

لائحة المحتويات لـ ASA/PIX: BGP

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[المنتجات ذات الصلة](#)

[الاصطلاحات](#)

[التكوين](#)

[الرسم التخطيطي للشبكة](#)

[السيناريو 1](#)

[السيناريو 2](#)

[مصادقة MD5 لجيران BGP من خلال PIX/ASA](#)

[تكوين PIX 6.x](#)

[PIX / ASA 7.x والإصدارات الأحدث](#)

[التحقق من الصحة](#)

[معلومات ذات صلة](#)

المقدمة

يوضح هذا التكوين العينة كيفية تشغيل بروتوكول العبارة الحدودية (BGP) عبر جهاز أمان (PIX/ASA) وكيفية تحقيق التكرار في بيئة BGP متعدد المنازل و PIX. مع [الرسم التخطيطي للشبكة](#) كمثال، يشرح هذا المستند كيفية توجيه حركة مرور البيانات تلقائياً إلى موفر خدمة الإنترنت (ISP-B) عندما يفقد AS 64496 الاتصال بـ ISP-A (أو العكس)، من خلال استخدام بروتوكولات التوجيه الديناميكية التي تعمل بين جميع الموجهات في AS 64496.

لأن BGP يستخدم حزم TCP للبت الأحادي على المنفذ 179 للاتصال بنظرائه، يمكنك تكوين PIX1 و PIX2 للسماح بحركة مرور البت الأحادي على منفذ 179 TCP. بهذه الطريقة، يمكن إنشاء نظير BGP بين الموجهات المتصلة من خلال جدار الحماية. يمكن تحقيق التكرار وسياسات التوجيه المطلوبة من خلال معالجة سمات BGP.

المتطلبات الأساسية

المتطلبات

قارئات هذا وثيقة سوفت كنت اعتاد مع [بشكل BGP](#) وأساسى جدار مانع للحريق.

المكونات المستخدمة

تستند سيناريوهات المثال في هذا المستند إلى إصدارات البرامج التالية:

- الموجهات طراز 2600 من Cisco المزودة بنظام التشغيل Cisco IOS ؟ برنامج الإصدار 12.2(27)

• PIX 515 مع جدار حماية Cisco PIX، الإصدار 6.3(3) والإصدارات الأحدث
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.

المنتجات ذات الصلة

كما يمكن استخدام هذا [التكوين](#) مع إصدارات الأجهزة والبرامج التالية:

- سلسلة أجهزة الأمان المعدلة Cisco Adaptive Security Appliance (ASA) 5500 مع الإصدار x.7 والإصدارات الأحدث
- الوحدة النمطية لخدمات جدار الحماية (FWSM) من Cisco التي تشغل الإصدار 3.2 من البرنامج والإصدارات الأحدث

الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

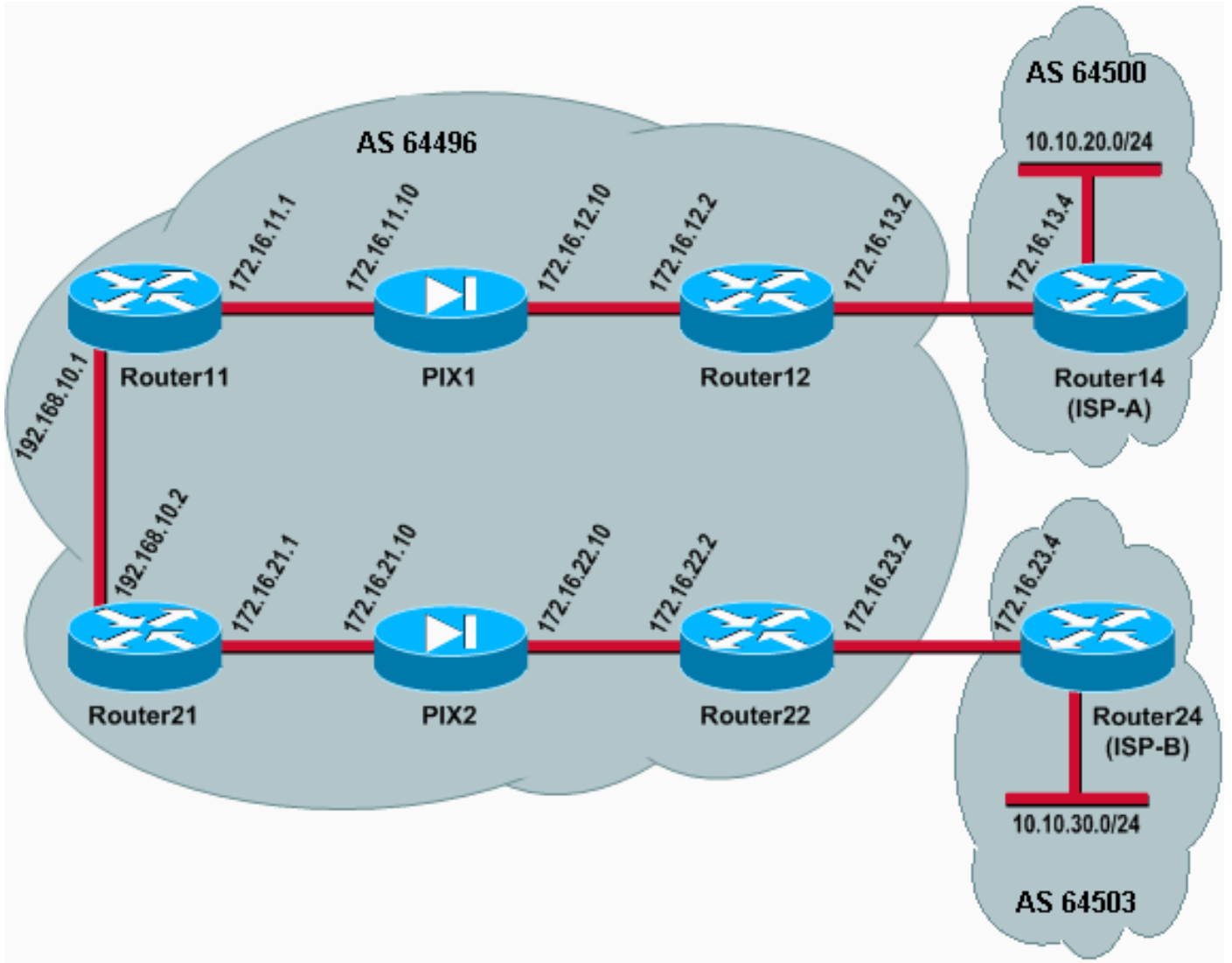
التكوين

يوفر هذا القسم معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر الواردة في هذا المستند، استخدم [أداة بحث الأوامر \(للعملاء المسجلين فقط\)](#).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



في إعداد الشبكة هذا، يتم تحويل الموجه 12 و Router22 (الذي ينتمي إلى AS 64496) إلى الموجه 14 (ISP-A) والموجه 24 (ISP-B) على التوالي للتركرار. توجد الشبكة الداخلية 24/192.168.10.0 داخل جدار الحماية. يتصل الموجه 11 والموجه 21 والموجه 12 والموجه 22 من خلال جدار الحماية. لم يتم تكوين PIX1 و PIX2 لإجراء ترجمة عنوان الشبكة (NAT).

السيناريو 1

في هذا السيناريو، يقوم الموجه 12 في AS 64496 بتدوير BGP الخارجي (eBGP) باستخدام الموجه 14 (ISP-A) في AS 64500. يقوم الموجه 12 أيضا بتقشير BGP داخلي (iBGP) باستخدام الموجه 11 عبر PIX1. إذا كانت الموجهات التي تتعلم بها eBGP من ISP-A، فإن الموجه 12 يعلن عن مسار افتراضي 0/0.0.0.0 على iBGP إلى الموجه 11. إذا فشل الارتباط ب ISP-A، يتوقف الموجه 12 عن إعلان المسار الافتراضي.

