瞭解Cisco AnyConnect安全移動客戶端

目標

本文重點介紹使用Cisco AnyConnect的功能、規格和優點。有關RV340系列路由器上的AnyConnect許可的資訊，請參閱RV340系列路由器的AnyConnect許可一文。

軟體版本

4.2.03013 （發行說明）

功能和規格

功能	優勢和詳細資訊
遠端存取VPN	
廣泛的作業系統支援	• Windows 10、8.1、8和7 • Mac OS X 10.8及更高版本 • Linux Intel(x64) •請參閱AnyConnect Mobile資料表，以獲取移動平台資訊。
最佳化網路訪問：VPN協定選擇SSL（TLS和DTLS）；IPsec IKEv2	• AnyConnect提供各種VPN協定，因此管理員可以使用最適合其業務需求的協定。 •隧道支援包括SSL（TLS 1.2和DTLS）和下一代IPsec IKEv2。 • DTLS為延遲敏感型流量（例如VoIP流量或基於TCP的應用訪問）提供最佳化連線。 • TLS 1.2（HTTP over TLS或SSL）有助於確保通過鎖定環境（包括使用Web代理伺服器的環境）的網路連線的可用性。 • IPsec IKEv2在安全策略要求使用IPsec時為延遲敏感型流量提供最佳化連線。
最佳網關選擇	•確定並建立到最佳網路接入點的連線，無需終端使用者確定最近的位置。
便於移動	•專為行動使用者設計 •可以配置為在IP地址更改、連線丟失或休眠或待機期間保持VPN連線。 •通過受信任網路檢測，當終端使用者在辦公室時，VPN連線會自動斷開；而當使用者在遠端位置時，VPN連線會自動斷開。
加密	• AES-256和3DES-168。（安全網關裝置必須啟用強加密許可證。） • NSA Suite B演算法、具有IKEv2的ESPv3、4096位RSA金鑰、Diffie-Hellman組24和增強型SHA2（SHA-256和SHA-384）。 僅適用於IPsec IKEv2連線。需要AnyConnect Apex許可證。
廣泛的部署和連線選項	**部署選項:** •預部署，包括Microsoft Installer • ActiveX（僅限Windows）和Java自動安全網關部署（初始安裝需要管理許可權） **連線模式：** • Standalone by system圖示 •瀏覽器啟動（Web啟動） •無客戶端門戶已啟動 • CLI已啟動 • API已啟動
廣泛的身份驗證選項	• RADIUS

	● RADIUS(密碼到期(MSCHAPv2)到NT LAN Manager(NTLM) ● RADIUS一次性密碼(OTP)支援（狀態和回複訊息屬性） ● RSA SecurID（包括SoftID整合） ● Active Directory或Kerberos ●內嵌式憑證授權單位(CA) ●數位證書或智慧卡（包括機器證書支援），自動或使用者選擇 ●密碼到期和老化的輕量型目錄存取通訊協定(LDAP) ●通用LDAP支援 ●組合的證書和使用者名稱 — 密碼多重身份驗證（雙重身份驗證）
一致的使用者體驗	●全通道客戶端模式支援需要一致類LAN使用者體驗的遠端訪問使用者。 ●多種交付方法有助於確保AnyConnect的廣泛相容性。 ●使用者可能推遲推送的更新。 ●提供客戶體驗反饋選項。
集中策略控制和管理	●策略可在本地預配置或配置，並可從VPN安全網關自動更新。 ●於AnyConnect的API通過網頁或應用程式簡化部署。 ●對不受信任的證書發出檢查和使用者警告。 ●可以在本地檢視和管理證書。
高級IP網路連線	●與IPv4和IPv6網路的公共連線 ●訪問內部IPv4和IPv6網路資源 ●管理員控制的拆分隧道和全隧道網路訪問策略 ●訪問控制策略 ● Google Android(Lollipop)和Samsung KNOX（4.0版中的新功能）的每應用VPN策略；需要具有OS 9.3或更高版本以及AnyConnect 4.0許可證的Cisco ASA 5500-X) **IP地址分配機制：** ● Static ●內部池 ●動態主機設定通訊協定(DHCP) ● RADIUS/LDAP
強大的統一端點合規性 （需要Apex許可證）	●有線和無線環境支援終端狀態評估和補救（替換思科身份服務引擎NAC代理）。 需要具有身份服務引擎Apex許可證的身份服務引擎1.3或更高版本。 ● Cisco Hostscan在授予網路訪問權之前，會嘗試檢測終端系統上是否存在防病毒軟體、個人防火牆軟體和Windows服務包。 ●管理員還可以根據是否存在正在運行的進程定義自定義狀態檢查。 ● Hostscan檢測遠端系統上是否存在水印。水印可用於標識企業擁有的資產，從而提供差異化訪問。水印檢查功能包括系統登錄檔值、匹配所需CRC32校驗和的檔案存在、IP地址範圍匹配以及由匹配證書頒發機構頒發或發給匹配證書頒發機構的證書。不支援不合規應用程式的其他功能。 ●功能因作業系統而異。有關詳細資訊，請參閱主機掃描支援圖表。
客戶端防火牆策略	●為分割隧道配置提供額外的保護。 ●與AnyConnect客戶端結合使用以允許本地訪問異常（例如，列印、繫結裝置支援等）。 ●支援IPv4的基於埠的規則，以及IPv6的網路和IP訪問控制清單(ACL)。 ●可用於Windows和Mac OS X平台。
本地化	**除英語外，還包括以下語言翻譯：** ●捷克語(cs-cz) ●德語(de-de) ●西班牙語(es-es) ●法語(fr-fr) ●日語(ja-jp)

