# ASA/PIX:BGP通過ASA配置示例

## 目錄



## 簡介

此示例配置演示了如何跨安全裝置(PIX/ASA)運行邊界網關協定(BGP)以及如何在多宿主BGP和PIX環境中實現冗餘。以網路圖表為例，本檔案將說明如何在AS 64496失去與ISP-A的連線時（或相反），通過使用在AS 64496中的所有路由器之間執行的動態路由通訊協定，將流量自動路由到網際網路服務供應商B(ISP-B)。

因為BGP在連線埠179上使用單點傳播TCP封包與它的對等路由器通訊，所以您可以設定PIX1和PIX2以允許TCP連線埠179上的單點傳播流量。透過這種方式，可以在透過防火牆連線的路由器之間建立BGP對等路由器。通過處理BGP屬性可以實現冗餘和所需的路由策略。

## 必要條件

### 需求

本文的讀者應熟悉設定BGP和基本防火牆組態。

### 採用元件

本檔案中的範例場景基於以下軟體版本：

- 採用Cisco IOS的Cisco 2600路由器？軟體版本12.2(27)

- 採用Cisco PIX防火牆版本6.3(3)及更高版本的PIX 515

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 相關產品

此設定也可以用於以下硬體和軟體版本：

- 採用7.x及更新版本的Cisco Adaptive Security Appliance(ASA)5500系列
- 執行軟體版本3.2和更新版本的思科防火牆服務模組(FWSM)

