FlexVPN مع مثال تكوين التشفير من الجيل التالي

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين FlexVPN بين موجهات تدعم مجموعة خوارزميات تشفير الجيل التالي (NGE) من Cisco.

تشفير الجيل التالي

تقوم تشفير NGE من Cisco بتأمين المعلومات التي تنتقل عبر الشبكات التي تستخدم أربع خوارزميات تشفير صالحة للتكوين وراسخة وفي المجال العام:

- التشفير القائم على معيار التشفير المتقدم (AES)، والذي يستخدم مفاتيح 128-بت أو 256-بت
- التوقيعات الرقمية مع خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA) التي تستخدم المنحنيات مع معدل Prime 256-بت و 384-بت
- تبادل المفاتيح الذي يستخدم أسلوب المنحنى البيضاوي (Diffie-Hellman (ECDH
- التجزئة (بصمات الأصابع الرقمية) استنادا إلى خوارزمية التجزئة الآمنة 2 (SHA-2)

ذكرت "وكالة الأمن القومي" أن هذه الخوارزميات الأربعة توفر في مجموعها ضمانات كافية بالمعلومات السرية. تم نشر تشفير NSA Suite B ل IPsec كمقياس في RFC 6379 وقد اكتسب القبول في الصناعة.

Suite Suite-B-GCM-128

وفقا لمعيار RFC 6379، هذه الخوارزميات مطلوبة للمجموعة B-GCM-128.

توفر هذه المجموعة الحماية والسرية لسلامة حمولة الأمان (ESP) من خلال AES-GCM إصدار 128 بت (راجع RFC4106). يجب إستخدام هذه المجموعة عندما تكون هناك حاجة إلى حماية تكامل ESP وتشفيرها.

ESP
تشفير AES مع مفاتيح 128-بت وقيمة تحقق سلامة 16-نظام ثماني (ICV) في وضع العداد/الكالوس ((GCM) ((RFC4106
قيمة التكامل خالية

IKEv2
تشفير AES باستخدام مفاتيح 128-بت في وضع توصيل كتل التشفير (CBC) (RFC3602)
دالة عشوائية زائفة HMAC-SHA-256 (RFC4868)
Integrity HMAC-SHA-256-128 (RFC4868)
مجموعة Diffie-Hellman العشوائية ل ECP بنظام 256 بت (RFC5903)

يمكن العثور على مزيد من المعلومات حول Suite B و NGE في الجيل التالي من التشفير.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- FlexVPN
- تبادل مفتاح الإنترنت الإصدار 2 (IKEv2)
- IPsec

المكونات المستخدمة

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

- الأجهزة: موجهات الخدمات المتكاملة (ISR) الجيل 2 (G2) التي تشغل ترخيص الأمان.
- البرنامج: برنامج Cisco IOS® ، الإصدار 15.2.3T2. يمكن إستخدام أي إصدار من برنامج Cisco IOS الإصدار M أو 15.1.2T أو إصدار أحدث منذ تقديم GCM.

لمزيد من التفاصيل، راجع متصفح الميزات.

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

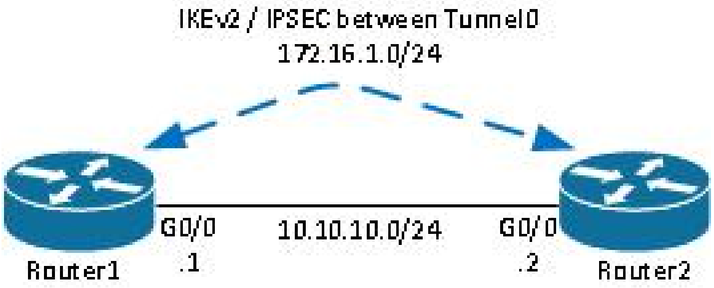
جهة منح الشهادة

حاليا، لا يدعم برنامج Cisco IOS خادم مرجع شهادة محلي (CA) يشغل ECDH، وهو مطلوب للمجموعة B. يجب تنفيذ خادم CA لجهة خارجية. يستخدم هذا المثال مرجع مصدق من Microsoft استنادا إلى PKI Suite B

التكوين

مخطط الشبكة

يستند هذا الدليل إلى هذه الطوبولوجيا المصورة. يجب تعديل عناوين IP لتناسب متطلباتك.



