تكوين مثال على FlexVPN بين موجه و ASA مع تشفير الجيل التالي

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل VPN بين مسحاج تخديد مع FlexVPN و ASA (Adaptive Security Appliance) أن يساند ال cisco التالي تشفير (NGE) خوارزمية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- FlexVPN
- تبادل مفتاح الإنترنت الإصدار 2 (IKEv2)
- IPsec
- ASA
- تشفير الجيل التالي

المكونات المستخدمة

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

- **الأجهزة:** IOS الجيل 2 (G2) من الموجه الذي يشغل ترخيص الأمان.
- **البرنامج:** برنامج Cisco IOS® الإصدار 15.2-T2.3. يمكن إستخدام أي إصدار من M أو T للإصدارات الأحدث من الإصدار 15.1.2T من برنامج Cisco IOS® Software لأن هذا يتم تضمينه مع إدخال وضع العداد Galois (GCM).
- **الأجهزة:** ASA الذي يدعم NGE.**ملاحظة:** لا تدعم إدارة قاعدة بيانات الإدارة (GCM) إلا الأنظمة الأساسية متعددة المراكز.
- **البرامج:** برنامج ASA الإصدار 9.0 أو إصدار أحدث يدعم NGE.
- فتح SSL.

للحصول على تفاصيل، راجع متصفح ميزات Cisco.

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

إنشاء اقترانات أمان IPSec ديناميكيا

واجهة IPSec الموصى بها على IOS هي واجهة النفق الظاهرية (VTI)، والتي تقوم بإنشاء واجهة تضمين التوجيه العام (GRE) التي يتم حمايتها بواسطة IPsec. ل VTI، الحركة مرور محدد (ما هي حركة المرور التي يجب حمايتها بواسطة اقترانات أمان IPSec (SA)، يتألف من حركة مرور GRE من مصدر النفق إلى وجهة النفق. نظرا لأن ASA لا يقوم بتنفيذ واجهات GRE، ولكن يقوم بدلا من ذلك بإنشاء نقاط وصول IPSec استنادا إلى حركة المرور المحددة في قائمة التحكم في الوصول (ACL)، فيجب علينا تمكين طريقة تسمح للموجه بالاستجابة إلى بدء IKEv2 باستخدام نسخة مطابقة من محددات حركة المرور المقترحة. يسمح إستخدام واجهة النفق الظاهرية الديناميكية (DVTI) على موجه FlexVPN لهذا الجهاز بالاستجابة إلى محدد حركة المرور المقدم باستخدام نسخة مطابقة من محدد حركة مرور البيانات الذي تم تقديمه.

يقوم هذا المثال بتشفير حركة مرور البيانات بين كلا الشبكتين الداخليتين. عندما يعرض ASA محددات حركة مرور بيانات شبكة ASA الداخلية إلى شبكة IOS الداخلية، `24/192.168.1.0` إلى `24/172.16.10.0`، تستجيب واجهة DVTI مع نسخة مطابقة من محددات حركة المرور، وهي من `24/172.16.10.0` إلى `24/192.168.1.0`.

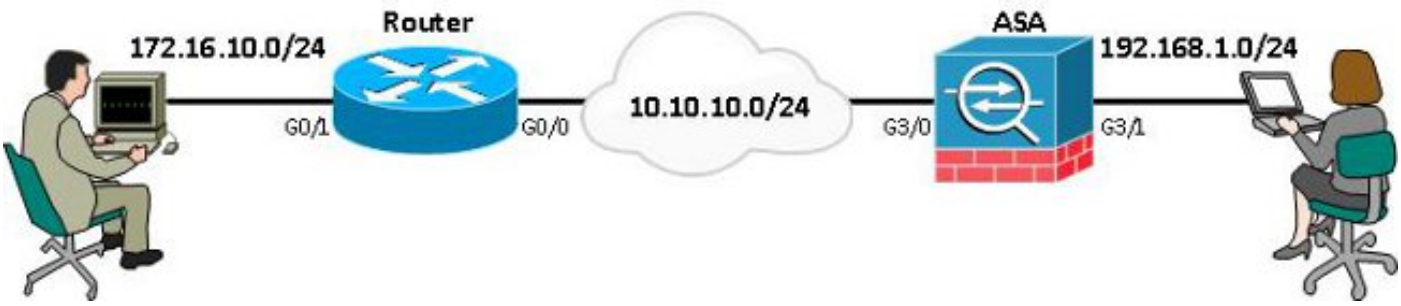
جهة منح الشهادة

حاليا، لا يدعم IOS و ASA خادم مرجع شهادة محلي (CA) بشهادات خوارزمية التوقيع الرقمي للمنحنى البيضاوي (ECDSA)، والتي تكون مطلوبة للمجموعة B. لذلك يجب تنفيذ خادم CA من إنتاج جهة خارجية. على سبيل المثال، أستخدم OpenSSL للعمل ك CA.

