ASA/PIX : Exemple de configuration de BGP via ASA

Contenu

Introduction

Cette configuration d'échantillon explique comment exécuter le Protocole BGP (Border Gateway Protocol) à travers des dispositifs de sécurité (PIX/ASA) et comment réaliser la Redondance dans un environnement multihomed BGP et PIX. Avec un schéma de réseau comme exemple, ce document explique comment conduire automatiquement le trafic au fournisseur d'accès Internet B (ISP B) quand PENDANT QUE 64496 perd la Connectivité à ISP-A (ou à l'inverse), par l'utilisation des protocoles de routage dynamique qui fonctionnent entre tous les Routeurs dedans EN TANT QUE 64496.

Puisque le BGP utilise des paquets TCP d'unicast sur le port 179 pour communiquer avec ses pairs, vous pouvez configurer PIX1 et PIX2 pour permettre le trafic unicast sur le port TCP 179. De cette façon, scruter BGP peut être établie entre les Routeurs qui sont connectés par le Pare-feu. La Redondance et les stratégies de acheminement désirées peuvent être réalisées par la manipulation des attributs BGP.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient être au courant de configurer le BGP et la configuration de

base de Pare-feu.

Composants utilisés

Les exemples de scénario dans ce document sont basés sur ces versions de logiciel :

- Routeurs de Cisco 2600 avec le Cisco IOS ? Version de logiciel 12.2(27)
- PIX 515 avec la version 6.3(3) et ultérieures de Pare-feu de Cisco PIX

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

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

- Gamme 5500 de l'appliance de sécurité adaptable Cisco (ASA) avec la version 7.x et plus tard
- Le Module de services de Pare-feu de Cisco (FWSM) ce exécute la version de logiciel 3.2 et plus tard

