الأسئلة المتداولة حول Cisco Aironet Wireless Security

المحتويات

المقدمة

يقدم هذا المستند معلومات حول الأسئلة المتداولة (FAQ) حول أمان Cisco Aironet اللاسلكي.

أسئلة شائعة عامة

س. ما هي الحاجة للأمان اللاسلكي؟

أ. في الشبكة السلكية، تظل البيانات موجودة في الكبلات التي تصل الأجهزة الطرفية. لكن الشبكات اللاسلكية تنقل وتستقبل البيانات من خلال بث إشارات التردد اللاسلكي في الهواء الطلق. نظرا لطبيعة البث التي تستخدمها الشبكات المحلية اللاسلكية (WLANs)، هناك تهديد أكبر من قبل المتسللين أو الدخلاء الذين يمكنهم الوصول إلى البيانات أو إتلافها. وللتخفيف من هذه المشكلة، تتطلب جميع شبكات WLAN إضافة ما يلي:

1. مصادقة المستخدم لمنع الوصول غير المصرح به إلى موارد الشبكة.
2. خصوصية البيانات لحماية سلامة البيانات المرسلة وخصوصيتها (المعروفة أيضا باسم التشفير).

س. ما هي طرق المصادقة المختلفة التي يحددها معيار 802.11 للشبكات المحلية اللاسلكية؟

ألف - يحدد معيار 802.11 آليتين لمصادقة عملاء الشبكات المحلية اللاسلكية:

1. فتح المصادقة
2. مصادقة المفتاح المشترك

وهناك آليتان أخريان يستخدمان بشكل شائع أيضا:

1. مصادقة قائمة على SSID
2. مصادقة عنوان MAC

س. ما هي المصادقة المفتوحة؟

أ. المصادقة المفتوحة هي أساسا خوارزمية مصادقة خالية، مما يعني أنه لا يوجد تحقق من المستخدم أو الجهاز. تسمح المصادقة المفتوحة لأي جهاز يضع طلب مصادقة على نقطة الوصول (AP). تستخدم المصادقة المفتوحة إرسال نص واضح للسماح لعميل بالاقتران بنقطة وصول. في حالة عدم تمكين أي تشفير، يمكن لأي جهاز معرفة

معرف SSID للشبكة المحلية اللاسلكية (WLAN) الوصول إلى الشبكة. إذا تم تمكين الخصوصية المكافئة للتوصيل السلكي (WEP) على نقطة الوصول، يصبح مفتاح WEP وسيلة للتحكم في الوصول. لا يمكن للجهاز الذي ليس لديه مفتاح WEP الصحيح إرسال البيانات من خلال نقطة الوصول حتى إذا نجحت المصادقة. ولا يستطيع هذا أداة فك تشفير البيانات أن ال ap يرسل.

س. ما الخطوات التي تتضمنها المصادقة المفتوحة لعميل ما لإقرانه بنقطة الوصول؟

1. يرسل العميل طلب تحقيق إلى نقاط الوصول.
2. ترسل نقاط الوصول استجابات المسبار العكسي.
3. يقيم العميل استجابات نقطة الوصول ويحدد أفضل نقطة وصول.
4. يرسل العميل طلب مصادقة إلى نقطة الوصول.
5. تؤكد نقطة الوصول (AP) المصادقة وتسجل العميل.
6. يرسل العميل بعد ذلك طلب اقتران إلى نقطة الوصول.
7. تؤكد نقطة الوصول الاقتران وتسجل العميل.

س. ما هي مزايا وعيوب المصادقة المفتوحة؟

أ. فيما يلي مميزات وعيوب المصادقة المفتوحة:

المزايا: المصادقة المفتوحة هي آلية مصادقة أساسية، يمكنك إستخدامها مع الأجهزة اللاسلكية التي لا تدعم خوارزميات المصادقة المعقدة. يتم توجيه المصادقة في مواصفات 802.11 نحو الاتصال. يسمح التصميم متطلبات المصادقة للأجهزة بالوصول السريع إلى الشبكة. في مثل هذه الحالة، يمكنك إستخدام المصادقة المفتوحة.

عيوب: لا توفر المصادقة المفتوحة أي طريقة للتحقق مما إذا كان العميل عميل صالح وليس عميل مخترق. إذا لم تستخدم تشفير WEP مع المصادقة المفتوحة، يمكن لأي مستخدم يعلم SSID للشبكة المحلية اللاسلكية (WLAN) الوصول إلى الشبكة.

س. ما هي مصادقة المفتاح المشترك؟

أ. تعمل مصادقة المفتاح المشترك كمصادقة مفتوحة مع أختلاف رئيسي واحد. عندما تستخدم المصادقة المفتوحة باستخدام مفتاح تشفير WEP، يستخدم مفتاح WEP لتشفير البيانات وفك تشفيرها، ولكنه لا يستخدم في خطوة المصادقة. في مصادقة المفتاح المشترك، يستخدم تشفير WEP للمصادقة. مثل المصادقة المفتوحة، تتطلب مصادقة المفتاح المشترك أن يكون للعميل و AP نفس مفتاح WEP. ترسل نقطة الوصول التي تستخدم مصادقة المفتاح المشترك حزمة نص التحدي إلى العميل. يستخدم العميل مفتاح WEP الذي تم تكوينه محليا لتشفير نص التحدي والرد مع طلب مصادقة لاحق. إذا كان بإمكان نقطة الوصول فك تشفير طلب المصادقة واسترداد نص التحدي الأصلي، فإن نقطة الوصول تستجيب باستجابة مصادقة تمنح الوصول إلى العميل.

