ASA/PIX : Exemple de configuration de BGP via ASA

Contenu

Introduction

Cet exemple de configuration montre comment exécuter le protocole BGP (Border Gateway Protocol) sur un dispositif de sécurité (PIX/ASA) et comment obtenir la redondance dans un environnement BGP et PIX à logements multiples. Avec un diagramme de réseau comme exemple, ce document explique comment acheminer automatiquement le trafic vers le fournisseur de services Internet B (ISP-B) lorsque le système autonome 64496 perd la connectivité avec le FAI-A (ou l'inverse), grâce à l'utilisation de protocoles de routage dynamique qui s'exécutent entre tous les routeurs du système autonome 64496.

Comme BGP utilise des paquets TCP de monodiffusion sur le port 179 pour communiquer avec ses homologues, vous pouvez configurer PIX1 et PIX2 pour autoriser le trafic de monodiffusion sur le port TCP 179. De cette manière, l'appairage BGP peut être établi entre les routeurs connectés via le pare-feu. La redondance et les politiques de routage souhaitées peuvent être obtenues par la manipulation des attributs BGP.

Conditions préalables

Conditions requises

Les lecteurs de ce document doivent être familiers avec Configuration de BGP et Configuration de

pare-feu de base.

Components Used

Les exemples de scénarios de ce document sont basés sur les versions de logiciel suivantes :

- Routeurs Cisco 2600 avec Cisco IOS ? Version du logiciel 12.2(27)
- PIX 515 avec Cisco PIX Firewall version 6.3(3) et ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée avec les versions de matériel et de logiciel suivantes :

- Cisco Adaptive Security Appliance (ASA) série 5500 avec version 7.x et ultérieure
- Module de services de pare-feu Cisco (FWSM) qui exécute les versions 3.2 et ultérieures du logiciel