	●朝鮮語(ko-kr) ●波蘭語(pl-pl) ●簡體中文(zh-cn) ●中文（台灣）(zh-tw) ●荷蘭語(nl-nl) ●匈牙利語(hu-hu) ●義大利語(it-it) ●葡萄牙語（巴西）(pt-br) ●俄語(ru-ru)
易於進行客戶端管理	●管理員可以從頭端安全裝置自動分發軟體和策略更新，從而消除與客戶端軟體更新相關的管理。 ●管理員可以確定哪些功能可用於終端使用者配置。 ●當無法使用域登入指令碼時，管理員可以在連線和斷開連線時觸發終端指令碼。 ●管理員可以完全自定義和本地化終端使用者可見消息。
配置檔案編輯器	●可以直接從思科自適應安全裝置管理器(ASDM)自定義AnyConnect策略。
診斷	●裝置上的統計資訊和日誌記錄資訊可用。 ●可以在裝置上檢視日誌。 ●可以輕鬆將日誌通過電子郵件傳送給思科或管理員進行分析。
聯邦資訊處理標準(FIPS)	● FIPS 140-2 2級相容（平台、功能和版本限制適用）
安全移動性和網路可視性	
Web安全整合 （需要雲網路安全許可證）	●使用雲網路安全(Cloud Web Security)(全球最大的軟體即服務(SaaS)網路安全提供商)將惡意軟體隔離於公司網路之外，並控制和保護員工的Web使用。 ●支援雲託管配置和動態載入。 ●通過支援基於雲的服務以及基於現場的服務，為組織提供靈活性和選擇。 ●與網路安全裝置整合。 ●支援可信網路檢測。 ●在每個事務中實施安全策略，與使用者位置無關。 ●要求始終處於開啟狀態的高度安全網路連線，並且策略允許或拒絕在無法訪問時的網路連線。 ●檢測熱點和強制網路門戶。
網路能見度模組 （需要Apex許可證）	●通過監控應用程式使用情況發現潛在的行為異常。 ●允許做出更明智的網路設計決策。 ●可與越來越多的支援Internet協定流資訊匯出(IPFIX)的網路分析工具共用使用資料。
適用於終端機的進階惡意軟體防護(AMP)啟用程式 （面向終端的AMP需單獨許可）	●通過分發和啟用面向終端的思科AMP，簡化對AnyConnect終端的威脅服務啟用。 ●將終端威脅服務擴展到遠端終端，增加終端威脅覆蓋範圍。 ●提供更主動的保護，以進一步確保在遠端終端快速緩解攻擊。
廣泛的作業系統支援	● Windows 10、8.1、8和7 ● Mac OS X 10.8及更高版本
網路存取管理員和802.1X	
媒體支援	●乙太網路(IEEE 802.3) ● Wi-Fi(IEEE 802.11a/b/g/n)
網路身份驗證	● IEEE 802.1X-2001、802.1X-2004和802.1X-2010 ●使企業能夠部署單個802.1X身份驗證框架來訪問有線和無線網路。 ●管理高度安全訪問所需的使用者和裝置身份以及網路訪問協定。 ●在連線到思科統一有線和無線網路時最佳化使用者體驗。
可擴展身份驗證協定(EAP)方法	● EAP — 傳輸層安全(TLS) ●EAP保護的可擴展身份驗證協定(PEAP)具有以下內部方法： - EAP-TLS - EAP-MSCHAPv2

