ASA/PIX: Ejemplo de Configuración de BGP a ASA

Contenido

Introducción

Esta configuración de ejemplo muestra cómo ejecutar el protocolo de gateway fronterizo (BGP) a través de un dispositivo de seguridad (PIX/ASA) y cómo lograr la redundancia en un entorno BGP y PIX con varias conexiones. Con un diagrama de red como ejemplo, este documento explica cómo rutear automáticamente el tráfico al proveedor de servicios de Internet B (ISP-B) cuando el AS 64496 pierde la conectividad con el ISP-A (o al revés), a través del uso de protocolos de ruteo dinámico que se ejecutan entre todos los routers en el AS 64496.

Debido a que BGP utiliza paquetes TCP de unidifusión en el puerto 179 para comunicarse con sus pares, puede configurar PIX1 y PIX2 para permitir el tráfico de unidifusión en el puerto TCP 179. De esta manera, se puede establecer el peering BGP entre los routers que están conectados a través del firewall. La redundancia y las políticas de ruteo deseadas se pueden lograr mediante la manipulación de los atributos BGP.

Prerequisites

Requirements

Los lectores de este documento deben estar familiarizados con Configuración de BGP y Configuración Básica del Firewall.

Componentes Utilizados

Los escenarios de ejemplo de este documento se basan en estas versiones de software:

- ¿Routers Cisco 2600 con Cisco IOS? Versión de software 12.2(27)
- PIX 515 con Cisco PIX Firewall versión 6.3(3) y posterior

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

Productos Relacionados

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

- Cisco Adaptive Security Appliance (ASA) serie 5500 con versión 7.x y posterior
- Cisco Firewall Services Module (FWSM) que ejecuta la versión de software 3.2 y posteriores