## 慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

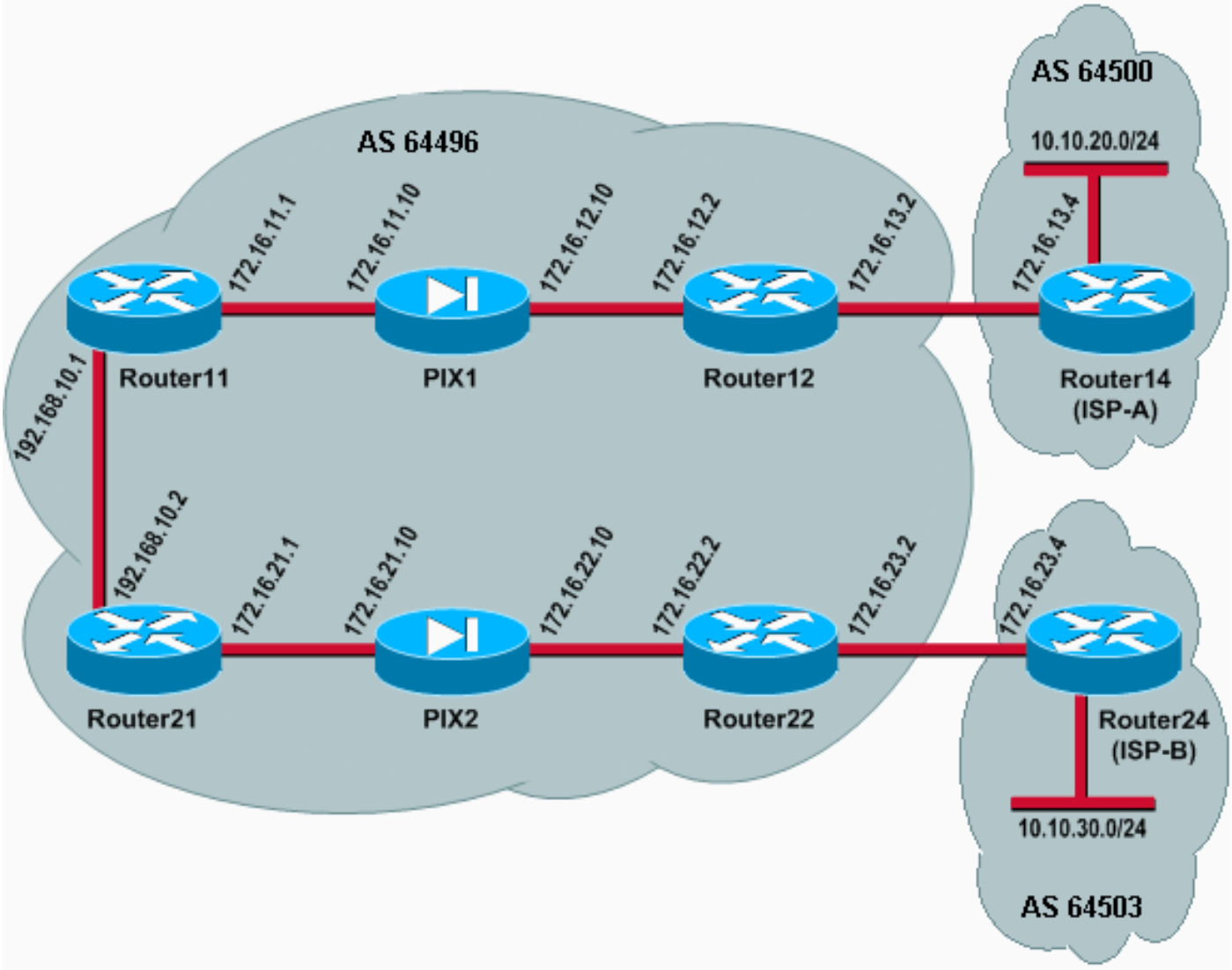
# 設定

本節提供設定本檔案中所述功能的資訊。

**注意：**要查詢有關本文檔中命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

## 網路圖表

本檔案會使用以下網路設定：




在此網路設定中，Router12和Router22(屬於AS 64496)分別多宿主到Router14(ISP-A)和Router24(ISP-B)以備冗餘。內部網路192.168.10.0/24位於防火牆內部。Router11和Router21通過防火牆連線到Router12和Router22。PIX1和PIX2未配置為執行網路地址轉換(NAT)。

## 案例 1

在此案例中，AS 64496中的Router12會與AS 64500中的Router14(ISP-A)進行外部BGP(eBGP)對等。Router12也會透過PIX1與Router11進行內部BGP(iBGP)對等。如果存在從ISP-A獲知的路由，Router12會在iBGP上向路由器11通告預設路由0.0.0.0/0。如果與ISP-A的連結失敗，Router會停止通告路由預設路由。

同樣地，AS 64496中的Router22會與AS 64503中的Router24(ISP-B)執行eBGP對等，並根據其路由表中是否存在ISP-B路由，有條件地向Router21通告iBGP上的預設路由。

