FlexVPN: IPv6 في موزع ومثال تكوين النشر المتصل

المحتويات

المقدمة

يصف هذا المستند تكوينا شائعا يستخدم طريقة اتصال FlexVPN Cisco IOS® ونشر الموزع في بيئة IPv6. كما توسع في المفاهيم التي تمت مناقشتها في FlexVPN: تكوين شبكة LAN الأساسية الخاصة ب IPv6 إلى تكوين شبكة LAN.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco IOS FlexVPN
- بروتوكولات التوجيه

المكونات المستخدمة

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

- الجيل 2 لموجهات الخدمات المدمجة من Cisco (ISR G2)
- برنامج IOS الإصدار 15.3 (أو الإصدار 15.4T للأنفاق الديناميكية التي يتم التحدث بها باستخدام IPv6) من Cisco

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.

التكوين

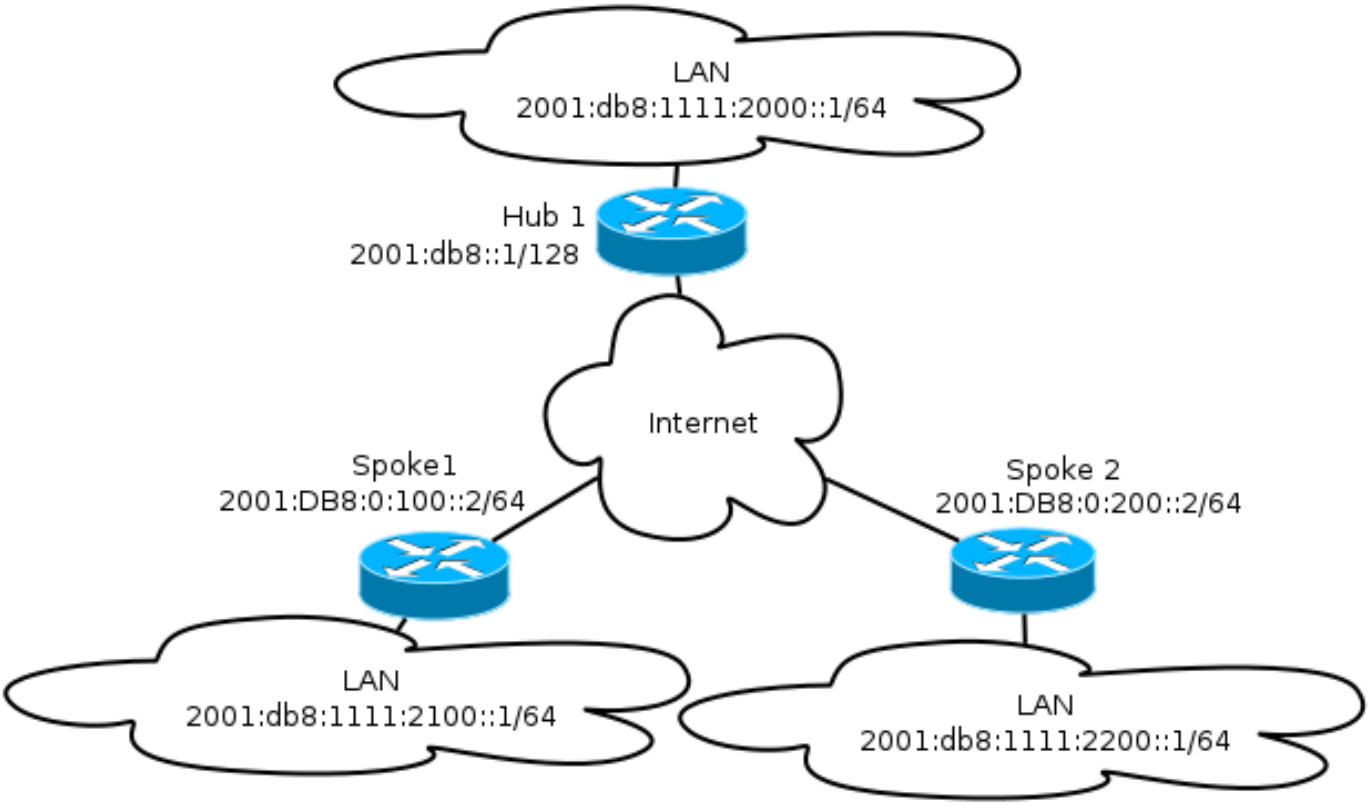
ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

بينما يستخدم مثال التكوين هذا ومخطط الشبكة IPv6 كشبكة النقل، يستخدم تضمين التوجيه العام (GRE) عادة في عمليات نشر FlexVPN. يسمح إستخدام GRE بدلا من IPsec للمسؤولين بتشغيل IPv4 أو IPv6 أو كليهما عبر نفس الأنفاق، بغض النظر عن شبكة النقل.