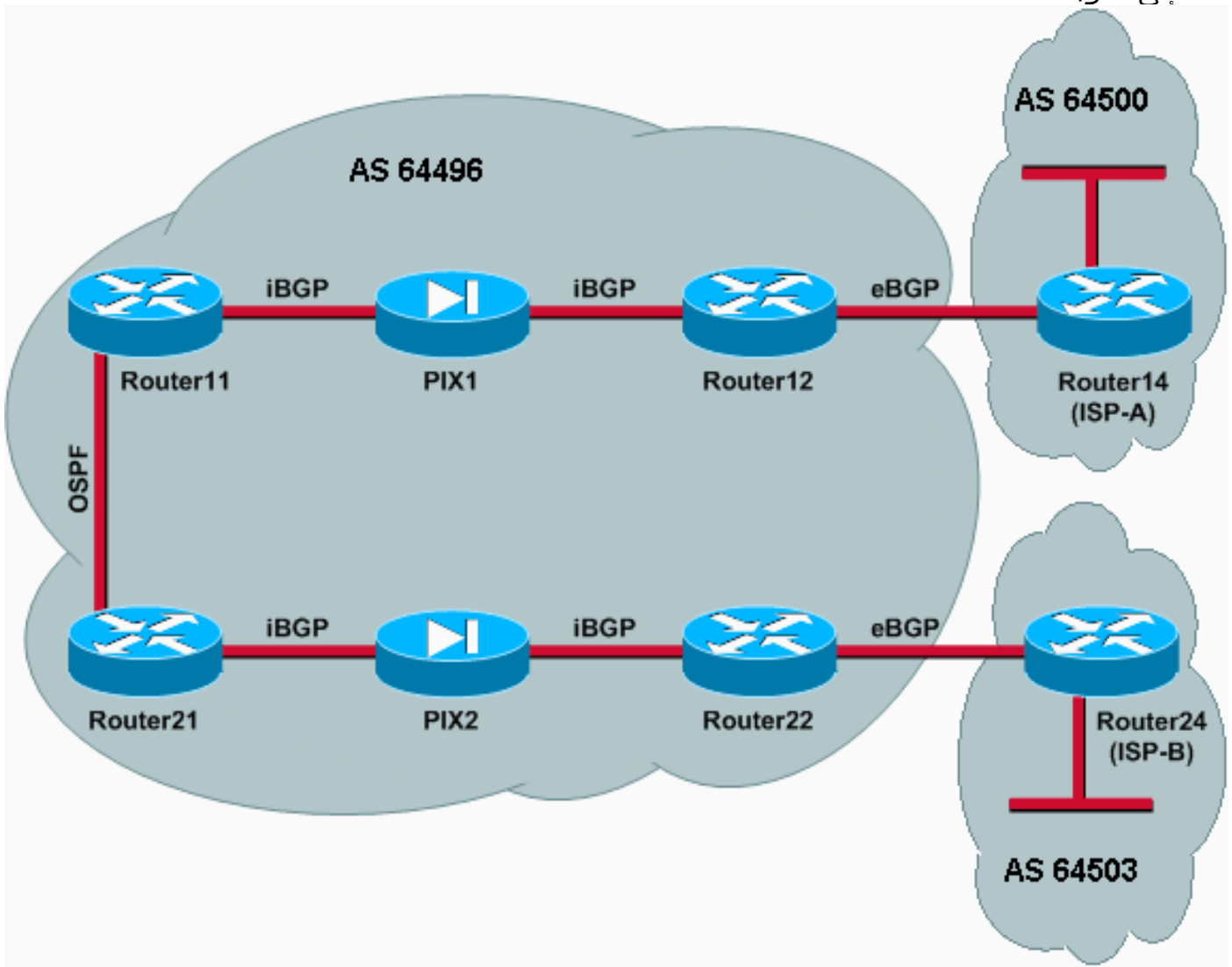
وبالمثل، فإن الموجه 22 في AS 64496 يقوم eBGP بالتفاف مع الموجه 24 (ISP-B) في AS 64503 ويعلن عن مسار افتراضي على iBGP إلى الموجه 21 بشروط بناء على وجود مسارات ISP-B في جدول التوجيه الخاص به.

من خلال استخدام قائمة الوصول، يتم تكوين PIX1 و PIX2 للسماح بحركة مرور (TCP) BGP، المنفذ (179) بين أقران iBGP. وذلك لأن واجهات PIX تحتوي على مستوى أمان مرتبط. بشكل افتراضي، تحتوي الواجهة الداخلية (إيثرنت1) على مستوى أمان 100 وتحتوي الواجهة الخارجية (إيثرنت0) على مستوى أمان 0. عادة ما يتم السماح بالاتصالات وحركة المرور من واجهات مستوى الأمان الأعلى إلى الأدنى. للسماح بحركة المرور من واجهة مستوى أمان أقل إلى واجهة مستوى أمان أعلى، ومع ذلك، يجب عليك تحديد قائمة وصول بشكل صريح على PIX. أيضا، أنت ينبغي شكلت ساكن إستاتيكي nat ترجمة على PIX1 و PIX2، أن يسمح مسحاج تحديد على الخارج أن يبدأ BGP جلسة مع مسحاج تحديد على الداخل من PIX.

يقوم كل من الموجه 11 والموجه 21 بالإعلان المشروط عن المسار الافتراضي إلى مجال فتح أقصر مسار أولاً (OSPF) استناداً إلى المسار الافتراضي الذي تم تعلمه من iBGP. يعلن الموجه 11 المسار الافتراضي إلى مجال OSPF بمقياس 5، ويعلن الموجه 21 المسار الافتراضي بمقياس 30، وبالتالي فيفضل المسار الافتراضي من الموجه 11. يساعد هذا التكوين في نشر المسار الافتراضي 0/0.0.0.0 إلى الموجه 11 والموجه 21 فقط، والذي يحافظ على إستهلاك الذاكرة على الموجهات الداخلية ويحقق الأداء الأمثل.

لذلك، ولتليخيص هذه الشروط، هذه هي سياسة التوجيه ل AS 64496:

- AS 64496 يفضل الارتباط من الموجه 12 إلى ISP-A لجميع حركة المرور الصادرة (من 24/192.168.10.0 إلى الإنترنت).
- إذا فشل الاتصال ب ISP-A، فسيتم توجيه حركة مرور البيانات بالكامل عبر الارتباط من الموجه 22 إلى ISP-B.
- تستخدم جميع حركات المرور الواردة من الإنترنت إلى 24/192.168.10.0 الارتباط من ISP-A إلى الموجه 12.
- إذا فشل الارتباط من ISP-A إلى الموجه 12، فسيتم توجيه جميع حركة المرور الواردة عبر الارتباط من ISP-B إلى الموجه 22.



التكوينات

يستخدم هذا السيناريو التكوينات التالية:

- [الموجه 11](#)
- [الموجه 12](#)
- [الموجه 14 \(ISP-A\)](#)
- [الموجه 21](#)

الموجه 22 •

PIX1 •

PIX2 •

الموجه 11

```
hostname Router11
!
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
Connected to Router21. ! interface FastEthernet0/1 ---!
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router ospf 1 log-adjacency-changes network
192.168.10.0 0.0.0.255 area 0 default-information
originate metric 5 route-map check-default !--- A
default route is advertised into OSPF conditionally
(based on whether the link !--- from Router12 to ISP-A
is active), with a metric of 5. router bgp 64496 no
synchronization bgp log-neighbor-changes network
192.168.10.0 neighbor 172.16.12.2 remote-as 64496 !---
Configures Router12 as an iBGP peer . distance bgp 20
105 200 !--- Administrative distance of iBGP learned
routes is changed from default 200 to 105. no auto-
summary ! ip route 172.16.12.0 255.255.255.0
172.16.11.10 !--- Static route to iBGP peer, because it
is not directly connected. ! access-list 30 permit
0.0.0.0 access-list 31 permit 172.16.12.2 route-map
check-default permit 10 match ip address 30 match ip
next-hop 31
```