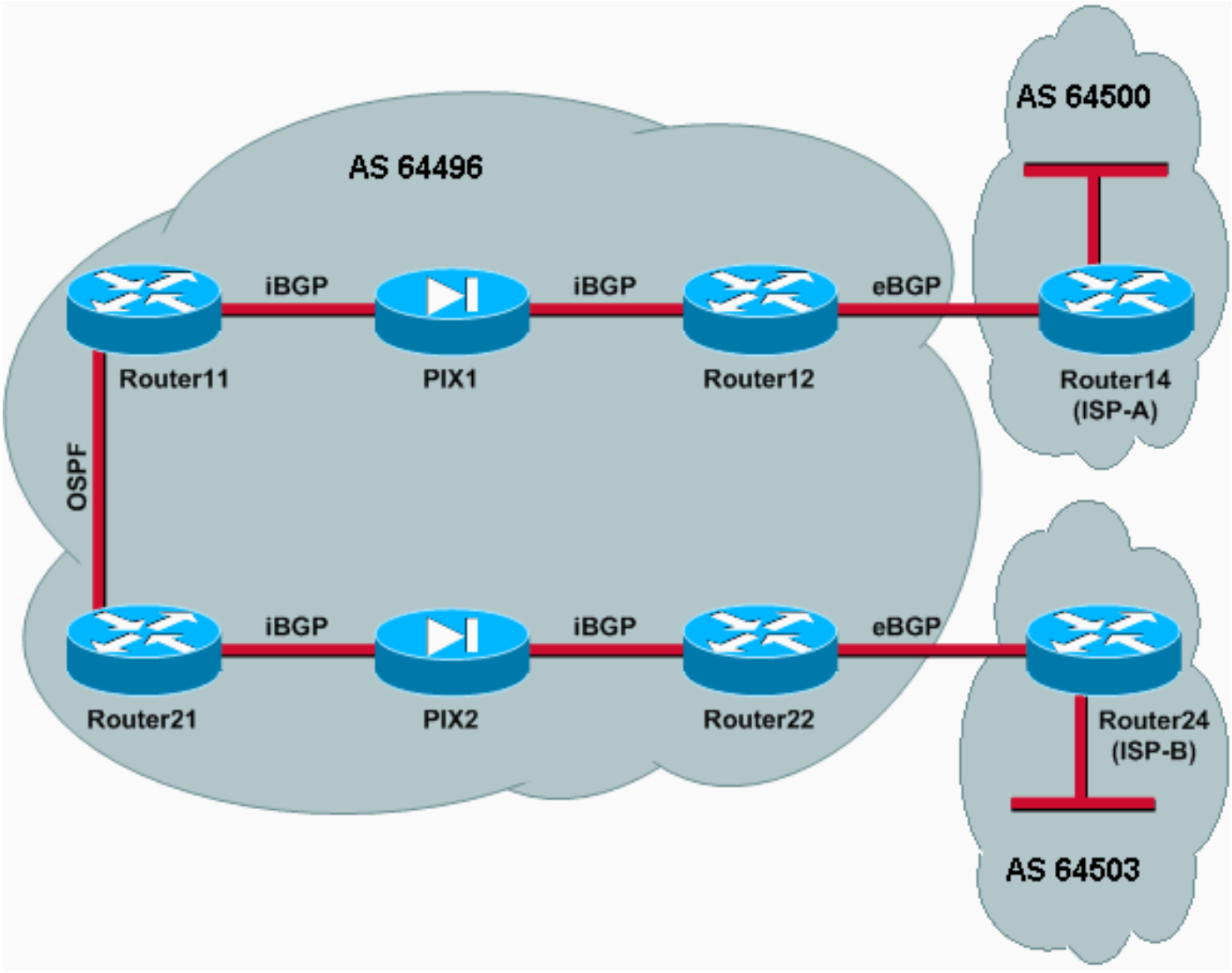
通過使用訪問清單，PIX1和PIX2配置為允許iBGP對等體之間的BGP流量（TCP，埠179）。這是因為PIX介面具有關聯的安全級別。預設情況下，內部介面(ethernet1)的安全級別為100，外部介面(ethernet0)的安全級別為0。通常允許從較高到較低安全級別的介面進行連線和通訊。但是，要允許從較低安全級別介面到較高安全級別介面的流量，必須在PIX上顯式定義訪問清單。此外，您還必須在PIX1和PIX2上配置靜態NAT轉換，以允許外部的路由器與PIX內部的路由器發起BGP會話。

Router11和Router21都會根據iBGP識別的預設路由有條件地將預設路由通告到開放最短路徑優先(OSPF)網域。Router11將預設路由通告到OSPF域，度量為5,Router21將通告預設路由，度量為30，因此首選來自Router11的預設路由。此配置有助於僅將預設路由0.0.0.0/0傳播到Router11和

Router21，從而節省內部路由器的記憶體消耗並實現最佳效能。

因此，概括這些條件，以下是AS 64496的路由策略：

- 對於所有出站流量(從192.168.10.0/24到Internet),AS 64496優先使用從Router12到ISP-A的鏈路。
- 如果到ISP-A的連線失敗，所有流量都通過鏈路從Router22路由到ISP-B。
- 從Internet到192.168.10.0/24的所有流量都使用從ISP-A到Router12的鏈路。
- 如果從ISP-A到Router12的鏈路發生故障，所有入站流量都會通過鏈路從ISP-B路由到Router22。




## 組態

此方案使用以下配置：

- Router11
- Router12
- Router14(ISP-A)
- Router21
- Router22
- PIX1
- PIX2

## Router11

```
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
```

## Router12

```
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-ispa-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-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
```