س. ما الخطوات التي تتضمنها مصادقة المفتاح المشترك لعميل ما لإقرانه بنقطة الوصول؟

1. يرسل العميل طلب تحقيق إلى نقاط الوصول.
2. ترسل نقاط الوصول استجابات المسبار العكسي.
3. يقيم العميل استجابات نقطة الوصول ويحدد أفضل نقطة وصول.
4. يرسل العميل طلب مصادقة إلى نقطة الوصول.
5. ترسل نقطة الوصول إستجابة مصادقة تحتوي على نص التحدي غير المشفر.
6. يقوم العميل بتشفير نص التحدي باستخدام مفتاح WEP ويرسل النص إلى نقطة الوصول.
7. تقوم نقطة الوصول بمقارنة نص الاستبيان غير المشفر مع نص الاستبيان المشفر. إذا كان بإمكان المصادقة فك تشفير نص التحدي الأصلي واسترداده، تكون المصادقة ناجحة.

تستخدم مصادقة المفاتيح المشتركة تشفير WEP أثناء عملية اقتران العميل.

س. ما هي مزايا وعيوب مصادقة المفتاح المشترك؟

أ. في مصادقة المفتاح المشترك، يتبادل العميل و AP نص التحدي (نص واضح) والتحدي المشفر. لذلك، يكون هذا النوع من المصادقة عرضة لهجوم الدخيل. يستطيع المخترق الاستماع إلى التحدي غير المشفر والتحدي المشفر، ثم يستخرج مفتاح WEP (المفتاح المشترك) من هذه المعلومات. عندما يعرف المخترق مفتاح WEP، يتم أختراق آلية المصادقة بأكملها ويمكن أن ينفذ المخترق شبكة WLAN. هذا هو العيب الرئيسي في مصادقة المفتاح المشترك.

س. ما هي مصادقة عنوان MAC؟

أ. على الرغم من أن معيار 802.11 لا يحدد مصادقة عنوان MAC، إلا أن شبكات WLAN تستخدم تقنية المصادقة هذه بشكل شائع. وبالتالي، فإن معظم موردي الأجهزة اللاسلكية، بما في ذلك Cisco، يؤيدون مصادقة عنوان MAC.

في مصادقة عنوان MAC، تتم مصادقة العملاء استنادا إلى عنوان MAC الخاص بهم يتم التحقق من عناوين MAC للعملاء مقابل قائمة عناوين MAC المخزنة محليا على نقطة الوصول أو على خادم مصادقة خارجي. مصادقة MAC هي آلية أمان أقوى من مصادقة المفاتيح المفتوحة والمشتركة التي يوفرها 802.11. وتعمل هذه الطريقة من المصادقة على تقليل أحتمالية الأجهزة غير المصرح لها بالوصول إلى الشبكة بشكل أكبر.

q. لماذا لا تعمل مصادقة MAC مع (WPA (Wi-Fi Protected Access في برنامج Cisco IOS الإصدار 12.3(8)JA2؟

أ. مستوى الأمان الوحيد لمصادقة MAC هو التحقق من عنوان MAC الخاص بالعميل مقابل قائمة من عناوين MAC المسموح بها. وهذا يعتبر ضعيفا جدا. في إصدارات برنامج Cisco IOS السابقة، يمكنك تكوين مصادقة MAC و WPA لتشفير المعلومات. ولكن لأن WPA نفسه له عنوان MAC الذي يتحقق، قررت Cisco عدم السماح بهذا النوع من التكوين في إصدارات برنامج Cisco IOS الأحدث وقررت فقط تحسين ميزات الأمان.

س. هل يمكنني إستخدام SSID كطريقة لمصادقة الأجهزة اللاسلكية؟

أ. معرف مجموعة الخدمة (SSID) عبارة عن قيمة أبجدية رقمية فريدة وحساسة لحالة الأحرف تستخدمها الشبكات المحلية اللاسلكية (WLANs) كاسم شبكة. SSID عبارة عن آلية تتيح الفصل المنطقي للشبكات المحلية اللاسلكية. لا يوفر SSID أي وظائف خصوصية للبيانات ولا يقوم SSID بمصادقة العميل إلى AP. يتم بث قيمة SSID كنص واضح في أجهزة الإرشاد، طلبات المسبار، استجابات المسبار، وأنواع أخرى من الإطارات. ويمكن لمزود الصوت تحديد SSID بسهولة باستخدام محلل حزمة شبكة LAN اللاسلكية 802.11، على سبيل المثال، Sniffer Pro. لا توصي Cisco باستخدام SSID كطريقة لتأمين شبكة WLAN الخاصة بك.

س. إذا قمت بتعطيل بث SSID، هل يمكنني تحقيق تأمين محسن على شبكة WLAN؟

أ. عند تعطيل بث SSID، لا يتم إرسال SSID في رسائل Beacon. ومع ذلك، لا تزال هناك إطارات أخرى مثل طلبات التحقيق واستجابات المسبار تحتوي على SSID في نص واضح. لذلك لا تحقق الأمان اللاسلكي المحسن إذا قمت بتعطيل SSID. لم يتم تصميم SSID أو إستخدامه كآلية تأمين. وبالإضافة إلى ذلك، في حالة تعطيل عمليات بث SSID، يمكنك مواجهة مشاكل مع إمكانية التشغيل البيني ل Wi-Fi لعمليات نشر الأجهزة العميلة المختلطة. لذلك، لا توصي Cisco باستخدام SSID كوضع أمان.

