التعرف على Cisco AnyConnect Secure Mobility Client

الهدف

تركز هذه المقالة على المميزات والمواصفات وفوائد إستخدام Cisco AnyConnect. للحصول على معلومات حول ترخيص AnyConnect على موجهات سلسلة RV340، يرجى مراجعة المقالة منح ترخيص AnyConnect لموجهات سلسلة RV340 .

إصدار البرامج

4.2.03013 (ملاحظات الإصدار)

الخصائص والمواصفات

الميزة	الميزات والتفاصيل
Remote-Access VPN	
دعم نظام التشغيل على نطاق واسع	• Windows 10 و 8.1 و 8 و 7 • Mac OS X 10.8 والإصدارات الأحدث • Linux Intel (x64) • راجع ورقة بيانات AnyConnect للأجهزة المحمولة للحصول على معلومات النظام الأساسي للأجهزة المحمولة.
الوصول المحسن إلى الشبكة: SSL لاختيار بروتوكول VPN (TLS و DTLS) و IPsec IKEv2	• يوفر AnyConnect مجموعة مختارة من بروتوكولات الشبكة الخاصة الظاهرية (VPN)، حتى يمكن للمسؤولين إستخدام أي بروتوكول يناسب إحتياجات شركاتهم على أفضل وجه. • يتضمن دعم الاتصال النفقي (TLS 1. 2 SSL و DTLS) والجيل التالي IPsec IKEv2. • توفر DTLS اتصالا محسنا لحركة المرور التي يمثل زمن الوصول فيها أمرا حيويا، مثل حركة مرور البيانات عبر بروتوكول VoIP أو الوصول إلى التطبيق المستند إلى بروتوكول TCP. • يساعد TLS 1.2 (HTTP عبر TLS أو SSL) على ضمان توفر اتصال الشبكة من خلال البيئات التي تم تأمينها، بما في ذلك تلك التي تستخدم خوادم وكيل الويب. • يوفر IPsec IKEv2 اتصالا محسنا لحركة مرور البيانات التي يمثل زمن الوصول فيها أمرا حيويا

	عندما تتطلب سياسات الأمان إستخدام IPsec.
تحديد البوابة الأمثل	• تحديد الاتصال بنقطة الوصول إلى الشبكة المثلى وإنشائه، مما يقلل من حاجة المستخدمين النهائيين إلى تحديد أقرب موقع.
طراز سهل التنقل	• مصممة خصيصا للمستخدمين كثيري التنقل • يمكن تكوينها بحيث يبقى اتصال الشبكة الخاصة الظاهرية (VPN) ثابتا أثناء تغييرات عنوان IP أو فقد الاتصال أو الإسبات أو الاستعداد. • من خلال "اكتشاف الشبكة الموثوق بها"، يمكن أن ينفصل اتصال الشبكة الخاصة الظاهرية (VPN) تلقائيا عندما يكون المستخدم النهائي في المكتب ويتصل عندما يكون المستخدم في موقع بعيد.
تشفير	• AES-256 و 3DES-168. (يجب أن يكون لجهاز عبارة الأمان ترخيص تشفير قوي ممكن.) • خوارزميات مجموعة NSA Suite B و ESPv3 مع IKEv2، مفاتيح RSA من فئة 4096 بت، ومجموعة Diffie-Hellman من فئة 24، و SHA2 المحسنة (SHA-256 و SHA-384). يطبق فقط على إتصالات IPsec IKEv2. مطلوب ترخيص AnyConnect Top.
مجموعة كبيرة من خيارات النشر والاتصال	**خيارات النشر:** • ما قبل النشر، بما في ذلك Microsoft Installer • النشر التلقائي لعبارة الأمان (يلزم توفر الحقوق الإدارية للتثبيت الأولي) بواسطة ActiveX (في Windows فقط) و Java **أوضاع الاتصال:** • مستقل حسب رمز النظام • بدء تشغيل المستعرض (بدء التشغيل عبر الويب) تم بدء • بوابة بدون عملاء تم بدء واجهة سطر الأوامر (CLI) • تم بدء تشغيل واجهة برمجة التطبيقات •
مجموعة كبيرة من خيارات المصادقة	• RADIUS • RADIUS مع انتهاء صلاحية كلمة المرور (MSCHAPv2) إلى مدير شبكة LAN NT (NTLM) • دعم كلمة مرور المرة الواحدة (OTP) ل RADIUS (سمات رسالة الحالة والرد)