## Router14(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. !
```

## Router21

```
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 !
```

## Router22

```
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.
```

## Router24(ISP-B)

```
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.
```

## 驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

當兩個BGP會話都啟動時，可以期望所有資料包通過ISP-A路由。以Router11上的BGP表為例。它使用下一躍點172.16.12.2從Router12獲取預設路由0.0.0.0/0。

```
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
*> 192.168.10.0     0.0.0.0                  0         32768 i
```

通過BGP獲知的0.0.0.0/0預設路由將安裝在路由表中，如**Router11上的show ip route**輸出所示。

```
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
     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
B*   0.0.0.0/0 [105/0] via 172.16.12.2, 00:27:24
```

現在考慮Router21上的BGP表。它也會通過Router22獲取預設路由。

```
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
*> 192.168.10.0     0.0.0.0                  0         32768
```

現在檢視此BGP獲知的預設路由是否安裝在Router21的路由表中。

```
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
     172.16.0.0/24 is subnetted, 2 subnets
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
```

Router21中的預設路由是通過OSPF獲知的(請注意0.0.0.0/0路由上的o字首)。 值得注意的是，有一個通過BGP從Router22獲知的預設路由，但**show ip route**輸出顯示了通過OSPF獲知的預設路由。

OSPF預設路由安裝在Router21中，因為Router21從兩個來源獲取預設路由：Router22通過iBGP，Router11通過OSPF。路由選擇過程將具有更佳管理距離的路由安裝到路由表中。OSPF的管理距離是110，而iBGP的管理距離是200。因此，路由表中將安裝OSPF學習的預設路由，因為110小於200。有關路由選擇的詳細資訊，請參閱Cisco路由器中的路由選擇。

## 疑難排解

使用本節內容，對組態進行疑難排解。

關閉Router12和ISP-A之間的BGP會話。

```
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
```

Router11沒有從Router12通過BGP獲知的預設路由。

```
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
*> 192.168.10.0     0.0.0.0                  0
```

檢查Router11上的路由表。預設路由是通過OSPF（管理距離110）獲知的，下一跳為Router21。

