التكوين الديناميكي ل FlexVPN مع قوائم سمات AAA المحلية

المحتويات

المقدمة

يوضح مثال التكوين التالي كيفية إستخدام قائمة سمات المصادقة والتفويض والمحاسبة (AAA) المحلية لتنفيذ تكوين ديناميكي يمكن تقديمه دون إستخدام خادم خدمة طلب اتصال المستخدم البعيد للمصادقة الخارجية (RADIUS).

وهذا أمر مرغوب فيه في سيناريوهات معينة، لا سيما عندما يكون النشر السريع أو الاختبار مطلوبا. وتكون عمليات النشر هذه في العادة عبارة عن مختبرات إثبات صحة المفاهيم أو إختبارات نشر جديدة أو أستكشاف الأخطاء وإصلاحها.

إن التكوين الديناميكي مهم على جانب مركز التركيز/المحور حيث يجب تطبيق سياسات أو سمات مختلفة على كل مستخدم ولكل عميل على أساس كل جلسة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية هذه، ولكن لا تقتصر عليها. لا تحدد هذه القائمة الحد الأدنى للمتطلبات، ولكنها تعكس حالة الجهاز طوال مرحلة إختبار هذه الميزة.

الأجهزة

- موجهات خدمات التجميع (ASR 1001 - ASR) - المعروفة باسم "BSNS-ASR1001-4"
- موجهات الخدمات المتكاملة الجيل 2 (ISR G2) - الطراز 3925e - المسمى "BSNS-3925e-1"
- موجهات الخدمات المتكاملة الجيل 2 (ISR G2) - الطراز 3945e - المسمى "BSNS-3945e-1"

البرنامج

- Cisco من S(1)15.3 - 3.8 الإصدار IOS XE
- برنامج Cisco IOS® الإصدار M1(4)15.2 و M2(4)15.2

التراخيص

- تحتوي موجهات ASR على تراخيص ميزة **المغامرة** و**IPsec** التي تم تمكينها.
- تتضمن موجهات ISR G2 تراخيص الميزات **ipbasek9**، و**securityYK9**، و**hseck9** الممكنة.

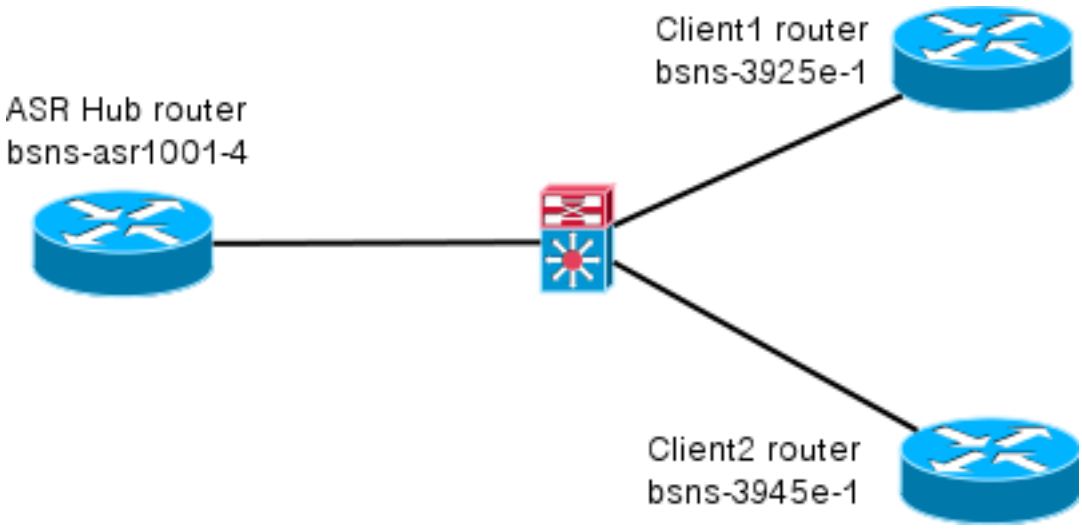
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

طوبولوجيا

الطوبولوجيا المستخدمة في هذا التمرين أساسية. يتم إستخدام موجه صرة (ASR) وموجهين متكلما (ISR)، مما يحاكي العملاء.



التكوينات

الغرض من التكوينات الواردة في هذا المستند هو عرض إعداد أساسي، مع إعدادات افتراضية ذكية قدر الإمكان. للحصول على توصيات Cisco حول التشفير، تفضل بزيارة صفحة التشفير من الجيل التالي على cisco.com.