	• RSA SecureID (بما في ذلك تكامل SoftID) • Active Directory أو Kerberos جهة منح الشهادة • المضمنة (CA) • الشهادة الرقمية أو البطاقة الذكية (بما في ذلك دعم الشهادات الآلية)، محددة آليا أو بواسطة المستخدم • البروتوكول الخفيف للوصول للدليل (LDAP) مع انتهاء صلاحية كلمة المرور والتقادم دعم LDAP العام • • الشهادة المجمعة والمصادقة متعددة العوامل باسم المستخدم (المصادقة المزدوجة)
تجربة مستخدم متناسقة	• يدعم وضع عميل النفق الكامل مستخدمي الوصول عن بعد ممن يحتاجون إلى تجربة مستخدم متناسقة شبيهة بتلك التي توفرها شبكة LAN. • تساعد طرق التسليم المتعددة على ضمان توافق AnyConnect على نطاق واسع. • يمكن للمستخدم تأجيل التحديثات المدفوعة. • يتوفر خيار الملاحظات حول تجربة العملاء.
التحكم والإدارة المركزيان للسياسات	• يمكن تكوين السياسات مسبقا أو تكوينها محليا ويمكن تحديثها تلقائيا من بوابة أمان VPN. • تعمل واجهة برمجة التطبيقات (API) ل AnyConnect على تسهيل عمليات النشر من خلال صفحات الويب أو التطبيقات. • يتم إصدار تحذيرات المستخدم والتحقق من التراخيص غير الموثوق بها. • يمكن عرض الشهادات وإدارتها محليا.
اتصال شبكة IP المتقدم	• اتصال عام بشبكات IPv4 و IPv6 ومن هذه الشبكات • الوصول إلى موارد شبكة IPv4 و IPv6 الداخلية • سياسة الوصول إلى الشبكة النفقي القائم على المسؤول والوصول إليها عبر قنوات الاتصال كلها سياسة التحكم بالوصول • • سياسة الشبكة الخاصة الظاهرية (VPN) لكل تطبيق ل Google Android (Lollipop) و Samsung KNOX (جديدة في

	الإصدار 4. 0؛ تتطلب ترخيص Cisco ASA 5500-X بنظام التشغيل 9. 3 أو إصدار أحدث وتراخيص AnyConnect 4. 0) **آليات تعيين عنوان IP:** • ثابت • مجموعة داخلية • بروتوكول تكوين الاستضافة الديناميكية (DHCP) • RADIUS/LDAP
توافق قوي وموحد لنقطة النهاية (ترخيص الحد الأعلى مطلوب)	• يتم دعم تقييم حالة نقطة النهاية وإصلاحها للبيئات السلكية واللاسلكية (إستبدال وكيل NAC لمحرك خدمات الهوية من Cisco). يتطلب محرك خدمات الهوية 1.3 أو إصدار أحدث مع ترخيص Identity Services Engine Apex. • يسعى Cisco Hostscan إلى اكتشاف وجود برامج مكافحة الفيروسات وبرامج جدار الحماية الشخصية وحزم خدمة Windows على نظام نقطة النهاية قبل منح الوصول إلى الشبكة. • للمسؤولين أيضا خيار تعريف تحققات الوضع المخصص بناء على وجود عمليات التشغيل. • يكتشف Hostscan وجود علامة مائية على نظام بعيد. ويمكن إستخدام العلامة المائية لتحديد الأصول التي تملكها الشركات والتي توفر وصولا متميزا نتيجة لذلك. تتضمن إمكانية التحقق من العلامة المائية قيم سجل النظام، ووجود الملف الذي يطابق المجموع الاختباري CRC32 المطلوب، ومطابقة نطاق عنوان IP، والشهادات الصادرة من أو إلى مرجع شهادة مطابقة. يتم دعم قدرات إضافية للتطبيقات التي لا تتوافق مع النظام. • تختلف الوظائف حسب نظام التشغيل. راجع مخططات دعم المسح الضوئي للمضيف للحصول على معلومات تفصيلية.
نهج جدار حماية العميل	• توفر حماية إضافية لتكوينات الاتصال النفقي المنقسم. • يستخدم بالاقتران مع عميل AnyConnect للسماح باستثناءات الوصول المحلي (على سبيل المثال، الطباعة ودعم الأجهزة المرتبطة وما إلى ذلك). • تدعم القواعد القائمة على