الموجه 12

```
hostname Router12
!
interface FastEthernet0/0
ip address 172.16.13.2 255.255.255.0
Connected to Router14 (ISP-A). ! interface ---!
FastEthernet0/1 ip address 172.16.12.2 255.255.255.0 !--
- Connected to PIX1. ! router bgp 64496 no
synchronization neighbor 172.16.11.1 remote-as 64496
neighbor 172.16.11.1 next-hop-self neighbor 172.16.11.1
default-originate route-map check-isp-a-route !--- A
default route is advertised to Router11 conditionally
(based on whether the link !--- from Router12 to ISP-A
is active). neighbor 172.16.11.1 distribute-list 1 out
neighbor 172.16.13.4 remote-as 64500 !--- Configures
Router14 (ISP-A) as an eBGP peer. neighbor 172.16.13.4
route-map adv-to-isp-a out no auto-summary ! ip route
172.16.11.0 255.255.255.0 172.16.12.10 !--- Static route
to iBGP peer, because it is not directly connected. !
access-list 1 permit 0.0.0.0 access-list 10 permit
192.168.10.0 access-list 20 permit 10.10.20.0 0.0.0.255
access-list 21 permit 172.16.13.4 ! route-map check-
isp-a-route permit 10 match ip address 20 match ip next-
hop 21 ! route-map adv-to-isp-a permit 10 match ip
address 10
```

الموجه 14 (ISP-A)

```
hostname Router14
!
```

```

interface Ethernet0/0
ip address 172.16.13.4 255.255.255.0
!
interface Ethernet0/1
ip address 10.10.20.1 255.255.255.0
!
router bgp 64500
network 10.10.20.0 mask 255.255.255.0
neighbor 172.16.13.2 remote-as 64496
! .Configures Router12 as an eBGP peer ---!

```

الموجه 21

```

hostname Router21
!
interface FastEthernet0/0
ip address 192.168.10.2 255.255.255.0
Connected to Router11. ! interface FastEthernet0/1 ---!
ip address 172.16.21.1 255.255.255.0 !--- Connected to
PIX2. ! router ospf 1 network 192.168.10.0 0.0.0.255
area 0 default-information originate metric 30 route-map
check-default !--- A default route is advertised into
OSPF conditionally (based on whether the link !--- from
Router22 to ISP-B is active), with a metric of 30. !
router bgp 64496 no synchronization network 192.168.10.0
neighbor 172.16.22.2 remote-as 64496 !--- Configures
Router22 as an iBGP peer. ! ip route 172.16.22.0
255.255.255.0 172.16.21.10 !--- Static route to iBGP
peer, because it is not directly connected. ! access-
list 30 permit 0.0.0.0 access-list 31 permit 172.16.22.2
route-map check-default permit 10 match ip address 30
! match ip next-hop 31

```

الموجه 22

```

hostname Router22
!
interface FastEthernet0/0
ip address 172.16.23.2 255.255.255.0
Connected to Router24 (ISP-B). ! interface ---!
FastEthernet0/1 ip address 172.16.22.2 255.255.255.0 !--
- Connected to PIX2. ! router bgp 64496 no
synchronization bgp log-neighbor-changes neighbor
172.16.21.1 remote-as 64496 !--- Configure Router21 as
an iBGP peer. neighbor 172.16.21.1 next-hop-self
neighbor 172.16.21.1 default-originate route-map check-
ispb-route !--- A default route is advertised to
Router21 conditionally (based on whether the link !---
from Router22 to ISP-B is active). ! neighbor
172.16.21.1 distribute-list 1 out neighbor 172.16.23.4
remote-as 64503 neighbor 172.16.23.4 route-map adv-to-
ispb out ! ip route 172.16.21.0 255.255.255.0
172.16.22.10 !--- Static route to iBGP peer, because it
is not directly connected. ! access-list 1 permit
0.0.0.0 access-list 10 permit 192.168.10.0 access-list
20 permit 10.10.30.0 0.0.0.255 access-list 21 permit
172.16.23.4 ! route-map check-ispb-route permit 10 match
ip address 20 match ip next-hop 21 ! route-map adv-to-
ispb permit 10 match ip address 10 set as-path prepend
10 10 10 !--- Route map used to change the AS path
.attribute of outgoing updates

```

(ISP-B) الموجه 24

```

                                hostname Router24
                                !
                                interface Loopback0
                                ip address 10.10.30.1 255.255.255.0
                                !
                                interface FastEthernet0/0
                                ip address 172.16.23.4 255.255.255.0
                                !
                                router bgp 64503
                                bgp log-neighbor-changes
                                network 10.10.30.0 mask 255.255.255.0
                                neighbor 172.16.23.2 remote-as 64496
                                ! .Configures Router22 as an eBGP peer ---!

```

PIX1

```

                                nameif ethernet0 outside security0
                                nameif ethernet1 inside security100
                                ip address outside 172.16.12.10 255.255.255.0
                                ip address inside 172.16.11.10 255.255.255.0
                                Configures the IP addresses for the inside and ---!
                                outside interfaces. access-list acl-1 permit tcp host
                                172.16.12.2 host 172.16.11.1 eq bgp
                                Access list allows BGP traffic to pass from outside ---!
                                to inside. access-list acl-1 permit icmp any any !---
                                .Allows ping to pass through for testing purposes only

                                access-group acl-1 in interface outside
                                nat (inside) 0 0.0.0.0 0.0.0.0 0 0
                                No NAT translation, to allow Router11 on the inside ---!
                                to initiate a BGP session !--- to Router12 on the
                                outside of PIX. static (inside,outside) 172.16.11.1
                                172.16.11.1 netmask 255.255.255.255 !--- Static NAT
                                translation, to allow Router12 on the outside to
                                initiate a BGP session !--- to Router11 on the inside of
                                PIX. route outside 0.0.0.0 0.0.0.0 172.16.12.2 1 route
                                inside 192.168.10.0 255.255.255.0 172.16.11.1 1

```

PIX2

```

                                nameif ethernet0 outside security0
                                nameif ethernet1 inside security100
                                ip address outside 172.16.22.10 255.255.255.0
                                ip address inside 172.16.21.10 255.255.255.0
                                Configures the IP addresses for the inside and ---!
                                outside interfaces. access-list acl-1 permit tcp host
                                172.16.22.2 host 172.16.21.1 eq bgp
                                Access list allows BGP traffic to pass from outside ---!
                                to inside. access-list acl-1 permit icmp any any !---
                                .Allows ping to pass through for testing purposes only

                                access-group acl-1 in interface outside
                                route outside 0.0.0.0 0.0.0.0 172.16.22.2 1
                                route inside 192.168.10.0 255.255.255.0 172.16.21.1 1
                                nat (inside) 0 0.0.0.0 0.0.0.0 0 0
                                No NAT translation, to allow Router21 on the inside ---!
                                to initiate a BGP session !--- to Router22 on the
                                outside of PIX. static (inside,outside) 172.16.21.1
                                172.16.21.1 netmask 255.255.255.255 ! -- Static NAT
                                translation, to allow Router22 on the outside to
                                initiate a BGP session !--- to Router21 on the inside of
                                .PIX

```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم **أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر **show**.

عندما تكون كلا جلسة BGP قيد التشغيل، يمكنك توقع توجيه جميع الحزم من خلال ISP-A. ضع في الاعتبار جدول BGP على الموجه 11. هو يعلم المسار الافتراضي 0/0.0.0.0 من الموجه 12 مع الخطوة التالية 172.16.12.2.

```
Router11# show ip bgp
```

```
BGP table version is 14, local router ID is 192.168.10.1
- Status codes: s suppressed, d damped, h history, * valid, > best, i
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
i0.0.0.0	172.16.12.2			100	0 i<*
i 32768	0	0.0.0.0	192.168.10.0		<*

يتم تثبيت المسار الافتراضي 0/0.0.0.0 الذي يتم التعرف عليه عبر BGP في جدول التوجيه، كما هو موضح في إخراج **show ip route** على الموجه 11.