التكوين الذي تم التحدث به

كما ذكر سابقا، يتم تنفيذ معظم الإجراءات في هذه الوثائق على الصرة. التكوين الذي تم التحدث به هنا للمرجع. في هذا التكوين، لاحظ أن التغيير فقط هو الهوية بين العميل1 و Client2 (معروض بخط غامق).

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 keyring Flex_key
peer Spokes
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco
pre-shared-key remote cisco
!!
crypto ikev2 profile Flex_IKEv2
match identity remote address 0.0.0.0
identity local email Client1@cisco.com
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1

crypto logging session

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel1
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source GigabitEthernet0/0
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
ip unnumbered Tunnel1
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

تكوين الموزع

يقسم تشكيل الصرة إلى قسمين:

1. **تكوين الاتصال الأساسي**، والذي يحدد التكوين المطلوب للاتصال الأساسي.

2. **التكوين الموسع**، والذي يوضح تغييرات التكوين اللازمة لتوضيح كيفية إستخدام المسؤول قائمة سمات AAA لإجراء تغييرات التكوين لكل مستخدم أو لكل جلسة عمل.

تكوين الاتصال الأساسي

هذا التكوين للمرجع فقط ولا يقصد به أن يكون مثاليا، ولكنه فعال فقط.

وأكبر تقييد لهذا التكوين هو إستخدام مفتاح مشترك مسبقا (PSK) كطريقة المصادقة. توصي Cisco باستخدام الشهادات كلما أمكن.

```
                                aaa new-model
                aaa authorization network default local

                                aaa session-id common
                crypto ikev2 authorization policy default
                                     pool FlexSpokes
                                   route set interface

                            crypto ikev2 keyring Flex_key
                                        peer Spokes
                                    address 0.0.0.0 0.0.0.0
                                  pre-shared-key local cisco
                                 pre-shared-key remote cisco
                                                      !!
                                        peer Client1
                              identity email Client1@cisco.com
                                      pre-shared-key cisco
                                                      !!
                                        peer Client2
                              identity email Client2@cisco.com
                                      pre-shared-key cisco

                              crypto ikev2 profile Flex_IKEv2
                                           match fvrf any
                                match identity remote address 0.0.0.0
                        match identity remote email domain cisco.com
                                    authentication remote pre-share
                                    authentication local pre-share
                                           keyring local Flex_key
                        aaa authorization group psk list default default
                                         virtual-template 1

                                no crypto ikev2 http-url cert

                                       crypto logging session

                                 crypto ipsec profile default
                                set ikev2-profile Flex_IKEv2

                        interface Virtual-Template1 type tunnel
                                        vrf forwarding IVRF
                                    ip unnumbered Loopback100
                                                ip mtu 1400
                                     ip nhrp network-id 2
                                         ip nhrp redirect
                                   ip tcp adjust-mss 1360
                                 tunnel path-mtu-discovery
                                       tunnel vrf INTERNET
                        tunnel protection ipsec profile default
```

التكوين الموسع

هناك بعض الأشياء اللازمة لتعيين سمات AAA إلى جلسة عمل معينة. يوضح هذا المثال العمل الكامل للعميل1، ثم يوضح كيفية إضافة عميل/مستخدم آخر.

تكوين الموزع الموسع للعميل1

1. تحديد قائمة سمات AAA.

```
aaa attribute list Client1
attribute type interface-config "ip mtu 1300" protocol ip
attribute type interface-config "service-policy output TEST" protocol ip
```

ملاحظة: تذكر أنه يجب أن يكون الكيان المعين بواسطة السمات موجودا محليا. في هذه الحالة، تم تكوين **خريطة السياسة** مسبقا.

```
policy-map TEST
class class-default
shape average 60000
```

2. قم بتعيين قائمة سمات AAA إلى **نهج تخويل.**

```
crypto ikev2 authorization policy Client1
pool FlexSpokes
aaa attribute list Client1
route set interface
```

3. تأكد من إستخدام هذه السياسة الجديدة من قبل العملاء المتصلين. في هذه الحالة، استخرج جزء **اسم المستخدم** من الهوية التي أرسلها العملاء. يجب على العملاء إستخدام عنوان بريد إلكتروني على العنوان ClientX@cisco.com (X = 1 أو 2، وفقا للعميل). يقسم المفتاح **عنوان البريد الإلكتروني إلى اسم المستخدم وجزء المجال ويستخدم واحدا فقط منهم (اسم المستخدم في هذه الحالة) لاختيار اسم نهج التخويل.**

```
crypto ikev2 name-mangler GET_NAME
email username

crypto ikev2 profile Flex_IKEv2
aaa authorization group psk list default name-mangler GET_NAME
```

عند تشغيل العميل 1، يمكن إضافة العميل 2 بسهولة نسبيا.

