مثال تكوين عميل L2TP-IPSec Android و ASA الأصلي

المحتويات

المقدمة

يوفر بروتوكول الاتصال النفقي للطبقة 2 (L2TP) عبر IPSec إمكانية نشر حل VPN L2TP وإدارته إلى جانب خدمات الشبكة الخاصة الظاهرية (VPN) عبر IPSec وجدار الحماية في نظام أساسي واحد. تتمثل الميزة الأساسية لتكوين بروتوكول L2TP عبر IPSec في سيناريو الوصول عن بعد في أنه يمكن للمستخدمين عن بعد الوصول إلى شبكة VPN عبر شبكة IP عامة دون الحاجة إلى بوابة أو خط مخصص، مما يتيح الوصول عن بعد من أي مكان تقريبا مزود بخدمة هاتف قديمة عادية (POTS). فائدة إضافية هي أن متطلبات العميل الوحيدة للوصول إلى شبكة VPN هي إستخدام Windows مع شبكة الطلب الهاتفي من Microsoft (DUN). لا يتطلب برامج عميل إضافية، مثل برنامج عميل Cisco VPN.

يقدم هذا المستند نموذجا لتكوين عميل L2TP/IPSec Android الأصلي. وهو يأخذك من خلال جميع الأوامر الضرورية المطلوبة على جهاز الأمان القابل للتكيف (ASA) من Cisco، بالإضافة إلى الخطوات التي يجب إتخاذها على جهاز Android نفسه.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- يتطلب Android L2TP/IPSec إصدار برنامج Cisco ASA الإصدار 8.2.5 أو إصدار أحدث، الإصدار 8.3.2.12 أو إصدار أحدث، أو الإصدار 8.4.1 أو إصدار أحدث.
- يدعم ASA دعم توقيع شهادة خوارزمية التجزئة الآمنة 2 (SHA2) لعملاء Microsoft Windows 7 و Android-native VPN عند إستخدام بروتوكول L2TP/IPSec.
- راجع دليل تكوين السلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6: تكوين L2TP عبر IPSec: متطلبات الترخيص ل L2TP عبر IPSec.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

يصف هذا القسم المعلومات التي قد يحتاج إليها لتكوين الميزات الموضحة في هذا المستند.

تكوين اتصال L2TP/IPSec على Android

يوضح هذا الإجراء كيفية تكوين اتصال L2TP/IPSec على Android:

1. افتح القائمة، واختر **الإعدادات**.
2. أختر **لاسلكي وشبكة** أو **عناصر تحكم لاسلكية**. يعتمد الخيار المتوفر على إصدار Android الخاص بك.
3. أختر **VPN عملية إعداد**.
4. أختر **يضيف VPN**.
5. أختر **يضيف L2TP/IPsec PSK VPN**.
6. أختر **VPN إسم**، ودخلت وصفي إسم.
7. أختر **مجموعة VPN نادل**، ودخلت اسم وصفي.
8. أختر **تعيين مفتاح IPSec المشارك مسبقا**.
9. قم بإلغاء تحديد **أمر تمكين سر L2TP**.
10. [إختياري] قم بتعيين معرف IPSec كاسم مجموعة نفق ASA. لا يوجد إعداد يعني أنه سيقع في DefaultRAGgroup على ASA.
11. افتح القائمة، واختر **حفظ**.

تكوين اتصال L2TP/IPSec على ASA

هذه هي إعدادات نهج ASA Internet Key Exchange الإصدار 1 (IKEv1) (اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح [ISAKMP]) المطلوبة التي تسمح لعملاء VPN الأصليين، المدمجين مع نظام التشغيل على نقطة نهاية، بإجراء اتصال VPN إلى ASA عند إستخدام L2TP عبر بروتوكول IPSec:

- المرحلة 1 من IKEv1 - تشفير معيار تشفير البيانات الثلاثي (3DES) باستخدام طريقة تجزئة SHA1
- المرحلة 2 من IPSec - تشفير معيار 3DES أو التشفير المتقدم (AES) باستخدام طريقة تجزئة الرسالة Digest 5 (MD5) أو SHA
- مصادقة PPP - بروتوكول مصادقة كلمة المرور (PAP) أو بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي ل Microsoft الإصدار 1 (MS-CHAPv1) أو MS-CHAPv2 (مفضل)