الرسم التخطيطي للشبكة

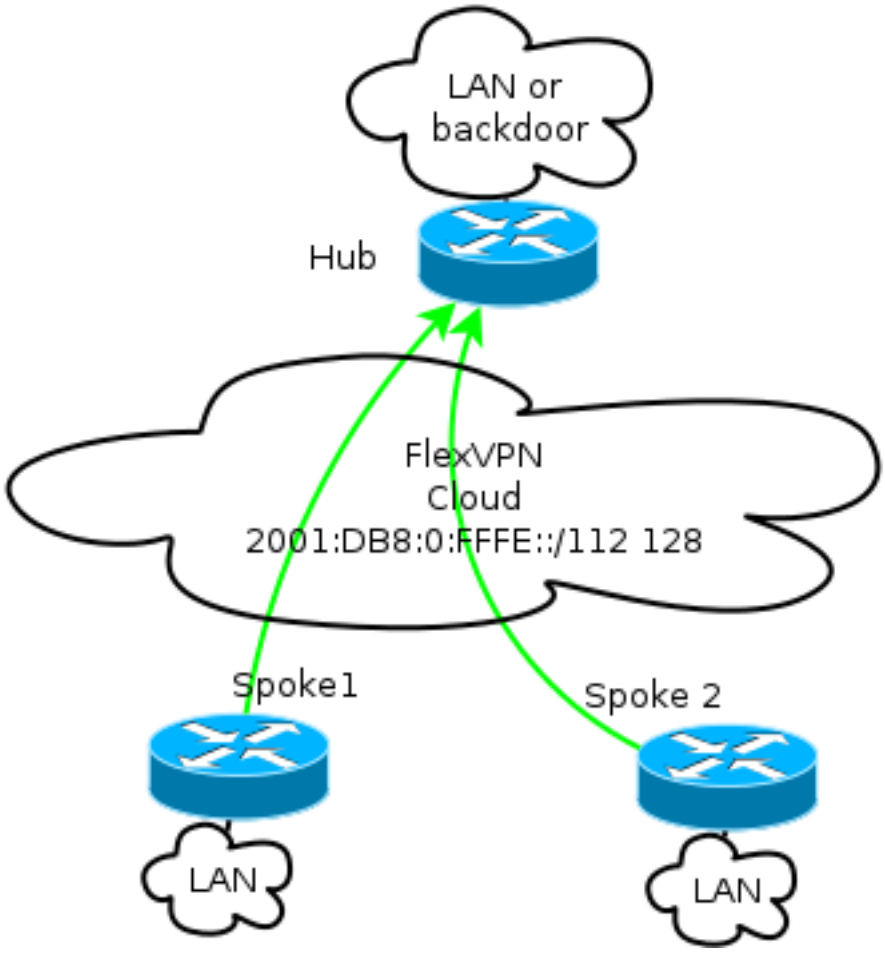
شبكة النقل

هذا رسم بياني لشبكة النقل المستخدمة في هذا المثال:



شبكة ترابية

هذا رسم بياني لطبولوجيا الشبكة التغشية الأساسية المستخدمة في هذا المثال:



يتم تعيين كل محادثة من مجموعة عناوين من /112، ولكنه يستلم عنوان /128. وبالتالي، يتم إستخدام التدوين "/112 128" في تكوين تجمع IPv6 للمحور.

التكوينات

يوضح هذا التكوين تغشية IPv4 و IPv6 التي تعمل عبر البنية الأساسية ل IPv6.

عند مقارنته بالأمثلة التي تستخدم IPv4 كعمود أساسي، لاحظ أنه يجب عليك إستخدام الأمر **tunnel mode** من أجل تغيير العقدة واستيعاب نقل IPv6.

سيتم إدخال ميزة النفق عبر بروتوكول IPv6 عبر تقنية الاتصال الهاتفي في البرنامج Cisco IOS Software، الإصدار 15.4T، والذي لم يتوفر بعد.

