ASA/PIX: BGP con el ejemplo de configuración ASA

Contenido

Introducción

Esta configuración de muestra demuestra cómo ejecutar el Border Gateway Protocol (BGP) a través de un dispositivo de seguridad (PIX/ASA) y cómo alcanzar la Redundancia en un BGP y un entorno PIX multihomed. Con un diagrama de la red como un ejemplo, este documento explica cómo rutear automáticamente el tráfico al Proveedor de servicios de Internet B (ISP-B) cuando COMO 64496 pierde la Conectividad al ISP-A (o al revés), con el uso de los Dynamic Routing Protocol que se ruedan entre todo el Routers COMO 64496.

Porque el BGP utiliza los paquetes TCP del unicast en el puerto 179 para comunicar con sus pares, usted puede configurar el PIX1 y el PIX2 para permitir el tráfico de unidifusión en el puerto TCP 179. Esta manera, peering BGP se puede establecer entre el Routers que está conectado con el Firewall. La Redundancia y los políticas de ruteo deseados se pueden alcanzar con la manipulación de los atributos BGP.

prerrequisitos

Requisitos

Los Quien lea este documento deben ser familiares con configurar el BGP y la configuración de escudo de protección básica.

Componentes Utilizados

Los ejemplos de escenario en este documento se basan en estas versiones de software:

- ¿Cisco 2600 Router con el Cisco IOS? Software Release 12.2(27)
- PIX 515 con la versión 6.3(3) y posterior del Cisco PIX Firewall

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración también se puede utilizar con las siguientes versiones de hardware y software:

- 5500 Series adaptantes del dispositivo de seguridad de Cisco (ASA) con la versión 7.x y posterior
- Módulo de servicios del escudo de protección Cisco (FWSM) esa versión de software 3.2 de los funcionamientos y posterior

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

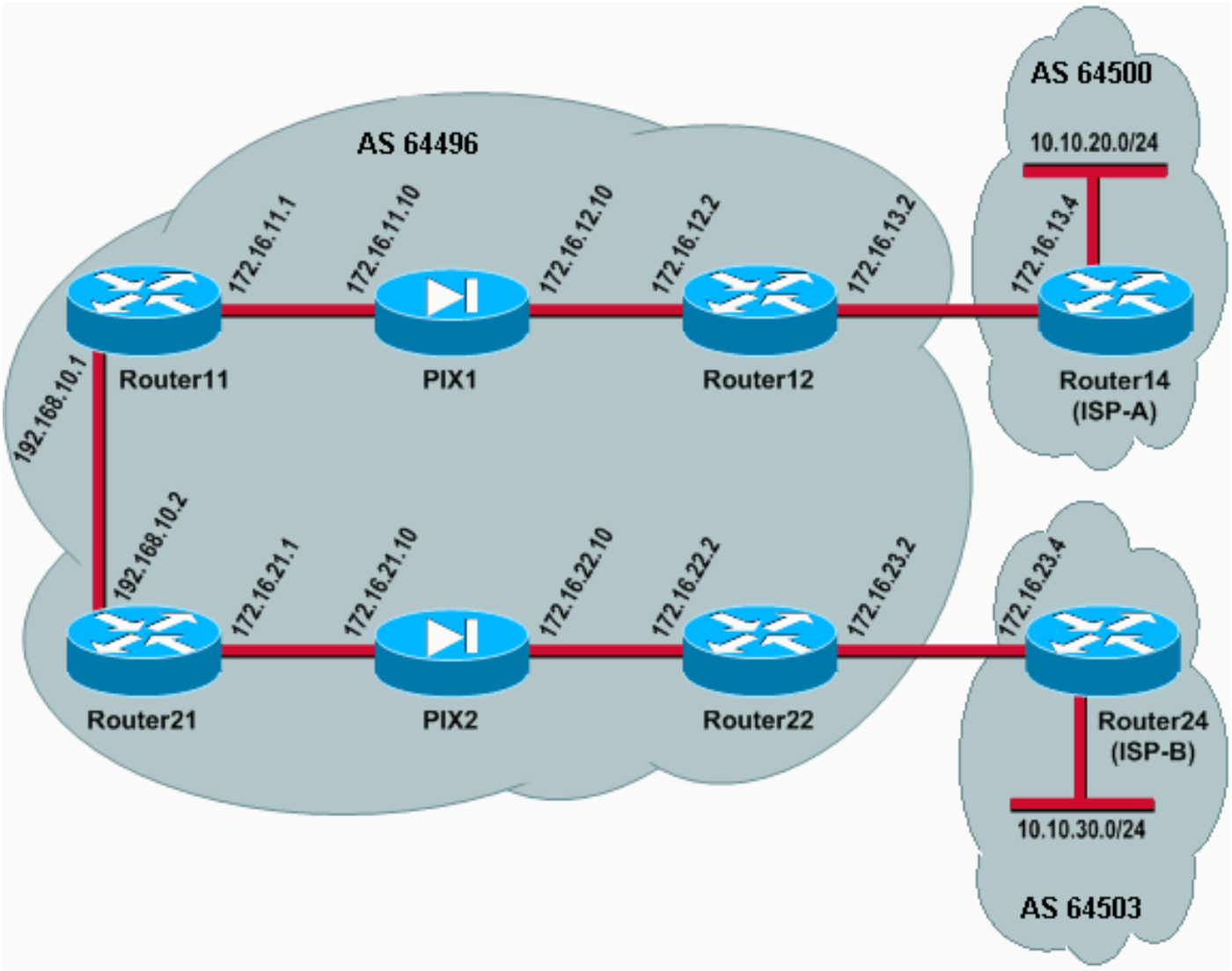
Configurar

Esta sección proporciona la información para configurar las características descritas en este documento.

Note: Para encontrar la información adicional sobre los comandos en este documento, utilice la herramienta de búsqueda de comandos (clientes registrados solamente).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



En esta configuración de la red, el Router12 y el Router22 (que pertenecen COMO a 64496) son multihomed al Router14 (ISP-A) y al Router24 (ISP-B) respectivamente, para la Redundancia. La red interna 192.168.10.0/24 está en el interior del Firewall. El Router11 y el Router21 conectan con el Router12 y el Router22 con el Firewall. El PIX1 y el PIX2 no se configuran para realizar el Network Address Translation (NAT).

Escenario 1

En este escenario, el Router12 adentro COMO 64496 hace el peering del BGP externo (eBGP) con el Router14 (ISP-A) adentro COMO 64500. El Router12 también hace el Internal BGP (iBGP) que mira con el Router11 con el PIX1. Si las rutas aprendido del eBGP del ISP-A están presentes, el Router12 anuncia una ruta predeterminado 0.0.0.0/0 en el iBGP al Router11. Si el link al ISP-A falla, el Router12 para el anunciar de la ruta predeterminado.

Semejantemente, el Router22 adentro COMO 64496 hace el eBGP que mira con el Router24 (ISP-B) adentro COMO 64503 y anuncia una ruta predeterminado en el iBGP al Router21 basado condicional en la presencia de rutas del ISP-B en su tabla de ruteo.

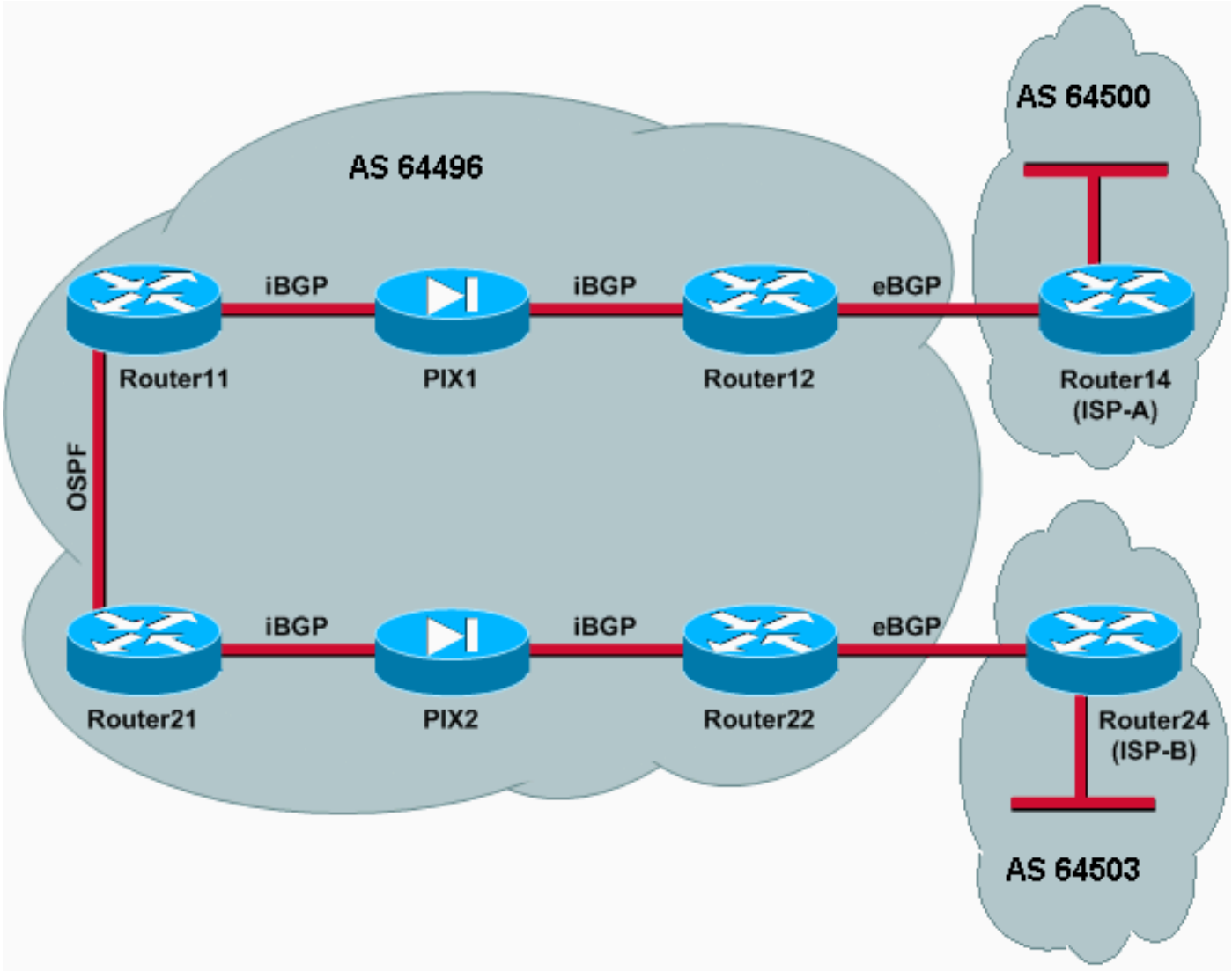
Con el uso de una lista de acceso, el PIX1 y el PIX2 se configuran para permitir el tráfico BGP (TCP, el puerto 179) entre los pares del iBGP. Esto es porque las interfaces PIX tienen un nivel de seguridad asociado. Por abandono, la interfaz interior (ethernet1) tiene un nivel de seguridad 100 y la interfaz exterior (ethernet0) tiene las conexiones y tráfico del nivel de seguridad un 0. se permite normalmente de más arriba a las interfaces de menor nivel de seguridad. Para permitir el

tráfico de una interfaz de menor nivel de seguridad a una interfaz de mayor nivel de seguridad, sin embargo, usted debe definir explícitamente una lista de acceso en el PIX. También, usted debe configurar una traducción NAT estática en el PIX1 y el PIX2, para permitir que el Routers en el exterior inicie a una sesión de BGP con el Routers en el interior del PIX.

El Router11 y el Router21 anuncian condicional la ruta predeterminado en el dominio del Open Shortest Path First (OSPF) basado en la ruta predeterminado iBGP-docta. El Router11 anuncia la ruta predeterminado en el dominio OSPF con un métrico de 5, el Router21 anuncia la ruta predeterminado con un métrico de 30, y por lo tanto la ruta predeterminado del Router11 se prefiere. Esta configuración ayuda a la propagación solamente la ruta predeterminado 0.0.0.0/0 al Router11 y al Router21, que conserva la consumición de la memoria en los routeres internos y alcanza el rendimiento óptimo.

Así, resumir estas condiciones, éste es el política de ruteo para COMO 64496:

- COMO 64496 prefiere el link del Router12 al ISP-A para todo el tráfico saliente (a partir del 192.168.10.0/24 a Internet).
- Si la Conectividad al ISP-A falla, todo el tráfico se rutea vía el link del Router22 al ISP-B.
- Todo el tráfico que viene de Internet a 192.168.10.0/24 utiliza el link del ISP-A al Router12.
- Si el link del ISP-A al Router12 falla, todo el tráfico entrante se rutea vía el link del ISP-B al Router22.



[Configuraciones]

Este escenario utiliza estas configuraciones:

- 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.
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Cuando ambas sesiones de BGP están para arriba, usted puede esperar que todos los paquetes sean ruteados vía el ISP-A. Considere la tabla BGP en el Router11. Aprende una ruta predeterminado 0.0.0.0/0 del Router12 con el salto siguiente 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
```

Las 0.0.0.0/0 rutas predeterminado que es docta vía el BGP están instaladas en la tabla de ruteo, tal y como se muestra en de la salida de la **ruta de IP de la demostración** en el 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
```

Ahora considere la tabla BGP en el Router21. También aprende la ruta predeterminado vía el 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
```

Ahora vea si esta ruta predeterminado BGP aprendida consigue instalada en la tabla de ruteo 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
```

La ruta predeterminado en el Router21 es docta vía el OSPF (observe el prefijo o en las 0.0.0.0/0 rutas). Es interesante observar que hay una ruta predeterminado aprendida vía el BGP del Router22, pero la salida de la **ruta de IP de la demostración** muestra la ruta predeterminado aprendida vía el OSPF.

La ruta predeterminado OSPF fue instalada en el Router21 porque el Router21 aprende la ruta predeterminado a partir de dos fuentes: Router22 vía el iBGP y Router11 vía el OSPF. El proceso de la selección de Route instala la ruta con una mejor distancia administrativa en la tabla de ruteo. La distancia administrativa del OSPF es 110 mientras que la distancia administrativa del iBGP es 200. Por lo tanto, la ruta predeterminado OSPF-docta consigue instalada en la tabla de ruteo, porque 110 es menos de 200. Para más información sobre la selección de Route, refiera a la selección de Route en los routeres Cisco.

Troubleshooting

Use esta sección para resolver problemas de configuración.

Derribe a la sesión de BGP entre el Router12 y el 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
```

El Router11 no tiene la ruta predeterminado aprendida vía el BGP del 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
```

Marque la tabla de ruteo en el Router11. La ruta predeterminado es docta vía OSPF (distancia administrativa de 110) con un salto siguiente del 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
```

Esta salida se espera según las directivas predefinidas. En este momento, sin embargo, es importante entender el **BGP 20 de la distancia el** comando configuration **105 200** en el Router11 y cómo influencia la selección de Route en el Router11.

Los valores predeterminados de este comando son **BGP 20 de la distancia 200 200**, donde las rutas eBGP-doctas tienen una distancia administrativa de 20, las rutas IBGP aprendidas tienen una distancia administrativa de 200, y las rutas BGP locales tienen una distancia administrativa de 200.

Cuando sube el link entre el Router12 y el ISP-A otra vez, el Router11 aprende la ruta predeterminado vía el iBGP del Router12. Sin embargo, porque la distancia administrativa predeterminada de esta ruta IBGP aprendida es 200, no substituirá la ruta OSPF-docta (porque 110 es menos de 200). Esto fuerza todo el tráfico saliente al link del Router21 al Router22 al ISP-B, aunque el link del Router12 al ISP-A está para arriba otra vez. Para solucionar este problema, cambie la distancia administrativa de la ruta IBGP aprendida a un valor menos que el Interior Gateway Protocol (IGP) usado. En este ejemplo, el IGP es OSPF, así que una distancia de 105 fue elegida (porque 105 es menos de 110).

Para más información sobre el **comando distance bgp**, refiera a los comandos bgp. Para más información sobre el multihoming con el BGP, refiera a la carga a compartir con el BGP en el entornos de una sola conexión y de varias conexiones: Configuraciones de muestra.

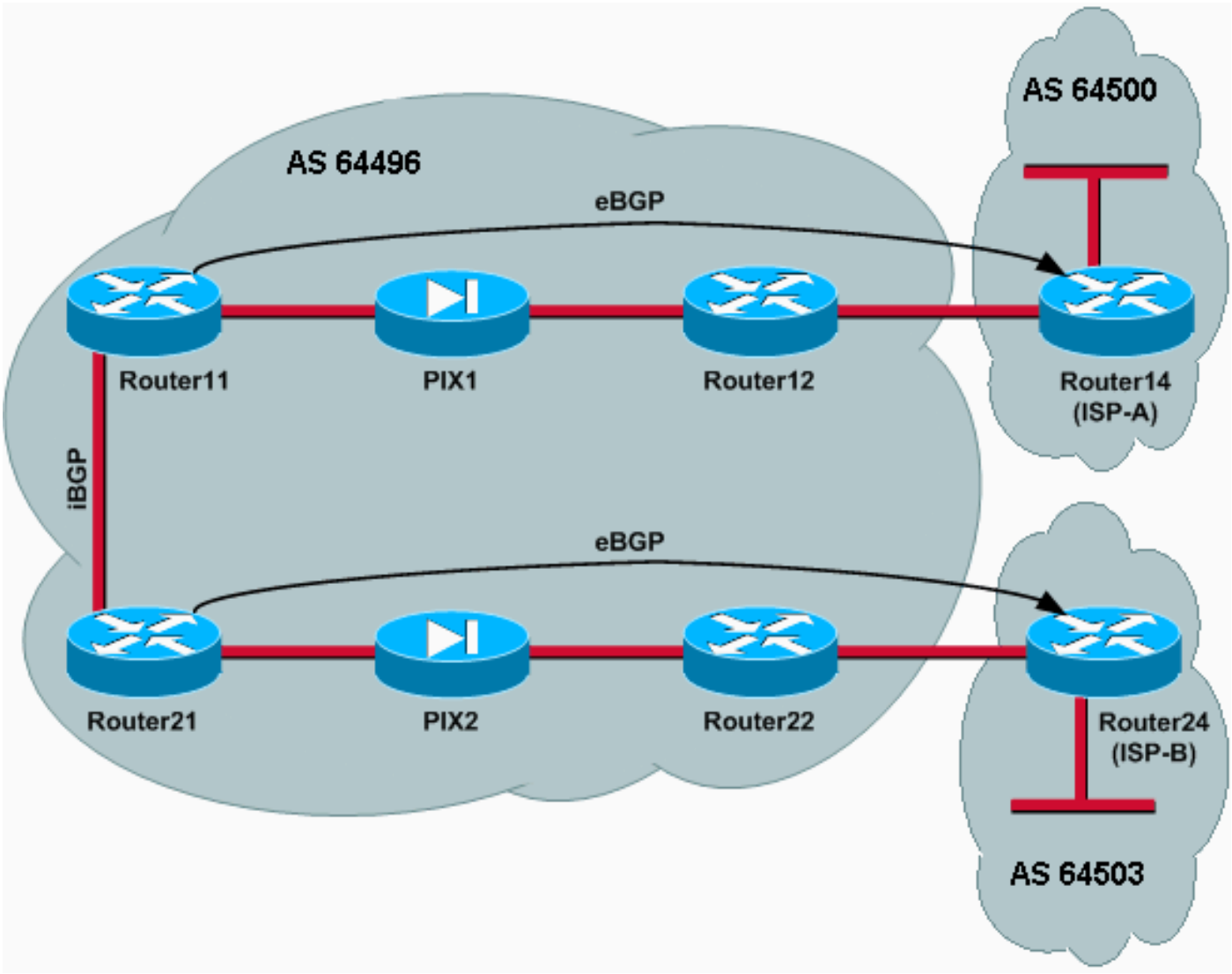
Escenario 2

En este escenario, el Router11 es directamente eBGP que mira con el Router14 (ISP-A), y el Router21 es directamente eBGP que mira con el Router24 (ISP-B). El Router12 y el Router22 no participan en el peering BGP, sino que proporcionan la conectividad del IP a los ISP. Porque los pares del eBGP no son directamente vecinos conectados, utilizan al **comando neighbor ebgp-multihop** en los routeres participantes. **El comando neighbor ebgp-multihop** permite al BGP para reemplazar el un límite predeterminado del eBGP del salto porque cambia el Time to Live (TTL) de los paquetes del eBGP del valor predeterminado de 1. En este escenario, el vecino eBGP es 3 saltos lejos, así que el **ebgp-multihop vecino 3** se configura en los routeres participantes para cambiar el valor de TTL a 3. También, las Static rutas se configuran en el Routers y el PIX para asegurarse de que el Router11 puede hacer ping el direccionamiento 172.16.13.4 del Router14 (ISP-A) y asegurarse de que el Router21 puede hacer ping el direccionamiento 172.16.23.4 del

Router24 (ISP-B).

Por abandono, el PIX no permite que los paquetes del Internet Control Message Protocol (ICMP) (enviados cuando usted publica el **comando ping**) pasen a través. Para permitir los paquetes icmp, utilice el **comando access-list** tal y como se muestra en de la configuración PIX siguiente. Para más información sobre el comando access-list, refiera al firewall PIX A a través de los comandos B.

El política de ruteo es lo mismo que en el escenario 1: el link entre el Router12 y el ISP-A se prefiere sobre el link entre el Router22 y el ISP-B, y cuando el link ISP-A va abajo del link del ISP-B se utiliza para todo el tráfico entrante y saliente.



Configuraciones

Este escenario utiliza estas configuraciones:

- 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
```

Verificación

Comience con la situación donde están los links al ISP-A y al ISP-B para arriba. La salida del **comando show ip bgp summary** en el Router11 y el Router21 confirma a las sesiones de BGP establecidas con el ISP-A y el ISP-B respectivamente.

```
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 tabla BGP en el Router11 muestra la ruta predeterminado (0.0.0.0/0) hacia el ISP-A 172.16.13.4 del salto siguiente.

```
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
```

Ahora marque la tabla BGP en el Router21. Tiene dos 0.0.0.0/0 rutas: uno aprendido del ISP-B con un salto siguiente de 172.16.23.4 en el eBGP, y el otro aprendido vía el iBGP con una preferencia local de 200. El Router21 prefiere las rutas IBGP aprendidas debido al atributo de preferencia local más alto, así que instala que ruta en la tabla de ruteo. Para más información sobre la selección de trayecto BGP, refiera al algoritmo de selección del mejor trayecto 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
```

Troubleshooting

Derribe el Router11 y a la sesión de BGP del 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 sesión eBGP al ISP-A va abajo de cuando expira el temporizador del asentamiento (180 segundos).

```
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
```

Con el link al ISP-A abajo, el Router11 instala 0.0.0.0/0 con un salto siguiente de 192.168.10.2 (Router21), que es docto vía el iBGP en su tabla de ruteo. Esto avanza todo el tráfico saliente con el Router21 y entonces al ISP-B, tal y como se muestra en de esta salida:

```
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
```

Autenticación de MD5 para los vecinos BGP con el PIX/ASA

Configuración PIX 6.x

Apenas como cualquier otro Routing Protocol, el BGP se puede configurar para la autenticación. Usted puede configurar autenticación de MD5 entre dos peeres BGP, así que significa que cada segmento enviado en la conexión TCP entre los pares está verificado. Autenticación de MD5 debe ser configurado con la misma contraseña en ambos peeres BGP; de lo contrario, la conexión entre ellos no se realizará. La configuración autenticación de MD5 del Cisco IOS Software de las causas para generar y para marcar la publicación MD5 de cada segmento envió encendido la conexión TCP. Si se invoca la autenticación y un segmento falla la autenticación, se genera un mensaje de error.

Cuando usted está configurando a los peeres BGP con autenticación de MD5 ese paso con un firewall PIX, es importante configurar el PIX entre los vecinos BGP de modo que los números de secuencia para los flujos TCP entre los vecinos BGP no sean al azar. Esto es porque la característica del número de la secuencia aleatoria TCP en el firewall PIX se habilita por

abandono, y cambia el número de secuencia TCP de los paquetes entrantes antes de que él adelante ellos.

Autenticación de MD5 se aplica en la encabezado, el encabezado TCP y los datos psuedo-IP TCP (refiera al RFC 2385). El TCP utiliza estos datos — que incluya la secuencia TCP y los números ACK — junto con la contraseña del vecino BGP para crear un número del hash del bit 128. El número del hash se incluye en el paquete en un campo de opción del encabezado de TCP. Por abandono, el PIX compensa el número de secuencia por un número aleatorio, por el flujo TCP. En el peer BGP de envío, el TCP utiliza el número de secuencia original para crear 128 el número del hash del bit MD5 e incluye este número del hash en el paquete. Cuando el peer BGP de recepción consigue el paquete, el TCP utiliza el número de secuencia PIX-modificado para crear 128 un número del hash del bit MD5 y lo compara al número del hash que se incluye en el paquete.

El número del hash es diferente porque el valor de la secuencia TCP fue cambiado por el PIX, y el TCP en el vecino BGP cae el paquete y registra un mensaje fallido MD5 similar éste:

```
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
```

Utilice la palabra clave del **norandomseq** con **(dentro, afuera) el comando norandomseq estático de 255.255.255.0 del netmask de 172.16.11.1 172.16.11.1** de solucionar este problema y de parar el PIX de compensar el número de secuencia TCP. Este ejemplo ilustra el uso de la palabra clave del **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

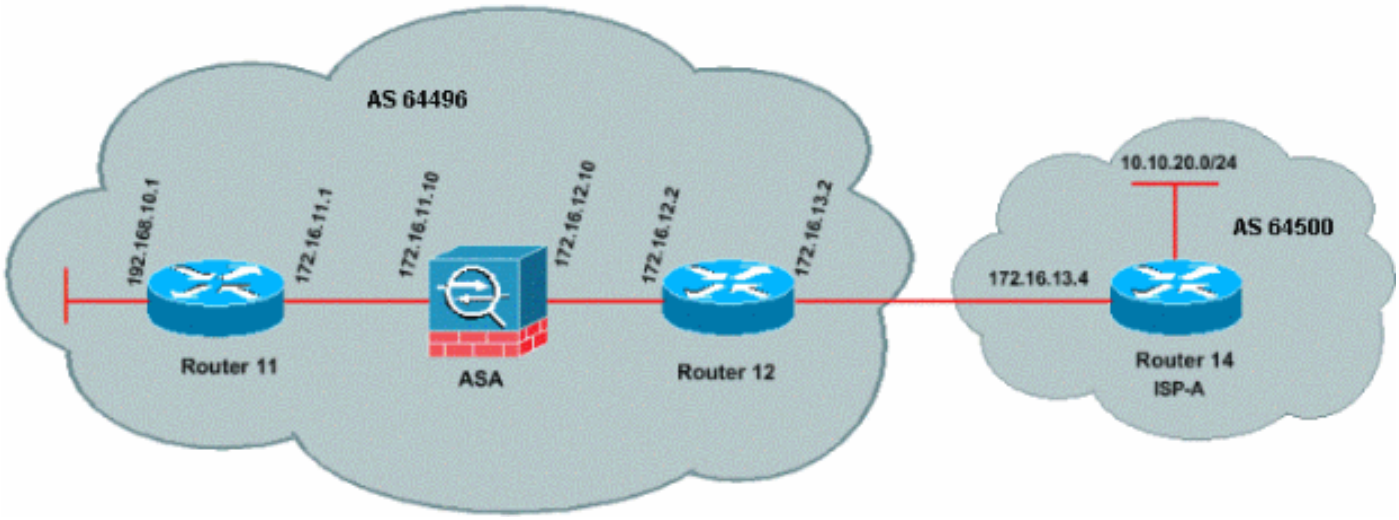
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside.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

Esta sección utiliza esta configuración de la red.



La versión 7.x y posterior del PIX/ASA introduce un desafío adicional cuando usted intenta establecer a una sesión de peer BGP con autenticación de MD5. Por abandono, la versión 7.x y posterior del PIX/ASA reescribe cualquier opción TCP MD5 incluida en un datagrama TCP que pase a través del dispositivo y substituya la clase de la opción, el tamaño y el valor por los bytes de opción NOP. Esto rompe con eficacia el BGP autenticación de MD5, y los resultados en los mensajes de error como esto en cada router para redes entre peers:

```
000296: 7 de abril de 2010 15:13:22.221 EDT: %TCP-6-BADAUTH: Ninguna publicación MD5 a partir de
172.16.11.1(28894) a 172.16.12.2(179)
```

Para que una sesión de BGP con autenticación de MD5 que se establecerá con éxito, estos tres problemas deben ser resueltos:

- Distribución aleatoria del número de secuencia de la neutralización TCP
- Reescritura de la opción de la neutralización TCP MD5
- Neutralización NAT entre los pares

Un clase-mapa y una lista de acceso se utilizan para seleccionar el tráfico entre los pares que deben ambos ser eximidos de la característica de la distribución aleatoria del número de secuencia TCP y ser permitidos llevar una opción MD5 sin la reescritura. Un tcp-mapa se utiliza para especificar el tipo de la opción que se permitirá, en este caso, la clase 19 (opción de la opción TCP MD5). El clase-mapa y el TCP-mapa ambos se conectan juntos a través de un directiva-mapa, parte de la infraestructura modular del Marco de políticas. La configuración entonces se activa con el **comando service-policy**.

Note: La necesidad de inhabilitar el NAT entre los pares es manejada por el **comando no nat-control**.

En la versión 7.0 y posterior, que la naturaleza predeterminada de un ASA no es **ningún NAT control**, que estado que cada conexión con el ASA, por abandono, no necesite pasar la prueba NAT. Se asume que el ASA tiene una configuración predeterminada de **ningún NAT control**.

Refiera al NAT control para más información. Si se aplica el **NAT control**, usted debe inhabilitar explícitamente el NAT para los peeres BGP. Esto se puede hacer con el **comando static** entre las interfaces interior y exterior.

```
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
```

Verificación

La salida del **comando show ip bgp summary** indica que la autenticación es acertada y que establecen a la sesión de BGP en el 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
```

Información Relacionada

- Página de Soporte de BGP
- Algoritmo de selección del mejor trayecto BGP
- Distribución de la Carga con BGP en Entornos con una Sola Conexión y con Varias Conexiones: Configuraciones de Ejemplo
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Firewall PIX que configura y de prueba
- Soporte Técnico y Documentación - Cisco Systems