تحديث FlexVPN في تصميم لوحة وصل مزدوجة شبكة نهج لتكوين مثال مع مركزة

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
التكوين
الرسم التخطيطي للشبكة
شبكة النقل
شبكة ترابية
التكوينات التي تم التحدث بها
تكوين واجهة النفق التي تم التحدث عنها
تكوين بروتوكول العبارة الحدودية التي يتم التحدث بها (BGP)
تكوينات لوحة الوصل
المجموعات المحلية
تكوين Hub BGP
التحقق من الصحة
استكشاف الأخطاء وإصلاحها

المقدمة

يوضح هذا المستند كيفية تكوين تحدث في شبكة FlexVPN باستخدام كتلة تكوين عميل FlexVPN في سيناريو تتوفر فيه مراكز متعددة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- FlexVPN
- بروتوكولات التوجيه من Cisco

المكونات المستخدمة

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

- موجه الخدمة المتكاملة (Cisco G2 Series Integrated Service Router (ISR
- Cisco IOS®، الإصدار 15.2M

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.

التكوين

لأغراض التكرار، قد يحتاج الشخص الذي يتحدث إليه إلى الاتصال بمراكز متعددة. حيث تسمح الوحدات الاحتياطية على الجانب المتصل بالتشغيل المستمر دون حدوث نقطة فشل واحدة على جانب الموزع.

إن تصميمي لوحة الوصل المتكررة FlexVPN الأكثر شيوعا اللذين يستخدمان التكوين الذي يتم التحدث به هما:

- **نهج السحابة المزدوجة**، حيث يكون للخطيب نفقين منفصلين ينطلقان إلى كلا المركزين في جميع الأوقات.
- **نهج تجاوز الفشل**، حيث يكون للخطيب نفق نشط مع محور واحد في أي نقطة زمنية معينة.

ولكل من النهجين مجموعة فريدة من إيجابياته وسلبياته.

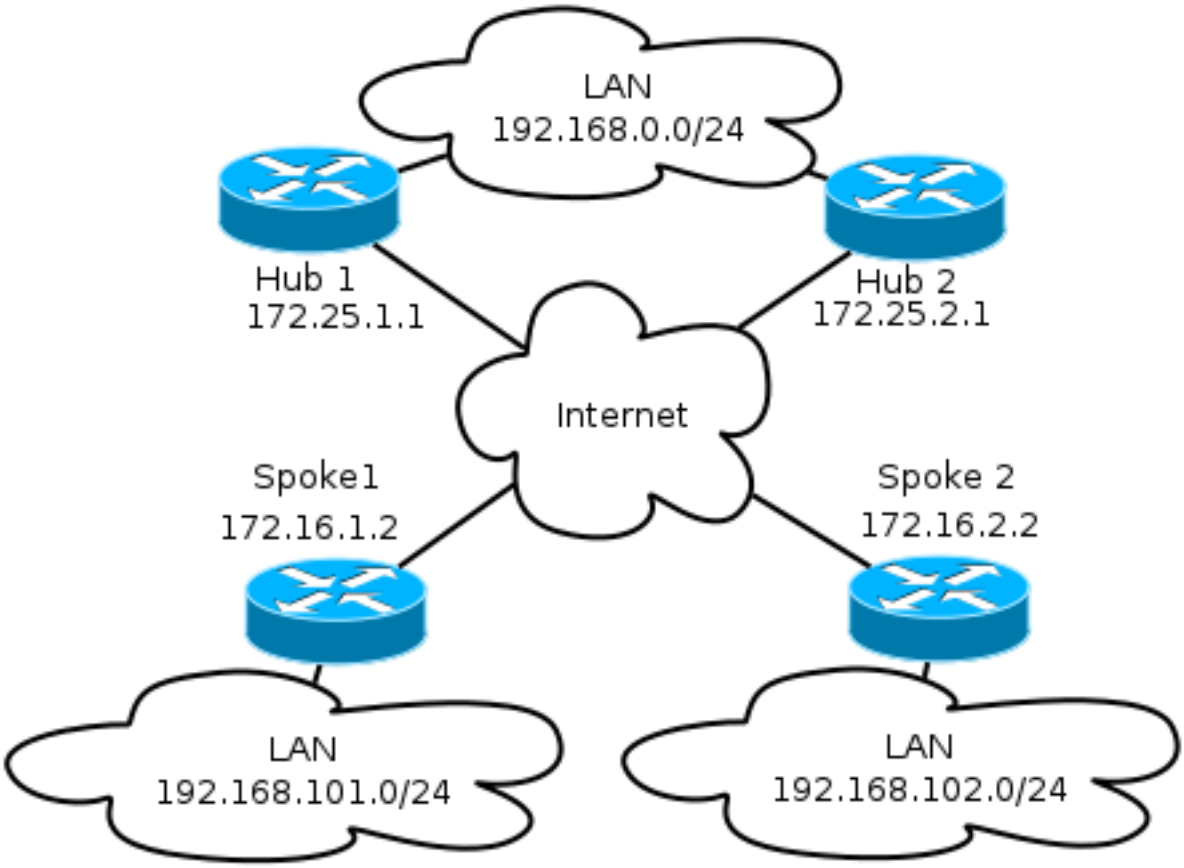
مقاربة	إيجابيات	مخاريط
سحابة مزدوجة	• إسترداد أسرع أثناء الفشل، استنادا إلى مؤقتات بروتوكول التوجيه • مزيد من إمكانيات توزيع حركة المرور بين المحاور، نظرا لأن الاتصال بكلا المركزين نشط	• ت ث إ ك ا ك ن ف ن س ا ت م ي ل ا ا ع ك ا ك ن
تجاوز الفشل	• سهولة التهيئة - مضمنة في شبكة FlexVPN • لا يعتمد على بروتوكول التوجيه في فشل	• و ت إ د أ - ا