Convenciones

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

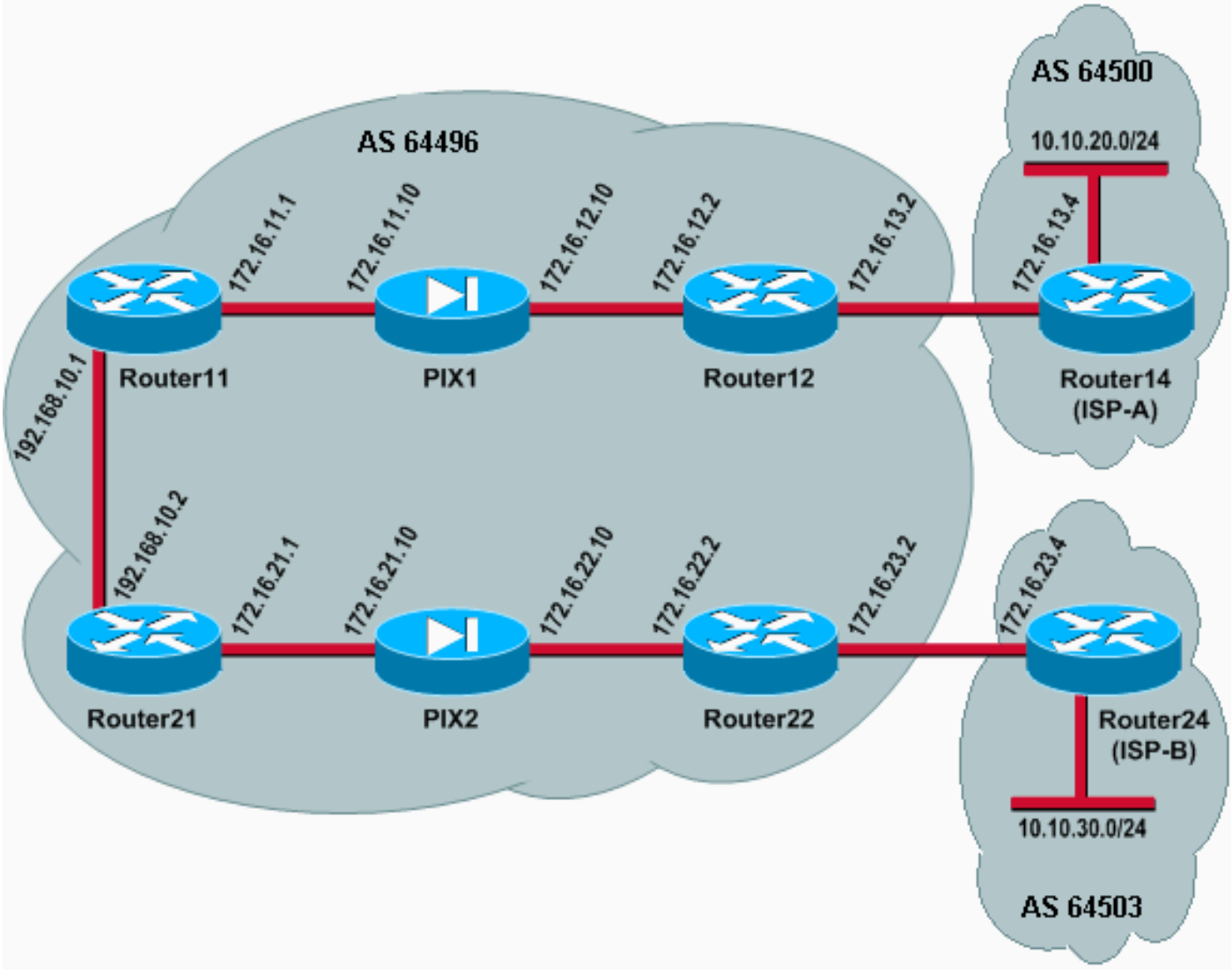
Configurar

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

Nota: Para encontrar información adicional sobre los comandos en este documento, utilice la Command Lookup Tool (sólo clientes registrados) .

Diagrama de la red

En este documento, se utiliza esta configuración de red:



En esta configuración de red, el router12 y el router22 (que pertenecen a AS 64496) se conectan al router14 (ISP-A) y al router24 (ISP-B) respectivamente para obtener redundancia. La red interna 192.168.10.0/24 se encuentra en el interior del firewall. El Router11 y el Router21 se conectan al Router12 y al Router22 a través del firewall. PIX1 y PIX2 no están configurados para realizar la traducción de direcciones de red (NAT).

Escenario 1

En este escenario, el router 12 en AS 64496 hace peering BGP externo (eBGP) con el router 14 (ISP-A) en AS 64500. El router 12 también hace peering BGP interno (iBGP) con el router 11 a través de PIX1. Si las rutas aprendidas eBGP del ISP-A están presentes, el Router12 anuncia una ruta predeterminada 0.0.0.0/0 en iBGP al Router11. Si el link a ISP-A falla, el Router12 deja de anunciar la ruta predeterminada.

De manera similar, el Router22 en AS 64496 hace peering eBGP con el Router24 (ISP-B) en AS 64503 y anuncia una ruta predeterminada en iBGP al Router21 condicionalmente basada en la presencia de rutas ISP-B en su tabla de ruteo.