```
Router11# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
candidate default, U - per-user static route, o - ODR - *
P - periodic downloaded static route
```

```
Gateway of last resort is 172.16.12.2 to network 0.0.0.0
```

```
C 192.168.10.0/24 is directly connected, FastEthernet0/0
is subnetted, 2 subnets 172.16.0.0/24
S 172.16.12.0 [1/0] via 172.16.11.10
C 172.16.11.0 is directly connected, FastEthernet0/1
B* 0.0.0.0/0 [105/0] via 172.16.12.2, 00:27:24
```

فكر الآن في جدول BGP على الموجه 21. كما يتعرف أيضا على المسار الافتراضي عبر الموجه 22.

```
Router21# show ip bgp
```

```
BGP table version is 8, local router ID is 192.168.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
i0.0.0.0	172.16.22.2			100	0 i<*
32768	0	0.0.0.0	192.168.10.0		<*

تعرف الآن ما إذا تم تثبيت المسار الافتراضي الذي تم تعلمه من BGP هذا في جدول التوجيه للموجه 21.

```
Router21# show ip route
```


Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 candidate default, U - per-user static route, o - ODR - *
 P - periodic downloaded static route

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

```
C    192.168.10.0/24 is directly connected, FastEthernet0/0
      is subnetted, 2 subnets 172.16.0.0/24
C      172.16.21.0 is directly connected, FastEthernet0/1
      S        172.16.22.0 [1/0] via 172.16.21.10
O*E2 0.0.0.0/0 [110/5] via 192.168.10.1, 00:27:06, FastEthernet0/0
```

يتم تعلم المسار الافتراضي في الموجه 21 عبر OSPF (لاحظ بادئة 0 على المسار 0/0.0.0.0). من المثير للاهتمام ملاحظة وجود مسار افتراضي تم تعلمه عبر BGP من الموجه 22، ولكن يعرض إخراج `show ip route` المسار الافتراضي الذي تم تعلمه عبر OSPF.

تم تثبيت المسار الافتراضي OSPF في الموجه 21 لأن الموجه 21 يعلم المسار الافتراضي من مصدرين: الموجه 22 عبر iBGP والموجه 11 عبر OSPF. تقوم عملية تحديد المسار بتثبيت المسار بمسافة إدارية أفضل في جدول التوجيه. وتبلغ المسافة الإدارية لبروتوكول فتح أقصر مسار أولاً (110 OSPF) في حين تبلغ المسافة الإدارية لبروتوكول iBGP 200. لذلك، يتم تثبيت المسار الافتراضي الذي تم تعلمه من OSPF في جدول التوجيه، لأن 110 هو أقل من 200. لمزيد من المعلومات حول تحديد المسار، ارجع إلى [تحديد المسار في موجهات Cisco](#).

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم لاستكشاف أخطاء التكوين وإصلاحها.

قم بإسقاط جلسة عمل BGP بين الموجه 12 و ISP-A.

```
Router12(config)# interface fas 0/0
```

```
Router12(config-if)# shut
```

```
,1w0d: %LINK-5-CHANGED: Interface FastEthernet0/0
      changed state to administratively down
```

```
,1w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0
      changed state to down
```

لا يحتوي الموجه 11 على المسار الافتراضي الذي تم تعلمه عبر BGP من الموجه 12.

```
Router11# show ip bgp
```

```
BGP table version is 16, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
	0	0.0.0.0		192.168.10.0	<*

تحقق من جدول التوجيه على الموجه 11. يتم تعلم المسار الافتراضي عبر OSPF (المسافة الإدارية من 110) مع الخطوة التالية من Router21.