س. ما هي نقاط الضعف الموجودة في أمن 802.11؟

ألف - يمكن تلخيص أوجه الضعف الرئيسية لأمن 802-11 على النحو التالي:

- مصادقة ضعيفة خاصة بالجهاز فقط: تتم مصادقة أجهزة العميل، وليس المستخدمين.
- تشفير البيانات الضعيف: تم إثبات عدم فعالية الخصوصية المكافئة للتوصيل السلكي (WEP) كوسيلة لتشفير البيانات.

• لا توجد تكامل للرسالة: أثبتت قيمة التحقق من السلامة (ICV) عدم فعاليتها كوسيلة لضمان تكامل الرسالة.

س. ما هو دور مصادقة 802.1x في WLAN؟

ألف - بغية معالجة أوجه القصور والضعف في مجال الأمان في الأساليب الأصلية للمصادقة التي يحددها معيار 802.11، يدرج إطار مصادقة 802.1X في مشروع تحسينات أمان طبقة MAC 802.11. يقوم فريق العمل IEEE 802.11 (TGi) حاليا بتطوير هذه التحسينات. يوفر إطار عمل 802.1X طبقة الارتباط بمصادقة موسعة، والتي لا ترى عادة إلا في الطبقات العليا.

س - ما هي الكيانات الثلاثة التي يحددها إطار عمل 802.1x؟

ج. يتطلب إطار عمل 802.1x من هذه الكيانات المنطقية الثلاثة التحقق من صحة الأجهزة الموجودة على شبكة WLAN.

1. **المستدعي**— **يقع** الملقم على عميل شبكة LAN اللاسلكية، ويعرف أيضا باسم عميل EAP.
2. **المصدق**— يوجد المصدق على نقطة الوصول.
3. **خادم المصادقة**— يتواجد خادم المصادقة على خادم RADIUS.

س. كيف تحدث مصادقة العميل اللاسلكي عند إستخدام إطار مصادقة 802.1x؟

أ. عندما يصبح العميل اللاسلكي (عميل EAP) نشطا، يصادق العميل اللاسلكي إما بمصادقة مفتوحة أو مشتركة. يعمل 802.1x بمصادقة مفتوحة ويبدأ بعد أن يرتبط العميل بنجاح بنقطة الوصول. يمكن أن تتصل محطة العميل، ولكن يمكن أن تمر حركة مرور البيانات فقط بعد مصادقة 802.1x الناجحة. فيما يلي الخطوات الواردة في مصادقة 802.1x:

1. تطلب نقطة الوصول (المصدق) التي تم تكوينها ل 802.1x معرف المستخدم من العميل.
2. ويستجيب الزبائن بهويته في غضون فترة زمنية محددة.
3. يقوم الخادم بالتحقق من هوية المستخدم ويبدأ المصادقة مع العميل إذا كانت هوية المستخدم موجودة في قاعدة بياناته.
4. يرسل الخادم رسالة نجاح إلى نقطة الوصول.
5. بمجرد مصادقة العميل، يقوم الخادم بإعادة توجيه مفتاح التشفير إلى نقطة الوصول (AP) التي يتم إستخدامها لتشفير/فك تشفير حركة مرور البيانات المرسلة من العميل وإليه.
6. في الخطوة 4، إذا لم تكن هوية المستخدم موجودة في قاعدة البيانات، يقوم الخادم بإسقاط المصادقة وإرسال رسالة فشل إلى نقطة الوصول.
7. تقوم نقطة الوصول بإعادة توجيه هذه الرسالة إلى العميل، ويجب أن يقوم العميل بالمصادقة مرة أخرى باستخدام بيانات الاعتماد الصحيحة.

ملاحظة: خلال مصادقة 802.1x ، تقوم نقطة الوصول بإعادة توجيه رسائل المصادقة من وإلى العميل.

س. ما هي متغيرات EAP المختلفة التي يمكنني إستخدامها مع إطار مصادقة 802.1x؟

ج. يحدد معيار 802.1x إجراء مصادقة العملاء. يحدد نوع EAP المستخدم في إطار عمل 802.1x نوع بيانات الاعتماد

وطريقة المصادقة المستخدمة في تبادل 802.1x. يمكن لإطار عمل 802.1x إستخدام أي من متغيرات EAP هذه:

- EAP-TLS—بروتوكول المصادقة المتوسع تأمين طبقة النقل
- مصادقة EAP—EAP-FAST المرنة عبر نفق آمن
- وحدة تعريف مشترك EAP—EAP-SIM
- بروتوكول المصادقة القابل للتوسع الخفيف الوزن من Cisco LEAP
- بروتوكول المصادقة المتوسع EAP—EAP-PEAP المحمي
- خوارزمية EAP-Message Digest 5—EAP-MD5
- كلمة مرور EAP—EAP-OTP في الوقت المحدد
- EAP-TTLS — أمان طبقة النقل النفقي ل EAP

س. كيف أختار طريقة EAP 802.1x من المتغيرات المختلفة المتوفرة؟

أ. أهم عامل يجب مراعاته هو ما إذا كان أسلوب EAP متوافقا مع الشبكة الموجودة أم لا. وبالإضافة إلى ذلك، توصي Cisco باختيار طريقة تدعم المصادقة المتبادلة.