تكوين الموزع الموسع للعميل2

تأكد من وجود سياسة ومجموعة منفصلة من السمات، إذا لزم الأمر.

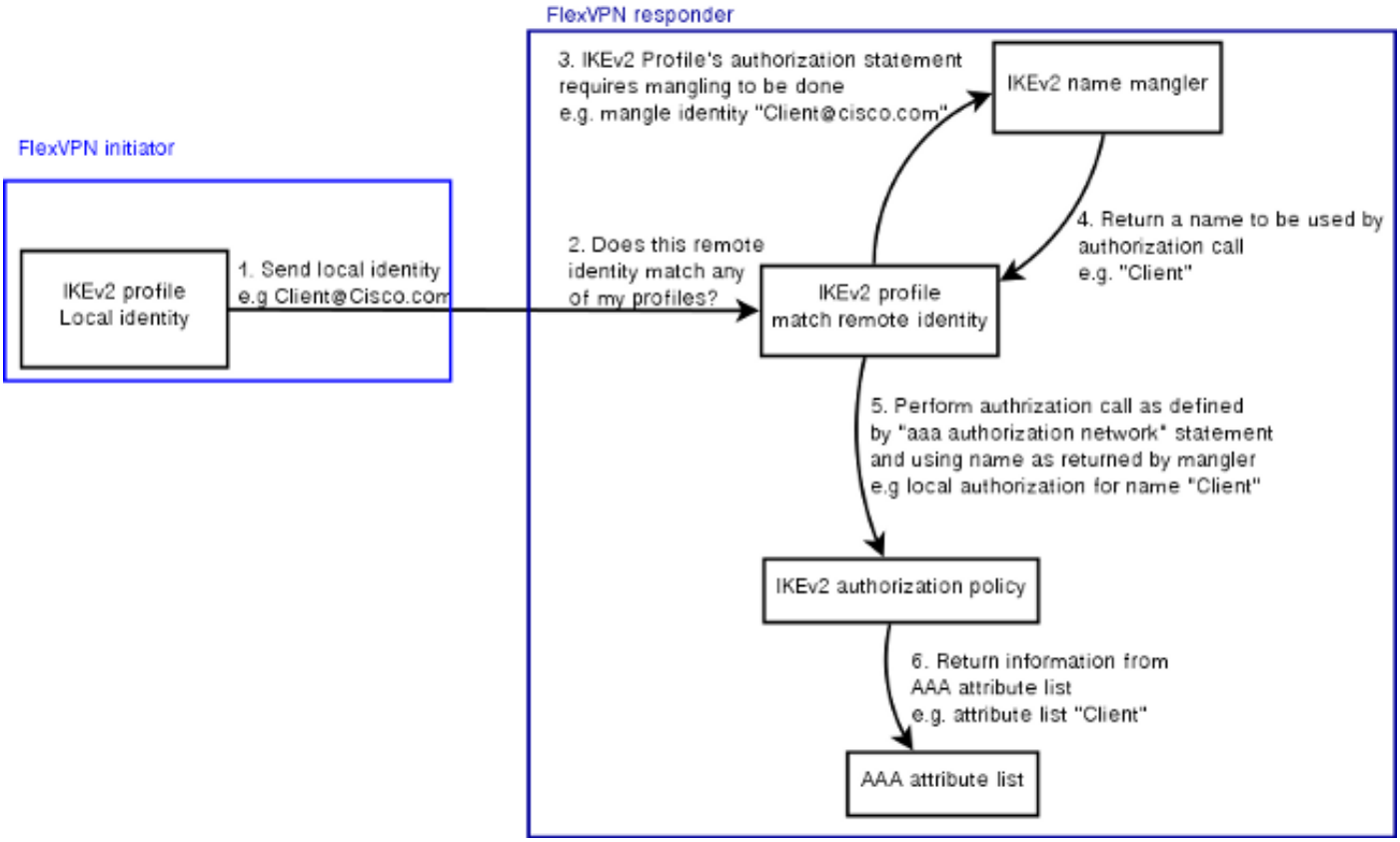
```
aaa attribute list Client2
attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
attribute type interface-config "ip access-group 133 in" protocol ip

crypto ikev2 authorization policy Client2
pool FlexSpokes
aaa attribute list Client2
route set interface
```

في هذا المثال، يتم تطبيق إعداد محدث للحد الأقصى لحجم المقطع (MSS) وقائمة وصول واردة ليتم تشغيلها لهذا العميل. يمكن إختيار إعدادات أخرى بسهولة. الإعداد النموذجي هو تخصيص توجيه ظاهري مختلف وإعادة توجيه (VRF) لعملاء مختلفين. وكما تمت الإشارة مسبقا، يجب أن يكون أي كيان تم تعيينه لقائمة السمات، مثل قائمة الوصول 133 في هذا السيناريو، موجودا بالفعل في التكوين.