	- EAP — 通用令牌卡(GTC) ●EAP — 通過安全隧道(FAST)進行靈活身份驗證，採用以下內部方法： - EAP-TLS - EAP-MSCHAPv2 - EAP-GTC ●EAP隧道TLS(TTLS)使用以下內部方法： — 密碼驗證通訊協定(PAP)。 — 質詢握手身份驗證協定(CHAP)。 - Microsoft CHAP(MSCHAP)。 - MSCHAPv2 - EAP-MD5 - EAP-MSCHAPv2 ●輕量EAP(LEAP)，僅Wi-Fi ● EAP-Message Digest 5(MD5)，已配置管理，僅乙太網 ● EAP-MSCHAPv2，已配置管理，僅乙太網 ● EAP-GTC，已配置管理，僅乙太網
無線加密方法（需要相應的802.11 NIC支援）	● Open ●有線等效保密(WEP) ●動態WEP ● Wi-Fi保護存取(WPA)企業版 ● WPA2企業版 ● WPA個人(WPA-PSK) ● WPA2個人(WPA2-PSK) ● CCKM（需要Cisco CB21AG無線網絡卡）
無線加密協定	●用進階加密標準(AES)演演算法的密碼塊鏈結訊息驗證碼通訊協定(CCMP)的計數器模式 ●使用Rivest Cipher 4(RC4)串流密碼的時間金鑰完整性通訊協定(TKIP)
會話恢復	●用EAP-TLS、EAP-FAST、EAP-PEAP和EAP-TTLS恢復RFC2716(EAP-TLS)會話 ● EAP-FAST無狀態會話恢復 ● PMK-ID快取（主動金鑰快取或機會金鑰快取），僅Windows XP
乙太網路加密	● Media Access Control:IEEE 802.1AE(MACsec) ●金鑰管理：MACsec金鑰協定(MKA) ●定義有線乙太網上的安全基礎設施，以提供資料機密性、資料完整性和資料來源驗證。 ●保護網路受信任元件之間的通訊。
一次一個連線	●僅允許到網路的單一連線，斷開所有其他連線。 ●介面卡之間沒有橋接。 ●乙太網連線自動優先。
複雜的伺服器驗證	●支援「結尾為」和「完全匹配」規則。 ●對於沒有名稱通用性的伺服器，支援30多個規則。
EAP — 連結(EAP-FASTv2)	●區分基於企業和非企業資產的訪問。 ●在單個EAP事務中驗證使用者和裝置。
企業連線執行(ECE)	●幫助確保使用者僅連線到正確的公司網路。 ●防止使用者在辦公室內連線到第三方接入點上網。 ●阻止使用者建立對訪客網路的訪問許可權。 ●消除繁瑣的黑名單。
下一代加密（套件B）	●支援最新的加密標準。 ●橢圓曲線Diffie-Hellman金鑰交換 ●橢圓曲線數位簽章演算法(ECDSA)證書
憑據型別	●互動式使用者密碼或Windows密碼 ● RSA SecurID令牌

	●一次性密碼(OTP)令牌 ●智慧卡(Axalto、Gemplus、SafeNet iKey、Alladin)。 ● X.509憑證。 ●橢圓曲線數位簽章演算法(ECDSA)證書。
遠端案頭支援	●使用遠端案頭協定(RDP)時向本地網路驗證遠端使用者憑據。
支援的作業系統	● Windows 10、8.1、8和7