س. ما هي مصادقة EAP المحلية؟

أ. EAP المحلي هي آلية يعمل فيها عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كخادم مصادقة. يتم تخزين بيانات اعتماد المستخدم محليا على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة العملاء اللاسلكيين، والذي يعمل كعملية توصيل خلفي في المكاتب البعيدة عند تعطل الخادم. يمكن إسترداد بيانات اعتماد المستخدم إما من قاعدة البيانات المحلية على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) أو من خادم LDAP خارجي. LEAP و EAP-FAST و EAP-TLS و PEAPv0/MSCHAPv2 و PEAPv1/GTC هي مصادقات EAP مختلفة مدعومة من قبل EAP المحلي.

س. ما هي Cisco LEAP؟

أ. بروتوكول المصادقة المتوسع الخفيف الوزن (LEAP) هو طريقة مصادقة خاصة من Cisco. Cisco LEAP هو نوع مصادقة 802.1X للشبكات المحلية اللاسلكية (WLANs). يدعم LEAP من Cisco المصادقة المتبادلة القوية بين العميل وخادم RADIUS من خلال كلمة مرور تسجيل دخول كالسر المشترك. يوفر Cisco LEAP مفاتيح تشفير ديناميكية لكل مستخدم ولكل جلسة. تعد LEAP الطريقة الأقل تعقيدا لنشر الإصدار 802.1x، وتتطلب خادم RADIUS فقط. ارجع إلى Cisco LEAP للحصول على معلومات عن LEAP.

س - كيف يعمل EAP-FAST ؟

ألف - يستخدم EAP-FAST خوارزميات مفاتيح متماثلة لتحقيق عملية مصادقة عبر قنوات. يعتمد إنشاء النفق على مسوغات الوصول المحمي (PAC) التي يمكن تزويد EAP-FAST وإدارتها ديناميكيا بواسطة EAP-FAST من خلال خادم المصادقة والتفويض والمحاسبة (AAA) (مثل خادم التحكم بالوصول الآمن من Cisco [ACS] الإصدار 3.2.3). باستخدام نفق تتم مصادقته بشكل متبادل، يوفر EAP-FAST الحماية من هجمات القاموس ومكامن الضعف التي يتعرض لها الدخيل. فيما يلي مراحل EAP-FAST:

لا يعمل EAP-FAST على تخفيف المخاطر الناجمة عن هجمات القاموس السلبية والهجمات التي يشنها الدخيل فحسب، بل يعمل أيضا على تمكين المصادقة الآمنة استنادا إلى البنية الأساسية المنشورة حاليا.

- المرحلة 1: إنشاء خادم النفق المصدق عليه بشكل متبادل - يستخدم خادم المصادقة والتفويض والمحاسبة (AAA) مسوغات الوصول المحمي (PAC) لمصادقة بعضهم البعض وإنشاء نفق آمن.
- المرحلة 2: إجراء مصادقة العميل في النفق المنشأ - يرسل العميل اسم المستخدم وكلمة المرور للمصادقة وإنشاء سياسة تفويض العميل.
- وبشكل إختياري، غالبا ما تستخدم مصادقة المرحلة 0—EAP-FAST هذه المرحلة لتمكين العميل من أن يتم

إمداده ديناميكيا بمسوغ وصول محمي. تقوم هذه المرحلة بإنشاء بيانات اعتماد وصول لكل مستخدم بشكل آمن بين المستخدم والشبكة. تستخدم المرحلة الأولى من المصادقة بيانات الاعتماد هذه لكل مستخدم، المعروفة باسم مسوغات الوصول المحمي (PAC).
راجع Cisco EAP-FAST للحصول على مزيد من المعلومات.

س. هل هناك وثائق على cisco.com تشرح كيفية تكوين EAP في شبكة Cisco WLAN؟

أ. راجع مصادقة EAP مع خادم RADIUS للحصول على معلومات حول كيفية تكوين مصادقة EAP في شبكة WLAN.

ارجع إلى ملاحظة تطبيق EAP المحمي للحصول على معلومات حول كيفية تكوين مصادقة PEAP.

ارجع إلى مصادقة LEAP مع خادم RADIUS محلي للحصول على معلومات حول كيفية تكوين مصادقة LEAP.

س. ما هي آليات التشفير المختلفة الأكثر إستخداما في الشبكات اللاسلكية؟

أ. فيما يلي أنظمة التشفير الأكثر إستخداما في الشبكات اللاسلكية:

- WEP
- تكيب
- AES

AES هو طريقة تشفير الأجهزة، بينما تتم معالجة تشفير WEP و TKIP على البرامج الثابتة. باستخدام أجهزة WEP لترقية البرامج الثابتة يمكن أن تدعم TKIP بحيث تكون قابلة للتشغيل البيني. تعد AES الطريقة الأكثر أمانا وأسرع، في حين أن WEP هو الأقل أمانا.