Conventions

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

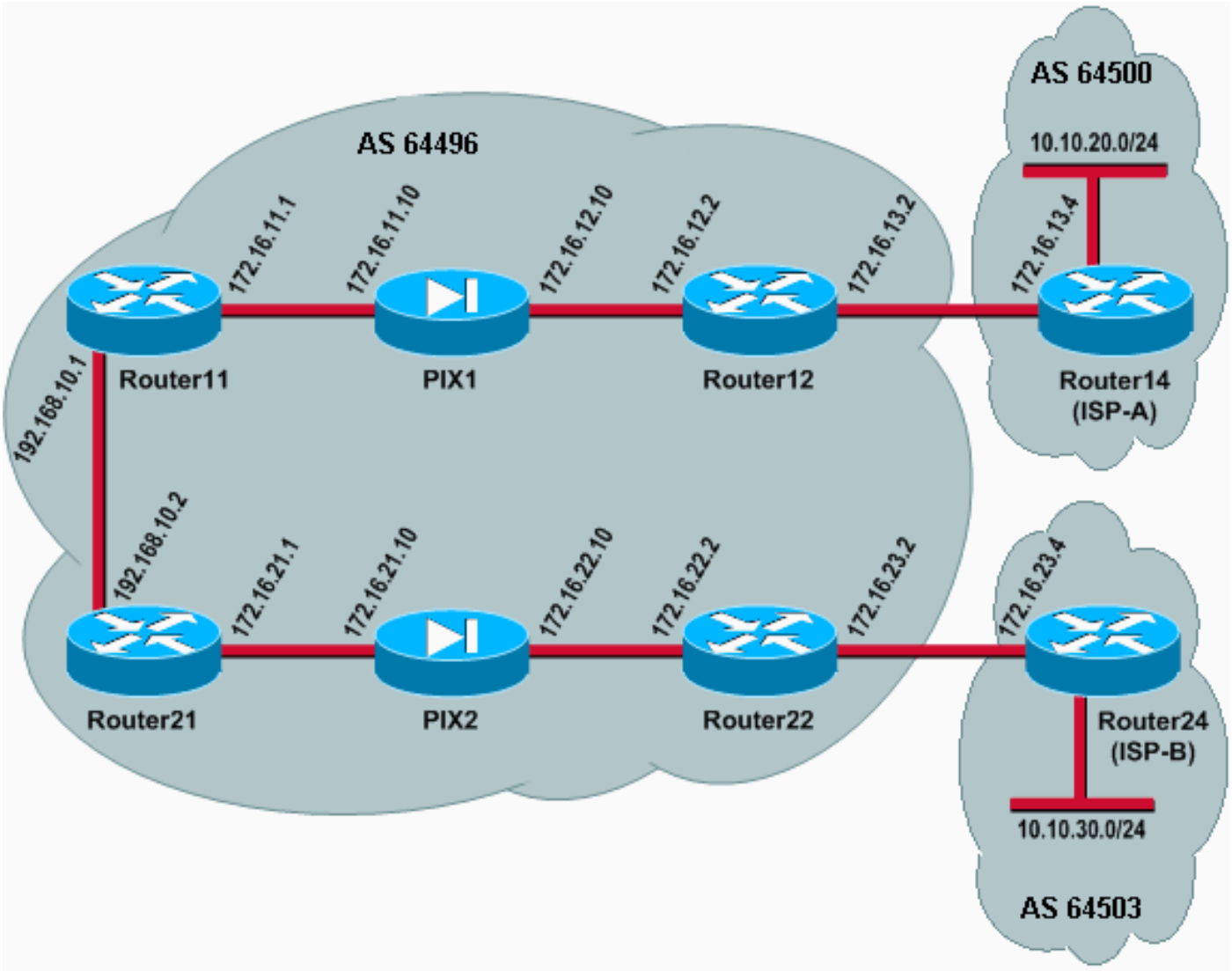
Configurez

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

Note: Pour trouver les informations complémentaires au sujet des commandes dans ce document, utilisez le Command Lookup Tool (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



En cette configuration réseau, Router12 et Router22 (qui appartiennent à EN TANT QUE 64496) sont multihomed à Router14 (ISP-A) et à Router24 (ISP B) respectivement, pour la Redondance. Le réseau interne 192.168.10.0/24 est sur l'intérieur du Pare-feu. Router11 et Router21 se connectent à Router12 et à Router22 par le Pare-feu. PIX1 et PIX2 ne sont pas configurés pour exécuter le Traduction d'adresses de réseau (NAT).

Scénario 1

Dans ce scénario, Router12 dedans EN TANT QUE 64496 fait le BGP externe (eBGP) scrutant avec Router14 (ISP-A) dedans EN TANT QUE 64500. Router12 fait également BGP interne (iBGP) scrutant avec Router11 par PIX1. Si les routes apprises d'eBGP d'ISP-A sont présentes, Router12 annonce un default route 0.0.0.0/0 sur l'iBGP à Router11. Si le lien à ISP-A échoue, Router12 cesse d'annoncer le default route.

De même, Router22 dedans EN TANT QUE 64496 fait l'eBGP scrutant avec Router24 (ISP B) dedans EN TANT QUE 64503 et annonce un default route sur l'iBGP à Router21 conditionnellement basé sur la présence des artères d'ISP B dans sa table de routage.