- مفتاح مشترك مسبقا

ملاحظة: يدعم ASA فقط مصادقة PPP و MS-CHAP (الإصدارين 1 و 2) على قاعدة البيانات المحلية. يتم تنفيذ بروتوكول المصادقة المتوسع (EAP) و CHAP بواسطة خوادم مصادقة الوكيل. لذلك، إذا كان المستخدم البعيد ينتمي إلى مجموعة نفق تم تكوينها باستخدام أوامر **المصادقة eap-proxy** أو **المصادقة chap** وإذا تم تكوين ASA لاستخدام قاعدة البيانات المحلية، فلن يتمكن ذلك المستخدم من الاتصال.

علاوة على ذلك، لا يدعم Android بروتوكول PAP، ولأن بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP) لا يدعم MS-CHAP، فإن LDAP لا يعد آلية مصادقة قابلة للتطبيق. الحل الوحيد هو إستخدام RADIUS. راجع "L2TP، CSCtw58945 Cisco Bug ID عبر إتصالات IPSec يفشل مع تفويض LDAP و MSCHAPV2،" للحصول على مزيد من التفاصيل حول المشاكل مع MS-CHAP و LDAP.

يوضح هذا الإجراء كيفية تكوين اتصال L2TP/IPSec على ASA:

1. قم بتحديد تجمع عناوين محلي أو أستخدم خادم DHCP لجهاز الأمان القابل للتكيف لتخصيص عناوين IP للعملاء لنهج المجموعة.
2. إنشاء نهج مجموعة داخلي. قم بتحديد بروتوكول النفق ليكون l2tp-ipsSec.قم بتكوين خادم اسم مجال (DNS) لاستخدامه من قبل العملاء.
3. إنشاء مجموعة نفق جديدة أو تعديل سمات DefaultRAGgroup الموجودة. (يمكن إستخدام مجموعة أنفاق جديدة إذا تم تعيين معرف IPSec كاسم مجموعة على الهاتف؛ راجع الخطوة 10 لتكوين الهاتف.)
4. قم بتعريف السمات العامة لمجموعة النفق المستخدمة. تعيين نهج المجموعة المعرف إلى مجموعة النفق هذه.قم بتعيين تجمع العناوين المحدد المطلوب إستخدامه بواسطة مجموعة النفق هذه.قم بتعديل مجموعة خادم المصادقة إذا كنت ترغب في إستخدام شيء آخر غير المحلي.
5. قم بتحديد المفتاح المشترك مسبقا ضمن سمات IPSec لمجموعة النفق التي سيتم إستخدامها.
6. قم بتعديل سمات PPP لمجموعة النفق المستخدمة بحيث يتم إستخدام CHAP و MS-CHAP-V1 و MS-CHAP-V2 فقط.
7. قم بإنشاء مجموعة تحويل باستخدام نوع تشفير حمولة أمان التضمين (ESP) ونوع المصادقة.
8. قم بتوجيه IPSec لاستخدام وضع النقل بدلا من وضع النفق.
9. تحديد سياسة ISAKMP/IKEv1 باستخدام تشفير 3DES باستخدام طريقة تجزئة SHA1.
10. إنشاء خريطة تشفير ديناميكية، وتخطيطها إلى خريطة تشفير.
11. تطبيق خريطة التشفير على واجهة.
12. قم بتمكين ISAKMP على هذه الواجهة.

أوامر ملف التكوين لتوافق ASA

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

يوضح هذا المثال أوامر ملف التكوين التي تضمن توافق ASA مع عميل VPN الأصلي على أي نظام تشغيل.