```
Router11# show ip route
!--- 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
```

根據預定義的策略，此輸出是預期的。但是，此時必須瞭解Router11中的**distance bgp 20 105 200**組態命令，以及它如何影響Router11上的路由選擇。

此命令的預設值為**distance bgp 20 200 200**，其中eBGP獲知的路由的管理距離為20,iBGP獲知的路

由的管理距離為200，本地BGP路由的管理距離為200。

當Router12和ISP-A之間的鏈路再次啟動時，Router11會通過iBGP從Router12獲取預設路由。但是，由於此iBGP獲取的路由的預設管理距離是200，因此它不會替換OSPF獲取的路由（因為110小於200）。 這會強制所有從Router21到Router22到ISP-B的出站流量，即使從Router12到ISP-A的鏈路再次處於工作狀態。要解決此問題，請將iBGP獲知的路由的管理距離更改為小於所使用的內部網關協定(IGP)的值。在本例中，IGP是OSPF，因此選擇距離105（因為105小於110）。

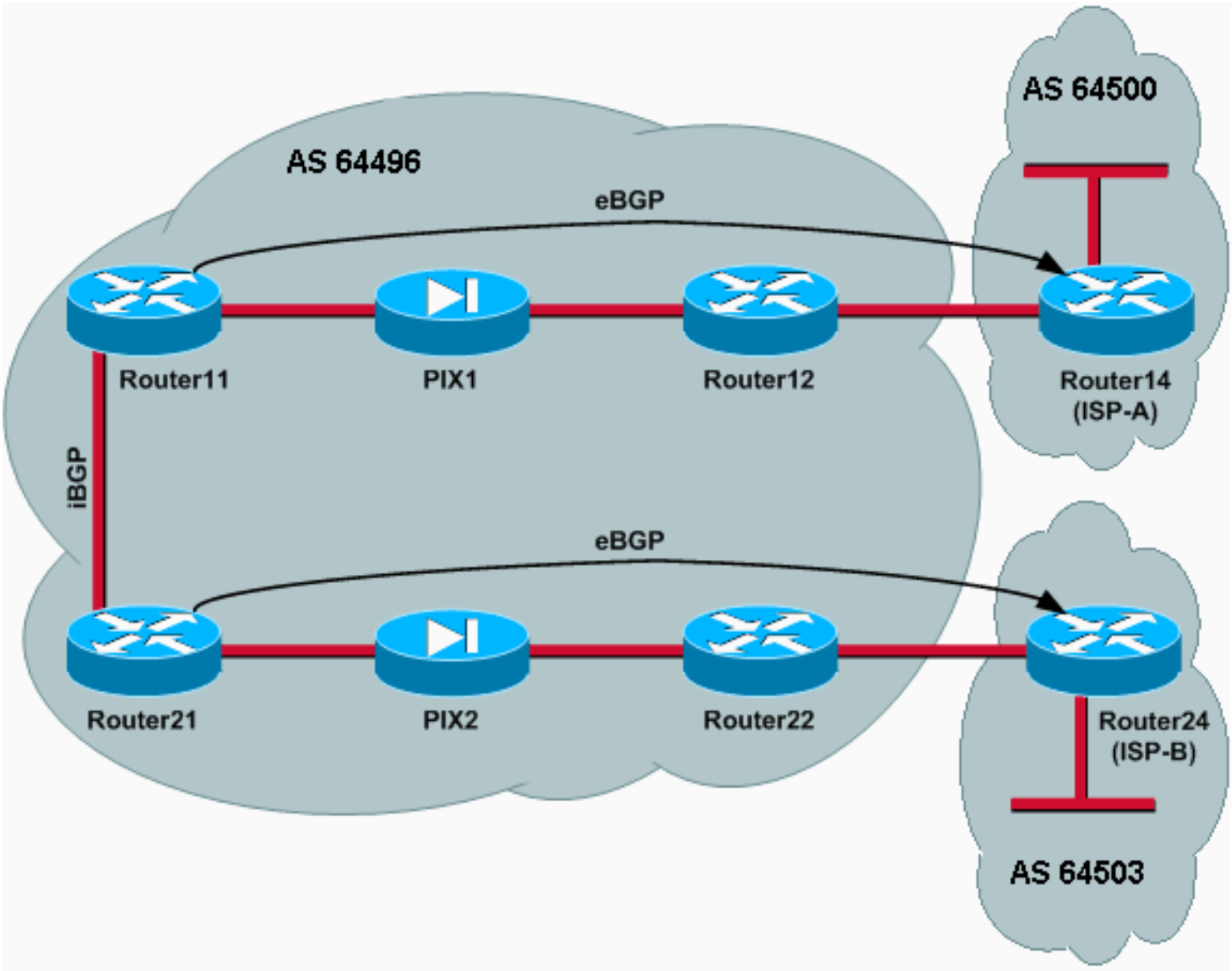
有關**distance bgp** 命令的詳細資訊，請參閱BGP命令。有關使用BGP的多宿主的詳細資訊，請參閱在單宿主和多宿主環境中使用BGP共用負載：配置示例。

## 案例 2

在此案例中，路由器11與路由器14(ISP-A)直接建立eBGP對等關係，路由器21與路由器24(ISP-B)直接建立eBGP對等關係。 Router12和Router22不參與BGP對等，但它們提供與ISP的IP連線。因為eBGP對等體不是直接連線的鄰居，所以在參與的路由器上使用**neighbor ebgp-multihop** 命令。**neighbor ebgp-multihop**命令使BGP能夠覆蓋預設的一跳eBGP限制，因為它將eBGP資料包的生存時間(TTL)從預設值1更改為預設值1。在此場景中，eBGP鄰居相隔3跳，因此在參與路由器上配置**neighbor ebgp-multihop 3**，以便將TTL值更改為3。此外，在路由器和PIX上配置靜態路由，以確保Router11能ping路由器14(ISP-A)地址2 ISP-B)地址172.16.23.4，並確保Router21能ping通Router24(ISP-B)地址。

預設情況下，PIX不允許網際網路控制消息協定(ICMP)資料包(在您發出**ping**命令時傳送)通過。要允許ICMP資料包，請使用**access-list**命令，如下一次PIX配置所示。有關**access-list** 命令的詳細資訊，請參閱PIX防火牆A至B命令。

路由策略與場景1相同:路由器12和ISP-A之間的鏈路優先於Router22和ISP-B之間的鏈路，當ISP-A鏈路斷開時，ISP-B鏈路用於所有入站和出站流量。




**組態**

此方案使用以下配置：

- Router11
- Router12
- Router14(ISP-A)
- Router21
- Router22
- PIX1
- PIX2

| Router11 |
| --- |
| 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 !
```