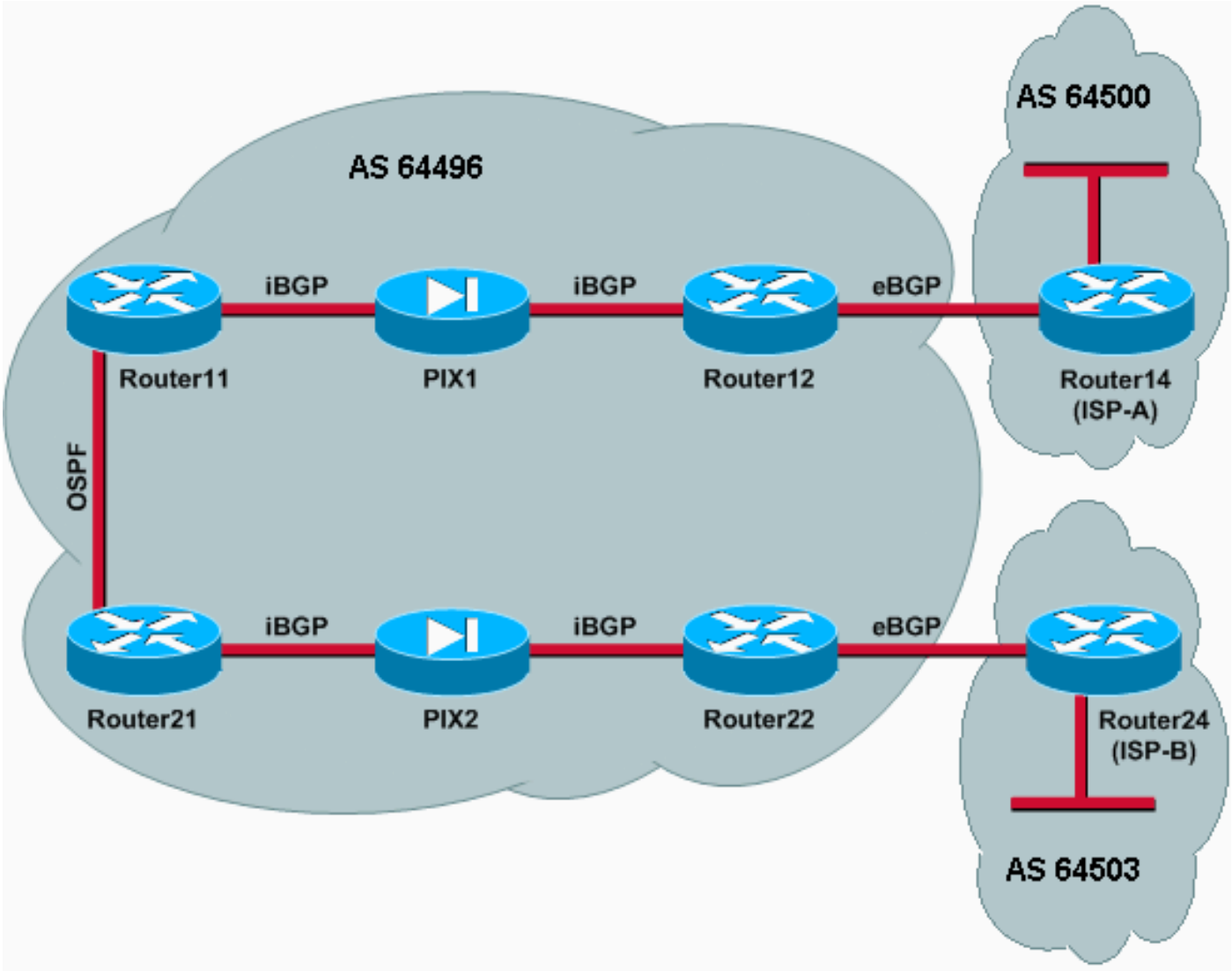
Mediante el uso de una lista de acceso, PIX1 y PIX2 se configuran para permitir el tráfico BGP (TCP, puerto 179) entre peers iBGP. Esto se debe a que las interfaces PIX tienen un nivel de seguridad asociado. De forma predeterminada, la interfaz interna (ethernet1) tiene un nivel de seguridad 100 y la interfaz externa (ethernet0) tiene un nivel de seguridad 0. Normalmente, las conexiones y el tráfico se permiten desde interfaces de nivel de seguridad superior a inferior. Para

permitir el tráfico de una interfaz de nivel de seguridad inferior a una interfaz de nivel de seguridad superior, sin embargo, debe definir explícitamente una lista de acceso en el PIX. Además, debe configurar una traducción NAT estática en PIX1 y PIX2, para permitir que los routers en el exterior inicien una sesión BGP con los routers en el interior del PIX.