ASA 8.2.5 أو مثال تكوين أحدث

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
<dns-server value <dns_server
vpn-tunnel-protocol l2tp-ipsec
```

```
tunnel-group DefaultRAGroup general-attributes
default-group-policy l2tp-ipsec_policy
address-pool l2tp-ipsec_address
tunnel-group DefaultRAGroup ipsec-attributes
* pre-shared-key
tunnel-group DefaultRAGroup ppp-attributes
no authentication pap
authentication chap
authentication ms-chap-v1
authentication ms-chap-v2
crypto ipsec transform-set trans esp-3des esp-sha-hmac
crypto ipsec transform-set trans mode transport
crypto dynamic-map dyno 10 set transform-set set trans
crypto map vpn 65535 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto isakmp enable outside
crypto isakmp policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
```

ASA 8.3.2.12 أو مثال تكوين أحدث

```
Username <name> password <passwd> mschap
ip local pool l2tp-ipsec_address 192.168.1.1-192.168.1.10
group-policy l2tp-ipsec_policy internal
group-policy l2tp-ipsec_policy attributes
<dns-server value <dns_server
vpn-tunnel-protocol l2tp-ipsec
tunnel-group DefaultRAGroup general-attributes
default-group-policy l2tp-ipsec_policy
address-pool l2tp-ipsec_addresses
tunnel-group DefaultRAGroup ipsec-attributes
* pre-shared-key
tunnel-group DefaultRAGroup ppp-attributes
no authentication pap
authentication chap
authentication ms-chap-v1
authentication ms-chap-v2
crypto ipsec ikev1 transform-set my-transform-set-ikev1 esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set my-transform-set-ikev1 mode transport
crypto dynamic-map dyno 10 set ikev1 transform-set my-transform-set-ikev1
crypto map vpn 20 ipsec-isakmp dynamic dyno
crypto map vpn interface outside
crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

يوضح هذا الإجراء كيفية إعداد التوصيل:

1. افتح القائمة، واختر **الإعدادات**.
2. حدد **لاسلكي وشبكة** أو **عناصر تحكم لاسلكية**. (يعتمد الخيار المتوفر على إصدار Android الخاص بك.)
3. حدد تكوين شبكة VPN من القائمة.
4. أدخل اسم المستخدم وكلمة المرور الخاصين بك.
5. حدد **تذكر اسم المستخدم**.
6. حدد **اتصال**.

يوضح هذا الإجراء كيفية قطع الاتصال:

1. افتح القائمة، واختر **الإعدادات**.
2. حدد **لاسلكي وشبكة** أو **عناصر تحكم لاسلكية**. (يعتمد الخيار المتوفر على إصدار Android الخاص بك.)
3. حدد تكوين شبكة VPN من القائمة.
4. حدد **قطع الاتصال**.

أستخدم هذه الأوامر لتأكيد عمل الاتصال بشكل صحيح.

- **show run crypto isakmp** - ل ASA صيغة 8.2.5
- **show run crypto ikev1** - ل ASA صيغة 8.3.2.12 أو فيما بعد
- **show vpn-sessiondb ra-ikev1-ips** - ل ASA الإصدار 8.3.2.12 أو إصدار أحدث
- **show vpn-sessiondb remote** - ل ASA الإصدار 8.2.5

ملاحظة: تدعم أداة مترجم الإخراج (العملاء المسجلون فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

المحاذير المعروفة

- معرف تصحيح الأخطاء من "ASA Traceback"، CSCtq21535 عند الاتصال مع عميل Android "L2TP/IPsec"
- معرف تصحيح الأخطاء من Cisco CSCtj57256، "لا يتم إنشاء اتصال L2TP/IPSec من Android إلى ASA55xx"
- يفشل معرف تصحيح الأخطاء من "L2TP"، CSCtw58945 عبر إتصالات Cisco IPSec مع تفويض LDAP و "MSCHAPV2"

معلومات ذات صلة

- دليل تكوين سلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6: تكوين L2TP عبر IPsec
- ملاحظات الإصدار الخاصة بسلسلة Cisco ASA 5500، الإصدار 8.4(x)
- cisco ASA 5500 sery تشكيل مرشد يستعمل ال CLI، 8.3: معلومة حول NAT
- أمثلة تكوين ASA ما قبل 8.3 إلى 8.3 nat
- 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).