```
Output suppressed. Gateway of last resort is 192.168.10.2 to network 0.0.0.0 C ---!
192.168.10.0/24 is directly connected, FastEthernet0/0 172.16.0.0/24 is subnetted, 2 subnets S
172.16.12.0 [1/0] via 172.16.11.10 C 172.16.11.0 is directly connected, FastEthernet0/1 O*E2
0.0.0.0/0 [110/30] via 192.168.10.2, 00:00:09, FastEthernet0/0
```

هذا المخرج متوقع طبقا للنهج المحددة مسبقا. ومع ذلك، عند هذه النقطة، من المهم فهم أمر التكوين **distance bgp 20 105 200** في الموجه 11 وكيف يؤثر على تحديد المسار على الموجه 11.

القيم الافتراضية لهذا الأمر هي **المسافة BGP 20 200 200**، حيث يكون للمسارات التي تم التعرف عليها من بروتوكول eBGP مسافة إدارية تبلغ 20، والمسارات التي تم التعرف عليها من بروتوكول iBGP مسافة إدارية تبلغ 200، ولمسارات BGP المحلية مسافة إدارية تبلغ 200.

عندما يظهر الارتباط بين الموجه 12 و ISP-A مرة أخرى، يعلم الموجه 11 المسار الافتراضي عبر iBGP من الموجه 12. ومع ذلك، نظرا لأن المسافة الإدارية الافتراضية لهذا المسار الذي تم تعلمه عبر بروتوكول iBGP هي 200، فإنها لن تحل محل المسار الذي تم تعلمه بواسطة OSPF (لأن 110 هي أقل من 200). وهذا يفرض جميع حركة المرور الصادرة على الارتباط من الموجه 21 إلى الموجه 22 إلى ISP-B، حتى ولو كان الارتباط من الموجه 12 إلى ISP-A قيد التشغيل مرة أخرى. لحل هذه المشكلة، قم بتغيير المسافة الإدارية للمسار الذي تم تعلمه من iBGP إلى قيمة أقل من بروتوكول العبارة الداخلية (IGP) المستخدم. في هذا المثال، بروتوكول العبارة الداخلية هو OSPF، لذلك تم اختيار مسافة 105 (لأن 105 هي أقل من 110).

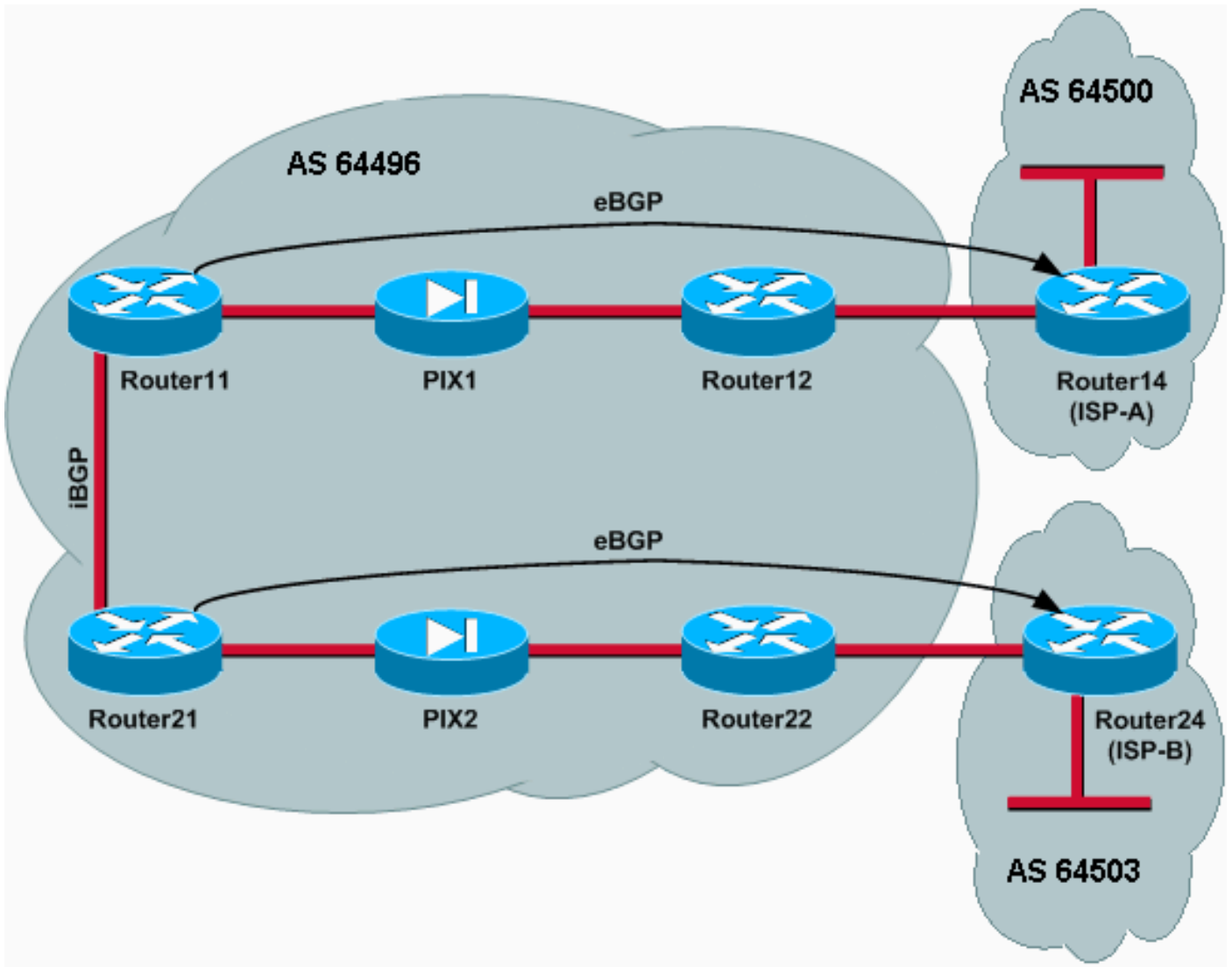
لمزيد من المعلومات حول أمر **المسافة BGP**، ارجع إلى **أوامر BGP**. لمزيد من المعلومات حول التجميع باستخدام BGP، ارجع إلى **مشاركة الحمل مع BGP في بيئات أحادية ومتعددة المسارات: نموذج للتكوينات**.

السيناريو 2

في هذا السيناريو، يكون الموجه 11 عبارة عن تجانب مباشر لبروتوكول eBGP مع الموجه 14 (ISP-A)، بينما يكون الموجه 21 هو تجميع بيانات بروتوكول eBGP مباشرة مع الموجه 24 (ISP-B). لا يشارك الموجه 12 والموجه 22 في تجميع BGP، ولكنهم يوفران اتصال IP إلى موجهات خدمات الإنترنت (ISPs). نظرا لأن نظراء eBGP ليسوا جيران متصلين مباشرة، يتم استخدام الأمر **neighbor ebgp-multihop** على الموجهات المشاركة. يمكن الأمر **neighbor ebgp-multihop** من تجاوز حد خطوة واحدة الافتراضي eBGP لأنه يغير زمن العيش (TTL) لحزم eBGP من القيمة الافتراضية ل 1. في هذا السيناريو، يتم تكوين جارة eBGP على بعد 3 نقلات، لذلك يتم تكوين **neighbor ebgp-multihop 3** على الموجهات المشاركة حتى يتم تغيير قيمة TTL إلى 3. أيضا، يتم تكوين المسارات الثابتة على الموجهات و PIX لضمان أن الموجه 11 يمكنه اختبار اتصال الموجه 14 (ISP-A) بالعنوان 172.16.13.4 ولضمان أن الموجه 21 يمكنه اختبار اتصال الموجه 24 (ISP-B) والعنوان 172.16.23.4.

بشكل افتراضي، لا يسمح PIX لحزم بروتوكول رسائل التحكم في الإنترنت (ICMP) (التي يتم إرسالها عند إصدار الأمر **ping**) بالمرور. للسماح بحزم ICMP، استخدم الأمر **access-list** كما هو موضح في تكوين PIX التالي. للحصول على مزيد من المعلومات حول الأمر **access-list**، ارجع إلى أوامر جدار حماية **A through B** PIX.

سياسة التوجيه هي نفسها الموجودة في **السيناريو 1**: يتم تفضيل الارتباط بين الموجه 12 و ISP-A على الارتباط بين الموجه 22 و ISP-B، وعندما ينزل ارتباط ISP-A إلى أسفل يتم استخدام ارتباط ISP-B لجميع حركة المرور الواردة والصادرة.



التكوينات

يستخدم هذا السيناريو التكوينات التالية:

- [الموجه 11](#)
- [الموجه 12](#)
- [الموجه 14 \(ISP-A\)](#)
- [الموجه 21](#)
- [الموجه 22](#)
- [PIX1](#)
- [PIX2](#)

الموجه 11

```

hostname Router11
!
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
Connected to Router21. ! interface FastEthernet0/1 ---!
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router bgp 64496 no synchronization bgp log-
neighbor-changes network 192.168.10.0 neighbor
172.16.13.4 remote-as 64500 neighbor 172.16.13.4 ebgp-

```

```

multihop 3 !--- To accept and attempt BGP connections to
external peers that reside on networks that !--- are not
directly connected. neighbor 172.16.13.4 route-map set-
pref in !--- Sets higher local-preference for learned
routes. neighbor 172.16.13.4 route-map adv_to_ispa out
neighbor 192.168.10.2 remote-as 64496 neighbor
192.168.10.2 next-hop-self no auto-summary ! ip route
172.16.12.0 255.255.255.0 172.16.11.10 ip
route172.16.13.4 255.255.255.255 172.16.11.10 !---
Static route to eBGP peer, because it is not directly
connected. ! access-list 20 permit 192.168.10.0 ! route-
map set-pref permit 10 set local-preference 200 ! route-
! map adv_to_ispa permit 10 match ip address 20

```

الموجه 12

```

hostname Router12
!
interface FastEthernet0/0
ip address 172.16.13.2 255.255.255.0
Connected to ISP-A. ! interface FastEthernet0/1 ip ---
address 172.16.12.2 255.255.255.0 !--- Connected to
PIX1. ! ip route 172.16.11.0 255.255.255.0 172.16.12.10
ip route 192.168.10.0 255.255.255.0 172.16.12.10

```

الموجه 14 (ISP-A)

```

hostname Router14
!
interface Ethernet0/0
ip address 172.16.13.4 255.255.255.0
!
interface Ethernet0/1
ip address 10.10.20.1 255.255.255.0
!
router bgp 64500
no synchronization
network 10.10.20.0 mask 255.255.255.0
neighbor 172.16.11.1 remote-as 64496
neighbor 172.16.11.1 ebgp-multihop 3
To accept and attempt BGP connections to external ---!
peers that reside on networks that !--- are not directly
connected. neighbor 172.16.11.1 default-originate !---
Advertises a default route to Router11. no auto-summary
! ip route 172.16.11.1 255.255.255.255 172.16.13.2 !---
Static route to eBGP peers, because it is not directly
.connected

```

الموجه 21

```

hostname Router21
!
interface FastEthernet0/0
ip address 192.168.10.2 255.255.255.0
Connected to Router11. ! interface FastEthernet0/1 ---
ip address 172.16.21.1 255.255.255.0 !--- Connected to
PIX2. ! router bgp 64496 no synchronization network
192.168.10.0 neighbor 172.16.23.4 remote-as 64503
neighbor 172.16.23.4 ebgp-multihop 3 !--- To accept and
attempt BGP connections to external peers that reside on
networks that !--- are not directly connected. neighbor
172.16.23.4 route-map adv_to_ispb out neighbor
192.168.10.1 remote-as 64496 neighbor 192.168.10.1 next-

```

```

hop-self no auto-summary ! ip route 172.16.22.0
255.255.255.0 172.16.21.10 ip route 172.16.23.4
255.255.255.255 172.16.21.10 !--- Static routes
configured to reach BGP peer. ! access-list 20 permit
192.168.10.0 ! route-map adv_to_ispb permit 10 match ip
address 20 set as-path prepend 10 10 10

```

الموجه 22