وتصف هذه الوثيقة النهج الأول. المنهج إلى هذا تشكيل مماثل إلى ال حركي Multipoint VPN (DMVPN) مزدوج سحابة تشكيل. يعتمد التكوين الأساسي للمحور والمحور على مستندات الترحيل من DMVPN إلى FlexVPN. ارجع إلى ترحيل FlexVPN: النقل الثابت من DMVPN إلى FlexVPN على مقالة الأجهزة نفسها للحصول على وصف لهذا التكوين.

الرسم التخطيطي للشبكة

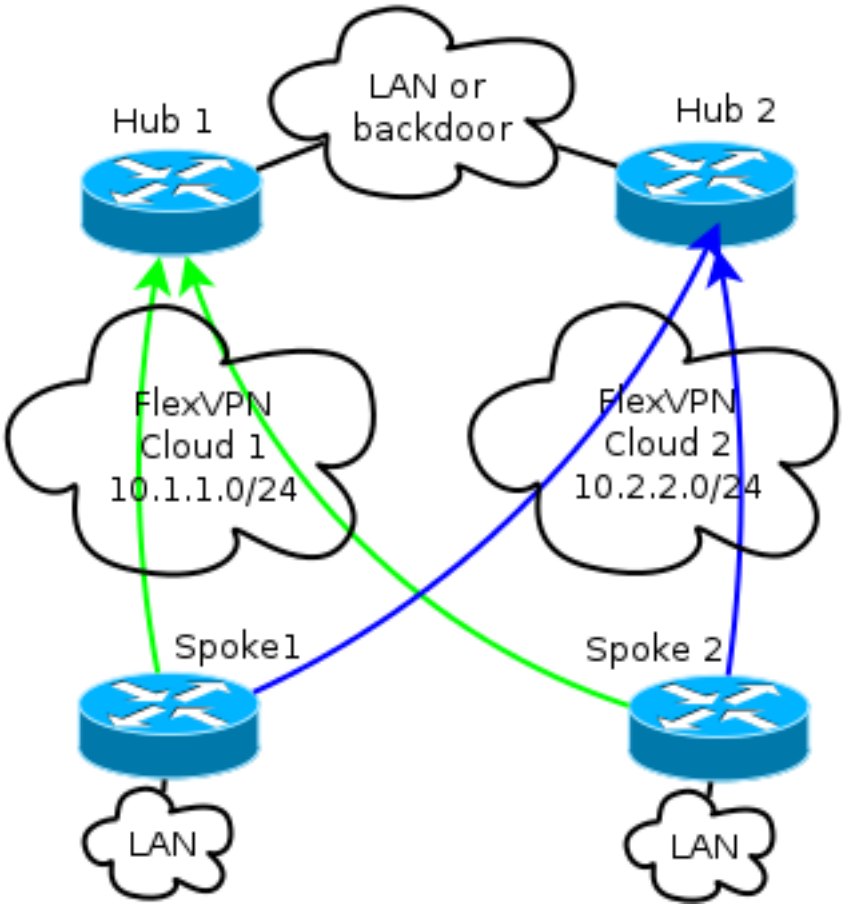
شبكة النقل

يوضح هذا المخطط شبكة النقل الأساسية المستخدمة عادة في شبكات FlexVPN.