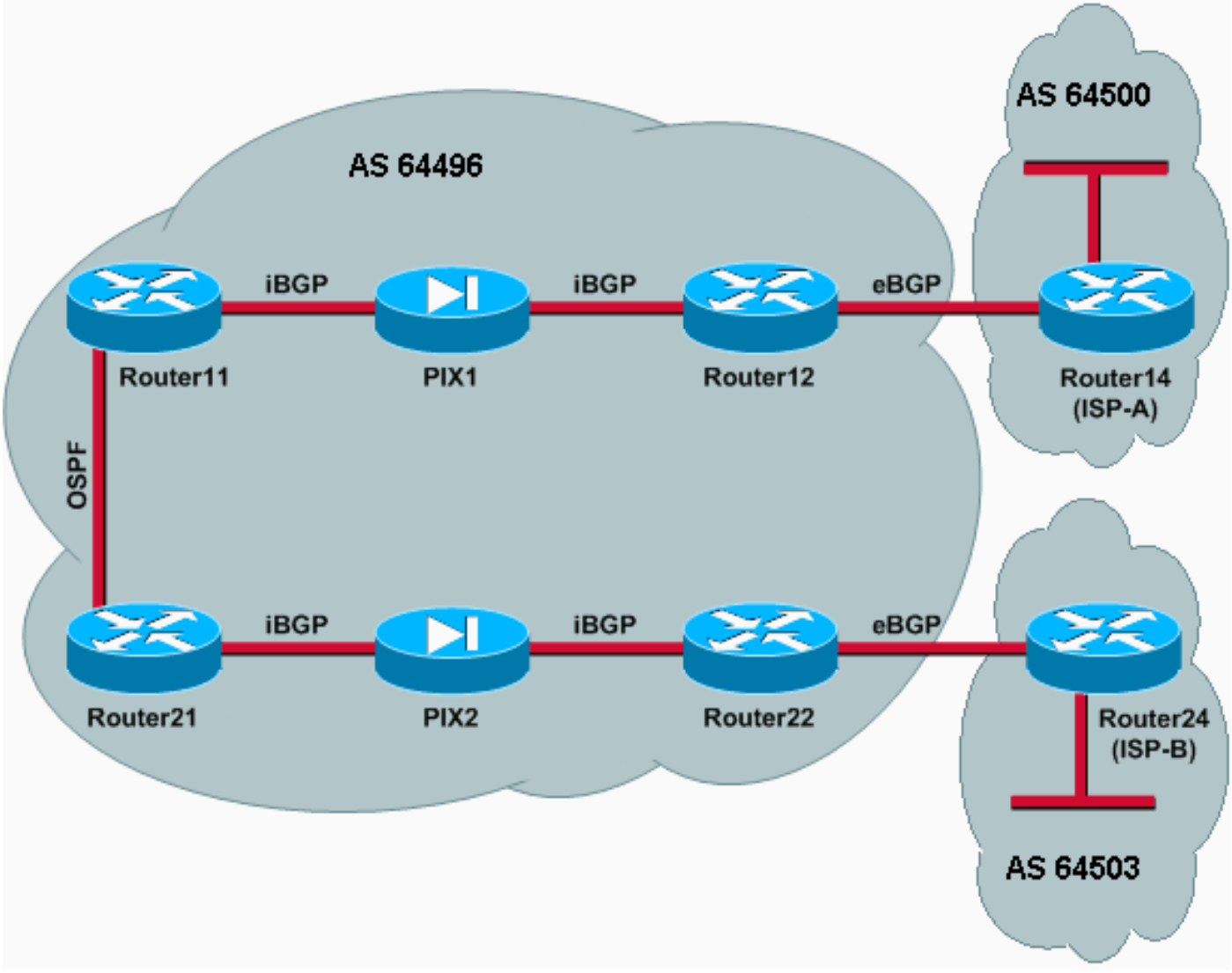
Par l'utilisation d'une liste d'accès, PIX1 et PIX2 sont configurés pour permettre le trafic BGP (TCP, port 179) entre les pairs d'iBGP. C'est parce que les interfaces PIX ont un niveau de Sécurité associé. Par défaut, l'interface interne (ethernet1) a un niveau de Sécurité 100 et l'interface extérieure (ethernet0) a les connexions et le trafic du niveau de Sécurité un 0. sont normalement autorisées de plus élevé aux interfaces à niveau de sécurité inférieur. Pour

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

Router11 et Router21 annoncent conditionnellement le default route dans le domaine de Protocole OSPF (Open Shortest Path First) basé sur le default route iBGP-instruit. Router11 annonce le default route dans le domaine OSPF avec une mesure de 5, Router21 annonce le default route avec une mesure de 30, et donc le default route de Router11 est préféré. Cette configuration aide la propagation seulement le default route 0.0.0.0/0 à Router11 et à Router21, qui économise la consommation de mémoire sur les routeurs internes et réalise la performance optimale.

Ainsi, pour récapituler ces conditions, c'est la stratégie de routage pour EN TANT QUE 64496 :

- COMME 64496 préfère le lien de Router12 à ISP-A pour tout le trafic sortant (de 192.168.10.0/24 à l'Internet).
- Si la Connectivité à ISP-A échoue, tout le trafic est conduit par l'intermédiaire du lien de Router22 à l'ISP B.
- Tout le trafic qui provient l'Internet à 192.168.10.0/24 utilise le lien d'ISP-A à Router12.
- Si le lien d'ISP-A à Router12 échoue, tout le trafic d'arrivée est conduit par l'intermédiaire du lien de l'ISP B à Router22.



[Configurations]

Ce scénario utilise ces configurations :

- 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.
```

Vérifiez

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** .

Quand les deux sessions BGP sont en hausse, vous pouvez attendre tous les paquets à conduire par l'intermédiaire d'ISP-A. Considérez la table BGP sur Router11. Il apprend un default route 0.0.0.0/0 de Router12 avec le prochain saut 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
```

Le 0.0.0.0/0 default route qui est appris par l'intermédiaire du BGP est installé dans la table de routage, suivant les indications de la sortie du **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
```

Considérez maintenant la table BGP sur Router21. Il apprend également le default route par l'intermédiaire de 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
```

Voyez maintenant si ce default route BGP-instruit obtient installé dans la table de routage de Router21.

```
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
```

Le default route dans Router21 est appris par l'intermédiaire de l'OSPF (notez le préfixe `O` sur la 0.0.0.0/0 artère). Il est intéressant de noter qu'il y a un default route appris par l'intermédiaire du BGP de Router22, mais la sortie de **show ip route** affiche le default route appris par l'intermédiaire de l'OSPF.