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

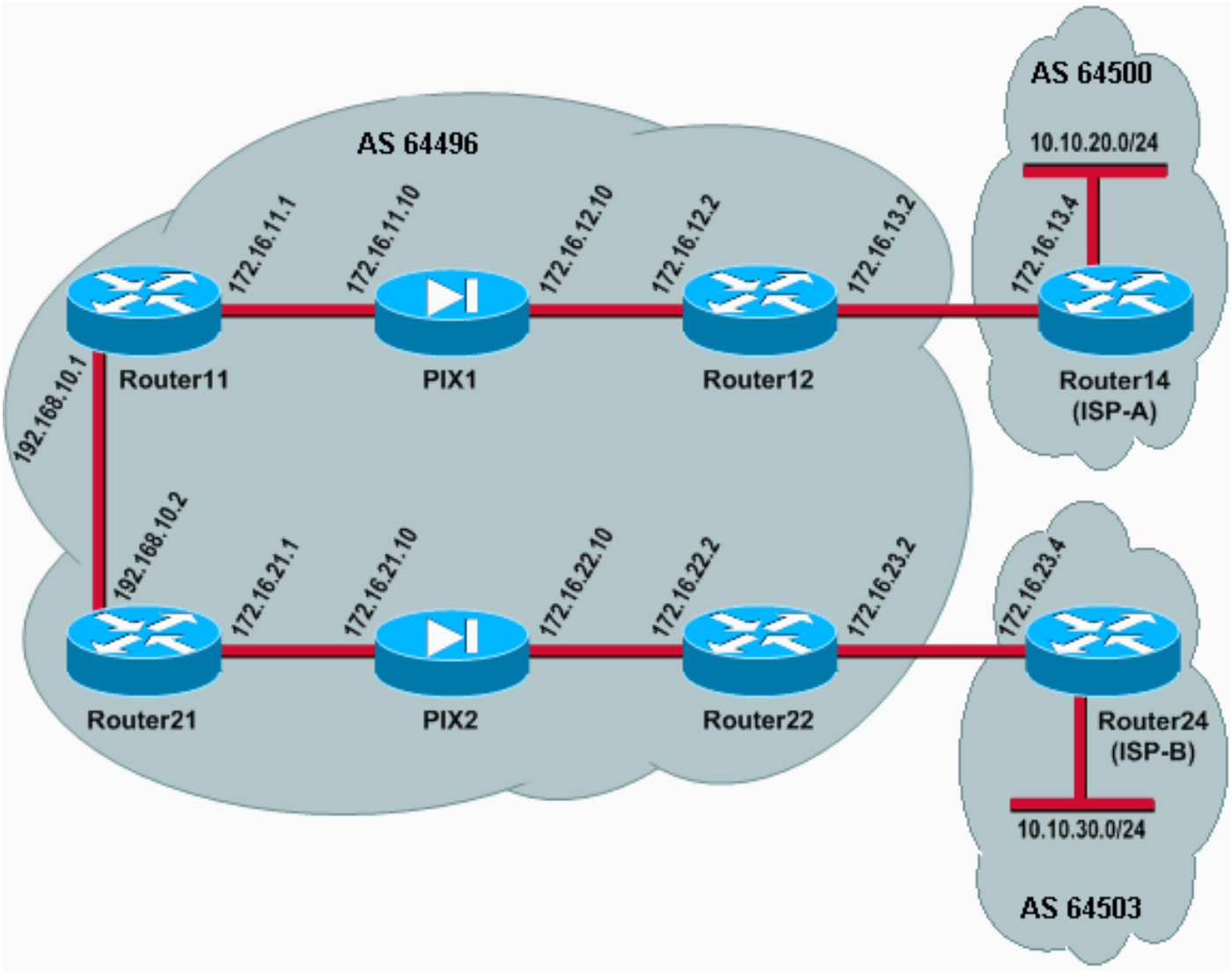
Configuration

Cette section fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour obtenir des informations supplémentaires sur les commandes de ce document, utilisez l'Outil de recherche de commandes (clients enregistrés uniquement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans cette configuration de réseau, les routeurs 12 et 22 (qui appartiennent à AS 64496) sont multihébergés par le routeur 14 (ISP-A) et le routeur 24 (ISP-B), respectivement, pour assurer la redondance. Le réseau interne 192.168.10.0/24 se trouve à l'intérieur du pare-feu. Les routeurs 11 et 21 se connectent aux routeurs 12 et 22 via le pare-feu. PIX1 et PIX2 ne sont pas configurés pour effectuer la traduction d'adresses de réseau (NAT).

Scénario 1

Dans ce scénario, le routeur 12 de l'AS 64496 effectue l'appairage BGP (eBGP) externe avec le routeur 14 (ISP-A) dans AS 64500. Le routeur 12 effectue également l'appairage BGP interne (iBGP) avec le routeur 11 à PIX1. Si eBGP a appris des routes du FAI-A, le routeur 12 annonce une route par défaut 0.0.0.0/0 sur iBGP vers le routeur 11. Si la liaison avec ISP-A échoue, le routeur 12 arrête d'annoncer la route par défaut.

De même, Router22 dans AS 64496 effectue l'appairage eBGP avec Router24 (ISP-B) dans AS 64503 et annonce une route par défaut sur iBGP vers Router21 sous réserve de la présence de routes ISP-B dans sa table de routage.

