认识Cisco AnyConnect安全移动客户端

客观

逗留用Cisco AnyConnect®安全移动性客户端获取并且连接忙个不停。提供必要的安全帮助保证您的组织的数据是安全和保护。Cisco AnyConnect是提供多个安全服务保护企业的一个统一的代理程序。它提供公开性和您需要识别的控制谁，并且在和在攻击以后期间，在什么前访问延长的企业。AnyConnect®安全移动性客户端提供有远程访问功能、状态实施和Web安全功能的一个全面的端点安全平台。起代理程序作用对于传送的状态在配线间的一致，高度安全的终端访问，无线和虚拟专用网络(VPN)。

此条款着重使用Cisco的功能、规格和好处AnyConnect。

软件版本

4.2.03013

功能和规格

功能	好处和详细资料
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及以后 ● Linux Intel (x64) ●看到AnyConnect便携数据表或宣传单页对于便携平台信息。
最优化的网络访问：VPN协议选择SSL (TLS和DTL);IPsec IKEv2	● AnyConnect提供VPN协议选择，因此管理员能使用协议最好适合他们的商业需要。 ●隧道技术支持包括SSL (TLS 1.2和DTL)和下一代IPsec IKEv2。 ● DTL为潜伏期敏感的数据流提供被最优化的连接，例如VoIP流量或基于TCP的应用程序访问。 ● TLS 1.2 (在TLS或SSL的HTTP)使用Web代理服务器，帮助通过锁着的下来环境保证网络连通性的可用性，包括那些。 当安全策略要求使用IPsec时，● IPsec IKEv2为潜伏期敏感的数据流提供被最优化的连接。
最佳的网关选择	●确定并且设立连接对最佳的访问接入点，排除需要对于终端用户确定最近的位置。
友好的移动性	为移动用户设计的● 可以配置●，以便VPN连接依然是设立在IP地址更改、连接损耗期间或者冬眠或者暂挂。 与可信的网络检测的●， VPN连接能自动切断，当终端用户在办公室和连接时，当用户在一个远端位置时。
加密	● AES-256和3DES-168。(安全网关设备必须有被启用的一个严格crypto许可证。) ● NSA套件B算法、ESPv3与IKEv2， 4096位RSA键、Diffie-Hellman第24组和改进的SHA2 (SHA-256和SHA-384)。仅适用于IPsec IKEv2连接。需要AnyConnect尖顶许可证。
大范围配置和连接选项	**部署选项：** ●预部署，包括Microsoft安装程序 ●自动安全网关配置(管理权限对于初始安装是必需的)由ActiveX (仅Windows)和Java