نظرة عامة على العملية

يوضح هذا الشكل ترتيب العملية عند معالجة تفويض AAA عبر ملف تعريف الإصدار 2 من تبادل مفتاح الإنترنت (IKEv2) ويحتوي على معلومات خاصة بمثال التكوين هذا.



التحقق

يوضح هذا القسم كيفية التحقق من تطبيق الإعدادات التي تم تعيينها مسبقا على العملاء.

العميل 1

هنا الأوامر التي تتحقق من تطبيق إعدادات الحد الأقصى لوحدات الإرسال (MTU)، بالإضافة إلى نهج الخدمة.

```
bsns-asr1001-4#show cef int virtual-access 1
(...)
Hardware idb is Virtual-Access1
Fast switching type 14, interface type 21
IP CEF switching enabled
IP CEF switching turbo vector
IP Null turbo vector
"VPN Forwarding table "IVRF
IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
(Tunnel VPN Forwarding table "INTERNET" (tableid 2
Input fast flags 0x0, Output fast flags 0x4000
(ifindex 16(16
Slot unknown (4294967295) Slot unit 1 VC -1
IP MTU 1300
Real output interface is GigabitEthernet0/0/0

bsns-asr1001-4#show policy-map interface virtual-access1
Virtual-Access1

Service-policy output: TEST
```

```
(Class-map: class-default (match-any
                                        packets, 620 bytes 5
minute offered rate 0000 bps, drop rate 0000 bps 5
                                        Match: any
                                          Queueing
                                    queue limit 64 packets
queue depth/total drops/no-buffer drops) 0/0/0)
                                pkts output/bytes output) 5/910)
shape (average) cir 60000, bc 240, be 240
                                target shape rate 60000
```

العميل 2

فيما يلي الأوامر التي تتحقق من دفع إعدادات MSS ومن تطبيق قائمة الوصول 133 أيضا كعامل تصفية وارد على واجهة الوصول الظاهري المكافئة.

```
bsns-asr1001-4#show cef int virtual-access 2
        (Virtual-Access2 is up (if_number 18
    Corresponding hwidb fast_if_number 18
  Corresponding hwidb firstsw->if_number 18
            Internet address is 0.0.0.0/0
(Unnumbered interface. Using address of Loopback100 (192.168.1.1
            ICMP redirects are never sent
        Per packet load-sharing is disabled
           IP unicast RPF check is disabled
Input features: Access List, TCP Adjust MSS
                                    (...)

bsns-asr1001-4#show ip interface virtual-access2
        Virtual-Access2 is up, line protocol is up
(Interface is unnumbered. Using address of Loopback100 (192.168.1.1
     Broadcast address is 255.255.255.255
                    MTU is 1400 bytes
          Helper address is not set
Directed broadcast forwarding is disabled
            Outgoing access list is not set
Inbound access list is 133, default is not set
                                    (...)
```

تصحيح الأخطاء

هناك قطاعان رئيسيان لتصحيح الأخطاء. ويكون هذا الإجراء مفيدا عندما تحتاج إلى فتح حالة مركز المساعدة الفنية والحصول على الأشياء على المسار بشكل أسرع.

debug IKEv2

ابدأ بأمر تصحيح الأخطاء الرئيسي هذا:

```
[debug crypto ikev2 [internal|packet
```

ثم أدخل الأوامر التالية:

```
show crypto ikev2 sa
show crypto ipsec sa peer a.b.c.d
```

تعيين سمة AAA ل debug

إذا كنت ترغب في تصحيح أخطاء تعيين سمات AAA، فقد تكون هذه الأخطاء مفيدة.

```
debug aaa authorization
debug aaa attr
debug aaa proto local
```

القرار

يوضح هذا المستند كيفية إستخدام قائمة سمات AAA للسماح بمرونة إضافية في عمليات نشر FlexVPN حيث قد لا يكون خادم RADIUS متوفرا أو غير مرغوب فيه. توفر قائمة سمات AAA خيارات تكوين إضافية لكل جلسة عمل، لكل مجموعة، إذا كانت مطلوبة.

معلومات ذات صلة

- دليل تكوين FlexVPN و Internet Key Exchange الإصدار 2، Cisco IOS الإصدار 15M&T
- خدمات مصادقة طلب اتصال المستخدم البعيد (RADIUS)
- طلبات التعليقات (RFCs)
- مفاوضة IPSec/بروتوكولات IKE
- 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).