```

hostname Router22
!
interface FastEthernet0/0
ip address 172.16.23.2 255.255.255.0
Connected to Router24 (ISP-B). ! interface ---
FastEthernet0/1 ip address 172.16.22.2 255.255.255.0 !---
- Connected to PIX2. ! ip route 172.16.21.0
255.255.255.0 172.16.22.10 ip route 192.168.10.0
255.255.255.0 172.16.22.10

```

(ISP-B) الموجه 24

```

hostname Router24
!
interface Loopback0
ip address 10.10.30.1 255.255.255.0
!
interface FastEthernet0/0
ip address 172.16.23.4 255.255.255.0
Connected to Router22. ! router bgp 64503 no ---
synchronization bgp log-neighbor-changes network
10.10.30.0 mask 255.255.255.0 neighbor 172.16.21.1
remote-as 64496 neighbor 172.16.21.1 ebgp-multihop 3 !---
- To accept and attempt BGP connections to external
peers that reside on networks that !--- are not directly
connected. neighbor 172.16.21.1 default-originate !---
Advertises a default route to Router21. no auto-summary
! ip route 172.16.21.1 255.255.255.255 172.16.23.2 !---
Static route for BGP peer Router11, because it is not
.directly connected

```

PIX1

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
Access list allows BGP traffic to pass from outside --!
to inside. access-list acl-1 permit icmp any any !---
.Allows ping to pass through for testing purposes only

access-group acl-1 in interface outside
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.11.1 172.16.11.1 netmask
255.255.255.255
route outside 0.0.0.0 0.0.0.0 172.16.12.2 1
route inside 192.168.10.0 255.255.255.0 172.16.11.1 1

```

PIX2

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100

```

```

ip address outside 172.16.22.10 255.255.255.0
ip address inside 172.16.21.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.23.4 host
172.16.21.1 eq bgp
Access list allows BGP traffic to pass from outside --!
to inside. access-list acl-1 permit icmp any any !--
.Allow ping to pass through for testing purposes only

access-group acl-1 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.22.2 1
route inside 192.168.10.0 255.255.255.0 172.16.21.1 1
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.21.1 172.16.21.1 netmask
255.255.255.255

```

التحقق من الصحة

ابداً بالحالة التي تكون فيها الارتباطات ب ISP-A و ISP-B قيد التشغيل. يؤكد إخراج الأمر `show ip bgp summary` على الموجه 11 و Router21 جلسات BGP المنشأة مع ISP-A و ISP-B على التوالي.

Router11# `show ip bgp summary`

```

BGP router identifier 192.168.10.1, local AS number 10
BGP table version is 13, main routing table version 13
network entries and 5 paths using 568 bytes of memory 4
BGP path attribute entries using 420 bytes of memory 7
BGP AS-PATH entries using 48 bytes of memory 2
BGP route-map cache entries using 0 bytes of memory 0
BGP filter-list cache entries using 0 bytes of memory 0
BGP activity 43/264 prefixes, 75/70 paths, scan interval 15 secs

```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
2	02:13:36	0	0	13	1623	1627	64500	4	172.16.13.4
2	02:08:47	0	0	13	1601	1596	64496	4	192.168.10.2

Router21# `show ip bgp summary`

```

Output suppressed. Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd ---!
172.16.23.4 4 64503 1610 1606 8 0 0 02:06:22 2 192.168.10.1 4 64496 1603 1598 8 0 0 02:10:16 3

```

يعرض جدول BGP على الموجه 11 المسار الافتراضي (0/0.0.0.0) نحو الخطوة التالية 172.16.13.4 ISP-A.

Router11# `show ip bgp`

```

BGP table version is 13, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
i 20 0	200	172.16.13.4			0.0.0.0 <*
i 64500 0	200 0	172.16.13.4	10.10.20.0/24		<*
i10.10.30.0/24	192.168.10.2	0	100	0	64503 i<*
i192.168.10.0	192.168.10.2		0	100	0 i *
i 32768	0	0.0.0.0			<*

تحقق الآن من جدول BGP على الموجه 21. وله طريقان 0/0.0.0.0: تعلم أحدهما من ISP-B بالخطوة التالية 172.16.23.4 على eBGP، وتعلم الآخر عبر iBGP بتفضيل محلي قدره 200. يفضل الموجه 21 المسارات التي تم التعرف عليها من خلال iBGP بسبب سمة التفضيل المحلي الأعلى، وبالتالي فإنه يثبت هذا المسار في جدول التوجيه. لمزيد من المعلومات حول تحديد مسار BGP، ارجع إلى [خوارزمية تحديد مسار BGP الأفضل](#).

```
Router21# show ip bgp
```

```
BGP table version is 8, local router ID is 192.168.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
i 64503 0		172.16.23.4		0	0.0.0.0 *
i	192.168.10.1	200	0	64500	i<*
i10.10.20.0/24	192.168.10.1	0	200	0	64500 i<*
i 64503 0	0	172.16.23.4		10.10.30.0/24	<*
i	32768	0	0.0.0.0		192.168.10.0 <*
i		192.168.10.1		0	100 0 i *

استكشاف الأخطاء وإصلاحها

قم بإسقاط جلسة عمل BGP الخاصة بالموجه 11 و ISP-A.

```
Router11(config)# interface fas 0/1
```

```
Router11(config-if)# shut
```

```
,4w2d: %LINK-5-CHANGED: Interface FastEthernet0/1
changed state to administratively down
,4w2d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1
changed state to down
4w2d: %BGP-5-ADJCHANGE: neighbor 172.16.13.4 Down BGP Notification sent
4w2d: %BGP-3-NOTIFICATION: sent to neighbor 172.16.13.4 4/0 (hold time expired)0 bytes
تنتهي صلاحية جلسة عمل eBGP إلى ISP-A عندما تنتهي صلاحية مؤقت الاحتجاز (180 ثانية).
```

```
Router11# show ip bgp summary
```

```
Output suppressed. Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd ---!
172.16.13.4 4 64500 1633 1632 0 0 0 00:00:58 Active 192.168.10.2 4 64496 1609 1615 21 0 0
02:18:09
```

مع الارتباط ب ISP-A down، يقوم الموجه 11 بتثبيت 0/0.0.0.0 مع الخطوة التالية 192.168.10.2 (Router21)، والتي يتم التعرف عليها عبر iBGP في جدول التوجيه الخاص به. وهذا يدفع جميع حركة المرور الصادرة عبر الموجه 21 ثم إلى ISP-B، كما هو موضح في هذا الإخراج:

```
Router11# show ip bgp
```

```
BGP table version is 21, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
i0.0.0.0	192.168.10.2		100	0	64503 i<*
i10.10.30.0/24	192.168.10.2	0	100	0	64503 i<*
i192.168.10.0	192.168.10.2		0	100	0 i *
i 32768	0	0.0.0.0			<*

```
Router21# show ip bgp
```

```
BGP table version is 14, local router ID is 192.168.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
i 64503 0		172.16.23.4			0.0.0.0 <*
i 64503 0	0	172.16.23.4	10.10.30.0/24		<*
i 32768	0	0.0.0.0	192.168.10.0		<*
i	192.168.10.1		0	100	0 i *

مصادقة MD5 لجيران BGP من خلال PIX/ASA

تكوين PIX 6.x

ومثل أي بروتوكول توجيه آخر، يمكن تكوين BGP للمصادقة. يمكنك تكوين مصادقة MD5 بين نظاري BGP، ما يعني أنه يتم التحقق من صحة كل مقطع يتم إرساله على اتصال TCP بين النظراء. يجب تكوين مصادقة MD5 باستخدام نفس كلمة المرور على كلا نظاري BGP؛ وإلا، فلن يتم الاتصال بينهما. يتسبب تكوين مصادقة MD5 في قيام برنامج Cisco IOS بإنشاء ملخص MD5 وفحصه لكل مقطع يتم إرساله على اتصال TCP. في حالة إستدعاء المصادقة وفشل مصادقة مقطع ما، يتم إنشاء رسالة خطأ.

عندما تقوم بتكوين أقران BGP باستخدام مصادقة MD5 التي تمر من خلال جدار حماية PIX، من المهم تكوين PIX بين جيران BGP حتى لا تكون أرقام التسلسل الخاصة بدفق TCP بين جيران BGP عشوائية. وذلك لأن ميزة رقم التسلسل العشوائي ل TCP على جدار حماية PIX يتم تمكينها بشكل افتراضي، كما أنها تغير رقم تسلسل TCP للحزم الواردة قبل إعادة توجيهها.

يتم تطبيق مصادقة MD5 على رأس بروتوكول TCP PSUEDO-IP ورأس بروتوكول TCP والبيانات (ارجع إلى [RFC 2385](#)). يستخدم TCP هذه البيانات- والتي تتضمن تسلسل TCP وأرقام ACK- مع كلمة مرور جار BGP لإنشاء تجزئة 128 بت. يتم تضمين رقم التجزئة في الحزمة في حقل خيار رأس TCP. بشكل افتراضي، يقوم PIX بالإزاحة عن الرقم التسلسلي برقم عشوائي، لكل تدفق TCP. على نظير BGP المرسل، يستخدم TCP رقم التسلسل الأصلي لإنشاء رقم تجزئة MD5 إصدار 128 بت ويتضمن رقم التجزئة هذا في الحزمة. عندما يحصل نظير BGP المستقبل على الحزمة، يستخدم TCP رقم التسلسل المعدل بواسطة PIX لإنشاء رقم تجزئة MD5 إصدار 128 بت ويقارنه برقم التجزئة الذي يتم تضمينه في الحزمة.

يختلف رقم التجزئة لأن قيمة تسلسل TCP تم تغييرها بواسطة PIX، ويقوم TCP على جار BGP بإسقاط الحزمة وتسجيل رسالة MD5 الفاشلة المماثلة لهذه الرسالة:

```
TCP-6-BADAUTH: Invalid MD5 digest from 172.16.11.1:1778 to 172.16.12.2:179%
```

أستخدم الكلمة الأساسية `norandomseq` مع الكلمة الأساسية الثابتة (في الداخل، الخارج) `172.16.11.1 netmask 255.255.255.0 norandomseq` لحل هذه المشكلة وإيقاف PIX عن موازنة رقم تسلسل TCP. يوضح هذا المثال استخدام الكلمة الأساسية `norandomseq`:

```

الموجه 11
hostname Router11
!
interface FastEthernet0/0
ip address 192.168.10.1 255.255.255.0
Connected to Router21. ! interface FastEthernet0/1 ---!
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router ospf 1 log-adjacency-changes network
192.168.10.0 0.0.0.255 area 0 default-information
originate metric 5 route-map check-default !--- A
default route is originated conditionally, with a metric
of 5. ! router bgp 64496 no synchronization bgp log-
neighbor-changes network 192.168.10.0 neighbor
172.16.12.2 remote-as 64496 neighbor 172.16.12.2
password 7 08345C5A001A1511110D04
Configures MD5 authentication on BGP. distance bgp ---!

```



```

20 105 200 !--- Administrative distance of iBGP-learned
          routes is changed from default 200 to 105. !--- MD5
authentication is configured for BGP. no auto-summary !
ip route 172.16.12.0 255.255.255.0 172.16.11.10 !---
          Static route to iBGP peer, because it is not directly
          connected. ! access-list 30 permit 0.0.0.0 access-list
31 permit 172.16.12.2 route-map check-default permit 10
          match ip address 30 match ip next-hop 31

```

الموجه 12

```

hostname Router12
!
interface FastEthernet0/0
ip address 172.16.13.2 255.255.255.0
Connected to ISP-A. ! interface FastEthernet0/1 ip ---!
address 172.16.12.2 255.255.255.0 !--- Connected to
PIX1. ! router bgp 64496 no synchronization neighbor
172.16.11.1 remote-as 64496 neighbor 172.16.11.1 next-
hop-self neighbor 172.16.11.1 default-originate route-
map neighbor 172.16.11.1 password 7
08345C5A001A1511110D04
Configures MD5 authentication on BGP. check-ispa- ---!
route !--- Originate default to Router11 conditionally
if check-ispa-route is a success. !--- MD5
.authentication is configured for BGP

neighbor 172.16.11.1 distribute-list 1 out
neighbor 172.16.13.4 remote-as 64500
neighbor 172.16.13.4 route-map adv-to-ispa out
no auto-summary
!
ip route 172.16.11.0 255.255.255.0 172.16.12.10
          Static route to iBGP peer, because it is not ---!
          directly connected. ! access-list 1 permit 0.0.0.0
access-list 10 permit 192.168.10.0 access-list 20 permit
10.10.20.0 0.0.0.255 access-list 21 permit 172.16.13.4 !
route-map check-ispa-route permit 10 match ip address 20
match ip next-hop 21 ! route-map adv-to-ispa permit 10
match ip address 10

```

PIX1

```

nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
Access list allows BGP traffic to pass from outside ---!
to inside. access-list acl-1 permit icmp any any !---
.Allow ping to pass through for testing purposes only

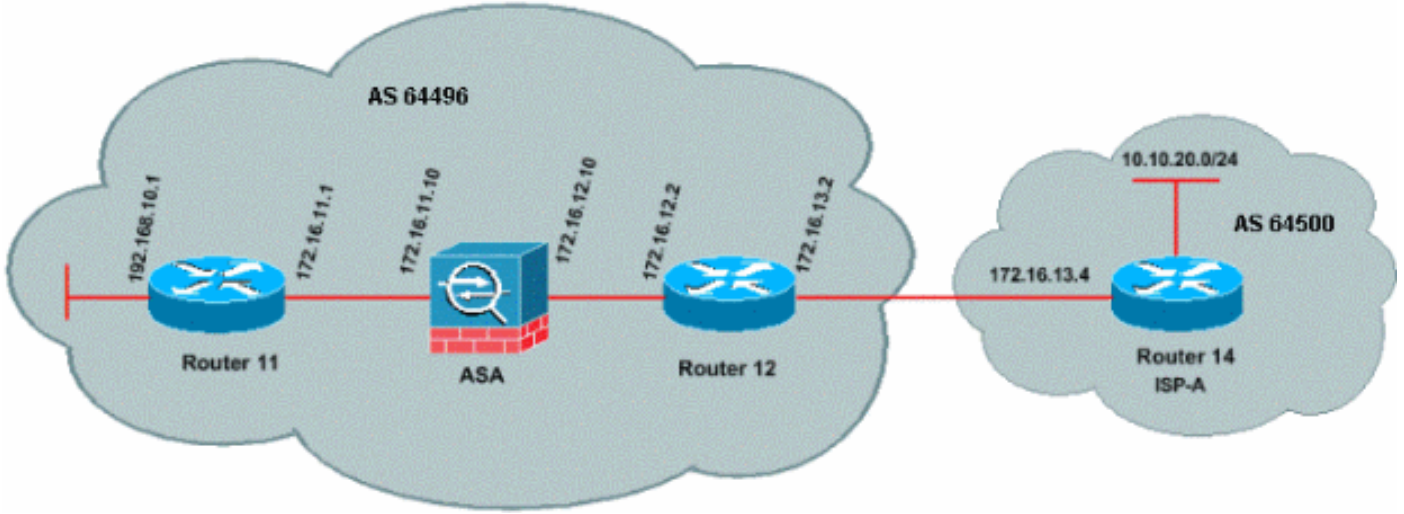
access-group acl-1 in interface outside
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.11.1 172.16.11.1 netmask
255.255.255.255 norandomseq