	连接方式： ●独立由系统图标 浏览器被起动的● (Web生成) ●被起动的无客户端门户 被起动的● CLI 被起动的● API
大范围认证选项	● RADIUS 与密码终止(MSCHAPv2)的● RADIUS对NT LAN Manager (NTLM) ● RADIUS一次性密码(OTP)技术支持(状态和回复消息属性) ● RSA SecurID (包括SoftID集成) ●激活目录或Kerberos ●嵌入式Certificate Authority (CA) ●数字认证或智能卡(包括机器认证技术支持)，自动或者用户选择 与密码终止和过期的●轻量级目录访问协议(LDAP) ●通用的LDAP支持 ●联合的认证和username password多种因素的认证(双重身份验证)
一致用户体验	●全通道客户端模式支持需要一一致象LAN的用户体验的远程访问用户。 ●多个发送方法帮助保证AnyConnect的清楚的兼容性。 ●用户可能延迟被推进的更新。 ●用户经验反馈选项是可用的。
集中策略控制和管理	本地预先配置或配置●策略并且可以从VPN安全网关自动地更新。 AnyConnect的● API通过网页或应用程序缓和配置。 ●检查和用户警告为不信任的证书发布。 ●证书可以查看和被管理本地。
先进的IP网络连接	到/从IPv4和IPv6网络的●公共连接 对内部IPv4和IPv6的●访问网络资源 ●管理员控制分割隧道和全隧道网络访问策略 ●访问控制策略 ●谷歌机器人(棒棒糖)和三星的诺克斯每APP VPN策略(新在版本4.0;要求与OS 9.3或以后和AnyConnect 4.0的Cisco ASA 5500-X准许) **IP地址分配机制：** ●静态 ●内部池 ●动态主机配置协议(DHCP) ● RADIUS/LDAP
稳健统一的终端标准 (需要的尖顶许可证)	●终端状态评估和修正为配线支持和无线环境(替换思科身份服务引擎NAC代理程序)。要求身份服务引擎1.3或以上与身份服务引擎尖顶许可证。 ● Cisco Hostscan寻求在准许网络访问之前发现抗病毒软件、个人防火墙软件和Windows服务包出现在终端系统。 ●管理员也有定义根据运行进程出现的自定义状态检查的选项。 ● Hostscan发现水印的出现在远程系统的。结果水印可以用于识别是公司拥有的资产和提供被区分的访问。水印检查的功能包括系统注册值，匹配一必需的CRC32校验和、IP地址范围配比和证书的文件存在被发行由或对配比的认证机关。另外的功能为外标准应用程序支持。 ●功能由操作系统变化。请参阅主机扫描支持图关于详细信息。
客户端防火墙策略	●提供添加了分割隧道配置的保护。 与AnyConnect客户端一道用于的●允许本地访问例外(例如，打印的，被束缚的设备支持，等等)。 ●支持IPv4和网络的基于端口的规则和IPv6的IP访问控制列表(ACL)。 ●可用为Windows和Mac OS X平台。
本地化	**除英语之外，以下语言翻译是包括的：**

	●捷克(电缆敷设船cz) ●德语(DE DE) ●西班牙语(ES ES) ●法语(FR FR) ●日语(ja jp) ●韩文(ko kr) ●波兰语(PL PL) ●简体中文(zh CN) ●汉语(台湾) (zh tw) ●荷兰语(NL NL) ●匈牙利(hu hu) ●意大利语(它它) ●葡萄牙(巴西) (pt增殖比) ●俄语(RU RU)
客户端管理方便	●管理员能自动地分配从数据转发器安全工具的软件和策略更新，从而排除与客户端软件更新产生关联的管理。 ●管理员能确定使可用的哪些功能为最终用户配置。 当域不可能使用时，●管理员能触发终端脚本在连接并且断开时期登录脚本。 ●管理员能充分地定制和本地化终端用户可视消息。
配置文件编辑器	● AnyConnect策略可能直接地从Cisco Adaptive Security Device Manager (ASDM)定制。
诊断	●在设备统计数据和日志信息是可用的。 ●日志在设备可以查看。 ●日志可以容易地被发电子邮件给Cisco或一个管理员分析的。
联邦信息处理的标准(FIP)	兼容● FIP 140-2的第2级(平台、功能和版本限制适用)
安全移动性和网络可见度	
Web安全集成 (Cloud Web需要的安全许可证)	●使用Cloud Web安全，软件和服务(SaaS) Web安全最大的全球提供商，保持malware公司网络和控制和保障雇员Web使用方法。 ●技术支持网云主机配置和动态加载。 除基于前提的服务之外，●通过支持基于网云的服务提供组织灵活性和选择。 ●集成Web安全工具。 ●支持可信的网络检测。 ●强制执行在每处理的安全策略，对立于用户位置。 如果访问变得未提供，●要求不间断工作的高度安全的网络连通性以策略允许或拒绝网络连通性。 ●发现热点和俘虏门户。
网络可见度模块 (需要的尖顶许可证)	●通过监控应用程序使用找到潜在的工作情况反常现象。 ●允许更加消息灵通的网络设计决策。 ●能与增加的互联网协议流信息导出(IPFIX)共享使用数据-能够网络分析工具。
先进的Malware保护(AMP)终端启动器的 (分开准许的终端的AMP)	●简化威胁服务的启动对AnyConnect终端通过分配和启用终端的CiscoAMP。 ●传播终端威胁服务到远程终点，增加终端威胁覆盖。 ●提供更加积极的防护进一步保证攻击在远程终点迅速被缓和。
广泛的操作系统支持	● Windows 10， 8.1， 8和7 ● Mac OS X 10.8及以后
网络接入管理器和802.1X	
媒介支持	●以太网(IEEE 802.3) ● Wi-Fi (IEEE 802.11a/b/g/n)
网络验证	● IEEE 802.1X-2001、802.1X-2004和802.1X-2010 ●配置单个802.1X身份验证框架的Enable (event)企业访问配线和无线网络。 ●管理用户和设备身份和对于安全访问高度是必需的网络访问协议。