ملاحظات:

يتكون الإعداد من موجهين متصلين مباشرة، قد يتم فصلهما بواسطة العديد من الخطوات. إذا كان الأمر كذلك، فتأكد من وجود مسار للوصول إلى عنوان IP للنظير. ولا يوضح هذا التكوين إلا تفاصيل التشفير المستخدم. يجب تنفيذ توجيه IKEv2 أو بروتوكول توجيه عبر الشبكة الخاصة الظاهرية (VPN) ل IPSec.

الخطوات المطلوبة لتمكين الموجه من إستخدام خوارزمية التوقيع الرقمي للمنحنى البيضاوي

1. قم بإنشاء اسم المجال واسم المضيف، وهما متطلبان مسبقان لإنشاء زوج مفاتيح EC.

```
ip domain-name cisco.com
hostname Router1
crypto key generate ec keysize 256 label Router1.cisco.com
```

ملاحظة: إذا لم تقم بتشغيل إصدار باستخدام الإصلاح لمعرف تصحيح الأخطاء من Cisco [CSCue59994](#)، فلن يسمح الموجه لك بتسجيل شهادة ذات حجم مفتاح أقل من 768.

2. قم بإنشاء نقطة ثقة محلية للحصول على شهادة من المرجع المصدق.

```
crypto pki trustpoint ecdh
 enrollment terminal
 revocation-check none
 eckeypair Router1.cisco.com
```

ملاحظة: نظرا لأن المرجع المصدق كان غير متصل، فقد تم تعطيل عمليات التحقق من الإبطال. يجب تمكين فحوصات الإبطال للحد الأقصى من الأمان في بيئة إنتاج.

3. مصادقة TrustPoint (يحصل هذا على نسخة من شهادة CA التي تحتوي على المفتاح العام).

```
crypto pki authenticate ecdh
```

4. أدخل شهادة المرجع المصدق الأساسية 64 التي تم ترميزها عند المطالبة. أدخل **إنهاء** ثم أدخل **نعم** للقبول.

5. تسجيل الموجه في PKI على CA.

```
crypto pki enrol ecdh
```

6. يتم إستخدام الإخراج المعروض لإرسال طلب شهادة إلى المرجع المصدق. بالنسبة ل Microsoft CA، اتصل بواجهة ويب ل CA وحدد **إرسال طلب شهادة**.

7. إستيراد الشهادة المستلمة من المرجع المصدق إلى الموجه. أدخل **إنهاء** بمجرد إستيراد الشهادة.

```
crypto pki import ecdh certificate
```

التكوين

التكوين المزود هنا هو للموجه 1. يتطلب الموجه 2 نسخة مطابقة من التكوين حيث تكون عناوين IP فقط على واجهة النفق فريدة.

1. قم بإنشاء خريطة شهادات لمطابقة شهادة جهاز النظير.

```
crypto pki certificate map certmap 10
 subject-name co cisco.com
```

2. تكوين مقترح IKEv2 للمجموعة B.

```
crypto ikev2 proposal default
 encryption aes-cbc-128
 integrity sha256
 group 19
```

ملاحظة: تقوم الإعدادات الافتراضية الذكية ل IKEv2 بتنفيذ عدد من الخوارزميات المكونة مسبقا ضمن اقتراح IKEv2 الافتراضي. بما أن AES-CBC-128 و SHA256 مطلوبان للمجموعة Suite B-GCM-128، يجب إزالة AES-CBC-256 و SHA384 و SHA512 ضمن هذه الخوارزميات. والسبب وراء ذلك هو أن IKEv2 يختار أقوى خوارزمية عند عرضها مع خيار ما. للحصول على أقصى قدر من الأمان، أستخدم الطرازين AES-CBC-256 و SHA512. غير أن هذا غير مطلوب بالنسبة للمجموعة B-GCM-128. لعرض مقترح IKEv2 الذي تم تكوينه، أدخل أمر **show crypto ikev2 proposal**.

3. قم بتكوين ملف تعريف IKEv2 لمطابقة خريطة الشهادة واستخدام ECDSA مع TrustPoint المحدد مسبقا.