	المنافذ ل IPv4 وقوائم التحكم في الوصول إلى الشبكة و IP ACLs)) ل IPv6. • متوفر لأنظمة Windows و Mac OS X الأساسية.
تعريب	**بالإضافة إلى اللغة الإنجليزية، يتم تضمين ترجمات اللغة التالية:** • التشيكية (cs-cz) • الألمانية (سحب) • الإسبانية (es-es) • الفرنسية (fr-fr) • اليابانية (ja-jp) • الكورية (ko-kr) • البولندية (pl-pl) • الصينية المبسطة (zh-cn) • الصينية (تايوان) (zh-tw) • الهولندية (nl-nl) • الهنغارية (هو-هو) • الإيطالية (تقنية المعلومات) • البرتغالية (البرازيل) (pt-br) • الروسية (ru-ru)
سهولة إدارة العملاء	• يمكن للمسؤولين توزيع تحديثات البرامج والسياسات تلقائيا من جهاز أمان وحدة الاستقبال والبث، وبالتالي تقليل الإدارة المرتبطة بتحديثات برامج العملاء. • يمكن للمسؤولين تحديد الإمكانات التي يمكنهم توفيرها لتكوين المستخدم النهائي. • يمكن للمسؤولين تشغيل برنامج نصي لنقطة النهاية في أوقات الاتصال وفصل الاتصال عندما يتعذر إستخدام البرامج النصية لتسجيل دخول المجال. • يستطيع المسؤولون تخصيص وتعريب الرسائل المرئية الخاصة بالمستخدم النهائي بالكامل.
محرر ملف التعريف	• قد يتم تخصيص سياسات AnyConnect مباشرة من مدير أجهزة الأمان المعدلة (ASDM) من Cisco.
التشخيص	• تتوفر إحصائيات ومعلومات تسجيل على الجهاز. • يمكن عرض السجلات على الجهاز. • يمكن إرسال السجلات عبر البريد الإلكتروني بسهولة إلى Cisco أو المسؤول للتحليل.
معيار معالجة المعلومات الفيدرالية (FIPS)	• متوافق مع معيار FIPS 140-2 المستوى 2 (يتم تطبيق قيود النظام الأساسي والميزات والإصدارات)
إمكانية التنقل الآمنة وإمكانية رؤية الشبكة	
تكامل أمان الويب	• يستخدم أمان الويب السحابي،