بروتوكولات التوجيه

توصي Cisco باستخدام بروتوكول العبارة الحدودية الداخلية (iBGP) للتجميع بين محاور الكلام لعمليات النشر الكبيرة لأن iBGP هو بروتوكول التوجيه الأكثر قابلية للتطوير.

لا يدعم نطاق الاستماع لبروتوكول العبارة الحدودية (BGP) نطاق IPv6، ولكنه يعمل على تبسيط الاستخدام مع نقل IPv4. على الرغم من أنه من الممكن إستخدام BGP في مثل هذه البيئة، يوضح هذا التكوين مثالا أساسيا، لذلك تم إختيار بروتوكول توجيه العبارة الداخلي المحسن (EIGRP).

تكوين الموزع

ومقارنة بالأمثلة الأقدم، يتضمن هذا التكوين إستخدام بروتوكولات النقل الجديدة.

لتكوين الموزع، يحتاج المسؤول إلى:

- تمكين توجيه البث الأحادي.
- توفير توجيه النقل.
- توفير مجموعة جديدة من عناوين IPv6 ليتم تخصيصها بشكل ديناميكي. التجمع هو DB8:0:FFFE:/112:2001؛ 16 وحدة بت تسمح بمعالجة 65،535 جهاز.
- قم بتمكين IPv6 لتكوين بروتوكول تحليل الخطوة (NHRP) التالية للسماح ل IPv6 في التراكب.
- حساب عنونة IPv6 في حلقة المفاتيح وكذلك ملف التعريف في تكوين التشفير.

في هذا المثال، يعلن الصرة عن ملخص EIGRP لجميع الخوادم الفرعية.

لا توصي Cisco باستخدام عنوان ملخص على واجهة القالب الظاهري في نشر FlexVPN؛ ومع ذلك، في شبكة VPN متعددة النقاط الديناميكية (DMVPN)، فإن هذا ليس شائعا فقط ولكنه يعد أيضا أفضل ممارسة. يمكنك الاطلاع على ترحيل FlexVPN: النقل الثابت من DMVPN إلى FlexVPN على الأجهزة نفسها: تكوين لوحة وصل محدث للحصول على تفاصيل.

```
ipv6 unicast-routing
ipv6 cef

ip local pool FlexSpokes 10.1.1.176 10.1.1.254
ipv6 local pool FlexSpokesv6 2001:DB8:0:FFFE::/112 128

crypto ikev2 authorization policy default
 ipv6 pool FlexSpokesv6
 pool FlexSpokes
 route set interface
crypto ikev2 keyring Flex_key
 peer ALL
 address ::/0
 pre-shared-key local cisco
 pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
aaa authorization group psk list default default
 virtual-template 1

crypto ikev2 dpd 30 5 on-demand

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp redirect
 ip tcp adjust-mss 1360
 ipv6 mtu 1400
 ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Loopback100
 ipv6 enable
 ipv6 eigrp 65001
```

```
 ipv6 nhrp network-id 2
 ipv6 nhrp redirect
 tunnel mode gre ipv6
tunnel protection ipsec profile default

interface Ethernet1/0
description LAN subnet
ip address 192.168.0.1 255.255.255.0
ipv6 address 2001:DB8:1111:2000::1/64
ipv6 enable
ipv6 eigrp 65001

interface Loopback0
ip address 172.25.1.1 255.255.255.255
ipv6 address 2001:DB8::1/128
ipv6 enable

ip route 192.168.0.0 255.255.0.0 Null0
ipv6 route 2001:DB8:1111::/48 Null0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ipv6 prefix-list EIGRP_SUMMARY_v6 seq 5 permit 2001:DB8:1111::/48

router eigrp 65001
distribute-list prefix EIGRP_SUMMARY_ONLY out Virtual-Template1
network 10.1.1.0 0.0.0.255
network 192.168.0.0 0.0.255.255
redistribute static metric 1500 10 10 1 1500

ipv6 router eigrp 65001
distribute-list prefix-list EIGRP_SUMMARY_v6 out Virtual-Template1
redistribute static metric 1500 10 10 1 1500
```

التكوين الذي تم التحدث به

كما هو الحال في تكوين الموزع، يحتاج المسؤول إلى توفير عنونة IPv6 وتمكين توجيه IPv6 وإضافة تكوين NHRP و crypto.