التكوين

مخطط الشبكة

يستند هذا الدليل إلى المخطط المبين في هذا المخطط. يجب تعديل عناوين IP لتناسب.



ملاحظة: يتضمن الإعداد اتصالا مباشرا بالموجه و ASA. ويمكن فصل هذه القفزات بواسطة نقلات كثيرة. إذا كان الأمر كذلك، فتأكد من وجود مسار للوصول إلى عنوان IP النظير. يوضح التكوين التالي تفاصيل التشفير المستخدم فقط.

الخطوات المطلوبة لتمكين الموجه من إستخدام ECDSA

جهة منح الشهادة

1. إنشاء **زوج مفاتيح منحنى بيضاوي.**
```
openssl ecparam -out ca.key -name secp256r1 -genkey
```
2. إنشاء **شهادة توقيع ذاتي لمنحنى بيضاوي**.
```
openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
```

FlexVPN

1. قم بإنشاء **اسم المجال** و**اسم المضيف**، وهما متطلبان مسبقان لإنشاء زوج مفاتيح للمنحنى البيضاوي (EC).
```
ip domain-name cisco.com
hostname Router1
crypto key generate ec keysize 256 label router1.cisco.com
```
2. قم بإنشاء **نقطة ثقة** محلية للحصول على شهادة من المرجع المصدق.
```
crypto pki trustpoint ec_ca
 enrollment terminal
 subject-name cn=router1.cisco.com
 revocation-check none
 eckeypair router1.cisco.com
 hash sha256
```
ملاحظة: نظرا لأن CA غير متصل، فقد تم تعطيل التحقق من الإبطال؛ ويجب تمكين التحقق من الإبطال للحصول على أقصى قدر من الأمان في بيئة إنتاج.
3. مصادقة **TrustPoint**. ويحصل هذا على نسخة من شهادة CA، التي تحتوي على المفتاح العام.
```
crypto pki authenticate ec_ca
```
4. يوصى بعد ذلك بإدخال الشهادة 64 المشفرة الأساسية ل CA. هذا هو الملف ca.pem، والذي تم إنشاؤه باستخدام OpenSSL. لعرض هذا الملف، قم بفتحه في محرر أو باستخدام الأمر OpenSSL **openssl x509 -in ca.pem**. أدخل **إنهاء** عند لصق هذا. ثم اكتب **نعم** للقبول.
5. قم بتسجيل الموجه في البنية الأساسية للمفتاح العام (PKI) على CA.
```
crypto pki enrol ec_ca
```
6. يجب إستخدام الإخراج الذي تتلقاه لإرسال طلب شهادة إلى المرجع المصدق. يمكن حفظ هذا كملف نصي (flex.csr) وتوقيعه باستخدام الأمر OpenSSL.
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
```
7. قم باستيراد الشهادة التي تحتوي على الملف flex.pem، والتي تم إنشاؤها من المرجع المصدق، إلى الموجه بعد إدخال هذا الأمر. ثم أدخل **إنهاء** عند الاكتمال.
```
crypto pki import ec_ca certificate
```

ASA

1. قم بإنشاء **domain-name** و**hostname**، وهما متطلبان مسبقان لإنشاء زوج مفاتيح EC.
```
domain-name cisco.com
hostname ASA1
crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
```
2. قم بإنشاء **نقطة ثقة** محلية للحصول على شهادة من المرجع المصدق.
```
crypto ca trustpoint ec_ca
enrollment terminal
subject-name cn=asa1.cisco.com
revocation-check none
keypair asa1.cisco.com
```
ملاحظة: نظرا لأن CA غير متصل، فقد تم تعطيل التحقق من الإبطال؛ ويجب تمكين التحقق من الإبطال للحصول على أقصى قدر من الأمان في بيئة إنتاج.
3. مصادقة **TrustPoint**. ويحصل هذا على نسخة من شهادة CA، التي تحتوي على المفتاح العام.
```
crypto ca authenticate ec_ca
```
4. يوصى بعد ذلك بإدخال الشهادة 64 المشفرة الأساسية ل CA. هذا هو الملف ca.pem، والذي تم إنشاؤه باستخدام OpenSSL. لعرض هذا الملف، قم بفتحه في محرر أو باستخدام الأمر OpenSSL **openssl x509 -in ca.pem**. أدخل **إنهاء** عند لصق هذا الملف، ثم اكتب **نعم** للقبول.
5. تسجيل ASA في PKI على CA.
```
crypto ca enrol ec_ca
```
6. يجب إستخدام الإخراج الذي تتلقاه لإرسال طلب شهادة إلى المرجع المصدق. يمكن حفظ هذا كملف نصي (asa.csr) ثم توقيعه باستخدام الأمر OpenSSL.
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
```
7. قم باستيراد الشهادة التي تحتوي على الملف على هيئة a.pem، والتي تم إنشاؤها من المرجع المصدق إلى الموجه بعد إدخال هذا الأمر. ثم **أدخل** "إنهاء" عند الاكتمال.
```
crypto ca import ec_ca certificate
```