(ترخيص أمان الويب السحابي مطلوب)	أكبر مزود عالمي لأمان الويب للبرامج كخدمة (SAAs)، لإبقاء البرامج الضارة خارج شبكات الشركات والتحكم في إستخدام الموظفين لموقع الويب وحمايته. • تدعم التكوينات المستضافة بواسطة السحابة والتحميل الديناميكي. • تمنح المؤسسات المرونة والاختيار من خلال دعم الخدمات القائمة على الشبكات بالإضافة إلى الخدمات القائمة على المباني. • التكامل مع جهاز أمان الويب. • تدعم اكتشاف الشبكة الموثوق به. • فرض سياسة الأمان في كل معاملة، بشكل مستقل عن موقع المستخدم. • يتطلب اتصال الشبكة عالي الأمان دائما مع سياسة للسماح باتصال الشبكة أو رفضه إذا أصبح الوصول غير متاح. • يكتشف النقاط الساخنة والبوابات الأسيرة.
الوحدة النمطية لإمكانية رؤية الشبكة (ترخيص الحد الأعلى مطلوب)	• اكتشاف حالات السلوك الشاذة المحتملة من خلال مراقبة إستخدام التطبيقات. • تسمح باتخاذ قرارات أكثر إستنارة حول تصميم الشبكة. • يمكن مشاركة بيانات الاستخدام مع عدد متزايد من أدوات تحليل الشبكة القادرة على تصدير معلومات تدفق بروتوكول الإنترنت (IPFIX).
الحماية المتقدمة من البرامج الضارة (AMP) لممكن نقاط النهاية (AMP لنقاط النهاية المرخصة بشكل منفصل)	• تبسيط تمكين خدمات التهديدات على نقاط نهاية AnyConnect من خلال توزيع CiscoAMP وتمكينها لنقاط النهاية. • توسيع خدمات تهديدات نقاط النهاية إلى نقاط النهاية البعيدة، مما يزيد من تغطية تهديدات نقاط النهاية. • توفر حماية أكثر إستباقية لضمان أن الهجوم سيتم تخفيفه بسرعة عند نقطة النهاية البعيدة.
دعم واسع النطاق لنظام التشغيل	• Windows 10 و 8.1 و 8 و 7 • Mac OS X 10.8 والإصدارات الأحدث
مدير الوصول إلى الشبكة و 802.1X	
دعم الوسائط	• إيثرنت (IEEE 802.3) • Wi-Fi (IEEE 802. 11a/b/g/n)
مصادقة الشبكة	• IEEE 802.1x-2001 و 802.1x-2004 و 802.1x-2010

	• يمكن الشركات من نشر إطار مصادقة 802.1X واحد للوصول إلى كل من الشبكات السلكية واللاسلكية. • إدارة هوية المستخدم والجهاز وبروتوكولات الوصول إلى الشبكة المطلوبة للوصول الآمن للغاية. • تحسين تجربة المستخدم عند الاتصال بشبكة Cisco سلكية ولاسلكية موحدة.
أساليب بروتوكول المصادقة المتوسع (EAP)	• أمان طبقة النقل (TLS) عبر EAP • بروتوكول المصادقة المتوسع المحمي ب PEAP) EAP) بالطرق الداخلية التالية: - EAP-TLS - EAP-MSCHAPv2 - بطاقة الرمز المميز العام EAP (GTC)) • مصادقة EAP-Flexible عبر الاتصال النفقي الآمن (FAST) باستخدام الأساليب الداخلية التالية: - EAP-TLS - EAP-MSCHAPv2 - EAP-GTC • EAP-Tunneleled TLS (TTLS)) باستخدام الأساليب الداخلية التالية: - بروتوكول مصادقة كلمة المرور (PAP). - بروتوكول مصادقة مصافحة الاستيبان (CHAP). - بروتوكول Microsoft CHAP (MSCHAP)). - MSCHAPv2 - EAP-MD5 - EAP-MSCHAPv2 • EAP خفيف الوزن (،(LEAP Wi-Fi فقط • EAP-Message Digest 5 (MD5))، مكون إداري، إيثرنت فقط • EAP-MSCHAPv2، مكون إداري، إيثرنت فقط • EAP-GTC، مكون إداري، إيثرنت فقط
طرق التشفير اللاسلكي (تتطلب دعم بطاقة واجهة الشبكة (NIC 802. 11 المطابقة)	• فتح • الخصوصية المكافئة للتوصيل السلكي (WEP) WEP • الديناميكي مؤسسة وصول • Wi-Fi المحمي (WPA) • WPA2 Enterprise • WPA شخصي (WPA-PSK)