Le default route OSPF a été installé dans Router21 parce que Router21 apprend le default route de deux sources : Router22 par l'intermédiaire d'iBGP et Router11 par l'intermédiaire d'OSPF. Le procédé de sélection de routes installe l'artère avec une meilleure distance administrative dans la table de routage. La distance administrative de l'OSPF est 110 tandis que la distance administrative de l'iBGP est 200. Par conséquent, le default route OSPF-instruit obtient installé dans la table de routage, parce que 110 est moins de 200. Pour plus d'informations sur la sélection de routes, référez-vous à la sélection de routes dans des Routeurs de Cisco.

Dépannez

Utilisez cette section pour dépanner votre configuration.

Réduisez 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
```

Router11 n'a pas le default route appris par l'intermédiaire du BGP de Router12.

```
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. Le default route est appris par l'intermédiaire d'OSPF (distance administrative de 110) avec un prochain saut 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
```

Cette sortie est prévue selon les stratégies prédéfinies. En ce moment, cependant, il est important de comprendre le **distance bgp 20** commande de configuration **105 200** dans Router11 et comment il influence la sélection de routes sur Router11.

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

Quand le lien entre Router12 et ISP-A est soulevé de nouveau, Router11 apprend le default route par l'intermédiaire de l'iBGP de Router12. Cependant, parce que la distance administrative par défaut de cette artère iBGP-instruite est 200, il ne remplacera pas l'artère OSPF-instruite (parce que 110 est moins de 200). Ceci force tout les trafic sortant au lien de Router21 à Router22 à l'ISP B, quoique le lien de Router12 à ISP-A soit en hausse de nouveau. Pour résoudre ce problème, changez la distance administrative de l'artère iBGP-instruite à une valeur moins que le Protocole IGP (Interior Gateway Protocol) utilisé. Dans cet exemple, l'IGP est OSPF, ainsi une distance de 105 a été choisie (parce que 105 est moins de 110).

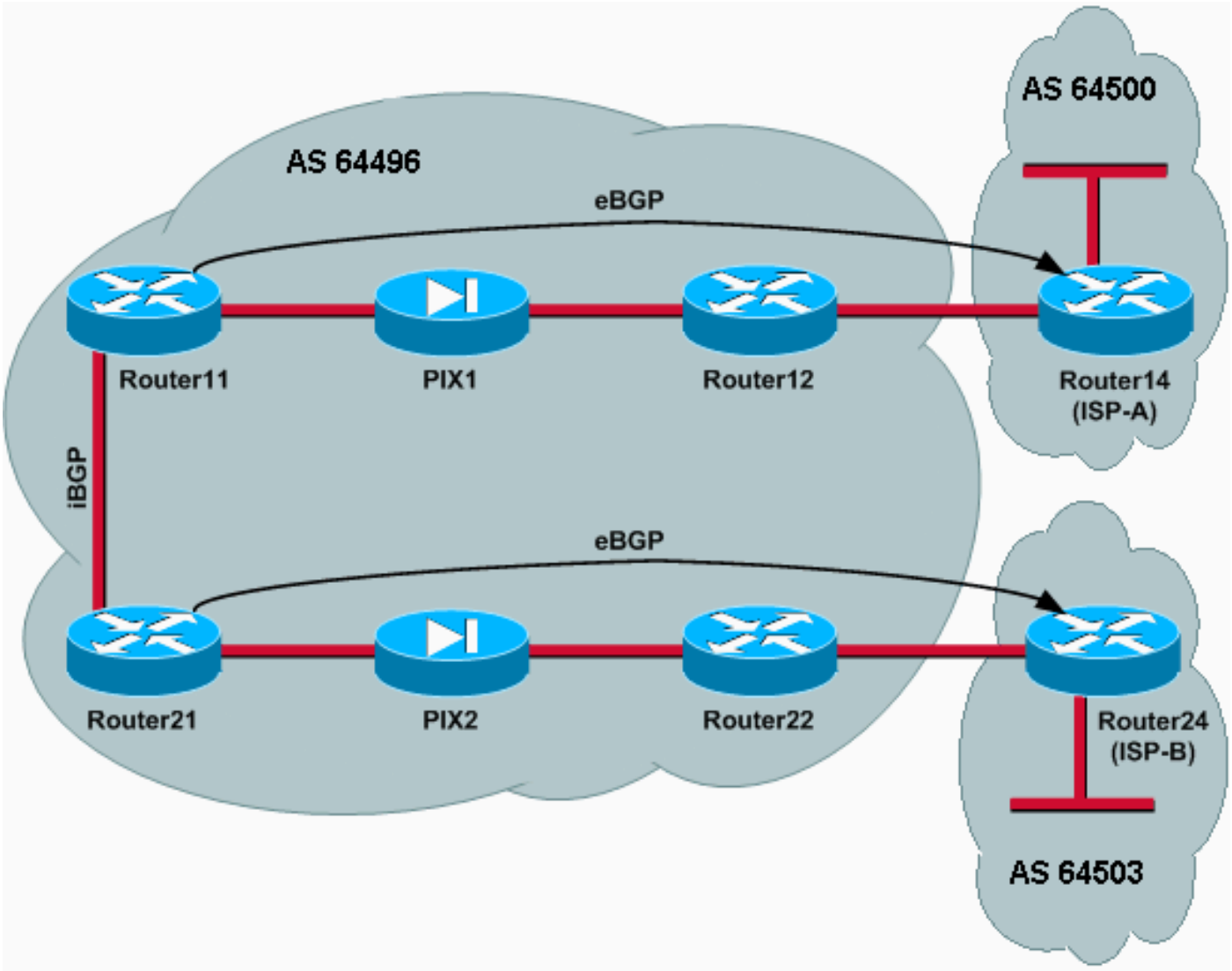