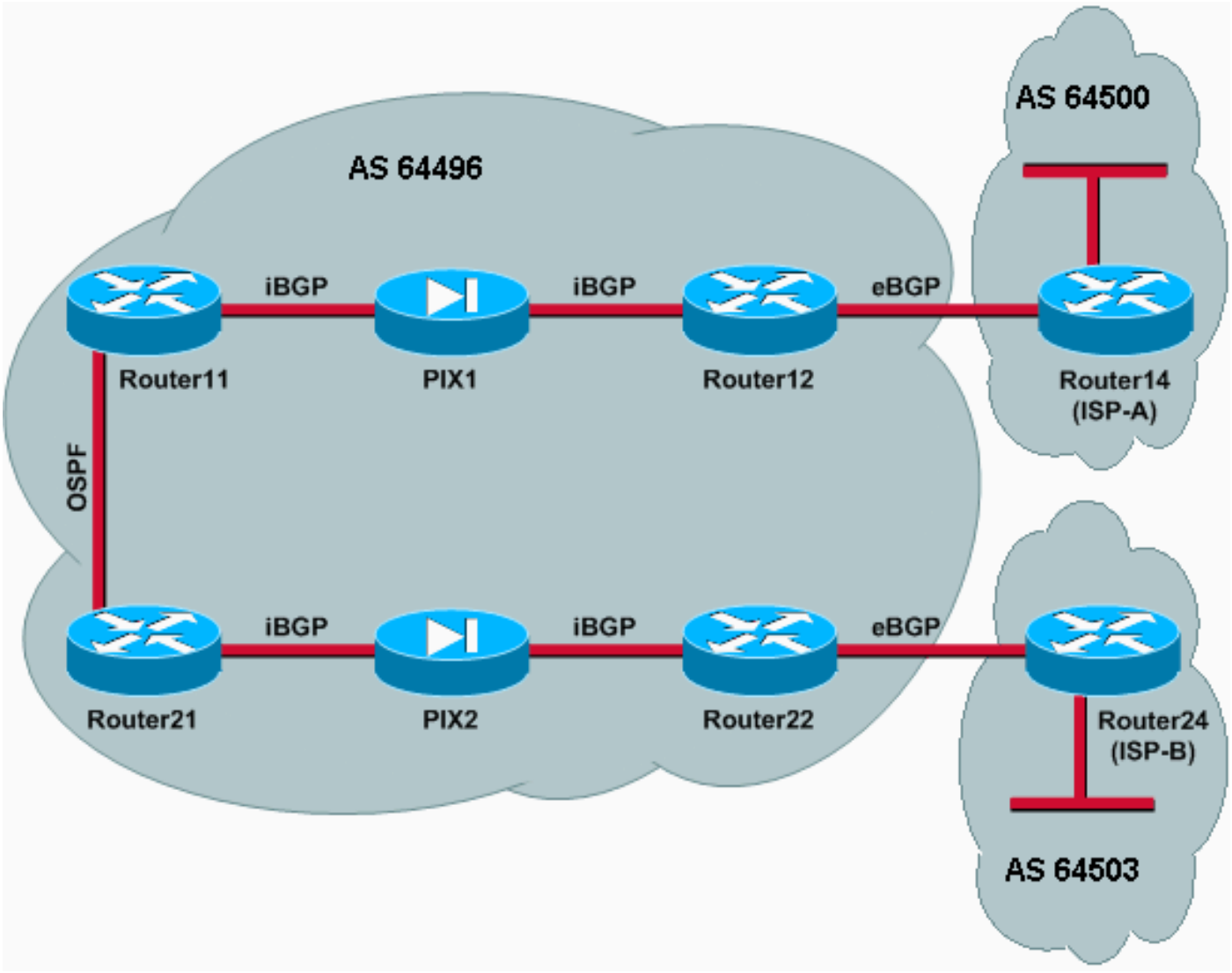
Grâce à l'utilisation d'une liste d'accès, PIX1 et PIX2 sont configurés pour autoriser le trafic BGP (TCP, port 179) entre homologues iBGP. En effet, les interfaces PIX ont un niveau de sécurité associé. Par défaut, l'interface interne (ethernet1) a un niveau de sécurité 100 et l'interface externe (ethernet0) un niveau de sécurité 0. Les connexions et le trafic sont normalement autorisés depuis les interfaces de niveau de sécurité supérieur à inférieur. Cependant, pour

autoriser le trafic d'une interface de niveau de sécurité inférieur à une interface de niveau de sécurité supérieur, vous devez définir explicitement une liste d'accès sur le PIX. En outre, vous devez configurer une traduction NAT statique sur PIX1 et PIX2, pour permettre aux routeurs de l'extérieur d'initier une session BGP avec des routeurs de l'intérieur de PIX.

Les routeurs 11 et 21 annoncent conditionnellement la route par défaut dans le domaine OSPF (Open Shortest Path First) en fonction de la route par défaut apprise par iBGP. Router11 annonce la route par défaut dans le domaine OSPF avec une métrique de 5, Router21 annonce la route par défaut avec une métrique de 30, et donc la route par défaut à partir du Router11 est préférée. Cette configuration permet de propager uniquement la route par défaut 0.0.0.0/0 vers Router11 et Router21, ce qui permet de conserver la consommation de mémoire sur les routeurs internes et d'obtenir des performances optimales.