التكوين

FlexVPN

قم بإنشاء خريطة شهادات لمطابقة شهادة جهاز النظير.

```
crypto pki certificate map certmap 10
subject-name co cisco.com
```
أدخل هذه الأوامر لمقترح IKEv2 لتكوين Suite-B:

ملاحظة: للحصول على أقصى درجات الأمان، قم بالتهيئة باستخدام الأمر **AES-CBC-256 with sha512 hash**.

```
crypto ikev2 proposal default
encryption aes-cbc-128
integrity sha256
group 19
```
مطابقة ملف تعريف IKEv2 مع 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 ec_ca
virtual-template 1
```

قم بتكوين مجموعة تحويل IPSec لاستخدام وضع عداد Galois (GCM).

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

قم بتكوين ملف تعريف IPSec باستخدام المعلمات التي تم تكوينها مسبقا.

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

تكوين واجهة النفق:

```
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
tunnel protection ipsec profile default
```

هنا القارن تشكيل:

```
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 172.16.10.1 255.255.255.0
```

ASA

استعملت هذا قارن تشكيل:

```
interface GigabitEthernet3/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
interface GigabitEthernet3/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

أدخل الأمر قائمة الوصول هذه لتحديد حركة المرور التي سيتم تشفيرها:

```
access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0 255.255.255.0
```

أدخل أمر اقتراح IPSec هذا مع NGE:

```
crypto ipsec ikev2 ipsec-proposal prop1
 protocol esp encryption aes-gcm
 protocol esp integrity null
```

أوامر خريطة التشفير:

```
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 10.10.10.1
crypto map mymap 10 set ikev2 ipsec-proposal prop1
```

```
crypto map mymap 10 set trustpoint ec_ca
crypto map mymap interface outside
```

يقوم هذا الأمر بتكوين سياسة IKEv2 باستخدام NGE:

```
crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable outside
```

مجموعة النفق التي تم تكوينها لأوامر النظير:

```
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 peer-id-validate cert
ikev2 remote-authentication certificate
ikev2 local-authentication certificate ec_ca
```

التحقق من الاتصال

تحقق من إنشاء مفاتيح ECDSA بنجاح.

```
Router1#show crypto key mypubkey ec router1.cisco.com
Key pair was generated at: 21:28:26 UTC Feb 19 2013 %
 Key name: router1.cisco.com
  Key type: EC KEYS
 Storage Device: private-config
  Usage: Signature Key
 .Key is not exportable
  ;Key Data&colon
  <...omitted...>

ASA-1(config)#show crypto key mypubkey ecdsa
Key pair was generated at: 21:11:24 UTC Feb 19 2013
 Key name: asa1.cisco.com
 Usage: General Purpose Key
  EC Size (bits): 256
  ;Key Data&colon
  <...omitted...>
```