من الممكن إستخدام بروتوكول التوجيه المحسن (EIGRP) وبروتوكولات التوجيه الأخرى لأخذ نظرة على المحادثات. ومع ذلك، في سيناريو نموذجي، لا تكون البروتوكولات ضرورية وقد تؤثر على قابلية التطوير والاستقرار.

في هذا المثال، يحتفظ تكوين التوجيه بتجاور EIGRP فقط بين المتصل والمحور، والواجهة الوحيدة التي ليست خاملة هي واجهة Tunnel1:

```
ipv6 unicast-routing
ipv6 cef

crypto logging session

crypto ikev2 authorization policy default
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/0
```

```
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
aaa authorization group psk list default default
 virtual-template 1

crypto ikev2 dpd 30 5 on-demand

 interface Tunnel1
 description FlexVPN tunnel
 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
 delay 1000
 ipv6 mtu 1400
 ipv6 tcp adjust-mss 1358
 ipv6 address negotiated
 ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
 tunnel source Ethernet0/0
 tunnel mode gre ipv6
 tunnel destination 2001:DB8::1
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 ip mtu 1400
 ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 1000
 ipv6 mtu 1400
 ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Ethernet1/0
 ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
 tunnel mode gre ipv6
tunnel protection ipsec profile default
```

اتبع هذه التوصيات عند إنشاء إدخالات بروتوكول التوجيه على مكالمة:

1. السماح لبروتوكول التوجيه بإنشاء علاقة عبر الاتصال (في هذه الحالة، واجهة Tunnel1) بالموجه. ليس من المفضل بشكل عام إنشاء توجيه التجاور بين الخوادم لأن هذا يزيد من التعقيد بشكل كبير في معظم الحالات.

2. قم بالإعلان عن شبكة (شبكات) LAN الفرعية المحلية فقط، وتمكين بروتوكول التوجيه على عنوان IP الذي تم تعيينه بواسطة الصرة. أحرص على عدم الإعلان عن شبكة فرعية كبيرة لأنها قد تؤثر على الاتصال عبر المحادثة.

يعكس هذا المثال كلا من التوصيات ل EIGRP على Talk1:

```
 router eigrp 65001
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0 0.0.0.255
 passive-interface default
 no passive-interface Tunnel1
```

```
ipv6 router eigrp 65001
 passive-interface default
 no passive-interface Tunnel1
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

جلسة التحدث إلى المركز

تحتوي جلسة العمل التي تم تكوينها بشكل صحيح بين أجهزة موزع وأجهزة موزع على جلسة عمل Internet Key Exchange الإصدار 2 (IKEv2) قيد التشغيل ولها بروتوكول توجيه يمكنه إنشاء التجاور. في هذا المثال، يكون بروتوكول التوجيه هو EIGRP، لذلك هناك أمران EIGRP:

- **show crypto ikev2 sa**
- **show ipV6 eigrp 65001 neighbor**
- **show ip eigrp 65001 neighbor**

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
    none/none              READY          1
          Local  2001:DB8:0:100::2/500
          Remote  2001:DB8::1/500
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
                                                verify: PSK
                Life/Active Time: 86400/1945 sec

Spoke1#sh ipv6 eigrp 65001 neighbor
(EIGRP-IPv6 Neighbors for AS(65001
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
 sec)         (ms)       Cnt Num)
 Link-local address:     Tu1                 14 00:32:29   72  1470  0  10   0
                                              FE80::A8BB:CCFF:FE00:6600

Spoke1#show ip eigrp neighbors
(EIGRP-IPv4 Neighbors for AS(65001
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
 sec)         (ms)       Cnt Num)
 Tu1                 11 00:21:05   11  1398  0  26                10.1.1.1   0
```

في IPv4، يستخدم EIGRP عنوان IP معين إلى النظير؛ في المثال السابق، يكون عنوان IP للمحور من 10.1.1.1.