Ainsi, pour résumer ces conditions, voici la stratégie de routage pour AS 64496 :

- Le système autonome 64496 préfère la liaison entre le routeur 12 et le routeur ISP-A pour tout le trafic sortant (de 192.168.10.0/24 à Internet).
- Si la connectivité au FAI-A échoue, tout le trafic est acheminé via la liaison entre le routeur 22 et le FAI-B.
- Tout le trafic provenant d'Internet vers 192.168.10.0/24 utilise la liaison entre ISP-A et le routeur12.
- Si la liaison entre ISP-A et Router12 échoue, tout le trafic entrant est acheminé via la liaison entre ISP-B et Router22.



Configurations

Ce scénario utilise les configurations suivantes :

- Routeur11
- Routeur12
- Routeur14 (ISP-A)
- Routeur21
- Routeur22
- PIX1
- PIX2

Routeur11

```
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
```

Routeur12

```
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
```

Routeur14 (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. !
```

Routeur21

```
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 !
```

Routeur22

```
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.
```

Routeur24 (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.
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Lorsque les deux sessions BGP sont actives, vous pouvez vous attendre à ce que tous les paquets soient routés via ISP-A. Considérez la table BGP sur Router11. Il apprend une route par défaut 0.0.0.0/0 à partir du routeur 12 avec le tronçon suivant 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
*> 192.168.10.0     0.0.0.0                  0         32768 i
```

La route par défaut 0.0.0.0/0 apprise via BGP est installée dans la table de routage, comme le montre le résultat de **show ip route** sur Router11.

```
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
```

Examinez maintenant la table BGP sur Router21. Il apprend également la route par défaut via Router22.

```
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
```

Maintenant, voyez si cette route par défaut apprise par BGP est installée dans la table de routage du routeur21.

```
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
```

La route par défaut dans Router21 est apprise via OSPF (notez le préfixe o sur la route 0.0.0.0/0). Il est intéressant de noter qu'il existe une route par défaut apprise via BGP à partir du routeur22, mais la sortie **show ip route** montre la route par défaut apprise via OSPF.

La route par défaut OSPF a été installée dans Router21 parce que Router21 apprend la route par défaut à partir de deux sources : Router22 via iBGP et Router11 via OSPF. Le processus de sélection de route installe la route avec une meilleure distance administrative dans la table de routage. La distance administrative du protocole OSPF est de 110 tandis que la distance administrative du protocole iBGP est de 200. Par conséquent, la route par défaut apprise par OSPF est installée dans la table de routage, car 110 est inférieur à 200. Pour plus d'informations sur la sélection de route, référez-vous à Sélection de route dans les routeurs Cisco.

Dépannage

Utilisez cette section pour dépanner votre configuration.

Arrêtez la session BGP entre Router12 et 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
```

La route par défaut apprise par le routeur11 via BGP n’est pas celle du routeur12.

```
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
```

Vérifiez la table de routage sur Router11. La route par défaut est apprise via OSPF (distance administrative de 110) avec un saut suivant de 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
```

Ce résultat est attendu conformément aux stratégies prédéfinies. À ce stade, cependant, il est important de comprendre la commande de configuration **distance bgp 20 105 200** dans Router11 et comment elle influence la sélection de route sur Router11.

Les valeurs par défaut de cette commande sont **distance bgp 20 200 200**, où les routes apprises par eBGP ont une distance administrative de 20, les routes apprises par iBGP ont une distance administrative de 200 et les routes BGP locales ont une distance administrative de 200.