ما هو تشفير WEP؟

أ. WEP يعني الخصوصية المكافئة للتوصيل السلكي. يستخدم WEP لتشفير إشارات البيانات التي تنقل بين أجهزة WLAN وفك تشفيرها. WEP هو ميزة IEEE 802.11 إختيارية تمنع الإفصاح عن الحزم أثناء النقل وتعديلها وتوفر أيضا التحكم في الوصول لاستخدام الشبكة. يجعل WEP إرتباط WLAN آمنا مثل إرتباط سلكي. وكما يحدد المقياس، يستخدم WEP خوارزمية RC4 بمفتاح 40-بت أو 104-بت. RC4 هو خوارزمية متماثلة لأن RC4 يستخدم المفتاح نفسه لتشفير البيانات وفك تشفيرها. لدى تمكين WEP يحتوي كل "محطة" راديو على مفتاح. يستخدم المفتاح لخردة البيانات قبل إرسال البيانات عبر موجات الهواء. إذا تلقت محطة حزمة لم يتم تشتيتها باستخدام المفتاح المناسب، فإن المحطة تتجاهل الحزمة ولا تسلم أبدا مثل هذه الحزمة إلى المضيف.

راجع تكوين الخصوصية المكافئة للتوصيل السلكي (WEP) للحصول على معلومات حول كيفية تكوين WEP.

س. ما هو تدوير مفتاح البث؟ ما هو تردد دوران مفتاح البث؟

أ. يسمح تدوير مفتاح البث لنقطة الوصول بإنشاء أفضل مفتاح مجموعة عشوائي ممكن. يعمل تدوير مفتاح البث دوريا على تحديث جميع العملاء القادرين على إدارة المفاتيح. عند تمكين تدوير مفتاح WEP للبث، توفر نقطة الوصول مفتاح WEP للبث الديناميكي وتقوم بتغيير المفتاح في الفاصل الزمني الذي قمت بتعيينه. يعد تدوير مفتاح البث بديلا ممتازا ل TKIP إذا كانت الشبكة المحلية اللاسلكية الخاصة بك تدعم أجهزة أو أجهزة عميلة لاسلكية غير تابعة ل Cisco لا يمكنك ترقيتها إلى أحدث برنامج ثابت لأجهزة عميل Cisco. راجع تمكين تدوير مفتاح البث وتعطيله للحصول على معلومات حول كيفية تكوين ميزة تدوير مفتاح البث.

س. ما هو TKIP؟

ألف - TKIP هو بروتوكول سلامة المفاتيح المؤقتة. تم إدخال TKIP لمعالجة أوجه القصور في تشفير WEP. يعرف

TKIP أيضا بتجزئة مفتاح WEP وكان يطلق عليه في البداية WEP2. TKIP هو حل مؤقت يعمل على إصلاح مشكلة إعادة إستخدام مفتاح WEPs. يستخدم TKIP خوارزمية RC4 لإجراء التشفير، والتي هي نفسها WEP. هناك فرق رئيسي عن WEP وهو أن TKIP يغير المفتاح المؤقت كل حزمة. يغير المفتاح المؤقت كل حزمة لأن قيمة التجزئة لكل حزمة تتغير.

س. هل يمكن للأجهزة التي تستخدم TKIP أن تعمل مع الأجهزة التي تستخدم تشفير WEP؟

ألف - من المزايا التي تتمتع بها TKIP أن شبكات WLAN مع نقاط الوصول وأجهزة الراديو القائمة على WEP يمكنها الترقية إلى TKIP من خلال برامج تصحيح بسيطة للبرامج الثابتة. كما أن أجهزة WEP فقط لا تزال تعمل مع الأجهزة التي تدعم TKIP والتي تستخدم WEP.

س. ما هو فحص تكامل الرسائل (MIC)؟

ألف - يمثل الميكروفون تحسينا آخر لمعالجة أوجه الضعف في تشفير WEP. يمنع MIC هجمات قلب البت على الحزم المشفرة. وأثناء هجوم قلب البت، يعترض الدخيل رسالة مشفرة، ويغير الرسالة ثم يرسل الرسالة التي تم تعديلها. لا يعرف المستقبل أن الرسالة فاسدة وليست شرعية. لمعالجة هذه المشكلة، تضيف ميزة MIC حقل MIC إلى الإطار اللاسلكي. يوفر مجال MIC فحصا لسلامة الإطارات غير معرض لنفس أوجه القصور الرياضية مثل ICV. كما يضيف MIC حقلا للرقم التسلسلي إلى الإطار اللاسلكي. تسقط نقطة الوصول الإطارات المستلمة بدون ترتيب.

س. ما هي WPA؟ كيف يختلف WPA 2 عن WPA؟

ألف - WPA هو حل تأمين قائم على المعايير من تحالف Wi-Fi يعالج مواطن الضعف في شبكات WLAN الأصلية. يوفر WPA حماية محسنة للبيانات والتحكم في الوصول لأنظمة WLAN. يعالج WPA كل نقاط الضعف المعروفة المتعلقة بالخصوصية المكافئة للتوصيل السلكي (WEP) في تنفيذ تأمين IEEE 802.11 الأصلي ويقدم حل أمان فوري لشبكات WLAN في بيئات كل من المؤسسات والمكاتب الصغيرة والمكاتب المنزلية (SOHO).