Pour plus d'informations sur la commande de **distance bgp**, référez-vous aux commandes BGP. Pour plus d'informations sur l'hébergement multiple avec le BGP, référez-vous au chargement partageant avec le BGP dans les environnements monos et multihébergés : Configurations d'échantillon.

Scénario 2

Dans ce scénario, Router11 est directement eBGP scrutant avec le routeur 14 (ISP-A), et Router21 est directement eBGP scrutant avec Router24 (ISP B). Router12 et Router22 ne participent pas au BGP scrutant, mais ils fournissent la connectivité IP aux ISP. Puisque les pairs d'eBGP ne sont pas directement des voisins connectés, la commande de **neighbor ebgp-multihop** est utilisée sur les routeurs participants. Le BGP de commandes enables de **neighbor ebgp-multihop** pour ignorer l'une limite par défaut d'eBGP de saut parce qu'elle change le Time to Live (TTL) des paquets d'eBGP de la valeur par défaut de 1. Dans ce scénario, le voisin d'eBGP est 3 sauts loin, ainsi le **neighbor ebgp-multihop 3** est configuré sur les routeurs participants de sorte que la valeur de TTL soit changée à 3. En outre, des artères statiques sont configurées sur les Routeurs et le PIX pour s'assurer que Router11 peut cingler l'adresse Router14 (ISP-A) 172.16.13.4 et s'assurer que Router21 peut cingler l'adresse Router24 (ISP B) 172.16.23.4.

Par défaut, PIX ne permet pas à des paquets de Protocole ICMP (Internet Control Message Protocol) (envoyés quand vous émettez la **commande ping**) pour traverser. Pour permettre des paquets d'ICMP, utilisez la **commande access-list** suivant les indications de dans la prochaine configuration PIX. Pour plus d'informations sur la **commande access-list**, référez-vous au Pare-feu A PIX aux commandes B.

La stratégie de routage est identique que dans le scénario 1 : le lien entre Router12 et ISP-A est préféré au-dessus du lien entre Router22 et ISP B, et quand le lien ISP-A descend le lien d'ISP B est utilisé pour tout le trafic en entrée et en sortie.



Configurations

Ce scénario utilise ces configurations :

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

Router11

```
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
```

Router12

```
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
```

Router14 (ISP-A)

```
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
```

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
```

Router22

```
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
```

Router24 (ISP B)

```
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
```

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
```

Vérifiez

Commencez par la situation où les liens à ISP-A et à ISP B sont en hausse. La sortie de commande de **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 affiche le default route (0.0.0.0/0) vers le prochain saut 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 a deux 0.0.0.0/0 artère : on a appris de l'ISP B avec un prochain saut de 172.16.23.4 sur l'eBGP, et l'autre a appris par l'intermédiaire de l'iBGP avec un local-preference de 200. Router21 préfère les artères iBGP-instruites en raison de l'attribut local preference plus élevé, ainsi il installe qu'artère dans la table de routage. Pour plus d'informations sur la sélection de chemin BGP, référez-vous à l'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
```

Dépannez

Réduisez le Router11 et la session BGP 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 d'eBGP à ISP-A va en bas de quand le temporisateur d'écrou de serrage (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
```

Avec le lien à ISP-A vers le bas, Router11 installe 0.0.0.0/0 avec un prochain saut de 192.168.10.2 (Router21), qui est appris par l'intermédiaire de l'iBGP dans sa table de routage. Ceci pousse tout le trafic sortant par Router21 et puis à l'ISP B, suivant les indications de cette sortie :

```
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 de MD5 pour des voisins BGP par le PIX/ASA

Configuration de PIX 6.x

Juste comme n'importe quel autre protocole de routage, le BGP peut être configuré pour l'authentification. Vous pouvez configurer l'authentification de MD5 entre deux pairs BGP, ainsi il signifie que chaque segment envoyé sur la connexion TCP entre les pairs est vérifié. L'authentification de MD5 doit être configurée avec le même mot de passe sur les deux pairs BGP ; autrement, le rapport entre eux ne sera pas établi. La configuration de l'authentification de MD5 fait générer et vérifier le logiciel de Cisco IOS le condensé de MD5 de chaque segment envoyé sur la connexion TCP. Si l'authentification est appelée et un segment échoue authentification, un message d'erreur est généré.

Quand vous configurez le BGP scrute avec l'authentification de MD5 qui traversent un Pare-feu PIX, il est important pour configurer le PIX entre les voisins BGP de sorte que les numéros de séquence pour les écoulements de TCP entre les voisins BGP ne soient pas aléatoires. C'est parce que la caractéristique aléatoire de numéro de séquence de TCP sur le Pare-feu PIX est activée par défaut, et elle change le numéro de séquence de TCP des paquets entrant avant qu'il

en avant ils.

L'authentification de MD5 est appliquée sur l'en-tête psuedo-IP de TCP, l'en-tête de TCP et les données (référez-vous à RFC 2385). Le TCP emploie ces données — qui incluent l'ordre de TCP et des nombres ACK — avec le neighbor password BGP pour créer un nombre d'informations parasites de 128 bits. Le nombre d'informations parasites est inclus dans le paquet dans un champ d'option d'en-tête de TCP. Par défaut, le PIX compense le numéro de séquence par un nombre aléatoire, par écoulement de TCP. Sur le pair de envoi BGP, le TCP utilise le numéro de séquence d'origine pour créer le nombre d'informations parasites de MD5 de 128 bits et inclut ce nombre d'informations parasites dans le paquet. Quand le pair de réception BGP obtient le paquet, le TCP utilise le numéro de séquence PIX-modifié pour créer un nombre d'informations parasites de MD5 de 128 bits et le compare au nombre d'informations parasites qui est inclus dans le paquet.

Le nombre d'informations parasites est différent parce que la valeur d'ordre de TCP a été changée par le PIX, et le TCP sur le voisin BGP relâche le paquet et se connecte un MD5 a manqué message semblable à celui-ci :

```
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
```

Utilisez le mot clé de **norandomseq** avec **(à l'intérieur, dehors) la** commande **statique de norandomseq de 255.255.255.0 de netmask de 172.16.11.1 172.16.11.1** de résoudre ce problème et d'arrêter le PIX de compenser le numéro de séquence de TCP. Cet exemple montre l'utilisation du mot clé de **norandomseq** :

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
```

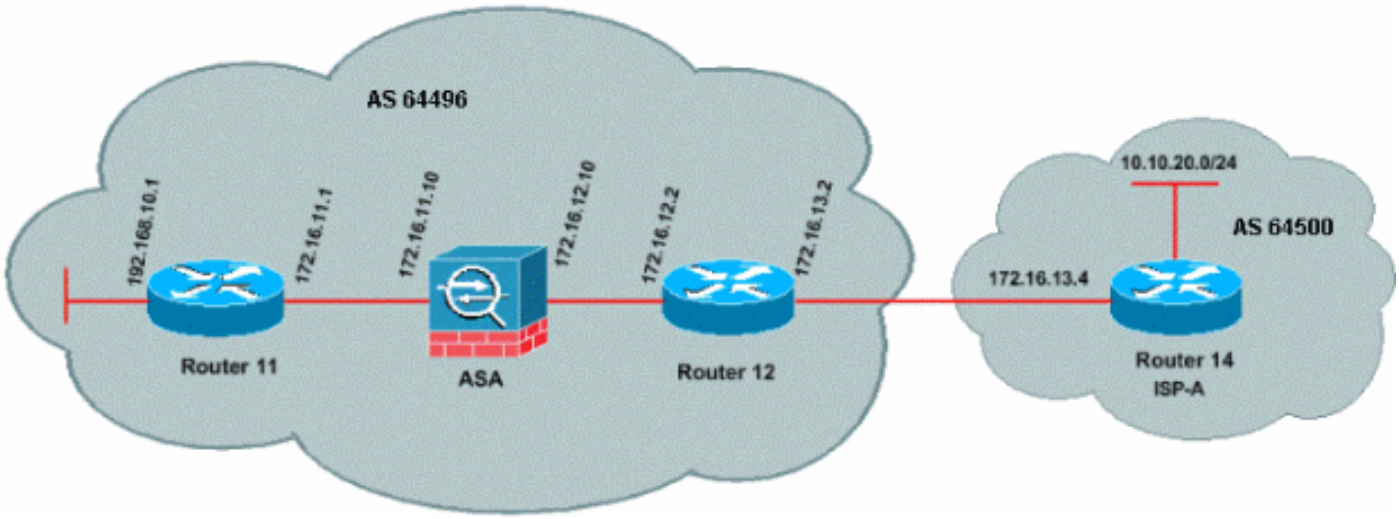
PIX1

```
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 et ultérieur

Cette section utilise cette configuration réseau.



La version 7.x et ultérieures PIX/ASA introduit un défi supplémentaire quand vous essayez d'établir une session scrutante BGP avec l'authentification de MD5. Par défaut, la version 7.x et ultérieures PIX/ASA réécrit n'importe quelle option de MD5 de TCP incluse sur un datagramme TCP qui passe par le périphérique et remplace la sorte d'option, la taille et la valeur par des octets d'option NOP. Ceci casse efficacement l'authentification de MD5 BGP, et les résultats dans les messages d'erreur comme ceci sur chaque routeur d'appairage :

```
000296 : Le 7 avril 2010 15:13:22.221 EDT : %TCP-6-BADAUTH : Aucun condensé de MD5 de
172.16.11.1(28894) à 172.16.12.2(179)
```

Afin d'une session BGP avec l'authentification de MD5 à établir avec succès, ces trois questions doivent être résolues :

- Randomisation de numéro de séquence de TCP de débronchement
- Réécrire d'option de MD5 de TCP de débronchement
- Débronchement NAT entre les pairs

Un class-map et une liste d'accès sont utilisés pour sélectionner le trafic entre les pairs qui doivent chacun des deux être exemptés de la caractéristique de randomisation de numéro de séquence de TCP et être permis pour porter une option de MD5 sans réécrire. Une tcp-MAP est utilisée pour spécifier le type d'option à laisser, dans ce cas, la sorte 19 (option d'option de MD5 de TCP). Le class-map et la TCP-MAP chacun des deux sont joints ensemble par un policy-map, une partie de l'infrastructure modulaire de cadre de stratégie. La configuration est alors lancée avec la commande de service-**stratégie**.

Note: La nécessité de désactiver NAT entre les pairs est manipulée par l'**aucune** commande de nat-**control**.

Dans la version 7.0 et ultérieures, la nature par défaut d'une ASA n'est **aucun nat-control**, qui déclare que chaque connexion par l'ASA, par défaut, n'a pas besoin de passer le test NAT. On le

suppose que l'ASA a une valeur par défaut sans nat-**control**. Référez-vous au pour en savoir plus de nat-control. Si le nat-**control** est imposé, vous devez explicitement désactiver NAT pour les pairs BGP. Ceci peut être fait avec la commande **statique** entre les interfaces internes et externes.

```
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/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)

```
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
```

Vérifiez

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

```
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
```

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
- Pare-feu configurant et de test PIX
- Support et documentation techniques - Cisco Systems