Lorsque la liaison entre Router12 et ISP-A redémarre, Router11 apprend la route par défaut via iBGP à partir du Router12. Cependant, comme la distance administrative par défaut de cette route apprise par iBGP est 200, elle ne remplacera pas la route apprise par OSPF (parce que 110 est inférieur à 200). Cela force tout le trafic sortant vers la liaison entre Router21 et Router22 et ISP-B, même si la liaison entre Router12 et ISP-A est à nouveau active. Pour résoudre ce problème, modifiez la distance administrative de la route apprise par iBGP à une valeur inférieure à celle du protocole IGP (Interior Gateway Protocol) utilisé. Dans cet exemple, le protocole IGP est OSPF, donc une distance de 105 a été choisie (parce que 105 est inférieur à 110).

Pour plus d'informations sur la commande **distance bgp**, référez-vous aux commandes BGP. Pour plus d'informations sur le multihébergement avec BGP, référez-vous à Partage de charge avec BGP dans les environnements à résidence unique et à résidence multiple : partage de charge avec BGP dans les environnements connectés à un ou plusieurs réseaux.

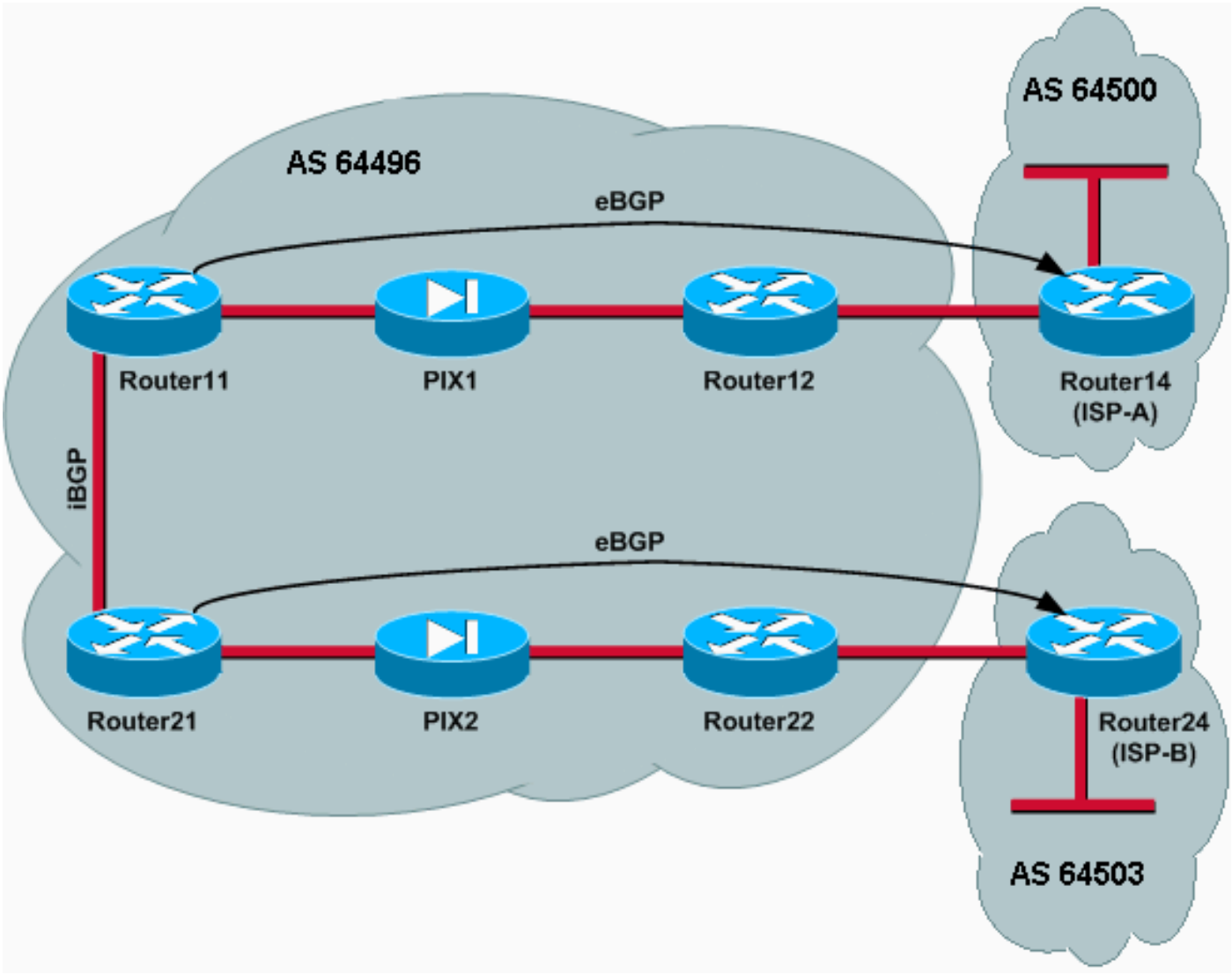
Scénario 2

Dans ce scénario, Router11 est l'appairage eBGP direct avec Router 14 (ISP-A) et Router21 est l'appairage eBGP direct avec Router24 (ISP-B). Les routeurs 12 et 22 ne participent pas à l'appairage BGP, mais ils fournissent la connectivité IP aux FAI. Comme les homologues eBGP ne sont pas des voisins directement connectés, la commande **neighbor ebgp-multihop** est utilisée sur les routeurs participants. La commande **neighbor ebgp-multihop** permet à BGP de remplacer la limite eBGP à un saut par défaut, car elle modifie la durée de vie (TTL) des paquets eBGP de la valeur par défaut 1. Dans ce scénario, le voisin eBGP se trouve à 3 sauts, de sorte que **neighbor ebgp-multihop 3** est configuré sur les routeurs participants de sorte que la valeur TTL soit modifiée à 3. En outre, des routes statiques sont configurées sur les routeurs et le PIX pour s’assurer que

Router11 peut envoyer une requête ping à l'adresse 172.16.13.4 du routeur14 (ISP-A) et pour s'assurer que Router21 peut envoyer une requête ping à l'adresse 172.16.23.4 du routeur.