## Router12

```
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
```

## Router14(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.
```

## Router21

```
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 route172.16.23.4
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
```

## Router22

```
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
```

## Router24(ISP-B)

```
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 !--
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
static (inside,outside) 172.16.21.1 172.16.21.1 netmask
255.255.255.255
```

## 驗證

從通往ISP-A和ISP-B的鏈路已開啟的情況開始。Router11和Router21上的**show ip bgp summary**命令輸出分別確認與ISP-A和ISP-B建立的BGP會話。

```
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
4 network entries and 5 paths using 568 bytes of memory
7 BGP path attribute entries using 420 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 43/264 prefixes, 75/70 paths, scan interval 15 secs


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

Router11上的BGP表顯示了通向下一跳ISP-A 172.16.13.4的預設路由(0.0.0.0/0)。

```
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
*> 0.0.0.0          172.16.13.4                      200      0 20 i
*> 10.10.20.0/24    172.16.13.4              0       200      0 64500 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
*>                  0.0.0.0                  0         32768 i
```

現在檢查Router21上的BGP表。它有兩個0.0.0.0/0路由：一個從ISP-B獲知，在eBGP上下一跳為172.16.23.4，另一個通過iBGP獲知，本地優先順序為200。Router21優先使用iBGP獲知的路由，因為本地優先順序屬性較高，所以它會將該路由安裝到路由表中。有關BGP路徑選擇的詳細資訊，請參閱BGP最佳路徑選擇演算法。

```
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
*  0.0.0.0          172.16.23.4                             0    64503 i
*>i                 192.168.10.1                 200      0    64500 i
*>i10.10.20.0/24    192.168.10.1               0    200      0    64500 i
*> 10.10.30.0/24    172.16.23.4                0             0    64503 i
*> 192.168.10.0     0.0.0.0                    0         32768       i
* i                 192.168.10.1               0    100      0 i
```

## 疑難排解

關閉Router11和ISP-A BGP會話。

```
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
```

當抑制計時器（180秒）過期時，到ISP-A的eBGP會話將關閉。

```
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
```

在通往ISP-A的鏈路斷開時，Router11將下一跳安裝為192.168.10.2(Router21)的0.0.0.0/0，該跳通過iBGP在其路由表中獲取。這會將所有出站流量推送到路由器21，然後到ISP-B，如以下輸出所示：

```
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
*>                  0.0.0.0                  0         32768 i

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
*> 0.0.0.0          172.16.23.4                            0 64503 i
*> 10.10.30.0/24    172.16.23.4              0             0 64503 i
*> 192.168.10.0     0.0.0.0                  0         32768 i
* i                 192.168.10.1             0    100      0 i
```

# 通過PIX/ASA進行BGP鄰居的MD5身份驗證

## PIX 6.x配置

與任何其他路由協定一樣，BGP也可配置為進行身份驗證。您可以在兩個BGP對等點之間配置MD5身份驗證，這意味著對等點之間的TCP連線上傳送的每個分段都經過驗證。MD5身份驗證必須在兩個BGP對等體上使用相同的密碼進行配置；否則將不會建立兩者之間的連線。MD5身份驗證的配置會導致Cisco IOS軟體生成並檢查TCP連線上傳送的每個資料段的MD5摘要。如果呼叫了身份驗證，並且分段未通過身份驗證，則會生成錯誤消息。