شبكة ترابية

يوضح الرسم التخطيطي الشبكة الفرعية مع الاتصال المنطقي الذي يوضح كيفية عمل تجاوز الفشل. خلال العملية العادية، يحافظ الخطابان 1 و 2 على علاقة بكلا المركزين. عند حدوث فشل، يتم تحويل بروتوكول التوجيه من موزع إلى آخر.



ملاحظة: في الرسم التخطيطي، تظهر الخطوط الخضراء اتصال واتجاه Internet Key Exchange الإصدار 2 (IKEv2)/Flex session to Hub 1، وتشير الخطوط الزرقاء إلى الاتصال بالموجه 2.

يحتفظ كلا المركزين بعنونة IP منفصلة في السحب المتداخلة. تمثل عناوين **/24** تجمع العناوين المخصصة لهذه السحابة، وليس عنونة الواجهة الفعلية. وذلك لأن موزع FlexVPN يقوم عادة بتخصيص عنوان IP ديناميكي للواجهة التي يتم التحدث بها، ويعتمد على المسارات التي يتم إدخالها بشكل ديناميكي عبر أوامر التوجيه في كتلة تفويض FlexVPN.

التكوينات التي تم التحدث بها

تكوين واجهة النفق التي تم التحدث عنها

التشكيل النموذجي يستعمل في هذا مثال ببساطة إثنان نفق قارن مع إثنان غاية عنوان منفصل.

```
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 Ethernet0/0
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

```
interface Tunnel2
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 Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

للسماح بتهيئة الأنفاق التي يتم الاتصال بها بشكل صحيح، يلزم وجود قالب ظاهري (VT).

```
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
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

يستعمل ال يتحدث قارن غير رقم أن يشير ال LAN قارن في الفعلي تحشد وإعادة توجيه (VRF)، أي يكون شامل في هذه الحالة. ومع ذلك، قد يكون من الأفضل الإشارة إلى واجهة إسترجاع. وذلك لأن واجهات الاسترجاع تبقى على الإنترنت تحت جميع الظروف تقريبا.

تكوين بروتوكول العبارة الحدودية التي يتم التحدث بها (BGP)

بما أن Cisco يوصي iBGP كبروتوكول التوجيه أن يكون استعملت في الشبكة الفرعية، فإن هذا وثيقة يذكر فقط هذا تشكيل.

ملاحظة: يجب أن تحتفظ المحولات الفرعية بقابلية الوصول إلى كلا المحورين.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

لا تحتوي FlexVPN في هذا التكوين على مفهوم موزع أساسي أو ثانوي. يقرر المسؤول ما إذا كان بروتوكول التوجيه يفضل مركزا واحدا على آخر أو، في بعض السيناريوهات، تنفيذ موازنة الأحمال.

اعتبارات تجاوز الفشل والتقريب التي تحدث عنها

ولتقليل الوقت الذي يستغرقه التكلم لاكتشاف الفشل إلى الحد الادنى، إستعملوا هاتين الطريقتين النموذجيتين.

- اختصر مؤقتات BGP. يتسبب وقت الانتظار الافتراضي في تجاوز الفشل.
- قم بتكوين ترحيل BGP، والذي يتم إلغاء تحديده في هذه المقالة، ودعم BGP لإلغاء تنشيط جلسة التجميع السريع.
- لا تستخدم اكتشاف إعادة التوجيه ثنائي الإتجاه (BFD)، لأنه لا يوصى به في معظم عمليات نشر FlexVPN.

الأنفاق التي يتم التحدث إليها وتجاوز الفشل

تستخدم أنفاق المحادثات المحكية تبديل إختصار بروتوكول تحليل الخطوة (Hop) التالية (NHRP). يشير Cisco IOS إلى أن هذه الاختصارات هي مسارات NHRP، على سبيل المثال:

```
Spoke1#show ip route nhrp
(...)

is variably subnetted, 2 subnets, 2 masks 192.168.102.0/24
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

ولا تنتهي صلاحية هذه المسارات عند انتهاء صلاحية اتصال BGP، وبدلا من ذلك، يتم الاحتفاظ بها لوقت انتظار NHRP، وهو ساعتين بشكل افتراضي. وهذا يعني أن الأنفاق النشطة التي يتم التحدث إليها لا تزال تعمل حتى في حال فشل هذه الأنفاق.

تكوينات لوحة الوصل

المجموعات المحلية

وكما تمت مناقشته في قسم **الرسم التخطيطي للشبكة**، تحتفظ كلا المركزين بعنونة IP منفصلة.