Par défaut, PIX ne permet pas aux paquets ICMP (Internet Control Message Protocol) (envoyés lorsque vous émettez la commande **ping**) de passer. Pour autoriser les paquets ICMP, utilisez la commande **access-list** comme indiqué dans la configuration PIX suivante. Pour plus d'informations sur la commande **access-list**, référez-vous aux commandes PIX Firewall A à B.

La stratégie de routage est identique à celle du scénario 1 : La liaison entre Router12 et ISP-A est préférée à la liaison entre Router22 et ISP-B, et lorsque la liaison ISP-A tombe en panne, la liaison ISP-B est utilisée pour tout le trafic entrant et sortant.



Configurations

Ce scénario utilise les configurations suivantes :

- Routeur11
- Routeur12
- Routeur14 (ISP-A)
- Routeur21
- Routeur22
- PIX1

- PIX2

Routeur11

```
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 !
```

Routeur12

```
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
```

Routeur14 (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.
```

Routeur21

```
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
```

Routeur22

```
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
```

Routeur24 (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
```

Vérification

Commencez par la situation dans laquelle les liaisons vers ISP-A et ISP-B sont actives. La sortie de la commande **show ip bgp summary** sur Router11 et Router21 confirme les sessions BGP établies avec ISP-A et ISP-B respectivement.

```
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
```

La table BGP sur Router11 indique la route par défaut (0.0.0.0/0) vers le tronçon suivant ISP-A 172.16.13.4.

```
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
```

Vérifiez maintenant la table BGP sur Router21. Il comporte deux routes 0.0.0.0/0 : l'un a appris de ISP-B avec le prochain saut 172.16.23.4 sur eBGP, et l'autre par iBGP avec une préférence locale de 200. Router21 préfère les routes apprises par iBGP en raison de l'attribut de préférence locale le plus élevé. Il installe donc cette route dans la table de routage. Pour plus d'informations sur la sélection du chemin BGP, référez-vous à Algorithme de sélection du meilleur chemin BGP.

```
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
```

Dépannage

Arrêtez la session BGP Router11 et 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
```

La session eBGP vers ISP-A tombe en panne lorsque le compteur de retenue (180 secondes) expire.