	• WPA2 شخصي (WPA2-PSK) • CCKM (يتطلب بطاقة واجهة شبكة (NIC) لاسلكية Cisco CB21AG)
بروتوكولات التشفير اللاسلكي	• وضع العداد باستخدام خوارزمية معيار التشفير المتقدم (AES) لبروتوكول مصادقة الرسائل المتسلسلة لتشفير التشفير (CCMP) • بروتوكول سلامة المفاتيح المؤقتة (TKIP) باستخدام تشفير الدفق Rivest Cipher 4 (RC4)
إستئناف جلسة العمل	• EAP-TLS (RFC2716) إستئناف الجلسة باستخدام EAP-TLS و EAP-FAST و EAP-PEAP و EAP-TTLS • EAP-FAST إستئناف الجلسة عديم الحالة • التخزين المؤقت لمعرف PMK (التخزين المؤقت الاستباقي للمفتاح أو التخزين المؤقت الانتهازي للمفتاح)، نظام التشغيل Windows XP فقط
تشفير إيثرنت	• التحكم في الوصول إلى الوسائط: IEEE 802.1AE (MacSec) • إدارة المفاتيح: إتفاقية مفتاح MACsec (MKA) • تحديد بنية أساسية للأمان على شبكة إيثرنت سلكية لتوفير سرية البيانات وسلامة البيانات ومصادقة أصل البيانات. • حماية الاتصال بين المكونات الموثوق بها للشبكة.
اتصال واحد في كل مرة	• تسمح فقط باتصال واحد بالشبكة، مما يؤدي إلى قطع اتصال كافة الشبكات الأخرى. • لا يوجد جسر بين المهايئات. • تأخذ إتصالات إيثرنت الأولوية تلقائيا.
التحقق من صحة الخادم المعقد	• تدعم قواعد "النهاية مع" و"المطابقة الدقيقة". • دعم أكثر من 30 قاعدة للخوادم التي لا تحتوي على خصائص مشتركة للأسماء.
ربط EAP (EAP-FASTv2)	• التمييز بين إمكانية الوصول على أساس الأصول الخاصة بالمؤسسة وغير الخاصة بالمؤسسة. • التحقق من صحة المستخدمين والأجهزة في معاملة EAP واحدة.
تنفيذ اتصال المؤسسات (ECE)	• تساعد على ضمان اتصال المستخدمين بشبكة الشركة الصحيحة فقط.

	• تمنع المستخدمين من الاتصال بنقطة وصول خارجية لتصفح الإنترنت أثناء وجودهم في المكتب. • تمنع المستخدمين من إنشاء وصول إلى شبكة الضيوف. • يزيل القائمة السوداء المرهقة.
تشفير الجيل التالي (المجموعة B)	• تدعم أحدث معايير التشفير. • تبادل مفتاح المنحنى البيضاوي Diffie-Hellman • شهادات خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA)
أنواع بيانات الاعتماد	• كلمات مرور المستخدم التفاعلية أو كلمات مرور نظام التشغيل Windows • الرموز المميزة SecureID ل RSA • الرموز المميزة لكلمة مرور المرة الواحدة (OTP) • البطاقات الذكية (Axalto و Gemplus و SafeNet iKey و Alladin). • شهادات X. 509. • شهادات خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA).
دعم سطح المكتب البعيد	• مصادقة بيانات اعتماد المستخدم البعيد إلى الشبكة المحلية عند إستخدام بروتوكول سطح المكتب البعيد (RDP).
أنظمة التشغيل المدعومة	• Windows 10 و 8.1 و 8 و 7

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).