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

الموزع 2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

تكوين Hub BGP

يبقى تكوين BGP للموزع مماثلا للأمثلة السابقة.

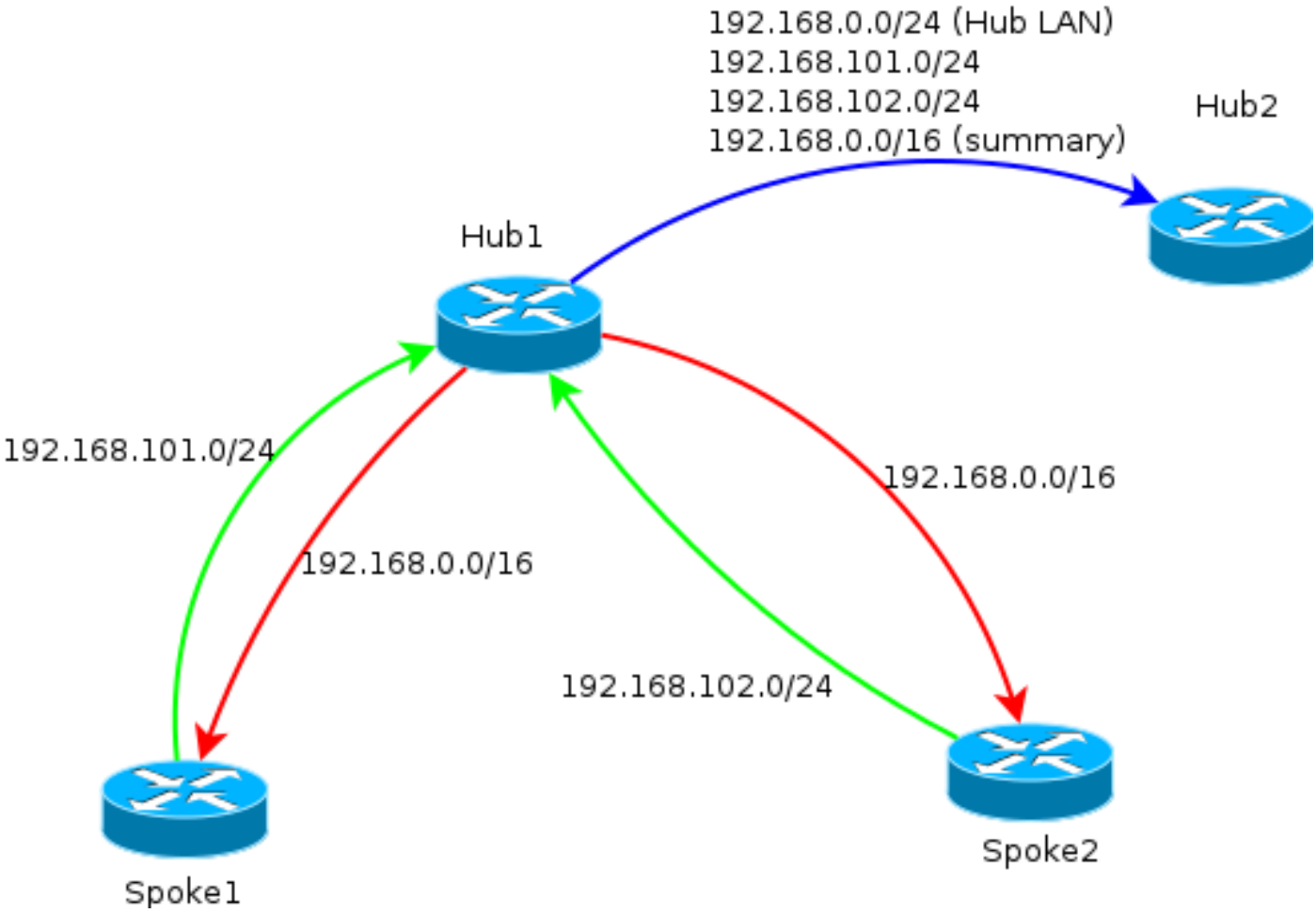
هذا إنتاج يأتي من صرة 1 مع lan عنوان **192.168.0.1**.

```
router bgp 65001
 bgp log-neighbor-changes
 bgp listen range 10.1.1.0/24 peer-group Spokes
 network 192.168.0.0
 aggregate-address 192.168.0.0 255.255.0.0 summary-only
 neighbor Spokes peer-group
 neighbor Spokes remote-as 65001
 neighbor Spokes fall-over
 neighbor 192.168.0.2 remote-as 65001
 neighbor 192.168.0.2 route-reflector-client
 neighbor 192.168.0.2 next-hop-self all
 neighbor 192.168.0.2 unsuppress-map ALL

route-map ALL permit 10
 match ip address 1

ip access-list standard 1
 permit any
```