```
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
```

Lorsque la liaison à ISP-A est désactivée, Router11 installe 0.0.0.0/0 avec le saut suivant 192.168.10.2 (Router21), appris via iBGP dans sa table de routage. Ceci pousse tout le trafic sortant via Router21, puis vers ISP-B, comme indiqué dans ce résultat :

```
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
```

Authentification MD5 pour les voisins BGP via PIX/ASA

Configuration de PIX 6.x

Comme tout autre protocole de routage, BGP peut être configuré pour l'authentification. Vous pouvez configurer l'authentification MD5 entre deux homologues BGP, ce qui signifie que chaque segment envoyé sur la connexion TCP entre les homologues est vérifié. L'authentification MD5 doit être configurée avec le même mot de passe sur les deux homologues BGP ; sinon, le lien entre eux ne sera pas établi. La configuration de l'authentification MD5 entraîne la génération et la vérification du résumé MD5 de chaque segment envoyé sur la connexion TCP par le logiciel Cisco IOS. Si l'authentification est appelée et qu'un segment échoue à l'authentification, un message d'erreur est généré.

Lorsque vous configurez des homologues BGP avec l'authentification MD5 qui passent par un pare-feu PIX, il est important de configurer le PIX entre les voisins BGP afin que les numéros de séquence des flux TCP entre les voisins BGP ne soient pas aléatoires. Ceci est dû au fait que la fonction de numéro de séquence aléatoire TCP sur le pare-feu PIX est activée par défaut, et qu'elle modifie le numéro de séquence TCP des paquets entrants avant de les transmettre.

L'authentification MD5 est appliquée à l'en-tête TCP Psuedo-IP, à l'en-tête TCP et aux données (reportez-vous à la RFC 2385). TCP utilise ces données, qui incluent les numéros de séquence et d'ACK TCP, ainsi que le mot de passe de voisin BGP pour créer un numéro de hachage de 128 bits. Le numéro de hachage est inclus dans le paquet dans un champ d'option d'en-tête TCP. Par défaut, le PIX annule le numéro de séquence par un nombre aléatoire, par flux TCP. Sur l'homologue BGP émetteur, TCP utilise le numéro de séquence d'origine pour créer le numéro de hachage MD5 de 128 bits et inclut ce numéro de hachage dans le paquet. Lorsque l'homologue BGP récepteur obtient le paquet, TCP utilise le numéro de séquence modifié par PIX pour créer un numéro de hachage MD5 de 128 bits et le compare au numéro de hachage inclus dans le paquet.

Le numéro de hachage est différent parce que la valeur de séquence TCP a été modifiée par le

PIX, et TCP sur le voisin BGP abandonne le paquet et enregistre un message d'échec MD5 similaire à celui-ci :

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

Utilisez le mot clé **norandomseq** avec la **commande static (inside, outside) 172.16.11.1 172.16.11.1 netmask 255.255.255.0 norandomseq pour résoudre ce problème et empêcher le PIX de décomposer le numéro de séquence TCP ..** Cet exemple illustre l'utilisation du mot clé **norandomseq** :

Routeur11

