP 应用 通过智能隧道，Microsoft Windows 用户无需管理权限即可访问 TCP 应用，VPN 管理员可以只授权经过批准的应用访问内部资源。
广泛的浏览器支持	多个浏览器支持（包括 Microsoft Internet Explorer、Firefox、Opera、Safari 和 Pocket Internet Explorer [PIE]）有助于确保从任何位置进行广泛连接的兼容性。
高级 IP 网络连接	访问内部 IPv4 和 IPv6 网络资源。

全面的身份验证和授权选择

Cisco ASA 5500 系列提供全面的一组选项，用于用户身份验证和授权，如表 4 所示。

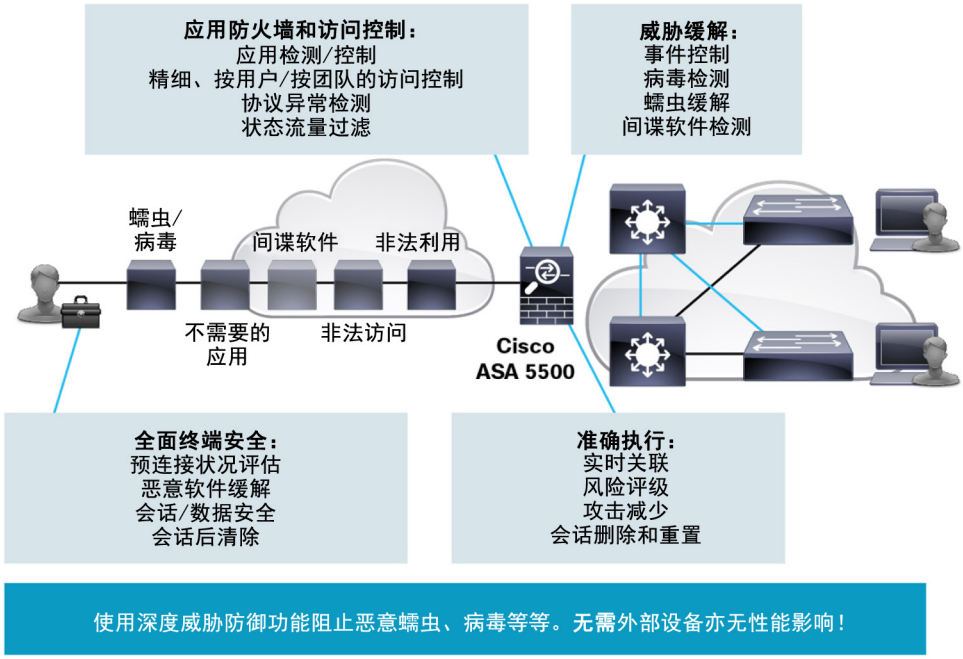
表 4. Cisco ASA 5500 系列身份验证和授权选项

功能	说明
身份验证选项	• RADIUS • 具有 Password Expiry (MSCHAPv2) 至 NT LAN Manager (NTLM) 的 RADIUS • RADIUS 一次性密码 (OTP) 支持（状态/回复消息属性） • RSA SecurID • 双重身份验证 • 活动目录/Kerberos • 嵌入式证书授权 (CA) • 数字证书/智能卡（包括 Cisco AnyConnect 的计算机证书） • 具有密码期限和时效的 LDAP • 一般 LDAP 支持 • 结合的证书和用户名/密码多因素身份验证 • 简化单点登录 (SSO) 的内部域密码提示 • SSL VPN 虚拟键盘身份验证，用于额外防范按键记录器。
复杂的授权	• 从 RADIUS 和 LDAP 的映射策略 • 动态访问策略直接使用域成员身份和状况状态创建用户策略
适用于无客户端 SSL VPN 用户的单点登录 (SSO)	• Computer Associates Siteminder • RSA Access Manager (ClearTrust) • 安全断言标记语言 (SAML) • Basic/NTLM 身份验证传递 • 基于表单的身份验证传递

威胁防护 VPN 功能

Cisco ASA 5500 系列 SSL/IPsec VPN 版通过其集成网络和终端安全技术为 VPN 部署提供高级安全性。必须确保 VPN 安全，防止网络攻击，例如蠕虫、病毒、间谍软件、按键记录器、特洛伊木马、rootkit 或黑客攻击。详细的应用和访问控制策略有助于确保个人用户和用户组仅能访问他们授权的应用和网络服务（图 2）。

图 2. 威胁防护 VPN 服务使用 Onboard Security 防范 VPN 威胁



VPN 网关的网络安全

蠕虫、病毒、应用嵌入攻击和应用滥用是当今网络面临的几个最大的安全问题。由于 VPN 设备上的安全功能有限，远程访问和远程办公 VPN 连接是此类威胁的一般进入点。部署 VPN 时，通常没有进行妥善检查，而且没有缓解位于总部位置的隧道终端点的威胁，这使来自远程办公室或用户的恶意软件可以潜入网络并传播。

凭借 Cisco ASA 5500 系列融入的威胁缓解功能，客户可以在恶意软件进入网络内部之前检测并阻止该恶意软件。针对应用嵌入攻击，如通过文件共享在 P2P 网络中传播的间谍软件或广告软件，Cisco ASA 5500 系列可深度检查应用流量。该解决方案可识别危险的有效负载，并在其到达目标或造成损害之前将其删除。

表 5 列出了 Cisco ASA 5500 系列提供的一些 VPN 网关安全功能。

表 5. Cisco ASA 5500 系列 VPN 网关的网络安全

功能	说明
大范围恶意软件防护	Cisco ASA 5500 系列 VPN 网关阻止了蠕虫、病毒、间谍软件、按键记录器、特洛伊木马和 rootkit，因此在这类恶意软件在网络中传播之前消除了威胁。
应用感知型防火墙和访问控制	应用感知型流量检查启用全面的用户访问控制，并有助于防止对不需要应用的滥用，例如跨 VPN 连接的 P2P 文件共享。
入侵防御	Cisco ASA 5500 系列抵御大量的网络漏洞。
访问限制	允许或拒绝访问机密资源取决于灵活的配置策略和当前的状况状态。
虚拟 LAN (VLAN) 映射	基于用户和基于组的流量访问限制的实施取决于配置的 VLAN。

SSL VPN 的全面终端安全

SSL VPN 部署支持从高安全性终端和非企业受管终端进行的一般访问，并能够将网络资源扩展到不同的用户社区。用户可以从企业受管 PC 、可访问网络的个人设备、公共终端或其他设备访问网络。扩展网络时，潜在的网络安全攻击点也会增加。

思科安全桌面可最大程度减少诸如 Cookie、浏览器历史记录、临时文件和在 SSL VPN 会话终止后遗留的已下载内容等相关数据。由于集成了 Cisco NAC Appliance 和 Cisco NAC Framework，还能检查全部网络访问用户的终端状况。表 6 突出了 Cisco 安全桌面的功能。（需要 Premium 许可证）。

表 6. Cisco 安全桌面全面保障了从网络到终端的信息的安全

功能	说明
预连接状况评估	主机完整性验证检查在允许网络访问之前，设法检测终端系统中是否存在防病毒软件、个人防火墙软件和 Windows 服务包。 通过该机制极大扩展了当前支持的应用及版本数量；经常提供更新，支持新产品发布。 管理员还可以选择根据是否存在运行的流程来定义自定义状况检查。
预连接资产评估	思科安全桌面可检测远程系统上是否存在水印，水印可用于识别属企业所有的资产并提供差异化访问；水印检查功能包括： • 系统注册表项值 • 已存在的文件数与所需的 CRC32 校验和相匹配 • IP 地址范围匹配 • 发布自/至的证书匹配
全面的会话保护	为会话相关的所有数据提供额外保护，包括密码、文件下载、历史记录、Cookie 和缓存文件，同时将会话数据加密至思科安全桌面的安全库中。
会话结束数据清除	会话结束时会覆写安全库中的数据。
按键记录器检测	Cisco 安全桌面在会话开始时初步检查某些基于软件的按键记录软件。如果异常程序开始在安全库中运行，则会话开始后，会提示用户停止可疑活动。
提供来宾权限	从远程设备访问网络的用户可能没有所有系统的管理员权限，思科安全桌面通常可以仅以来宾权限安装。这有助于确保所有系统中的交付和安装。
高级终端评估许可证	高级终端评估选项可以用于自动修复不合规应用。

网络感知型站点间 VPN 功能

Cisco ASA 5500 系列 SSL/IPsec VPN 版使用网络感知型 IPsec 站点到站点 VPN 功能。企业可通过该功能将其网络从低成本的互联网连接安全地扩展至业务合作伙伴以及远程和全世界范围内的卫星办公室（表 7）。

表 7. Cisco ASA 5500 系列 SSL/IPsec VPN 版站点到站点 VPN 连接

功能	说明
支持 QoS	支持延迟敏感型应用，例如音频、视频和终端服务。
网络感知型路由	在整个隧道邻居上支持开放最短路径优先 (OSPF) 和边缘网关协议 (BGP)，帮助启用网络拓扑意识，从而轻松实现网络集成。

通过平台集成实现的 VPN 成本效益

Cisco ASA 5500 系列集成了众多功能（如安全性和负载平衡），这可以减少扩展和保护 VPN 所需的设备数量，从而降低设备成本、架构复杂性和运营成本（表 8）。

表 8. 补充 VPN 部署的集成功能

功能	说明
网络和终端安全	机载恶意软件减少、IPS 和防火墙功能增加了 VPN 安全性，同时也降低了需要部署的设备数量。
负载平衡	集成的负载平衡功能支持多机箱集群，而不需要昂贵的外部负载平衡设备。

Cisco ASA 5500 系列平台概述

Cisco ASA 5500 系列可交付从小型办公室到企业总部的特定站点的可扩展性。该扩展性通过其以下型号进行交付：5505、5512-X、5515-X、5525-X、5545-X、5555-X、5585-10、5585-20、5585-40 和 5585-60（图 3）。型号 5512 到 5555 共享机箱，在并发服务可扩展性、投资保护和未来技术延展性这一基础上构建。

图 3. Cisco ASA 5500 系列组合

表 9 列出了 Cisco ASA 5500 系列型号的规格。

表 9. Cisco ASA 5500 系列 自适应安全设备型号的规格

平台	ASA 5505	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X	ASA 5585-S10	ASA 5585-S20	ASA 5585-S40	ASA 5585-S60
3DES/AES VPN 最大吞吐量 [1]	100 Mbps	200 Mbps	250 Mbps	300 Mbps	400 Mbps	700 Mbps	1 Gbps	2 Gbps	3 Gbps	5 Gbps
站点到站点和 IPsec IKEv1 客户端 VPN 用户会话数上限 [1]	25	250	250	750	2500	5000	5000	10,000	10,000	10,000
Cisco AnyConnect 或无客户端 VPN 用户会话数上限	25	250	250	750	2500	5000	5000	10,000	10,000	10,000
捆绑的 Premium 用户会话	2									
状态故障切换	否	是								
VPN 负载平衡	否	是								
Shared VPN 许可证选项	否	是								

	ASA 5505	ASA 5512-X	ASA 5515-X	ASA 5525-X	ASA 5545-X	ASA 5555-X	ASA 5585 (SSP-10/20)	ASA 5585 SSP-40/60
硬件								
CPU	单核	多核，企业级						
内存 (RAM)	512 MB	4 GB	8 GB		12 GB	16 GB	6/12 GB	12/24 GB
闪存	128 MB	4 GB	8 GB				2 GB	
集成网络 (GE) 端口数	8 个 10/100 交换机端口和 2 个 PoE 端口	6		8			8 个 10/100/1000 2 个 10 GE3 SFP+ (SSP-10/20) 16 个 10/100/1000 4 个 10GE3 SFP+ （SSP-10/20 或 IPS SSP-10/20）	6 个 10/100/1000 4 个 10GE SFP+ (SSP-40/60) 12 个 10/100/1000 8 个 10GE SFP+ （SSP-40/6 或 IPS SSP-40/60）
接口卡插槽数	1 个 SSC	1 个 SSM						
接口卡选项	N/A	6 端口 10/100/1000，6 端口 GE SFP SX、LH、LX						
冗余电源	否				是			
电源	外部，96W	400W			450W		370W	
物理规格								
外形规格	桌面	1 RU，19 英寸 机架安装型					2 RU，19 英寸 机架安装型	
机架安装选项	是的，包括机架安装或墙面安装套件	随附支架（可选滑轨）			随附滑轨		包括机架安装	

尺寸（长 x 宽 x 高）	1.75 x 7.89 x 6.87 英寸（4.45 x 20.04 x 17.45 厘米）	1.67 x 16.7 x 15.6 英寸（4.24 x 42.9 x 39.5 厘米）			1.67 x 16.7 x 19.1 英寸（4.24 x 42.9 x 48.4 厘米）	3.47 x 19 x 26.5 英寸（8.8 x 48.3 x 67.3 厘米）
重量	4.0 磅（1.8 千克）	13.39 磅（6.07 千克）	13.39 磅（6.07 千克）	14.92 磅（6.77 千克）	16.82 磅（7.63 千克），含单电源 18.86 磅（8.55 千克），含双电源	50 磅（22.7 千克），含单电源 62 磅（28.2 千克），含双电源

[1] 设备包括两个 SSL VPN 用户进行评估和远程管理所需的许可证。所有并发 IPsec 和 SSL（无客户端和基于隧道的）VPN 会话可能不会超过表中所示的最多并发 IPsec 会话计数。SSL VPN 会话数量可能还不会超过设备中许可会话的数量。在总 SSL VPN 吞吐量与 ASA 5550 相当的前提下，Cisco ASA 5580 支持的并发用户数量比 ASA 5550 多。作为容量规划的一部分，应考虑这些因素。

[2] 可通过 Cisco ASA 5512 Security Plus 许可证进行升级。

Shared VPN 许可证选项	否	有	有	有	有	有	有

平台兼容性

Cisco AnyConnect 安全移动客户端与所有的 Cisco ASA 5500 和 5500-X 系列自适应安全设备型号（运行 Cisco ASA 软件版本 8.0.3 和更高版本）和各种 Cisco IOS® 基于软件的路由器兼容。

有关兼容性的更多信息，请访问：http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html。

电子许可证交付

多数许可证可实现电子交付；可大大缩短许可证执行时间。要以电子形式订购许可证，请确保订购的部件号以“L”开头。如果您有关于许可的任何疑问或想评估许可证，

如果您已经有 Essentials ASA 或 Premium ASA 许可证，您可以使用 https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=717 上的自动许可证请求工具。

保修信息

您可以在“思科产品保修”页面上查找保修信息。

订购信息

要订购安全网关许可证，请访问“思科订购首页”。有关兼容平台和软件访问信息，请参见表 1。

开始连接时需要安全网关许可证。有关可用选项的其他信息，请参阅前面的“Cisco AnyConnect 许可选项”部分。有关使用 Cisco AnyConnect 实现连接的可用许可选项列表，请参阅 Cisco AnyConnect 安全移动客户端功能、许可证和操作系统网页。

致谢

此产品含有由 OpenSSL Project 开发的软件，可用于 OpenSSL Toolkit：(http://www.openssl.org/)。

此产品含有由 Eric Young (eay@cryptsoft.com) 编写的加密软件。

此产品含有由 Tim Hudson (tjh@cryptsoft.com) 编写的软件。

此产品包含 libcurl HTTP 库：版权所有 © 1996-2006，Daniel Stenberg (Daniel@haax.se)。

更多详情

Cisco AnyConnect 安全移动客户端首页：http://www.cisco.com/go/anyconnect

Cisco AnyConnect 文档：http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html

Cisco ASA 5500 系列自适应安全设备：http://www.cisco.com/go/asa

思科自适应安全设备管理器：http://www.cisco.com/go/asdm

Cisco ASA 5500 系列自适应安全设备许可信息：
http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html

AnyConnect 最终用户许可证协议和隐私政策：
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/eula-seula-privacy/AnyConnect_Supplemental_End_User_License_Agreement.htm

思科产品证书：http://www.cisco.com/go/securitycert

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

美国印刷 C78-529285-02 09/12