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ecdh
```

4. قم بتكوين تحويل IPSec لاستخدام GCM.

```
crypto ipsec transform-set ESP_GCM esp-gcm
```

```
mode transport
```

5. قم بتكوين ملف تعريف IPSec باستخدام المعلمات التي تم تكوينها سابقا.

```
crypto ipsec profile default
 set transform-set ESP_GCM
 set pfs group19
 set ikev2-profile default
```

6. قم بتكوين واجهة النفق.

```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel source Gigabit0/0 tunnel destination 10.10.10.2
 tunnel protection ipsec profile default
```

التحقق من الاتصال

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. تحقق من إنشاء مفاتيح ECDSA بنجاح.

```
Router1#show crypto key mypubkey ec
Key pair was generated at: 04:05:07 JST Jul 6 2012 %
Key name: Router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 .Key is not exportable
 ;Key Data&colon
 06072A86 48CE3D02 0106082A 8648CE3D 03010703 4200048F 2B0B5B5E 30593013
(...omitted...)
```

2. تحقق من إستيراد الشهادة بنجاح ومن إستخدام ECDH.

```
Router1#show crypto pki certificates verbose ecdh
Certificate
 Status: Available
 Version: 3
 Certificate Serial Number (hex): 6156E3D5000000000009
(...omitted...)
```

3. تحقق من إنشاء IKEv2 SA بنجاح واستخدم خوارزميات Suite B.

```
Router1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                  Remote                  fvrf/ivrf            Status
 none/none            READY         10.10.10.2/500         10.10.10.1/500         1
:Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: ECDSA, Auth verify
ECDSA
 Life/Active Time: 86400/20 sec
```

4. تحقق من إنشاء IKEv2 SA بنجاح واستخدم خوارزميات Suite B.

```
Router1#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

(...omitted...)

local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
(current outbound spi: 0xAC5845E1(2891466209
PFS (Y/N): N, DH group: none

:inbound esp sas
(spi: 0xAEF7FD9C(2935487900
, transform: esp-gcm
{ ,in use settings ={Transport
conn id: 6, flow_id: SW:6, sibling_flags 80000000, crypto map: Tunnel0-head-0
(sa timing: remaining key lifetime (k/sec): (4341883/3471
IV size: 8 bytes
replay detection support: N
(Status: ACTIVE(ACTIVE
```

ملاحظة: في هذا الإخراج، على عكس الإصدار 1 من تبادل مفتاح الإنترنت (IKEv1)، تظهر قيمة مجموعة سرية إعادة التوجيه المثالية (DH) Diffie-Hellman (PFS) على أنها **PFS (Y/N): N، مجموعة DH: لا شيء** أثناء تفاوض النفق الأول، ولكن بعد حدوث إعادة المفتاح، تظهر القيم الصحيحة. هذا ليس خطأ رغم أن السلوك موضح في معرف تصحيح الأخطاء من Cisco CSCug67056. والفارق بين IKEv1 و IKEv2 هو أنه، في الفئة الثانية، يتم إنشاء رابطات أمن الطفل كجزء من عملية تبادل حقوق الطفل ذاتها. يتم إستخدام مجموعة DH التي تم تكوينها ضمن خريطة التشفير فقط أثناء المفتاح. وبالتالي، يمكنك رؤية **PFS (Y/N): N، مجموعة DH: لا شيء** حتى المفتاح الأول. ولكن مع IKEv1، سترى سلوكا مختلفا لأن إنشاء SA التابع يحدث أثناء "الوضع السريع" ولرسالة CREATE_CHILD_SA توفير لحمل حمولة Key Exchange التي تحدد معلمات DH لاستخراج سر مشترك جديد.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

القرار

وتوفر خوارزميات التشفير الفعالة والقوية المعرفة في الشبكة الوطنية للمعلومات ضمانا طويل الأجل بأن البيانات يتم توفيرها وصيانتها على نحو سري وسليم بتكلفة منخفضة لتجهيزها. يمكن تنفيذ NGE بسهولة باستخدام FlexVPN، التي توفر تشفير قياسي للمجموعة B.

يمكن العثور على مزيد من المعلومات حول تنفيذ Cisco للمجموعة B في تشفير الجيل التالي.

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).