Tanto el router 11 como el router 21 anuncian condicionalmente la ruta predeterminada en el dominio OSPF (Open Shortest Path First) basado en la ruta predeterminada aprendida por iBGP. El Router11 anuncia la ruta predeterminada al dominio OSPF con una métrica de 5, el Router21 anuncia la ruta predeterminada con una métrica de 30 y, por lo tanto, se prefiere la ruta predeterminada del Router11. Esta configuración ayuda a propagar solamente la ruta predeterminada 0.0.0.0/0 al Router11 y al Router21, que conserva el consumo de memoria en los routers internos y logra un rendimiento óptimo.

Por lo tanto, para resumir estas condiciones, esta es la política de ruteo para AS 64496:

- AS 64496 prefiere el link del Router12 al ISP-A para todo el tráfico saliente (desde 192.168.10.0/24 a Internet).
- Si falla la conectividad con ISP-A, todo el tráfico se rutea a través del link del Router22 al ISP-B.
- Todo el tráfico que viene de Internet a 192.168.10.0/24 utiliza el enlace de ISP-A al router12.
- Si el link de ISP-A al Router12 falla, todo el tráfico entrante se rutea a través del link de 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 BGP están activas, puede esperar que todos los paquetes sean enrutados a través de ISP-A. Considere la tabla BGP en el Router11. Aprende una ruta predeterminada 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
```

La ruta predeterminada 0.0.0.0/0 que se aprende a través de BGP se instala en la tabla de ruteo, como se muestra en el resultado de **show ip route** 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 predeterminada a través del 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 predeterminada aprendida por BGP se instala en la tabla de ruteo del 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 predeterminada en el Router21 se aprende a través de OSPF (observe el prefijo o en la ruta 0.0.0.0/0). Es interesante observar que hay una ruta predeterminada aprendida a través de BGP desde el Router22, pero el resultado **show ip route** muestra la ruta predeterminada aprendida a través de OSPF.

La ruta predeterminada OSPF se instaló en el Router21 porque el Router21 aprende la ruta predeterminada de dos orígenes: Router22 a través de iBGP y Router11 a través de OSPF. El proceso de selección de ruta instala la ruta con una mejor distancia administrativa en la tabla de ruteo. La distancia administrativa de OSPF es 110 mientras que la distancia administrativa de iBGP es 200. Por lo tanto, la ruta predeterminada aprendida por OSPF se instala en la tabla de ruteo, porque 110 es menor que 200. Para obtener más información sobre la selección de rutas, consulte Selección de rutas en routers Cisco.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Apague la sesión 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 predeterminada aprendida a través de BGP desde el 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
```

