ASA/PIX: BGP door ASA-configuratievoorbeeld

Inhoud

Inleiding

Deze voorbeeldconfiguratie laat zien hoe u Border Gateway Protocol (BGP) over een security applicatie (PIX/ASA) kunt gebruiken en hoe u redundantie kunt bereiken in een multihomed BGP- en PIX-omgeving. Met een netwerkdiagram als voorbeeld, legt dit document uit hoe automatisch verkeer naar Internet Service provider B (ISP-B) moet worden geleid wanneer AS 64496 connectiviteit met ISP-A (of de omgekeerde) verliest, door het gebruik van dynamische routingprotocollen die tussen alle routers in AS 6496 lopen.

Omdat BGP éénasts TCP-pakketten op poort 179 gebruikt om met zijn peers te communiceren, kunt u PIX1 en PIX2 configureren om eenastverkeer toe te staan op TCP poort 179. Op deze manier kan BGP-peering worden ingesteld tussen de routers die worden aangesloten via de firewall. Redundantie en het gewenste routingbeleid kunnen worden bereikt door manipulatie van de BGP-eigenschappen.

Voorwaarden

Vereisten

Lezers van dit document dienen bekend te zijn met de BGP-configuratie en de basisfirewallconfiguratie.

Gebruikte componenten

De voorbeeldscenario's in dit document zijn gebaseerd op deze softwareversies:

- Cisco 2600 routers met Cisco IOS-softwarereleases? IOS-softwarerelease 12.2(27)E
- PIX 515 met Cisco PIX-firewall versie 6.3(3) en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

Deze configuratie kan ook met deze hardware- en softwareversies worden gebruikt:

- Cisco adaptieve security applicatie (ASA) 5500 Series met 7.x versie en hoger
- Cisco Firewall Services Module (FWSM) die softwareversie 3.2 en hoger uitvoert

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

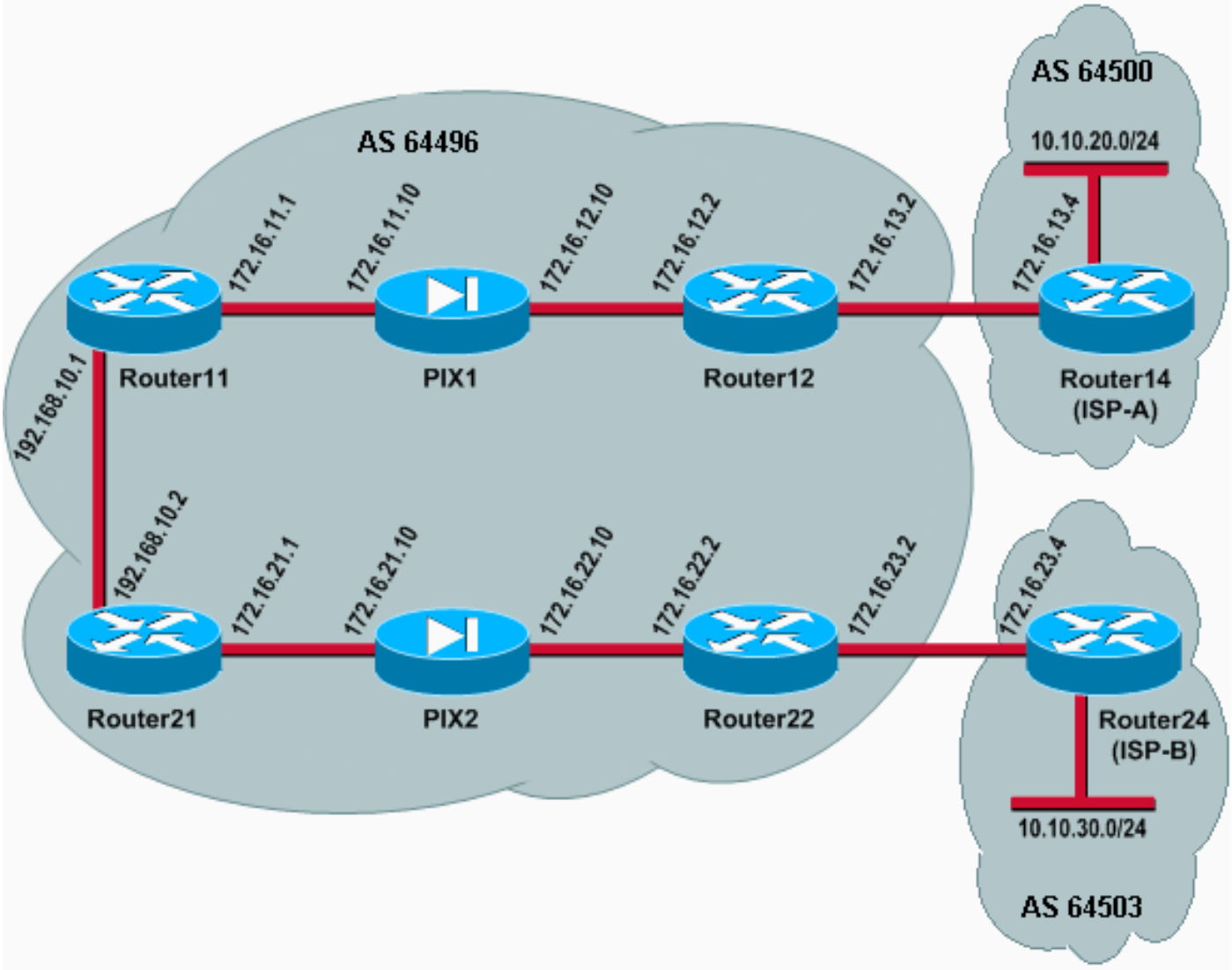
Configureren

Deze sectie verschaft informatie om de functies te configureren die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanninggereedschap (alleen geregistreerd klanten).

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



In deze netwerkinstelling worden Router12 en Router22 (die behoren tot AS 64496) naar Router14 (ISP-A) en Router24 (ISP-B) gemultiformeerd voor redundantie. Het interne netwerk 192.168.10.0/24 bevindt zich binnen in de firewall. Router11 en Router21 verbinden met Router12 en Router22 door de firewall. PIX1 en PIX2 zijn niet geconfigureerd voor het uitvoeren van netwerkadresomzetting (NAT).

Scenario 1

In dit scenario werkt Router12 in AS 64496 extern BGP (eBGP) die met Router14 (ISP-A) in AS 64500 werkt. Router12 doet ook interne BGP (iBGP) die met Router11 door PIX1 werkt. Als eBGP van routes heeft geleerd - A zijn aanwezig, kondigt Router12 een standaardroute 0.0.0.0/0 op iBGP aan op Router11. Als de verbinding met ISP-A faalt, stopt Router12 de standaardroute aan te kondigen.

Op dezelfde manier werkt Router22 in AS 6496 met Router24 (ISP-B) in AS 64503 en kondigt een standaardroute op iBGP naar Router21 aan, voorwaardelijk gebaseerd op de aanwezigheid van ISP-B routes in zijn routingtabel.

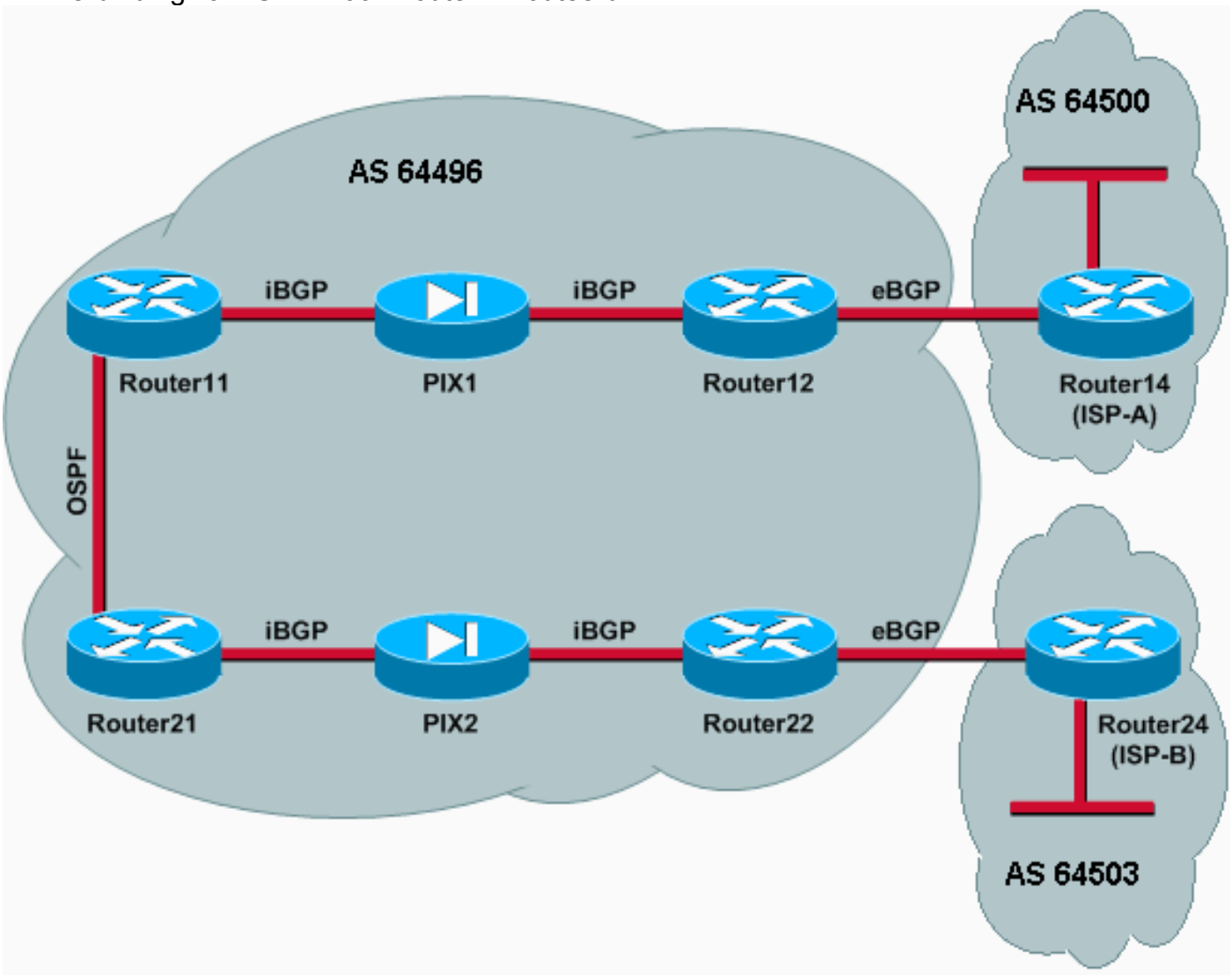
Door het gebruik van een toegangslijst worden PIX1 en PIX2 geconfigureerd om het BGP-verkeer (TCP, poort 179) tussen iBGP-peers toe te staan. Dit komt doordat PIX-interfaces een gekoppeld beveiligingsniveau hebben. Standaard heeft de binneninterface (Ethernet1) een beveiligingsniveau 100 en heeft de externe interface (Ethernet0) een beveiligingsniveau 0. Aansluitingen en verkeer zijn normaal gesproken toegestaan van hoger naar lager

veiligheidsniveau. Om verkeer van een lagere veiligheidsniveau interface naar een hoger veiligheidsniveau toe te staan, moet u echter expliciet een toegangslijst op de PIX definiëren. U moet ook een statische NAT-vertaling op PIX1 en PIX2 configureren, zodat routers aan de buitenkant een BGP-sessie kunnen starten met routers aan de binnenkant van PIX.

Zowel Router11 als Router21 kondigen voorwaardelijk de standaardroute aan in het Open Kortste Pad Eerste (OSPF) domein dat op de iBGP-geleerde standaardroute is gebaseerd. Router11 kondigt de standaardroute in het OSPF domein met een metrische van 5 aan, Router21 kondigt de standaardroute met een metrische van 30 aan, en daarom is de standaardroute van Router11 bij voorkeur. Deze configuratie helpt alleen de standaardroute 0.0.0.0/0 naar Router11 en Router21 te verspreiden, die geheugenconsumptie op de binnenrouters bespaart en optimale prestaties bereikt.

Om deze voorwaarden samen te vatten, is dit het routingbeleid voor AS 64496:

- AS 64496 verkiest de verbinding van Router12 aan ISP-A voor al het uitgaande verkeer (van 192.168.10.0/24 aan Internet).
- Als de connectiviteit met ISP-A mislukt, wordt al het verkeer via de verbinding van Router22 naar ISP-B routeerd.
- Al verkeer dat van het Internet aan 192.168.10.0/24 komt gebruikt de verbinding van ISP-A aan Router12.
- Als de verbinding van ISP-A naar Router12 mislukt, wordt al het inkomende verkeer via de verbinding van ISP-B naar Router22 routeerd.



Configuraties

In dit scenario worden deze configuraties gebruikt:

- 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.
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Wanneer beide BGP sessies omhoog zijn, kunt u verwachten dat alle pakketten via ISP-A worden routeerd. Neem de BGP tabel op Router11. Het leert een standaardroute 0.0.0.0/0 van Router12 met de volgende hop 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
```

De standaardroute 0.0.0.0/0 die via BGP wordt geleerd is geïnstalleerd in de routingtabel, zoals weergegeven in de output van **show ip route** op 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
```

Denk nu aan de BGP-tabel op Router21. Het leert ook de standaardroute 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
```

Zie of deze BGP-geleerde standaardroute in de routingtabel van Router21 wordt geïnstalleerd.

```
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
```

De standaardroute in Router21 wordt geleerd via OSPF (let op het prefix `O` op de route 0.0.0.0/0). Het is interessant om op te merken dat er een standaardroute is die via BGP van Router22 wordt geleerd, maar de **IP route** output toont de standaardroute die via OSPF is geleerd.

De OSPF standaardroute werd geïnstalleerd in Router21 omdat Router21 de standaardroute uit twee bronnen leert: Router22 via iBGP en router11 via OSPF. Het proces van de routeselectie installeert de route met een betere administratieve afstand in de routingtabel. De administratieve afstand van OSPF is 110 terwijl de administratieve afstand van iBGP 200 is. Daarom wordt de OSPF-geleerde standaardroute geïnstalleerd in de routingtabel, omdat 110 minder dan 200 is. Raadpleeg voor meer informatie over routeselectie in Cisco Routers.

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

Breng de BGP sessie tussen Router12 en ISP-A naar beneden.

```
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 heeft niet de standaardroute die via BGP van Router12 wordt geleerd.

```
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
```

Controleer de routingtabel op Router11. De standaardroute wordt geleerd via OSPF (administratieve afstand van 110) met een volgende hop van 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
```

Deze output wordt verwacht volgens het vooraf gedefinieerde beleid. Op dit punt is het echter belangrijk om de **afstand** te begrijpen **bgp 20 105 200** configuratie opdracht in Router11 en hoe deze de routeselectie op Router11 beïnvloedt.

De standaardwaarden van deze opdracht zijn **op afstand bgp 20 200 200**, waar eBGP-leerde routes een administratieve afstand van 20 hebben, iBGP-geleerde routes een administratieve afstand van 200 hebben en lokale BGP-routes een administratieve afstand van 200.

Wanneer het verband tussen Router12 en ISP-A opnieuw op komt, leert Router11 de standaardroute via iBGP van Router12. Maar omdat de standaard administratieve afstand van deze iBGP-geleerde route 200 is, zal deze niet de OSPF-geleerde route vervangen (omdat 110 minder dan 200 is). Dit dwingt al het uitgaande verkeer naar de verbinding van Router21 tot Router22 aan ISP-B, zelfs al is de verbinding van Router12 aan ISP-A weer omhoog. Om dit probleem op te lossen, verander de administratieve afstand van de iBGP-route naar een waarde minder dan het gebruikte Protocol van de Gateway (IGP). In dit voorbeeld is IGP OSPF, dus is een afstand van 105 geselecteerd (omdat 105 minder dan 110 is).

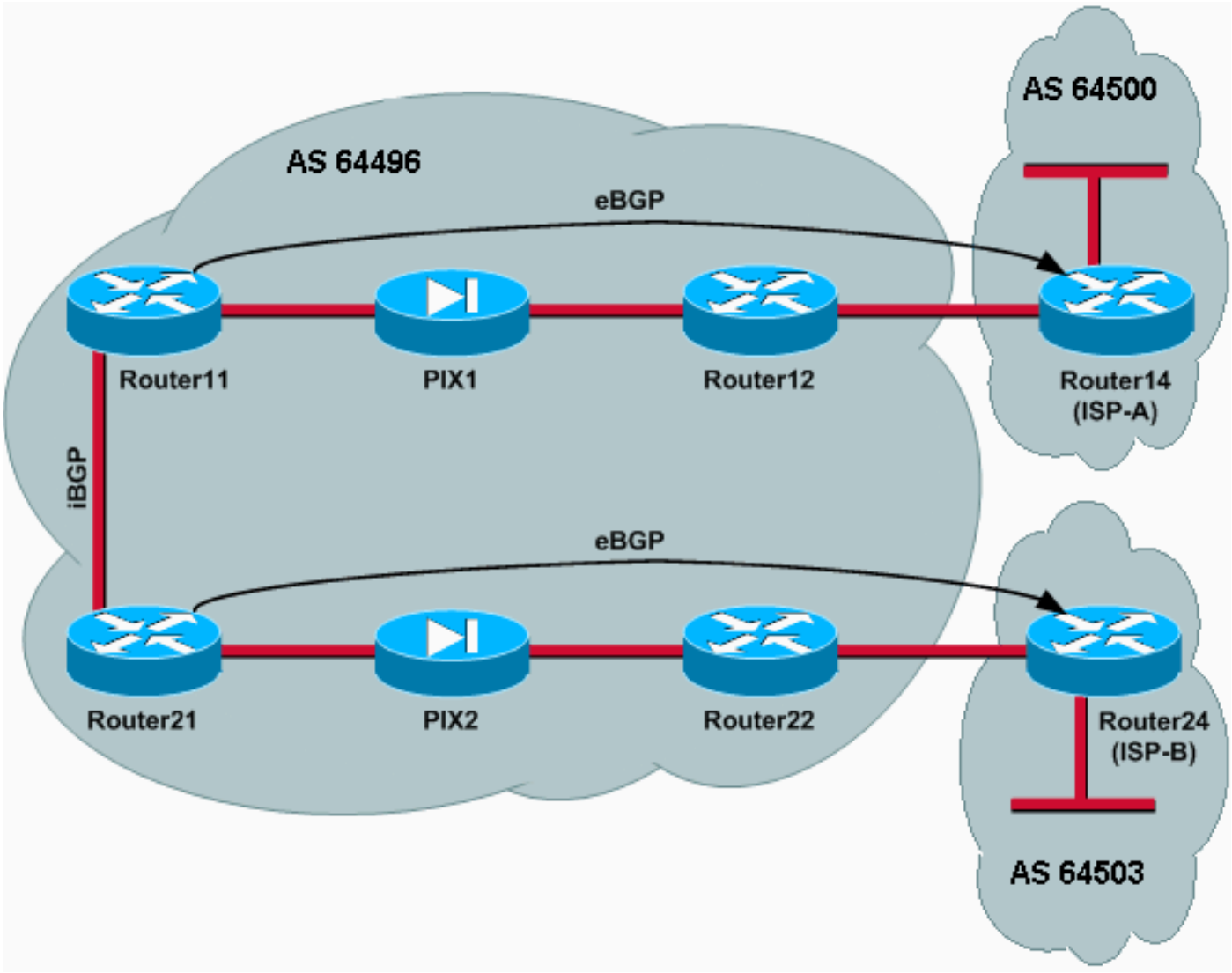
Raadpleeg de BGP-opdrachten voor meer informatie over de opdracht bgp op afstand. Raadpleeg voor meer informatie over multihoming met BGP de taakverdeling met BGP in enkelvoudige en meervoudige omgevingen: Configuraties van monsters.

Scenario 2

In dit scenario wordt Router11 rechtstreeks eBGP uitgevoerd met router 14 (ISP-A) en Router21 wordt rechtstreeks eBGP uitgevoerd met Router24 (ISP-B). Router12 en Router22 nemen niet deel aan het peeren van BGP, maar zij verstrekken de IP connectiviteit aan de ISPs. Omdat de eBGP peers niet direct verbonden buren zijn, wordt de **buurebgp-multihop** opdracht op de deelnemende routers gebruikt. De **buurgebruiker ebgp-multihop** opdracht stelt BGP in staat om de standaard één hop eBGP limiet te omzeilen omdat het de Tijd om te leven (TTL) van eBGP pakketten van de standaardwaarde van 1 verandert. In dit scenario is de eBGP buurman 3 hoop verder, zodat **buurman ebgp-multihop 3** op de deelnemende routers wordt gevormd TTL-waarde wordt gewijzigd in 3. Tevens worden statische routes geconfigureerd op de routers en PIX om er zeker van te zijn dat Router11 het Router14 (ISP-A)-adres 172.16.13.4 kan pingelen en dat Router21 het Router24 (ISP-B)-adres 172.16.23.4 kan.

Standaard staat PIX niet toe dat ICMP-pakketten (Internet Control Message Protocol) (verzonden wanneer u de **ping**-opdracht geeft) worden doorgevoerd. Om ICMP-pakketten toe te staan, gebruikt u de **toegangslijst** opdracht zoals in de volgende PIX-configuratie getoond. Raadpleeg de opdracht **toegangslijst** voor meer informatie over de opdracht PIX-firewall A door B-opdrachten.

Het routebeleid is hetzelfde als in scenario 1: Het verband tussen Router12 en ISP-A wordt geprefereerd over het verband tussen Router22 en ISP-B, en wanneer de verbinding ISP-A omlaag gaat wordt de verbinding ISP-B gebruikt voor al het inkomende en uitgaande verkeer.



Configuraties

In dit scenario worden deze configuraties gebruikt:

- router11
- router12
- router14 (ISP-A)
- router21
- router22
- PIX1
- PIX2

router11

```
hostname Router11
 !
 interface FastEthernet0/0
  ip address 192.168.10.1 255.255.255.0
!--- Connected to Router21. ! interface FastEthernet0/1
ip address 172.16.11.1 255.255.255.0 !--- Connected to
PIX1. ! router bgp 64496 no synchronization bgp log-
neighbor-changes network 192.168.10.0 neighbor
172.16.13.4 remote-as 64500 neighbor 172.16.13.4 ebgp-
multihop 3 !--- To accept and attempt BGP connections to
external peers that reside on networks that !--- are not
directly connected. neighbor 172.16.13.4 route-map set-
pref in !--- Sets higher local-preference for learned
routes. neighbor 172.16.13.4 route-map adv_to_ispa out
neighbor 192.168.10.2 remote-as 64496 neighbor
192.168.10.2 next-hop-self no auto-summary ! ip route
172.16.12.0 255.255.255.0 172.16.11.10 ip
route172.16.13.4 255.255.255.255 172.16.11.10 !---
Static route to eBGP peer, because it is not directly
connected. ! access-list 20 permit 192.168.10.0 ! route-
map set-pref permit 10 set local-preference 200 ! route-
map adv_to_ispa permit 10 match ip address 20 !
```

router12

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

router14 (ISP-A)

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

router21

```
hostname Router21
 !
 interface FastEthernet0/0
```

```
  ip address 192.168.10.2 255.255.255.0
!--- Connected to Router11. ! interface FastEthernet0/1
ip address 172.16.21.1 255.255.255.0 !--- Connected to
PIX2. ! router bgp 64496 no synchronization network
192.168.10.0 neighbor 172.16.23.4 remote-as 64503
neighbor 172.16.23.4 ebgp-multihop 3 !--- To accept and
attempt BGP connections to external peers that reside on
networks that !--- are not directly connected. neighbor
172.16.23.4 route-map adv_to_ispb out neighbor
192.168.10.1 remote-as 64496 neighbor 192.168.10.1 next-
hop-self no auto-summary ! ip route 172.16.22.0
255.255.255.0 172.16.21.10 ip route172.16.23.4
255.255.255.255 172.16.21.10 !--- Static routes
configured to reach BGP peer. ! access-list 20 permit
192.168.10.0 ! route-map adv_to_ispb permit 10 match ip
address 20 set as-path prepend 10 10 10
```

router22

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

router24 (ISP-B)

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

PIX1

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

access-group acl-1 in interface outside
```

```
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 172.16.11.1 172.16.11.1 netmask
255.255.255.255
route outside 0.0.0.0 0.0.0.0 172.16.12.2 1
route inside 192.168.10.0 255.255.255.0 172.16.11.1 1
```

PIX2

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.22.10 255.255.255.0
ip address inside 172.16.21.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.23.4 host
172.16.21.1 eq bgp
!-- Access list allows BGP traffic to pass from outside
to inside. access-list acl-1 permit icmp any any !--
Allows ping to pass through for testing purposes only.

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

Verifiëren

Begin met de situatie waarin de verbindingen met ISP-A en ISP-B zijn. De **samenvatting van het** commando van de **show ip** op Router11 en Router21 bevestigt de gevestigde BGP sessies met ISP-A en ISP-B respectievelijk.

```
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
```

De BGP-tabel op Router11 toont de standaardroute (0.0.0.0/0) naar de volgende hop-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
```

Controleer nu de BGP-tabel op Router21. Deze heeft twee 0.0.0.0/0-routes: Een van ISP-B met een volgende hop van 172.16.23.4 op eBGP, en de andere geleerde via iBGP met een lokale voorkeur van 200. Router21 geeft de voorkeur aan iBGP-geleerde routes vanwege de hogere lokale preferentie eigenschap, dus installeert hij die route in de routingtabel. Raadpleeg voor meer informatie over de BGP-selectie het BGP-algoritme voor selectie van beste pad.

```
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
```

Problemen oplossen

Breng de router11 en ISP-A BGP zitting neer.

```
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
```

De eBGP-sessie aan ISP-A gaat omlaag wanneer de timer voor de hold-down-timer (180 seconden) verloopt.

```
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
```

Dankzij de link naar beneden van ISP-A, installeert Router11 0.0.0.0/0 met een volgende hop van 192.168.10.2 (Router21), die via iBGP in zijn routingtabel wordt geleerd. Dit duwt al uitgaande verkeer door Router21 en dan aan ISP-B, zoals in deze uitvoer:

```
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
```

MD5-verificatie voor BGP-buren via de PIX/ASA

PIX 6.x-configuratie

Net zoals elk ander routingprotocol kan BGP worden ingesteld voor verificatie. U kunt MD5-verificatie configureren tussen twee BGP-peers, wat betekent dat elk segment dat wordt verzonden op de TCP-verbinding tussen de peers, wordt geverifieerd. MD5-verificatie moet op beide BGP-peers met hetzelfde wachtwoord worden ingesteld; anders wordt er geen verband tussen hen gelegd . De configuratie van MD5 authenticatie veroorzaakt Cisco IOS software om de MD5 samenvatting van elk segment te produceren en te controleren dat op de TCP verbinding wordt verstuurd. Als de authenticatie wordt ingeroepen en een segment geen echtheidscontrole heeft, wordt een foutmelding gegenereerd.

Wanneer u BGP-peers configureren met MD5-verificatie die door een PIX-firewall leiden, is het belangrijk om de PIX tussen de BGP-buren te configureren zodat de sequentienummers voor de TCP-stromen tussen de BGP-buren niet willekeurig zijn. Dit is omdat de TCP willekeurige reeks sequentienummer functie in de PIX firewall standaard is ingeschakeld en het wijzigt het TCP sequentienummer van de inkomende pakketten voordat het ze doorgeeft.

MD5-verificatie wordt toegepast op de TCP-onderdrukking, TCP-header en TCP-gegevens (raadpleeg RFC 2385). TCP gebruikt deze gegevens-die de TCP sequentie en ACK getallen-samen met het BGP buurwachtwoord omvatten om een 128 bit haasnummer te maken. Het hashnummer is in het pakket in een veld met de TCP-headeroptie opgenomen. Standaard wordt het volgnummer door de PIX gecompenseerd met een willekeurig aantal TCP-stromen. Op het verzenden van BGP peer, gebruikt TCP het originele sequentienummer om het 128 bit MD5 haasnummer te maken en omvat dit haasnummer in het pakket. Wanneer het ontvangende BGP-peer het pakket krijgt, gebruikt TCP het PIX-gewijzigde sequentienummer om een 128 bit MD5 hash-nummer te maken en vergelijkt het met het hashnummer dat in het pakket is opgenomen.

Het hashnummer is anders omdat de TCP-sequentiewaarde is gewijzigd door PIX en TCP in de BGP-buurman bevat het pakket en slaat een MD5 mislukt bericht op zoals dit:

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

Gebruik het sleutelwoord **norandomseq** met het **statische (binnenkant, buiten)** bevel **172.11.1 172.16.11.1 netwerkmasker 255.255.255.0 norandomseq** om dit sequentieprobleem op te lossen en te voorkomen PIX van het TCP-nummer . Dit voorbeeld illustreert het gebruik van het **norandomseq** sleutelwoord:

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

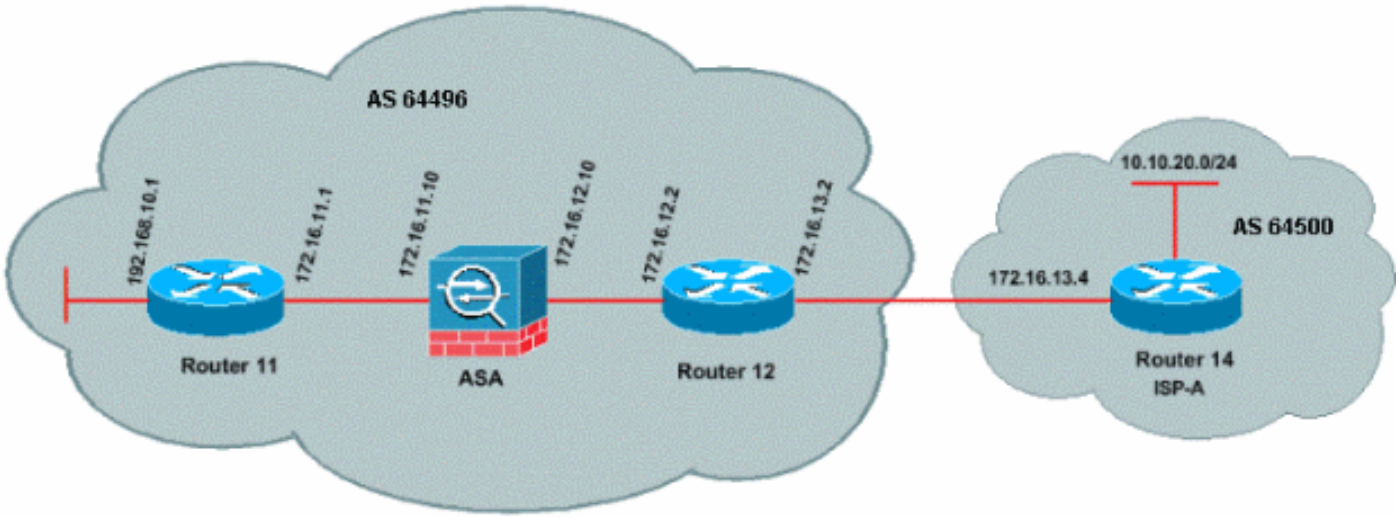
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside.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

Deze sectie gebruikt deze netwerkinstellingen.



PIX/ASA versie 7.x en introduceert later een extra uitdaging wanneer u probeert een BGP-sessie met MD5 verificatie op te zetten. Standaard wordt PIX/ASA versie 7.x en later herschrijft elke TCP MD5-optie die is opgenomen in een TCP-datagram dat door het apparaat gaat en de optie-type, -grootte en -waarde vervangt door NOP optie-bytes. Dit breekt effectief de BGP MD5 authenticatie uit en resulteert in foutmeldingen zoals deze bij elke peerrouter:

```
000296: 7 apr. 2010 15:13:22.221 EDT: %TCP-6-BADAUTH: No MD5 digest van 172.16.11.1(2894) tot
172.16.12.2(179)
```

Om een BGP-sessie met MD5-verificatie succesvol tot stand te brengen, moeten deze drie kwesties worden opgelost:

- TCP-sequentienummer willekeurig uitschakelen
- TCP MD5 optie-herschrijven
- NAT tussen peers uitschakelen

Een class-map en een access-list worden gebruikt om het verkeer tussen de peers te selecteren dat beiden moeten worden vrijgesteld van de TCP sequentienummer randomization en een MD5 optie mogen dragen zonder het opnieuw schrijven. Een tcp-map wordt gebruikt om het optietype aan te geven dat in dit geval optie-type 19 (TCP MD5-optie) moet zijn. De class-map en de tcp-map zijn allebei gekoppeld door een beleidsmandaat, een onderdeel van de modulaire infrastructuur van het beleidskader. De configuratie wordt dan geactiveerd met de opdracht **Service-beleid**.

Opmerking: De noodzaak om NAT tussen de peers uit te schakelen wordt verwerkt door de opdracht **Geen** bediening **om deze uit te schakelen**.

In versie 7.0 en later is het standaard karakter van een ASA **geen nat-control**, dat stelt dat elke verbinding door ASA standaard niet de NAT-test hoeft te doorstaan. Aangenomen wordt dat ASA een standaardinstelling van **non-control heeft**. Raadpleeg NAT-controle voor meer informatie. Als **nat-control** wordt afgedwongen, moet u NAT expliciet uitschakelen voor de BGP-peers. Dit kan worden gedaan met de **statische** opdracht tussen binnen- en buitenkant interfaces.

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

PIX/ASA 7.x/8.x

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

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


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


!
!--- TCP-MAP to allow MD5 Authentication. tcp-map BGP-
MD5-OPTION-ALLOW
  tcp-options range 19 19 allow
!
!--- Apply the ACL that allows traffic !--- from the
```

```
outside peer to the inside peer access-group OUTSIDE-
ACL-IN in interface outside
!
asdm image disk0:/asdm-621.bin
no asdm history enable
arp timeout 14400

route outside 0.0.0.0 0.0.0.0 172.16.12.2 1
route inside 192.168.10.0 255.255.255.0 172.16.11.1 1
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes
4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!
class-map inspection_default
 match default-inspection-traffic
class-map BGP-MD5-CLASSMAP
 match access-list BGP-MD5-ACL
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
 class BGP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options BGP-MD5-OPTION-ALLOW

!
service-policy global_policy global
prompt hostname context
Cryptochecksum:64ea55d7271e19eea87c8603ab3768a2
: end
```

router11

```
Router11#sh run
```

```
hostname Router11
!
ip subnet-zero
!
interface Loopback0
 no ip address
 shutdown
!
interface Loopback1
 ip address 192.168.10.1 255.255.255.0
!
interface Ethernet0
 ip address 172.16.11.1 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
!
router bgp 64496
 no synchronization
 bgp log-neighbor-changes
 network 192.168.10.0
 neighbor 172.16.12.2 remote-as 64496

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

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

router12

```
Router12#sh run
hostname Router12
!
aaa new-model
!
ip subnet-zero
!
interface Ethernet0
 ip address 172.16.13.2 255.255.255.0
!
interface Ethernet1
```

```
 ip address 172.16.12.2 255.255.255.0
!
interface Serial0
 no ip address
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
router bgp 64496
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.11.1 remote-as 64496

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

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

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

!--- Static route to iBGP peer, because it is not
directly connected. ip route 172.16.11.0 255.255.255.0
172.16.12.10 ip http server ! access-list 1 permit
0.0.0.0 access-list 10 permit 192.168.10.0 access-list
20 permit 10.10.20.0 0.0.0.255 access-list 21 permit
172.16.13.4 route-map check-ispa-route permit 10 match
ip address 20 match ip next-hop 21 ! route-map adv-to-
ispa permit 10 match ip address 10 ! !--- Output
suppressed
```

router14 (ISP-A)

```
Router14#sh run
hostname Router14
!
!
ip subnet-zero
!
interface Ethernet0
 ip address 172.16.13.4 255.255.255.0
!
interface Ethernet1
 ip address 10.10.20.1 255.255.255.0
!
interface Serial0
 no ip address
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
```

```
router bgp 64500
 bgp log-neighbor-changes
 network 10.10.20.0 mask 255.255.255.0

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

Verifiëren

Uitvoer van het **tonen IP Bgp samenvatting** bevel wijst erop dat de authenticatie succesvol is en dat de BGP sessie op Router11 wordt gevestigd.

```
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#
```

Gerelateerde informatie

- BGP-ondersteuningspagina
- BGP-algoritme voor selectie van het beste pad
- Laad het delen met BGP in enkele en multifunctionele omgevingen: Configuraties van voorbeelden
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- PIX-firewall configureren en testen
- Technische ondersteuning en documentatie – Cisco Systems