當您使用通過PIX防火牆的MD5身份驗證配置BGP對等體時，在BGP鄰居之間配置PIX非常重要，這樣BGP鄰居之間TCP流的序列號就不是隨機的。這是因為PIX防火牆上的TCP隨機序列號功能預設啟用，並且在轉發傳入資料包之前會更改這些資料包的TCP序列號。

MD5驗證應用於TCP Psuedo-IP報頭、TCP報頭和資料上(請參閱RFC 2385 )。TCP使用此資料（包括TCP序列和ACK號）以及BGP鄰居密碼來建立128位雜湊值。雜湊數包含在TCP報頭選項欄位的資料包中。預設情況下，PIX將每個TCP流的序列號偏移一個隨機數。在傳送BGP對等體上，TCP使用原始序列號建立128位MD5雜湊值，並將此雜湊值包含在資料包中。當接收BGP對等體收到資料包時，TCP使用PIX修改的序列號建立128位MD5雜湊號，並將其與資料包中包含的雜湊號進行比較。

雜湊編號不同，因為PIX更改了TCP序列值，而BGP鄰居上的TCP丟棄該資料包並記錄與以下類似的MD5失敗消息：

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

使用帶有**static(inside，outside)172.16.11.1 172.16.11.1 netmask 255.255.255.0 norandomseq**命令的**norandomseq**關鍵字可解決此問題，並停止PIX偏移TCP序列號。此示例說明了**norandomseq**關鍵字的使用：

**Router11**

```
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
```

### Router12

```
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

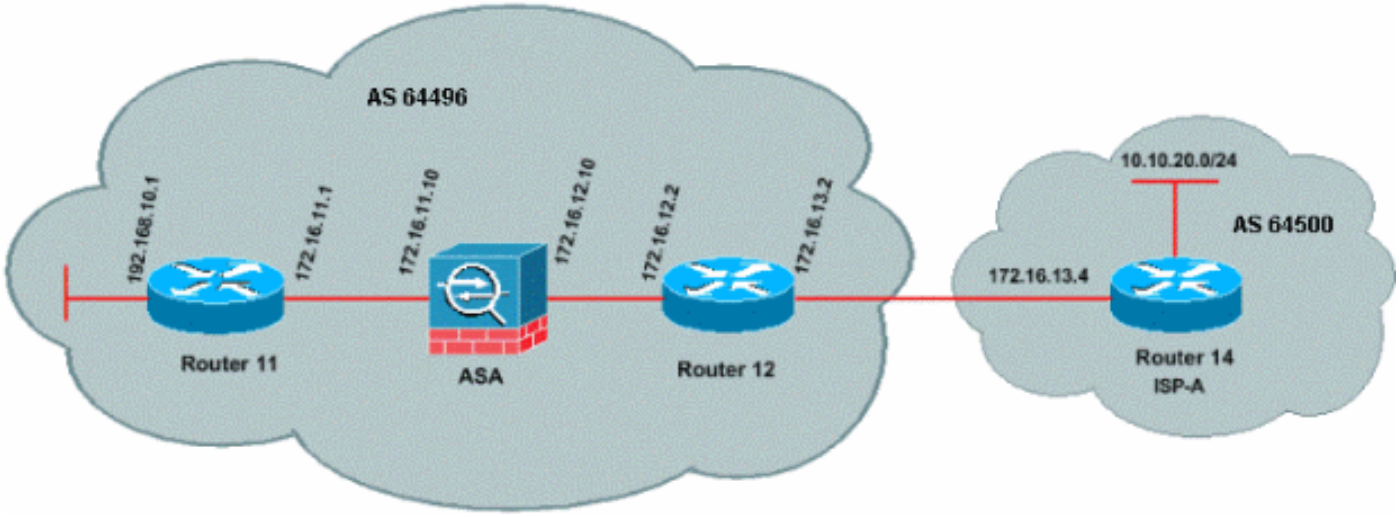
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside. access-list acl-1 permit icmp any any !---
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 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及更高版本

此部分使用此網路設定。




當您嘗試使用MD5身份驗證建立BGP對等會話時，PIX/ASA版本7.x及更高版本引入了一個額外的挑戰。預設情況下，PIX/ASA版本7.x及更高版本會重寫通過裝置的TCP資料包中包含的任何TCP MD5選項，並用NOP選項位元組替換選項種類、大小和值。這實際上會中斷BGP MD5驗證，並在每台對等路由器上產生如下錯誤消息：