	当连接到Cisco Unified有线的和无线网络时，●优化用户体验。
可扩展的认证协议(EAP)方法	●传输层安全(TLS) ● EAP保护可扩展的认证协议(PEAP)与以下内在方法： - EAP-TLS - EAP-MSCHAPv2 - EAP通用的令牌卡(GTC) ● EAP灵活认证通过获取建立隧道(快速)有以下内在方法的： - EAP-TLS - EAP-MSCHAPv2 - EAP-GTC ● EAP被建立隧道的TLS (TTL)与以下内在方法： -密码认证协议。 -质询握手验证协议(CHAP)。 -微软Chap (MSCHAP)。 - MSCHAPv2 - EAP-MD5 - EAP-MSCHAPv2 ●轻量级EAP (LEAP)，仅Wi-Fi ●消息摘要5 (MD5)，管理配置，仅以太网 ● EAP-MSCHAPv2，管理配置，仅以太网 ● EAP-GTC，管理配置，仅以太网
无线加密方法(要求对应的802.11 NIC技术支持)	开放的● ●有线等效保密(WEP) ●动态WEP ● Wi-Fi保护访问(WPA)企业 ● WPA2企业 私有●的WPA (WPA-PSK) 私有的● WPA2 (WPA2-PSK) ● CCKM (要求Cisco CB21AG无线NIC)
无线加密协议	●与密码块连锁消息认证编码协议(CCMP)的计数器模式使用高级加密标准(AES)算法 ●临时密钥完整性协议(TKIP)使用Rivest密码4 (RC4)流密码
会话恢复	● RFC2716 (EAP-TLS)会话恢复使用EAP-TLS、EAP-FAST、EAP-PEAP和EAP-TTLS ● EAP-FAST无状态的会话恢复 ● PMK-ID缓存(积极的关键缓存或机会主义的关键缓存)，仅Windows XP
以太网加密	●媒体访问控制：IEEE 802.1AE (MACsec) ●密钥管理：MACsec键协议(MKA) ●定义了在有线以太网络的安全基础设施提供数据保密性、数据起始点的数据完整性和认证。 ●网络的委托的组件的之间保障通信。
一连接每次	●允许与网络的仅单个连接，断开其他。 ●在适配器之间的没有桥接。 ●以太网连接自动地采取优先级。
复杂服务器验证	●支持"末端与"和"完全匹配"规则。 超过30个规则的●技术支持没有命名公共的服务器的。
EAP连锁(EAP-FASTv2)	●区分根据企业和非企业资产的访问。 ●验证用户和设备在单个EAP处理。
企业连接实施(ECE)	●帮助保证用户仅连接到正确的公司网络。 ●防止用户到一第三方接入点浏览互联网的连接，当在办公室时。 ●防止用户设立对客户网络的访问。 ●排除笨重列入黑名单。
下一代加密(套件B)	●支持最新的密码标准。

	●椭圆曲线Diffie-Hellman密匙交换 ●椭圆曲线数字签名算法(ECDSA)证书
证件类型	●交互用户密码或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。
远程桌面技术支持	●验证远程用户凭证对本地网络，当曾经远程桌面协议时(RDP)。
操作系统支持的	● Windows 10， 8.1， 8和7

关于准许在RV340系列路由器的AnyConnect的信息，请参阅条款AnyConnect准许关于RV340系列路由器。