```
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
```

Routeur12

```
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

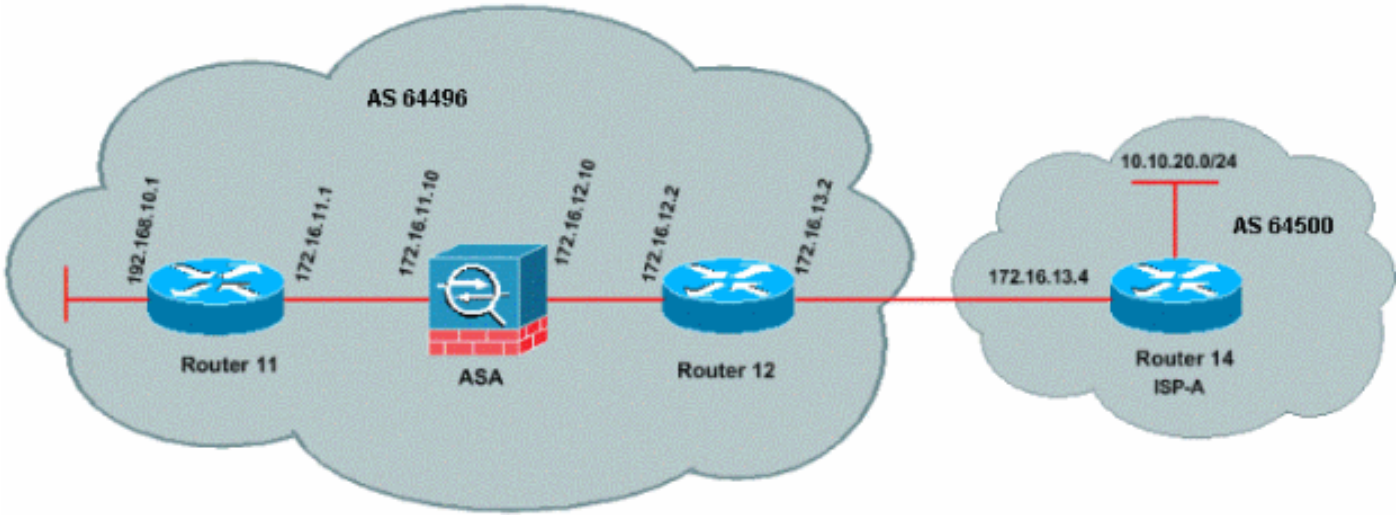
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside. 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 et versions ultérieures

Cette section utilise cette configuration du réseau .



PIX/ASA version 7.x et ultérieure introduit un défi supplémentaire lorsque vous essayez d'établir une session d'appairage BGP avec authentification MD5. Par défaut, PIX/ASA version 7.x et ultérieure réécrit toute option TCP MD5 incluse dans un datagramme TCP qui passe par le périphérique et remplace le type, la taille et la valeur de l'option par des octets d'option NOP. Ceci rompt efficacement l'authentification MD5 BGP et génère des messages d'erreur comme celui-ci sur chaque routeur homologue :

```
000296: 7 avril 2010 15:13:22.221 HAE : %TCP-6-BADAUTH : Pas de digest MD5 de 172.16.11.1(28894)
à 172.16.12.2(179)
```

Pour qu'une session BGP avec authentification MD5 soit établie avec succès, ces trois problèmes doivent être résolus :

- Désactiver l'aléatoire des numéros de séquence TCP
- Désactiver la réécriture de l'option TCP MD5
- Désactiver NAT entre homologues

Une carte-classe et une liste d'accès sont utilisées pour sélectionner le trafic entre les homologues qui doivent être exemptés de la fonctionnalité de randomisation des numéros de séquence TCP et autorisés à transporter une option MD5 sans réécriture. Un tcp-map est utilisé pour spécifier le type d'option à autoriser, dans ce cas, l'option type 19 (option TCP MD5). La carte-classe et la carte-tcp sont toutes deux reliées par une carte-politique, faisant partie de l'infrastructure du Cadre de politique modulaire. La configuration est ensuite activée à l'aide de la commande **service-policy**.

Remarque : la nécessité de désactiver la NAT entre les homologues est gérée par la commande **no nat-control**.

Dans les versions 7.0 et ultérieures, la nature par défaut d'un ASA est **no nat-control**, qui indique que chaque connexion via ASA, par défaut, n'a pas besoin de réussir le test NAT. Il est supposé qu'ASA a un paramètre par défaut de **no nat-control**. Référez-vous à nat-control pour plus d'informations. Si **nat-control** est appliqué, vous devez explicitement désactiver NAT pour les homologues BGP. Cela peut être fait avec la commande **static** entre les interfaces internes et externes.

```
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
```

Routeur11

```
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
```

Routeur12

```
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
```

Routeur14 (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
```

Vérification

Le résultat de la commande **show ip bgp summary** indique que l'authentification est réussie et que la session BGP est établie sur Router11.

```
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#
```

Informations connexes

- Page de support BGP
- Algorithme de sélection de la meilleure route BGP
- Partage de charge avec BGP en environnement mono et multihébergé : Exemples de configuration
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Configuration et test du pare-feu PIX
- Support et documentation techniques - Cisco Systems