تحقق من إستيراد الشهادة بنجاح ومن إستخدام ECDSA.

```
Router1#show crypto pki certificates verbose
  Certificate
 Status: Available
  Version: 3
 Certificate Serial Number (hex): 0137
  Certificate Usage: General Purpose
  :Issuer
  <...omitted...>
 :Subject Key Info
 Public Key Algorithm: rsaEncryption
  (EC Public Key:  (256 bit
 Signature Algorithm: SHA256 with ECDSA
```

```
ASA-1(config)#show crypto ca certificates
                                                    CA Certificate
                                                  Status: Available
                                  Certificate Serial Number: 00a293f1fe4bd49189
                                        Certificate Usage: General Purpose
                                         (Public Key Type: ECDSA (256 bits
                                 Signature Algorithm: SHA256 with ECDSA Encryption
                                                    <...omitted...>
```

تحقق من إنشاء IKEv2 SA بنجاح واستخدم خوارزميات NGE التي تم تكوينها.

```
                                                Router1#show crypto ikev2 sa  detailed
                                                     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: SHA384, DH Grp:19, Auth sign: ECDSA
                                                        Auth verify: ECDSA
                                                   Life/Active Time: 86400/94 sec


                                                  ASA-1#show crypto ikev2 sa detail

                                                                  :IKEv2 SAs

                                          Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

    Tunnel-id                 Local                 Remote     Status         Role
    READY    INITIATOR      10.10.10.1/500        10.10.10.2/500        268364957
    ,Encr: AES-CBC, keysize: 128, Hash: SHA384, DH Grp:19, Auth sign: ECDSA
                                                        Auth verify: ECDSA
                                                             <...omitted...>
                          Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
                          remote selector 172.16.10.0/0 - 172.16.10.255/65535
                                         ESP spi in/out: 0xe847d8/0x12bce4d
                                                    AH spi in/out: 0x0/0x0
                                                       CPI in/out: 0x0/0x0
                                      Encr: AES-GCM, keysize: 128, esp_hmac: N/A
                                    ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

تحقق من إنشاء IPSec SA بنجاح واستخدام خوارزميات NGE التي تم تكوينها.

ملاحظة: يمكن ل FlexVPN إنهاء إتصالات IPSec من عملاء من خارج IOS الذين يدعمون كلا من بروتوكولات IKEv2 و IPSec.

```
                                                  Router1#show crypto ipsec sa

                                                    interface: Virtual-Access1
                                  Crypto map tag: Virtual-Access1-head-0, local addr 10.10.10.1

                                                      (protected vrf: (none
                              (local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0
                              (remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0
                                                 current_peer 10.10.10.2 port 500
                                                 {,PERMIT, flags={origin_is_acl
                                                              <...omitted...>

                                                                 :inbound esp sas
                                                     (spi: 0x12BCE4D(19648077
                                                       , transform: esp-gcm
                                                    { ,in use settings ={Tunnel
```

```
ASA-1#show crypto ipsec sa detail
                                                    interface: outside
                                Crypto map tag: mymap, seq num: 10, local addr: 10.10.10.2

                      access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0
                                                                                  255.255.255.0
                            (local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0
                           (remote ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0
                                                                  current_peer: 10.10.10.1
                                                                        <...omitted...>


                                                                      :inbound esp sas
                                                                 (spi: 0x00E847D8 (15222744
                                                transform: esp-aes-gcm esp-null-hmac no compression
                                                                 { ,in use settings ={L2L, Tunnel, IKEv2
```

لمزيد من المعلومات حول تنفيذ Cisco ل Suite-B، ارجع إلى التقرير الرسمي للتشفير من الجيل التالي.

ارجع إلى صفحة حل التشفير من الجيل التالي لمعرفة المزيد حول تنفيذ Cisco لتشفير الجيل التالي.

معلومات ذات صلة

- تقرير رسمي حول التشفير من الجيل التالي
- صفحة حل التشفير من الجيل التالي
- القشرة الآمنة (SSH)
- مفاوضة IPSec/بروتوكولات IKE
- تصحيح أخطاء ASA IKEv2 لشبكة VPN من موقع إلى موقع مع PSKs TechNote
- تصحيح أخطاء ASA IPSec و IKE (الوضع الرئيسي IKEv1) أستكشاف أخطاء TechNote وإصلاحها
- تصحيح أخطاء الوضع الرئيسي ل IPSec و IKE - IKEv1 Main Mode Troubleshooting TechNote
- تصحيح أخطاء ASA IPSec و IKE - IKEv1 Aggressive Mode TechNote
- 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).