```
000296:20104715:13:22.221 EDT:%TCP-6-BADAUTH:172.16.11.1(28894)172.16.12.2(179)MD5
```

若要成功建立具有MD5身份驗證的BGP會話，必須解決以下三個問題：

- 禁用TCP序列號隨機化
- 禁用TCP MD5選項重寫
- 禁用對等體之間的NAT

類別對映和存取清單用於選擇對等路由器之間的流量，這些對等路由器必須免除TCP序號隨機化功能，並允許在不重寫的情況下承載MD5選項。使用tcp對映指定要允許的選項型別，在本例中是選項型別19（TCP MD5選項）。 類對映和tcp對映通過策略對映（模組化策略框架基礎設施的一部分）連結在一起。然後使用**service-policy**命令啟用配置。

**附註：** 使用**no nat-control**命令可以處理在對等體之間禁用NAT的需要。

在7.0及更高版本中，ASA的預設性質是**no nat-control**，這表示預設情況下通過ASA的每個連線都不需要通過NAT測試。假設ASA的預設設定**no nat-control**。有關詳細資訊，請參閱nat-control。如果強制執行**nat-control**，則必須明確禁用BGP對等體的NAT。這可以通過**static**命令在內部和外部介面之間完成。

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

**PIX/ASA 7.x/8.x**

```
ciscoasa# sh run
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
domain-name example.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
```

```
!

!--- Configure the outside interface. interface
Ethernet0/0 nameif outside security-level 0 ip address
172.16.12.10 255.255.255.0 ! !--- Configure the inside
interface. interface Ethernet0/1 nameif inside security-
level 100 ip address 172.16.11.10 255.255.255.0 ! !--
Output suppressed. !--- Access list to allow incoming
BGP sessions !--- from the outside peer to the inside
peer access-list OUTSIDE-ACL-IN extended permit tcp host
172.16.12.2 host 172.16.11.1 eq  bgp


!--- Access list to match BGP traffic. !--- The next
line matches traffic from the inside peer to the outside
peer access-list BGP-MD5-ACL extended permit tcp host
172.16.11.1 host 172.16.12.2 eq  bgp
!--- The next line matches traffic from the outside peer
to the inside peer access-list BGP-MD5-ACL extended
permit tcp host 172.16.12.2 host 172.16.11.1 eq  bgp


!
!--- TCP-MAP to allow MD5 Authentication. tcp-map BGP-
MD5-OPTION-ALLOW
  tcp-options range 19 19 allow
!
!--- Apply the ACL that allows traffic !--- from the
outside peer to the inside peer access-group OUTSIDE-
ACL-IN in interface outside
!
asdm image disk0:/asdm-621.bin
no asdm history enable
arp timeout 14400

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
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes
4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!
class-map inspection_default
 match default-inspection-traffic
class-map BGP-MD5-CLASSMAP
 match access-list BGP-MD5-ACL
!
!
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
```

## Router11

```
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
```

## Router12

```
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-ispa-route permit 10 match
```

```
ip address 20 match ip next-hop 21 ! route-map adv-to-
ispa permit 10 match ip address 10 ! !--- Output
suppressed
```

**Router14(ISP-A)**

```
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
```

## 驗證

**show ip bgp summary**命令的輸出表示驗證成功並在Router11上建立BGP會話。

```
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
3 network entries using 360 bytes of memory
3 path entries using 156 bytes of memory
2/2 BGP path/bestpath attribute entries using 248 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
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
172.16.13.2     4        64496     137     138        8    0    0 02:01:16        1
Router11#
```

# 相關資訊

- BGP 支援頁面
- BGP 最佳路徑選取演算法
- 在單宿和多宿環境中使用 BGP 進行負載共用:配置示例

- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 配置和測試PIX防火牆
- 技術支援與文件 - Cisco Systems