يستخدم IPv6 عنوان ربط محلي؛ في هذا المثال، الموزع هو FE80::A8bb:CCFF:FE00:6600. أستخدم الأمر **ping** للتحقق من إمكانية الوصول إلى الموزع من خلال IP المحلي الخاص به من خلال الارتباط:

```
Spoke1#ping FE80::A8BB:CCFF:FE00:6600
                Output Interface: tunnel1
.Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
:seconds 2
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnel1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

جلسة تحاور

يتم طرح الجلسات الحوارية بشكل ديناميكي عند الطلب. أستخدم أمر **ping** بسيط لتشغيل جلسة:

```
Spoke1#ping  2001:DB8:1111:2200::100 source e1/0
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 2001:DB8:1111:2200::100, timeout is 2 seconds
Packet sent with a source address of 2001:DB8:1111:2100::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/10 ms
```

لتأكيد الاتصال المباشر عبر المحادثة، يحتاج المسؤول إلى:

- تحقق من أن جلسة اتصال بينية ديناميكية تقوم بتشغيل واجهة وصول ظاهري جديدة:

```
LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed%
                                                        state to up
.CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP%
Peer 2001:DB8:0:200::2:500       Id: 2001:DB8:0:200::2
```

- تحقق من حالة جلسة عمل IKEv2:

```
Spoke1#show crypto ikev2 sa
IPv4 Crypto IKEv2  SA

IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
    none/none             READY          1
          Local  2001:DB8:0:100::2/500
         Remote  2001:DB8::1/500
,Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK
                                    Auth verify: PSK
     Life/Active Time: 86400/3275 sec

Tunnel-id    fvrf/ivrf              Status
    none/none             READY          2
          Local  2001:DB8:0:100::2/500
         Remote  2001:DB8:0:200::2/500
,Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK
                                    Auth verify: PSK
    Life/Active Time: 86400/665 sec
```

لاحظ أن هناك دورتين متاحتين: واحدة تحاكي المركز والأخرى تحاور.

- التحقق من NHRP:

```
Spoke1#show ipv6 nhrp
```

```
::DB8:0:FFFE::/128 via 2001:DB8:0:FFFE:2001
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router nhop rib nho
NBMA address: 2001:DB8:0:200::2
::DB8:1111:2200::/64 via 2001:DB8:0:FFFE:2001
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router rib nho
NBMA address: 2001:DB8:0:200::2
```

يظهر الناتج أن DB8:1111:2200::/64:2001 (الشبكة المحلية ل Talk2) متاحة عبر DB8:0:FFFE:2001::، وهو عنوان IPv6 الذي تم التفاوض عليه على واجهة Tunnel1 ل Talk2. تتوفر واجهة Tunnel1 عبر عنوان الوصول المتعدد غير للبث (NBMA) 2001:db8:0:200::2، وهو عنوان IPv6 المعين ل Talk2 بشكل ثابت.

- دققت أن حركة مرور يمر عبر أن قارن:

```
Spoke1#sh crypto ipsec sa peer 2001:DB8:0:200::2

interface: Virtual-Access1
Crypto map tag: Virtual-Access1-head-0, local addr 2001:DB8:0:100::2

(protected vrf: (none
(local  ident (addr/mask/prot/port): (2001:DB8:0:100::2/128/47/0
(remote ident (addr/mask/prot/port): (2001:DB8:0:200::2/128/47/0
current_peer 2001:DB8:0:200::2 port 500
{,PERMIT, flags={origin_is_acl
pkts encaps: 196, #pkts encrypt: 196, #pkts digest: 196#
pkts decaps: 195, #pkts decrypt: 195, #pkts verify: 195#
(...)
```

- تحقق من مسار التوجيه وإعدادات CEF:

```
Spoke1#show ipv6 route
(...)
[D   2001:DB8:1111:2200::/64 [90/27161600
[via 2001:DB8:0:FFFE::, Virtual-Access1 [Shortcut
via FE80::A8BB:CCFF:FE00:6600, Tunnel1
(...)
::Spoke1#show ipv6 cef 2001:DB8:1111:2200
DB8:1111:2200::/64:2001
nexthop 2001:DB8:0:FFFE:: Virtual-Access
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

تساعدك أوامر تصحيح الأخطاء هذه على أستكشاف المشاكل وإصلاحها:

- FlexVPN/IKEv2 و **debug crypto ipSecdebug crypto ikev2 [packet|internal** :IPsec**]**
- برنامج الشبكة الوطنية لحقوق الإنسان (تكلم):
  - **debug nhrp pack**
  - **debug nhrp extension**
  - **ذاكرة التخزين المؤقت ل NHRP للتصحيح**
  - **مسار تصحيح الأخطاء**

راجع قائمة الأوامر الرئيسية من Cisco IOS، جميع الإصدارات للحصول على مزيد من المعلومات حول هذه الأوامر.

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).