وفي جوهر الأمر، فإن هذا هو ما يحدث:

- يوجد تجمع عناوين FlexVPN المحلي في نطاق إستماع BGP.
- الشبكة المحلية هي 24/192.168.0.0.
- يتم الإعلان عن الملخص فقط للسلسلات. يقوم تكوين عنوان التجميع بإنشاء مسار ساكن إستاتيكي لتلك البادئة عبر واجهة null0، وهي مسار discard يتم إستخدامه لمنع حلقات تكرار التوجيه.
- يتم الإعلان عن جميع البادئات المحددة للمحور الآخر. ونظرا لأنه أيضا اتصال iBGP، فإنه يتطلب تكوين عاكس مسار.

يمثل هذا الرسم التخطيطي تبادل بادئات BGP بين الفروع والمراكز في سحابة FlexVPN واحدة.



ملاحظة: في الرسم التخطيطي، يمثل الخط الأخضر المعلومات المقدمة من قبل الفروع إلى المحور، ويمثل الخط الأحمر المعلومات المقدمة من كل محور إلى الفروع (ملخص فقط)، ويمثل الخط الأزرق البادئات المتبادلة بين المحاور.

التحقق من الصحة

ونظرا لأن كل كلمة تحتفظ باقتران بكلا المحورين، تشاهد جلستان من جلسات IKEv2 باستخدام الأمر **show crypto ikev2 sa**.

```
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
none/none READY 172.16.2.2/500 172.16.1.2/500 3
```

```
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
                                                Life/Active Time: 86400/3147 sec

                                                Tunnel-id Local Remote fvrf/ivrf Status
                                              none/none READY 172.25.2.1/500 172.16.1.2/500 1
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
                                                Life/Active Time: 86400/3256 sec
```

لعرض معلومات بروتوكول التوجيه، أدخل الأوامر التالية:

```
show bgp ipv4 unicast

show bgp summary
```

على المحورين، ينبغي أن ترى أن الموجز إستلمت بادئة من المحاور، وأن الاتصالات إلى كلا المحاورين نشط.

```
                                                Spoke1#show bgp ipv4 unicast
                                        BGP table version is 4, local router ID is 192.168.101.1
                ,Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
                                ,r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter
                                            ,x best-external, a additional-path, c RIB-compressed
                                                Origin codes: i - IGP, e - EGP, ? - incomplete
                                            RPKI validation codes: V valid, I invalid, N Not found

                                                    Network Next Hop Metric LocPrf Weight Path
                                                 i 192.168.0.0/16 10.1.1.1 0 100 0 i<*
                                                               i 10.2.2.1 0 100 0 i *
                                                  i 32768 0 0.0.0.0 192.168.101.0 <*
                                                                Spoke1#show bgp summa
                                                               Spoke1#show bgp summary
                                        BGP router identifier 192.168.101.1, local AS number 65001
                                              BGP table version is 4, main routing table version 4
                                                    network entries using 296 bytes of memory 2
                                                      path entries using 192 bytes of memory 3
                                    BGP path/bestpath attribute entries using 408 bytes of memory 3/2
                                                BGP route-map cache entries using 0 bytes of memory 0
                                            BGP filter-list cache entries using 0 bytes of memory 0
                                                        BGP using 896 total bytes of memory
                                        BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

                                    Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
                                                 1 00:00:17 0 0 4 7 7 65001 4 10.1.1.1
                                                1 01:02:24 0 0 4 72 75 65001 4 10.2.2.1
```

استكشاف الأخطاء وإصلاحها

هناك قطاعان رئيسيان لاستكشاف الأخطاء وإصلاحها:

- تبادل مفتاح الإنترنت (IKE)
- أمان بروتوكول الإنترنت (IPsec)

هنا العرض أمر ذو صلة:

```
show crypto ipsec sa

show crypto ikev2 sa
```

هنا أوامر تصحيح الأخطاء ذات الصلة:

[debug crypto ikev2 [internal|packet

debug crypto ipsec

debug vtemplate event

فيما يلي بروتوكول التوجيه ذي الصلة:

(show bgp ipv4 unicast (or show ip bgp

show bgp summary

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).