يمثل WPA2 الجيل التالي من تأمين Wi-Fi. WPA2 هو التطبيق البيني لتحالف Wi-Fi لمقياس IEEE 802.11i المصدق عليه. يطبق WPA2 خوارزمية التشفير المتقدمة (AES) التي يوصى بها المعهد الوطني للمعايير والتكنولوجيا باستخدام وضع العداد مع بروتوكول مصادقة رسائل ربط التشفير (CCMP). يعد وضع عداد AES تشفير كتل يقوم بتشفير كتل بيانات 128 بت في كل مرة باستخدام مفتاح تشفير 128 بت. يقدم WPA2 مستوى تأمين أعلى من WPA. ينشئ WPA2 مفاتيح جلسات جديدة على كل اقتران. تكون مفاتيح التشفير التي يستخدمها WPA2 لكل عميل على الشبكة فريدة ومحددة لذلك العميل. وفي نهاية المطاف، يتم تشفير كل حزمة يتم إرسالها عبر الهواء باستخدام مفتاح فريد.

يمكن لكل من WPA1 و WPA2 إستخدام تشفير TKIP أو CCMP. (صحيح أن بعض نقاط الوصول وبعض العملاء يقيدون التركيبات، لكن هناك أربع تركيبات ممكنة). يكمن الفرق بين WPA1 و WPA2 في عناصر المعلومات التي يتم وضعها في المنارات وإطارات الاقتران وإطارات المصافحة الرباعية الإتجاه. البيانات في عناصر المعلومات هذه هي نفسها بشكل أساسي، لكن المعرف المستخدم مختلف. يكمن الاختلاف الرئيسي في مصافحة المفتاح في أن WPA2 يتضمن مفتاح المجموعة الأولي في المصافحة الرباعية الإتجاه ويتم تخطي مصافحة مفتاح المجموعة الأولى، بينما يحتاج WPA إلى القيام بهذه المصافحة الإضافية لتسليم مفاتيح المجموعة الأولية. تحدث عملية إعادة إدخال مفتاح المجموعة بنفس الطريقة. تحدث المصافحة قبل تحديد مجموعة التشفير (TKIP أو AES) واستخدامها لإرسال مخططات بيانات المستخدم. أثناء مصافحة WPA1 أو WPA2، يتم تحديد مجموعة التشفير المراد إستخدامها. بمجرد تحديده، يتم إستخدام مجموعة التشفير لكل حركة مرور المستخدم. وهكذا فإن WPA1 بالإضافة إلى AES ليست WPA2. يسمح WPA1 (لكن غالبا ما يكون جانب العميل محدودا) إما بشفرة TKIP أو AES.

س. ما هو AES؟

A. AES هو معيار التشفير المتقدم. يوفر معيار التشفير المتطور تشفيرا أقوى بكثير. يستخدم AES خوارزمية Rijndael، والتي هي تشفير كتل مزود بدعم رئيسي من 128 و 192 و 256 بت وهي أقوى بكثير من RC4. بالنسبة لأجهزة WLAN لدعم AES، يجب أن يدعم الجهاز AES بدلا من WEP.

س. ما طرق المصادقة التي يدعمها خادم خدمة مصادقة إنترنت (IAS) من Microsoft؟

ألف - يدعم المعيار الدولي للمحاسبة بروتوكولات المصادقة التالية:

- بروتوكول مصادقة كلمة المرور (PAP)
- بروتوكول مصادقة كلمة مرور Shiva (SPAP)
- بروتوكول مصادقة مصافحة الاستيبان (CHAP)
- بروتوكول مصادقة مصافحة الاستيبان ل Microsoft (MS-CHAP)
- بروتوكول مصادقة مصافحة الاستيبان الخاص ب Microsoft الإصدار 2 (MS-CHAP v2)
- بروتوكول المصادقة المتوسع-الرسالة CHAP (EAP-MD5 CHAP) (Digest 5 CHAP)
- أمان طبقة النقل-EAP (EAP-TLS)
- PEAP-MS-CHAP v2) EAP-MS-CHAP v2) (يعرف أيضا ب PEAPv0/EAP-MSCHAPv2) المحمي

يدعم IAS PEAP-TLS في Windows 2000 Server PEAP-MS-CHAP v2 و PEAP-TLS عند تثبيت Windows 2000 Server Service Pack 4. لمزيد من المعلومات، ارجع إلى طرق المصادقة للاستخدام مع IAS .

س. كيف يتم تنفيذ VPN في بيئة لاسلكية؟

ألف - الشبكة الخاصة الظاهرية (VPN) هي آلية أمان من الطبقة الثالثة؛ وتنفذ آليات التشفير اللاسلكي في الطبقة 2. VPN منفذ على 802. 1x و EAP و WEP و TKIP و AES. عند وجود آلية من الطبقة 2، تضيف الشبكة الخاصة الظاهرية (VPN) عبئا إضافيا إلى التنفيذ. في أماكن مثل النقاط الساخنة العامة والفنادق حيث لا يتم تطبيق إجراءات أمنية، يمكن أن تكون شبكة خاصة ظاهرية حلا مفيدا لتنفيذها.

الأسئلة المتداولة حول أستكشاف الأخطاء وإصلاحها والتصميم

س. هل هناك أي أفضل الممارسات لنشر الأمان اللاسلكي في شبكة محلية لاسلكية خارجية؟

أ. راجع أفضل الممارسات لأمان الشبكات اللاسلكية الخارجية. يقدم هذا المستند معلومات حول أفضل ممارسات الأمان لنشر شبكة محلية لاسلكية خارجية.

س. هل يمكنني إستخدام خادم Windows 2000 أو 2003 مع خدمة Active Directory لخادم RADIUS لمصادقة عملاء اللاسلكي؟

أ. يمكن لخادم Windows 2000 أو 2003 المزود بدليل نشط العمل كخادم RADIUS. للحصول على معلومات حول كيفية تكوين خادم RADIUS هذا، يلزمك الاتصال ب Microsoft، لأن Cisco لا تدعم تكوين خادم Windows.

