AnyConnect إلى وحدة الاستقبال والبث عبر IPsec مع IKEv2 ومثال تكوين الشهادات

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
مخطط الشبكة
جهة منح الشهادة (إختياري)
تكوين IOS CA
كيفية التحقق من تعيين EKU الصحيح على الشهادة
تكوين وحدة الاستقبال والبث
تكوين PKI
تكوين التشفير/IPsec
العميل
تسجيل الشهادة
توصيف AnyConnect
التحقق من الاتصال
تشفير الجيل التالي
المحاذير والمشكلات المعروفة
معلومات ذات صلة

المقدمة

يقدم هذا المستند معلومات حول كيفية تحقيق اتصال محمي ب IPsec من جهاز يشغل عميل AnyConnect إلى موجه Cisco IOS®مع مصادقة الشهادة فقط باستخدام إطار عمل FlexVPN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- FlexVPN

- AnyConnect

المكونات المستخدمة

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

محطه الاستقبال والبث

يمكن أن يكون موجه Cisco IOS أي موجه قادر على تشغيل IKEv2، وتشغيل إصدار M&T 15.2 على الأقل. مهما، أنت ينبغي استعملت إطلاق أحدث (راجع المعروف تحذير قسم)، إن يتوفر.

العميل

إصدار AnyConnect 3.x

جهة منح الشهادة

في هذا المثال، سيقوم مرجع التصديق (CA) بتشغيل الإصدار 15.2(3)T.

من المهم للغاية إستخدام أحد الإصدارات الأحدث بسبب الحاجة إلى دعم إستخدام المفتاح الموسع (EKU).

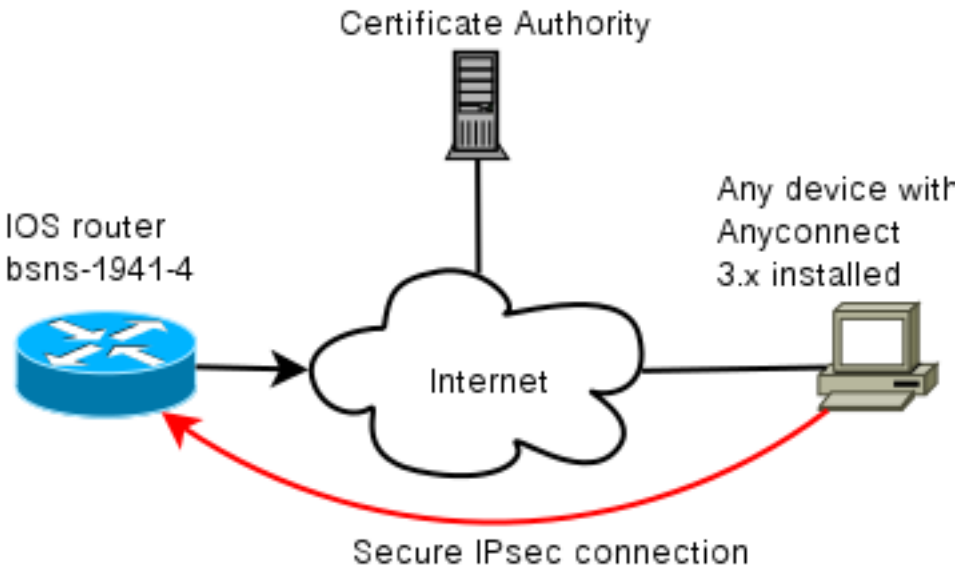
في هذا النشر، يتم إستخدام موجه IOS ك CA. غير أنه ينبغي أن يكون أي تطبيق للترخيص المصدق قائم على المعايير وقادر على إستخدام وحدة المعالجة المركزية (EKU) على ما يرام.

الاصطلاحات

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

التكوين

مخطط الشبكة



جهة منح الشهادة (إختياري)

إذا أخترت إستخدامه، يمكن أن يعمل موجه IOS لديك كمرجع مصدق.

تكوين IOS CA

يجب تذكر أنه يجب على خادم CA وضع EKU الصحيح على شهادات العميل والخادم. في هذه الحالة تم تعيين مصادقة الخادم و EKU مصادقة العميل لكل الشهادات.

```
bsns-1941-3#show run | s crypto pki
crypto pki server CISCO
database level complete
database archive pem password 7 00071A1507545A545C
issuer-name cn=bsns-1941-3.cisco.com,ou=TAC,o=cisco
grant auto rollover ca-cert
grant auto
auto-rollover
eku server-auth client-auth
```