Stops the PIX from offsetting the TCP sequence ---!
number. route outside 0.0.0.0 0.0.0.0 172.16.12.2 1
route inside 192.168.10.0 255.255.255.0 172.16.11.1 1

```

PIX / ASA 7.x والإصدارات الأحدث

يستخدم هذا القسم إعداد الشبكة هذا.



يقدم الإصدار x.7 من بروتوكول PIX/ASA والإصدارات الأحدث تحدياً إضافياً عند محاولة إنشاء جلسة تجميع BGP باستخدام مصادقة MD5. بشكل افتراضي، يقوم PIX/ASA الإصدار x.7 والإصدارات الأحدث بإعادة كتابة أي خيار TCP MD5 مضمن في مخطط بيانات TCP الذي يمر عبر الجهاز ويحل محل نوع الخيار وحجمه وقيمه مع وحدات بايت خيار NOP. يؤدي هذا إلى كسر مصادقة BGP MD5 بشكل فعال، وينتج عنه رسائل خطأ مثل هذه على كل موجه نظير:

```
00296 : 2010 7 : 15:13:22.221 TCP-6-Badauth : MD5 172.16.11.1 (28894) 172.16.12.2 (179)
```

لكي يتم إنشاء جلسة BGP مع مصادقة MD5 بنجاح، يجب حل هذه المشاكل الثلاث:

- تعطيل عشوائية رقم تسلسل TCP
- تعطيل إعادة كتابة خيار TCP MD5
- تعطيل NAT بين الأقران

يتم استخدام خريطة الفئة وقائمة الوصول لتحديد حركة المرور بين الأقران الذين يجب إعفاؤهم من ميزة العشوائية لرقم تسلسل TCP والسماح لهم لحمل خيار MD5 دون إعادة الكتابة. يتم استخدام خريطة TCP لتحديد نوع الخيار الذي سيتم السماح به، في هذه الحالة، نوع الخيار 19 (خيار TCP MD5). يتم ربط كل من خريطة الفئة وخريطة tcp معا من خلال خريطة السياسة، وهي جزء من البنية الأساسية لإطار عمل السياسة النمطية. ثم يتم تنشيط التكوين باستخدام الأمر `service-policy`.

ملاحظة: تتم معالجة الحاجة إلى تعطيل NAT بين الأقران بواسطة الأمر `no nat-control`.

في الإصدار 7.0 والإصدارات الأحدث، لا تعد الطبيعة الافتراضية ل ASA هي `nat-control`، والتي تشير إلى أن كل اتصال عبر ASA، بشكل افتراضي، لا يلزم أن يجتاز اختبار NAT. من المفترض أن ASA لديه إعداد افتراضي بدون `NAT-control`. راجع [التحكم في nat](#) للحصول على مزيد من المعلومات. إذا تم فرض عنصر تحكم `nat`، فيجب عليك تعطيل NAT بشكل صريح لأقران BGP. يمكن القيام بذلك باستخدام الأمر الثابت بين الواجهات الداخلية والخارجية.

```
static (inside, outside) 172.16.11.1 172.16.11.1 netmask 255.255.255.255
```

PIX/ASA 7.x/8.x
<pre>ciscoasa# sh run Saved : : (ASA Version 8.2(1 !</pre>


```

policy-map type inspect dns preset_dns_map
    parameters
        message-length maximum 512
    policy-map global_policy
        class inspection_default
            inspect dns preset_dns_map
                inspect ftp
                inspect h323 h225
                inspect h323 ras
                inspect netbios
                inspect rsh
                inspect rtsp
                inspect skinny
                inspect esmtp
                inspect sqlnet
                inspect sunrpc
                inspect tftp
                inspect sip
                inspect xdmcp
            class BGP-MD5-CLASSMAP
                set connection random-sequence-number disable
                set connection advanced-options BGP-MD5-OPTION-ALLOW
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:64ea55d7271e19eea87c8603ab3768a2
end :

```

الموجه 11

```

Router11#sh run
hostname Router11
!
ip subnet-zero
!
interface Loopback0
no ip address
shutdown
!
interface Loopback1
ip address 192.168.10.1 255.255.255.0
!
interface Ethernet0
ip address 172.16.11.1 255.255.255.0
!
interface Serial0
no ip address
shutdown
no fair-queue
!
interface Serial1
no ip address
shutdown
!
interface BRI0
no ip address
encapsulation hdlc
shutdown
!
router bgp 64496
no synchronization
bgp log-neighbor-changes

```

```

network 192.168.10.0
neighbor 172.16.12.2 remote-as 64496

Configures MD5 authentication on BGP. neighbor ---!
172.16.12.2 password 7 123456789987654321

Administrative distance of iBGP-learned routes is ---!
changed from default 200 to 105. !--- MD5 authentication
is configured for BGP. distance bgp 20 105 200
no auto-summary
!
ip classless
Static route to iBGP peer, because it is not ---!
directly connected. ip route 172.16.12.0 255.255.255.0
172.16.11.10
ip http server
!
Output suppressed ---!

```

الموجه 12

```

Router12#sh run
hostname Router12
!
aaa new-model
!
ip subnet-zero
!
interface Ethernet0
ip address 172.16.13.2 255.255.255.0
!
interface Ethernet1
ip address 172.16.12.2 255.255.255.0
!
interface Serial0
no ip address
no fair-queue
!
interface Serial1
no ip address
shutdown
!
router bgp 64496
no synchronization
bgp log-neighbor-changes
neighbor 172.16.11.1 remote-as 64496

Configures MD5 authentication on BGP. neighbor ---!
172.16.11.1 password 7 123456789987654321
neighbor 172.16.11.1 next-hop-self

Originate default to Router11 conditionally if ---!
check-ispa-route is a success

neighbor 172.16.11.1 default-originate route-map check-
ispa-route
neighbor 172.16.11.1 distribute-list 1 out
neighbor 172.16.13.4 remote-as 64500
no auto-summary
!
ip classless

Static route to iBGP peer, because it is not ---!

```

```

directly connected. ip route 172.16.11.0 255.255.255.0
172.16.12.10 ip http server ! access-list 1 permit
0.0.0.0 access-list 10 permit 192.168.10.0 access-list
20 permit 10.10.20.0 0.0.0.255 access-list 21 permit
172.16.13.4 route-map check-isp-a-route permit 10 match
ip address 20 match ip next-hop 21 ! route-map adv-to-
isp-a permit 10 match ip address 10 ! !--- Output
suppressed

```

(ISP-A) 14 الموجه

```

Router14#sh run
hostname Router14
!
!
ip subnet-zero
!
interface Ethernet0
ip address 172.16.13.4 255.255.255.0
!
interface Ethernet1
ip address 10.10.20.1 255.255.255.0
!
interface Serial0
no ip address
shutdown
no fair-queue
!
interface Serial1
no ip address
shutdown
!
router bgp 64500
bgp log-neighbor-changes
network 10.10.20.0 mask 255.255.255.0

Configures Router12 as an eBGP peer. neighbor ---!
172.16.13.2 remote-as 64496 ! !--- Output suppressed ip
classless

```

التحقق من الصحة

يشير الإخراج من الأمر `show ip bgp summary` إلى أن المصادقة ناجحة وأن جلسة BGP يتم إنشاؤها على الموجه .11

```

Router11#show ip bgp summary
BGP router identifier 192.168.10.1, local AS number 64496
BGP table version is 8, main routing table version 8
network entries using 360 bytes of memory 3
path entries using 156 bytes of memory 3
BGP path/bestpath attribute entries using 248 bytes of memory 2/2
BGP route-map cache entries using 0 bytes of memory 0
BGP filter-list cache entries using 0 bytes of memory 0
BGP using 764 total bytes of memory
BGP activity 25/22 prefixes, 26/23 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
1             2      0      8      138    137   64496    4       172.16.13.2
Router11#

```

معلومات ذات صلة

- [صفحة دعم بروتوكول العبارة الحدودية \(BGP\)](#)
- [خوارزمية تحديد مسار BGP الأفضل](#)
- [مشاركة الأحمال مع بروتوكول بوابة الحدود \(BGP\) في بيئات أحادية ومتعددة المستويات: نموذج للتكوينات](#)
- [برنامج جدار حماية Cisco PIX](#)
- [مراجع أوامر جدار حماية PIX الآمن من Cisco](#)
- [تكوين جدار حماية PIX واختباره](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل