了解Cisco AnyConnect安全移动客户端

目标

本文重点介绍使用Cisco AnyConnect的功能、规格和优势。有关RV340系列路由器上AnyConnect许可的信息，请参阅RV340系列路由器的AnyConnect许可文章。

软件版本

4.2.03013(发行说明)

功能和规格

功能	优势和详细信息
远程访问 VPN	
广泛的操作系统支持	• Windows 10、8.1、8和7 • Mac OS X 10.8及更高版本 • Linux Intel(x64) •有关移动平台信息，请参阅AnyConnect Mobile产品手册。
优化网络访问：VPN协议选择SSL（TLS和DTLS）；IPsec IKEv2	• AnyConnect提供VPN协议选择，因此管理员可以使用最适合其业务需求的任何协议。 •隧道支持包括SSL（TLS 1.2和DTLS）和下一代IPsec IKEv2。 • DTLS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 1.2（HTTP over TLS或SSL）有助于通过锁定环境（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在安全策略需要使用IPsec时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接入点的连接，从而无需最终用户确定最近的位置。
移动友好	•专为移动用户设计 •可以进行配置，以便在IP地址更改、连接中断或休眠或待机期间保持VPN连接。 •通过受信任网络检测，当最终用户在办公室时，VPN连接可自动断开，当用户在远程位置时，VPN连接可自动断开。
加密	• AES-256和3DES-168。（安全网关设备必须启用强加密许可证。） • NSA Suite B算法、带IKEv2的ESPv3、4096位RSA密钥、Diffie-Hellman组24和增强型SHA2（SHA-256和SHA-384）。 仅适用于IPsec IKEv2连接。需要AnyConnect Apex许可证。
广泛的部署和连接选项	**部署选项：** •预部署，包括Microsoft Installer •由ActiveX（仅限Windows）和Java自动安全网关部署（初始安装需要管理权限） **连接模式：** •按系统独立图标 •浏览器启动（网络启动） •启动的无客户端门户 • CLI启动 •启动的API
多种身份验证选项	• RADIUS

	● RADIUS具有密码到期(MSCHAPv2)到NT LAN Manager(NTLM) ● RADIUS一次性密码(OTP)支持（状态和回复消息属性） ● RSA SecurID（包括SoftID集成） ● Active Directory或Kerberos ●嵌入式证书颁发机构(CA) ●数字证书或智能卡（包括机器证书支持），自动或用户选择 ●轻量级目录访问协议(LDAP)，带密码到期和过期 ●通用LDAP支持 ●组合证书和用户名 — 密码多重身份验证（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局域网的用户体验的远程访问用户。 ●多种交付方法有助于确保AnyConnect的广泛兼容性。 ●用户可以推迟推送的更新。 ●提供客户体验反馈选项。
集中策略控制和管理	●策略可以预先配置或在本地配置，并可以从VPN安全网关自动更新。 ● AnyConnect的API通过网页或应用简化部署。 ●检查不受信任的证书并发出用户警告。 ●可在本地查看和管理证书。
高级IP网络连接	● IPv4和IPv6网络之间的公共连接 ●访问内部IPv4和IPv6网络资源 ●管理员控制的分割隧道和全隧道网络访问策略 ●访问控制策略 ●针对Google Android(Lollipop)和Samsung KNOX（4.0版中新增）的每应用VPN策略；需要带OS 9.3或更高版本和AnyConnect 4.0许可证的Cisco ASA 5500-X) **IP地址分配机制：** ●静态 ●内部池 ●动态主机配置协议(DHCP) ● RADIUS/LDAP
强大的统一终端合规性 （需要Apex许可证）	●有线和无线环境支持终端状态评估和补救（取代思科身份服务引擎NAC代理）。 需要Identity Services Engine 1.3或更高版本，并具备Identity Services Engine Apex许可证。 ● Cisco Hostscan在授予网络访问权限之前尝试检测终端系统上是否存在防病毒软件、个人防火墙软件和Windows服务包。 ●管理员还可以选择根据运行进程的存在定义自定义状态检查。 ● HostScan检测远程系统上是否存在水印。水印可用于识别企业拥有的资产并因此提供差异化访问。水印检查功能包括系统注册表值、匹配所需CRC32校验和的文件存在、IP地址范围匹配以及由匹配的证书颁发机构颁发或颁发给匹配的证书颁发机构的证书。对于不合规的应用，还支持其他功能。 ●功能因操作系统而异。有关详细信息，请参阅主机扫描支持图表。
客户端防火墙策略	●为分割隧道配置提供额外保护。 ●与AnyConnect客户端配合使用，以允许本地访问异常（例如，打印、系留设备支持等）。 ●支持基于端口的IPv4规则和IPv6网络和IP访问控制列表(ACL)。 ●适用于Windows和Mac OS X平台。
本地化	**除英文外，还包括以下语言译文：** ●捷克语(cs-cz) ●德语(de-de) ●西班牙语(es-es) ●法语(fr-fr) ●日语(ja-jp)

	●韩语(ko-kr) ●波兰语(pl-pl) ●简体中文(zh-cn) ●中文（台湾）(zh-tw) ●荷兰语（荷兰） ●匈牙利语（胡胡） ●意大利语(it-it) ●葡萄牙语（巴西）(pt-br) ●俄语(ru-ru)
易于客户端管理	●管理员可以从头端安全设备自动分发软件和策略更新，从而消除与客户端软件更新相关的管理。 ●管理员可以确定哪些功能可用于最终用户配置。 ●管理员可以在无法使用域登录脚本的连接和断开时触发终端脚本。 ●管理员可以完全自定义和本地化最终用户可见消息。
配置文件编辑器	● AnyConnect策略可以直接从思科自适应安全设备管理器(ASDM)定制。
诊断	●提供设备内统计信息和日志记录信息。 ●可以在设备上查看日志。 ●日志可以轻松地通过电子邮件发送给思科或管理员进行分析。
联邦信息处理标准(FIPS)	●符合FIPS 140-2 2级（适用平台、功能和版本限制）
安全移动性和网络可视性	
Web安全集成 （需要云网络安全许可证）	●使用云网络安全(软件即服务(SaaS)Web安全的全球最大提供商)来防止恶意软件进入公司网络，并控制和保护员工Web使用。 ●支持云托管配置和动态加载。 ●通过支持基于云的服务以及基于本地的服务，为组织提供灵活性和选择。 ●与网络安全设备集成。 ●支持受信任网络检测。 ●在每个事务中实施安全策略，与用户位置无关。 ●要求始终在线且高度安全的网络连接，并制定策略以在访问不可用时允许或拒绝网络连接。 ●检测热点和强制网络门户。
网络可视性模块 （需要Apex许可证）	●通过监控应用使用情况来发现潜在的行为异常。 ●支持更明智的网络设计决策。 ●可以与越来越多支持互联网协议流信息导出(IPFIX)的网络分析工具共享使用数据。
面向终端的高级恶意软件防护(AMP)启用程序 （面向终端的AMP单独许可）	●通过分发和启用面向终端的思科AMP，简化对AnyConnect终端的威胁服务的实施。 ●将终端威胁服务扩展到远程终端，从而增加终端威胁覆盖。 ●提供更主动的保护，以进一步确保在远程终端快速缓解攻击。
广泛的操作系统支持	● Windows 10、8.1、8和7 ● Mac OS X 10.8及更高版本
网络接入管理器和802.1X	
媒体支持	●以太网(IEEE 802.3) ● Wi-Fi(IEEE 802.11a/b/g/n)
网络身份验证	● IEEE 802.1X-2001、802.1X-2004和802.1X-2010 ●使企业能够部署单个802.1X身份验证框架来访问有线和无线网络。 ●管理用户和设备身份以及高度安全访问所需的网络访问协议。 ●在连接到思科统一有线和无线网络时优化用户体验。
可扩展身份验证协议(EAP)方法	● EAP — 传输层安全(TLS) ●采用以下内部方法的EAP保护可扩展身份验证协议(PEAP): - EAP-TLS - EAP-MSCHAPv2 - EAP — 通用令牌卡(GTC) ●通过安全隧道(FAST)使用以下内部方法进行EAP灵活身份验证：

	- EAP-TLS - EAP-MSCHAPv2 - EAP-GTC ● EAP — 隧道TLS(TTLS)，采用以下内部方法： — 密码身份验证协议(PAP)。 — 质询握手身份验证协议(CHAP)。 - Microsoft CHAP(MSCHAP)。 - MSCHAPv2 - EAP-MD5 - EAP-MSCHAPv2 ●轻量EAP(LEAP)，仅Wi-Fi ● EAP-Message Digest 5(MD5)，已配置管理，仅以太网 ● EAP-MSCHAPv2，已配置管理，仅以太网 ● EAP-GTC，已配置管理，仅以太网
无线加密方法（需要相应的802.11网卡支持）	●打开 ●有线等效保密(WEP) ●动态WEP ● Wi-Fi保护访问(WPA)企业 ● WPA2企业 ● WPA个人(WPA-PSK) ● WPA2个人(WPA2-PSK) ● CCKM（需要思科CB21AG无线网卡）
无线加密协议	●使用高级加密标准(AES)算法的密码块链消息验证码协议(CCMP)计数器模式 ●使用Rivest Cipher 4(RC4)流密码的临时密钥完整性协议(TKIP)
会话恢复	●使用EAP-TLS、EAP-FAST、EAP-PEAP和EAP-TTLS恢复RFC2716(EAP-TLS)会话 ● EAP-FAST无状态会话恢复 ● PMK-ID缓存（主动密钥缓存或专案密钥缓存），仅Windows XP
以太网加密	●介质访问控制：IEEE 802.1AE(MACsec) ●主要管理：MACsec密钥协议(MKA) ●在有线以太网网络上定义安全基础设施，以提供数据机密性、数据完整性和数据来源的身份验证。 ●保护网络受信任组件之间的通信。
一次连接一个	●仅允许与网络的单个连接，断开所有其它连接。 ●适配器之间没有桥接。 ●以太网连接自动优先。
复杂的服务器验证	●支持“以”和“完全匹配”规则。 ●支持30多条规则，用于没有名称通用性的服务器。
EAP链(EAP-FASTv2)	●根据企业和非企业资产区分访问权限。 ●在单个EAP事务中验证用户和设备。
企业连接实施(ECE)	●帮助确保用户仅连接到正确的企业网络。 ●防止用户在办公室内连接到第三方接入点上网。 ●防止用户建立访客网络访问。 ●消除繁琐的黑名单。
下一代加密(Suite B)	●支持最新的加密标准。 ●椭圆曲线Diffie-Hellman密钥交换 ●椭圆曲线数字签名算法(ECDSA)证书
凭据类型	●交互式用户密码或Windows密码 ● RSA SecurID令牌 ●一次性密码(OTP)令牌 ●智能卡(Axalto、Gemplus、SafeNet iKey、Alladin)。 ● X.509证书。 ●椭圆曲线数字签名算法(ECDSA)证书。
远程桌面支持	●使用远程桌面协议(RDP)时，对本地网络的远程用户凭证进行身份验

	证。
支持的操作系统	• Windows 10、8.1、8和7