س - موقعي على وشك الانتقال من شبكة لاسلكية مفتوحة (نقاط وصول من السلسلة 350 و 1200) إلى شبكة PEAP. أود أن يعمل كل من SSID المفتوح (SSID مكون للمصادقة المفتوحة) و PEAP SSID (SSID مكون لمصادقة PEAP) على نفس AP في نفس الوقت. وهذا يتيح لنا الوقت لترحيل العملاء إلى PEAP SSID. هل توجد طريقة لاستضافة SSID مفتوح و PEAP SSID في نفس نقطة الوصول في نفس الوقت؟

a. تدعم نقاط الوصول من Cisco شبكات VLAN (الطبقة 2 فقط). هذه هي الطريقة الوحيدة لتحقيق ما تريد القيام به. أنت تحتاج أن يخلق إثنان VLANs، (أهلي طبيعي وأنت آخر VLAN). ثم يمكنك الحصول على مفتاح WEP لأحدهما ولا يوجد مفتاح WEP لآخر. بهذه الطريقة، يمكنك تكوين إحدى شبكات VLAN للمصادقة المفتوحة وشبكة VLAN الأخرى لمصادقة PEAP. أحلت بستعمل VLANs مع cisco Aironet جهاز لاسلكي إن يريد أنت أن يفهم كيف أن يشكل VLANs.

يرجى ملاحظة أنك بحاجة إلى تكوين محولاتك للنقطة1Q وللتوجيه بين شبكات VLAN، أو محول L3 أو الموجه

الخاص بك.

q. أريد إعداد نقطة الوصول VxWorks 1200 من Cisco لتمكين المستخدمين اللاسلكيين من المصادقة على مركز Cisco 3005 VPN. ما هو التكوين الذي يلزم وجوده على نقطة الوصول والعملاء لتحقيق ذلك؟

أ. لا يوجد تشكيل خاص ضروري على ال ap أو الزبون لهذا سيناريو. يجب عليك تنفيذ جميع التكوينات على مركز الشبكة الخاصة الظاهرية (VPN).

Q. أنا ينشر cisco 1232 AG ap. أود أن أعرف الطريقة الأكثر أمانا التي يمكنني نشرها مع نقطة الوصول هذه. ليس لدي خادم AAA وموارد الوحيدة هي AP ومجال Windows 2003. أنا على دراية بكيفية إستخدام مفاتيح WEPs الثابتة ذات 128 بت، وقيود عناوين SSID و MAC التي لا تستخدم للبث. يعمل المستخدمون غالبا مع محطات عمل Windows XP وبعض أجهزة PDA. ما هو التنفيذ الأكثر أمانا لهذا الإعداد؟

a. إذا لم يكن لديك خادم RADIUS مثل Cisco ACS، فيمكنك تكوين نقطة الوصول كخادم RADIUS محلي لمصادقة LEAP أو EAP-FAST أو MAC.

ملاحظة: ثمة نقطة هامة جدا يجب مراعاتها وهي ما إذا كنت تريد إستخدام عملائك مع LEAP أو EAP-FAST. إذا كان الأمر كذلك، فيجب أن يكون لدى عملائك أداة لدعم LEAP أو EAP-FAST. لا تدعم الأداة المساعدة Windows XP إلا PEAP أو EAP-TLS.

q. تفشل مصادقة PEAP مع حدوث الخطأ "فشل مصادقة EAP-TLS أو PEAP أثناء مصافحة SSL". لماذا؟

a. هذا خطأ يستطيع وقعت واجب إلى cisco بق CSCee06008 id (يسجل **زبون فقط**) . يفشل PEAP مع ADU 1.2.0.4. الحل البديل لهذه المشكلة هو إستخدام أحدث إصدار من ADU.

س. هل يمكنني الحصول على مصادقة WPA و MAC محلية على نفس SSID؟

أ. لا تدعم نقطة الوصول من Cisco مصادقة MAC المحلية ومفتاح المشاركة المسبقة للوصول المحمي ل Wi-Fi (WPA-PSK)) في معرف مجموعة الخدمة (SSID) نفسه. عند تمكين مصادقة MAC المحلية باستخدام WPA-PSK، لا يعمل WPA-PSK. تحدث هذه المشكلة لأن مصادقة MAC المحلية تزيل خط كلمة مرور WPA-PSK ASCII من التكوين.

q. لدينا حاليا ثلاثة نقاط وصول لاسلكية Cisco 1231 مع تشفير WEP 128-بت لشبكة VLAN الخاصة ببياناتنا. لا نبث SSID. لا يوجد لدينا خادم RADIUS منفصل في بيئتنا. تمكن أحدهم من تحديد مفتاح WEP من خلال أداة المسح الضوئي، واستخدم الأداة لمدة أسبوعين لمراقبة حركة المرور اللاسلكية. كيف يمكننا منع هذا الأمر وجعل الشبكة آمنة؟

أ. يكون WEP الثابت عرضة لهذه المشكلة، ويمكن اشتقاقه إذا قام قراصنة الإنترنت بتجميع حزم كافية وكان قادرا على الحصول على حزمتين أو أكثر بنفس متجه التهيئة (IV).