كيفية التحقق من تعيين EKU الصحيح على الشهادة

لاحظ أن BSNS-1941-3 هو خادم CA بينما BSNS-1941-4 هو وحدة الاستقبال والبث ل IPsec. أجزاء من الناتج محذوفة للإيجاز.

```
BSNS-1941-4#show crypto pki certificate verbose
Certificate
(...omitted...)

Public Key Algorithm: rsaEncryption
(RSA Public Key: (1024 bit
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: C3D52BE9 1EE97559 C7323995 3C51DC53
Fingerprint SHA1: 76BC7CD4 F298F8D9 A95338DC E5AF7602 9B57BE31
:X509v3 extensions
X509v3 Key Usage: A0000000
Digital Signature
Key Encipherment
X509v3 Subject Key ID: 83647B09 D3300A97 577C3E2C AAE7F47C F2D88ADF
X509v3 Authority Key ID: B3CC331D 7159C3CD 27487322 88AC02ED FAF2AE2E
:Authority Info Access
:Extended Key Usage
Client Auth
Server Auth
Associated Trustpoints: CISCO2
Storage: nvram:bsns-1941-3c#5.cer
Key Label: BSNS-1941-4.cisco.com
Key storage device: private config

CA Certificate
(...omitted...)
```

تكوين وحدة الاستقبال والبث

يتكون تكوين وحدة الاستقبال والبث من جزئين: جزء وحدة PKI و flex/IKEv2 فعليا.

تكوين PKI

ستلاحظ أن CN من bsns-1941-4.cisco.com مستخدم. يجب أن يتطابق هذا مع إدخال DNS مناسب ويجب تضمينه في ملف تعريف AnyConnect تحت <hostname>.

```
crypto pki trustpoint CISCO2
enrollment url http://10.48.66.14:80
serial-number
ip-address 10.48.66.15
subject-name cn=bsns-1941-4.cisco.com,ou=TAC,o=cisco
revocation-check none

crypto pki certificate map CMAP 10
subject-name co cisco
```

تكوين التشفير/IPsec

لاحظ أن إعداد PRF/التكامل في الاقتراح **يحتاج** إلى تطابق ما تؤيده شهادتك. هذا عادة SHA-1.

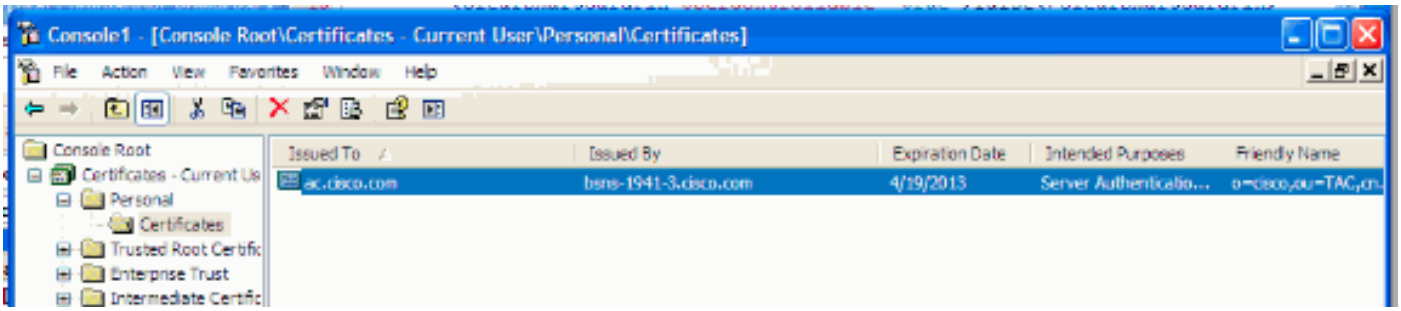
```
crypto ikev2 authorization policy AC
pool AC

crypto ikev2 proposal PRO
encryption 3des aes-cbc-128
integrity sha1
group 5 2

crypto ikev2 policy POL
match fvrf any
proposal PRO

crypto ikev2 profile PRO
match certificate CMAP
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

no crypto ikev2 http-url cert
crypto ipsec transform-set TRA esp-3des esp-sha-hmac

crypto ipsec profile PRO
set transform-set TRA
set ikev2-profile PRO

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

العميل

يتكون تكوين العميل لاتصال AnyConnect بنجاح باستخدام IKEv2 والشهادات من جزأين.

تسجيل الشهادة

عندما يتم تسجيل الشهادة بشكل صحيح، يمكنك التحقق من أنها موجودة إما في المتجر الآلي أو الشخصي. تذكر أن شهادات العميل تحتاج أيضا إلى EKU.



توصيف AnyConnect

يتسم ملف تعريف AnyConnect بالطول والبساطة الفائقة.

والجزء ذو الصلة هو تحديد ما يلي:

1. المضيف الذي تتصل به
2. نوع البروتوكول
3. المصادقة المراد إستخدامها عند الاتصال بذلك المضيف

ما هو مستخدم:

```
<ServerList>
<HostEntry>
<HostName>bsns-1941-4.cisco.com</HostName>
PrimaryProtocol>IPsec>
StandardAuthenticationOnly>true>
<AuthMethodDuringIKENegotiation>
IKE-RSA
<AuthMethodDuringIKENegotiation/>
<StandardAuthenticationOnly/>
<PrimaryProtocol/>
<HostEntry/>
<ServerList/>
```

في حقل الاتصال من AnyConnect، يلزمك توفير FQDN بالكامل، وهي القيمة المرئية في <HostName>.

التحقق من الاتصال

تم حذف بعض المعلومات من أجل الإيجاز.

```
BSNS-1941-4#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
none/none READY 10.55.193.212/65311 10.48.66.15/4500 2
,Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:5
Auth sign: RSA, Auth verify: RSA
Life/Active Time: 86400/180 sec
```

```
IPv6 Crypto IKEv2 SA

BSNS-1941-4#show crypto ipsec sa

interface: Virtual-Access1
Crypto map tag: Virtual-Access1-head-0, local addr 10.48.66.15

(protected vrf: (none
(local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
(remote ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/0/0
current_peer 10.55.193.212 port 65311
{,PERMIT, flags={origin_is_acl
pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2#
pkts decaps: 26, #pkts decrypt: 26, #pkts verify: 26#

local crypto endpt.: 10.48.66.15, remote crypto endpt.: 10.55.193.212
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
(current outbound spi: 0x5C171095(1545015445
PFS (Y/N): N, DH group: none

:inbound esp sas
(spi: 0x8283D0F0(2189676784
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel UDP-Encaps
,conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000040
crypto map: Virtual-Access1-head-0
(sa timing: remaining key lifetime (k/sec): (4215478/3412
IV size: 8 bytes
replay detection support: Y
(Status: ACTIVE(ACTIVE

:outbound esp sas
(spi: 0x5C171095(1545015445
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel UDP-Encaps
,conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000040
crypto map: Virtual-Access1-head-0
(sa timing: remaining key lifetime (k/sec): (4215482/3412
IV size: 8 bytes
replay detection support: Y
(Status: ACTIVE(ACTIVE
```

تشفير الجيل التالي

يتم توفير التكوين أعلاه للمرجع لإظهار تكوين عامل أدنى. توصي Cisco باستخدام تشفير الجيل التالي (NGC) حيثما كان ذلك ممكنا.

يمكن الاطلاع على التوصيات الحالية المتعلقة بالهجرة هنا:
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

عند إختيار تكوين NGC، تأكد من أن كل من برنامج العميل وجهاز وحدة الاستقبال والبث يدعمان هذا التكوين. يوصى بأن تكون موجهات ISR من الجيل 2 و ASR 1000 بمثابة محولات طرفية نظرا لدعم أجهزتها ل NGC.

على الجانب "AnyConnect"، اعتبارا من إصدار AnyConnect 3.1، يتم دعم مجموعة الخوارزمية B الخاصة ب من NSA.

المحاذير والمشكلات المعروفة

- تذكر أنه تم تكوين هذا الخط على وحدة الاستقبال والبث الخاصة بنظام IOS لديك: **لا يوجد تشفير -ikev2 http url cert**. الخطأ الناتج عن IOS و AnyConnect عند عدم تكوينه مضلل تماما.
- قد لا يأتي برنامج IOS 15.2M&T السابق مع جلسة عمل IKEv2 لمصادقة RSA-SIG. يمكن أن يكون هذا مرتبطا بمعرف تصحيح الأخطاء من CSCtx31294 Cisco (العملاء المسجلون فقط). تأكد من تشغيل أحدث برنامج 15.2M أو 15.2T.
- في بعض السيناريوهات، قد لا يتمكن IOS من انتقاء نقطة الثقة الصحيحة للمصادقة. cisco على علم بالمشكلة، وهو ثابت اعتبارا من 15.2T1(3) و 15.2M1(4) إطلاق.
- إذا كان AnyConnect يقوم بالإبلاغ عن رسالة مماثلة لهذه:

```
(The client certificate's cryptographic service provider(CSP
does not support the sha512 algorithm
```

بعد ذلك، تحتاج إلى التأكد من تطابق إعداد التكامل/PRF في اقتراحات IKEv2 مع ما يمكن لشهاداتك معالجته. في مثال التكوين أعلاه، يتم إستخدام SHA-1.

معلومات ذات صلة

- 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).