هناك عدة طرق لمنع حدوث هذا إصدار:

1. إستخدام مفاتيح WEP الديناميكية.
2. إستخدام WPA.
3. إن يتلقى أنت فقط cisco مهايئات، مكنت لكل ربط مفتاح و mic.

س. إذا كانت لدي شبكتي WLAN مختلفتين، وكلتاهما تم تكوينهما لمفتاح Wi-Fi Protected Access (WPA) - المشترك مسبقا (PSK)، هل يمكن أن تكون المفاتيح المشتركة مسبقا مختلفة لكل شبكة WLAN؟ إذا كانت مختلفة، هل تؤثر على شبكة WLAN الأخرى التي تم تكوينها باستخدام مفتاح مشترك مسبقا مختلف؟

ألف - ينبغي أن يكون إعداد WPA-PSK لكل شبكة محلية لاسلكية (WLAN). إذا قمت بتغيير أحد WPA-PSK، فيجب ألا يؤثر على شبكة WLAN الأخرى التي تم تكوينها.

س. في بيئتي أستخدم في الغالب Intel PRO/Wireless، وبروتوكول المصادقة المتوسع - المصادقة المرنة عبر الاتصال النفقي الآمن (EAP-FAST)، و Cisco Secure Access Server 3.3 (ACS) المرتبط بحسابات Windows Active Directory (AD). المشكلة هي عندما تكون كلمة مرور المستخدم على وشك الانتهاء، لا يقوم Windows بمطالبة المستخدم بتغيير كلمة المرور. في نهاية المطاف، ينتهي الحساب. هل يوجد حل لجعل Windows يطلب من المستخدم تغيير كلمة المرور؟

أ. تتيح لك ميزة "تأمين كلمة مرور ACS" الخاصة ب Cisco إمكانية إجبار المستخدمين على تغيير كلمات المرور الخاصة بهم تحت شرط واحد أو أكثر من هذه الشروط:

- بعد عدد محدد من الأيام (قواعد العمر حسب التاريخ)
- بعد عدد محدد من عمليات تسجيل الدخول (قواعد العمر حسب الاستخدام)
- أول مرة يقوم مستخدم جديد بتسجيل الدخول (قاعدة تغيير كلمة المرور)

أحلت لتفاصيل على كيف أن يشكل cisco يأمن ACS ل هذا سمة، يمكن كلمة شيخوخة ل ال cisco يأمن مستعمل قاعدة معطيات.

Q. عند تسجيل دخول المستخدم لاسلكيا باستخدام LEAP، فإنه يحصل على نصوص تسجيل الدخول لرسم خريطة لمحركات أقراص الشبكة. ومع ذلك، فباستخدام WPA (Wi-Fi Protected Access) أو WPA2 مع مصادقة PEAP، لا يتم تشغيل البرامج النصية لتسجيل الدخول. يكون كل من العميل ونقطة الوصول من Cisco كما هو ACS (RADIUS). لماذا لا يتم تشغيل برنامج نصي تسجيل الدخول على ACS (RADIUS)؟

أ. مصادقة الجهاز إلزامية لعمل برامج تسجيل الدخول النصية. يتيح هذا للمستخدمين اللاسلكيين اكتساب حق الوصول إلى الشبكة لتحميل البرامج النصية قبل تسجيل دخول المستخدم.

للحصول على معلومات حول كيفية تكوين مصادقة الجهاز باستخدام PEAP-MS-CHAPv2، راجع تكوين ACS الآمن من Cisco ل Windows v3.2 باستخدام مصادقة جهاز PEAP-MS-CHAPv2.

q. باستخدام الإصدار 3.0 من Cisco Aironet Desktop Utility (ADU)، عندما يقوم المستخدم بتكوين مصادقة الجهاز لبروتوكول المصادقة المتوسع - أمان طبقة النقل (EAP-TLS)، لا تسمح وحدة التحكم المتقدمة للمستخدم بإنشاء ملف تعريف. لماذا؟

a. هذا بسبب cisco بق CSCsg32032 id (يسجل زبون فقط). قد يحدث هذا إذا كان الكمبيوتر العميل مثبتا عليه شهادة الجهاز وليس به شهادة مستخدم.

الحل البديل هو نسخ شهادة الجهاز إلى مخزن المستخدم وإنشاء توصيف EAP-TLS ثم إزالة الشهادة من مخزن المستخدم لتكوين مصادقة الجهاز فقط.

س. هل هناك أي طريقة لتخصيص VLAN على شبكة LAN اللاسلكية استنادا إلى عنوان MAC الخاص بالعميل؟

أ. لا. هذا غير ممكن. يعمل تعيين شبكة VLAN من خادم RADIUS فقط مع 802.1x، وليس بمصادقة MAC. يمكنك إستخدام RADIUS لدفع VSAs مع مصادقة MAC، إذا تمت مصادقة عناوين MAC في خادم RADIUS (المعرف بمعرف المستخدم/كلمة المرور في LEAP/PEAP).

معلومات ذات صلة

- أمان الشبكة اللاسلكية
- التقرير الرسمي لأمان شبكة LAN اللاسلكية
- نظرة عامة على أمان شبكة LAN اللاسلكية
- دليل نشر EAP-TLS لشبكات LAN اللاسلكية
- Cisco LEAP
- تكوين الخصوصية المكافئة للتوصيل السلكي (WEP)
- دعم المنتج اللاسلكي
- الدعم التقني والمستندات - Cisco Systems

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).