Verifique la tabla de ruteo en el Router11. La ruta predeterminada se detecta a través de 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
```

Se espera este resultado según las políticas predefinidas. En este punto, sin embargo, es importante comprender el comando de configuración **distance bgp 20 105 200** en el Router11 y cómo influye en la selección de ruta en el Router11.

Los valores predeterminados de este comando son **distance bgp 20 200 200**, donde las rutas aprendidas por eBGP tienen una distancia administrativa de 20, las rutas aprendidas por iBGP tienen una distancia administrativa de 200 y las rutas BGP locales tienen una distancia administrativa de 200.

Cuando vuelve a aparecer el link entre el Router12 y el ISP-A, el Router11 aprende la ruta predeterminada a través de iBGP desde el Router12. Sin embargo, debido a que la distancia administrativa predeterminada de esta ruta aprendida por iBGP es 200, no reemplazará la ruta aprendida por OSPF (porque 110 es menor que 200). Esto fuerza todo el tráfico saliente al link del Router21 al Router22 al ISP-B, aunque el link del Router12 al ISP-A vuelva a funcionar. Para solucionar este problema, cambie la distancia administrativa de la ruta aprendida por iBGP a un valor inferior al protocolo de gateway interior (IGP) utilizado. En este ejemplo, el IGP es OSPF, por lo que se eligió una distancia de 105 (porque 105 es menor que 110).

Para obtener más información sobre el comando **distance bgp, consulte** Comandos BGP. Para obtener más información sobre la conexión múltiple con BGP, consulte Carga Compartida con BGP en Entornos de Conexión Única y Multidireccional: Configuraciones de Ejemplo.

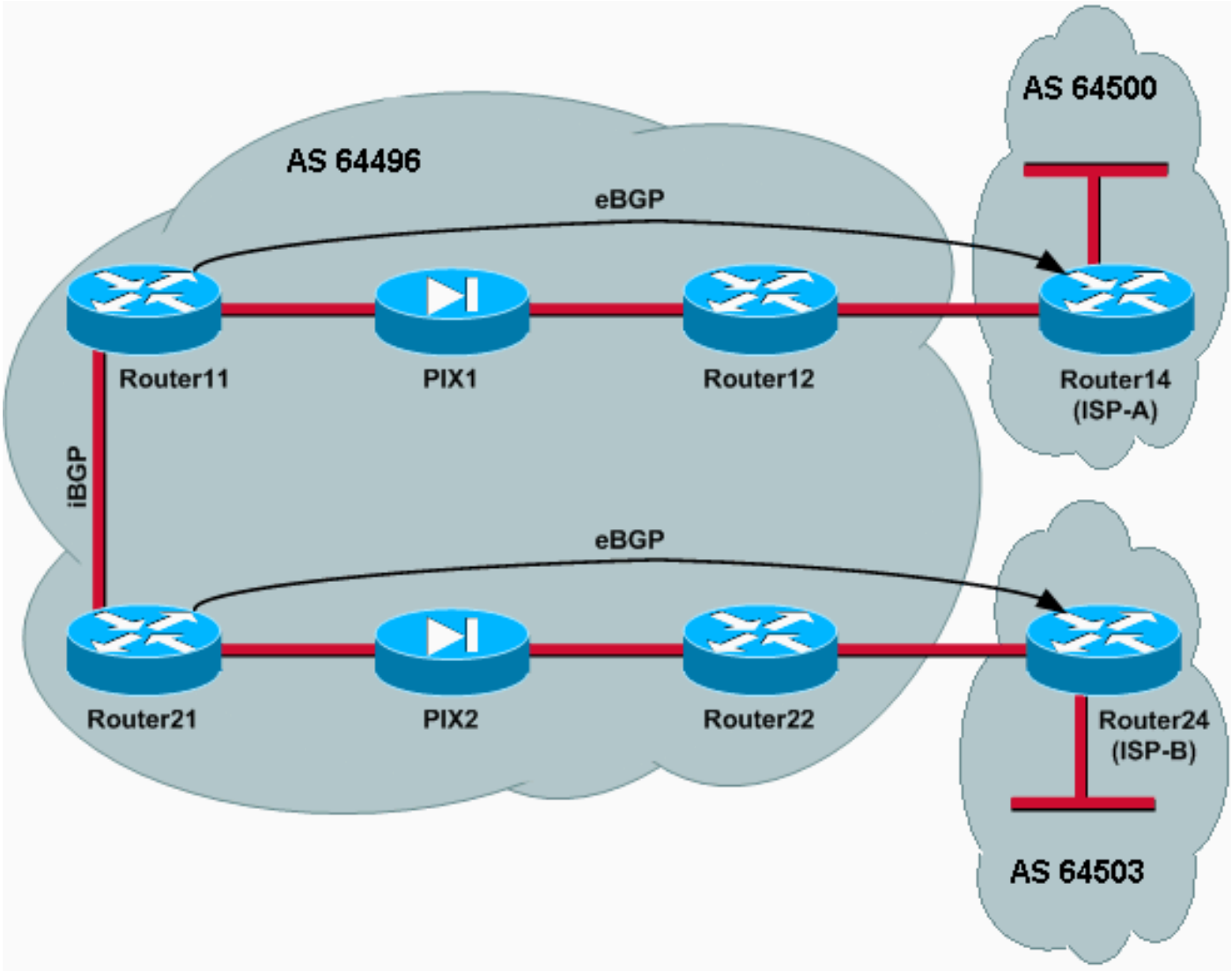
Escenario 2

En este escenario, el Router11 es un peering eBGP con el Router 14 (ISP-A) y el Router21 es un peering eBGP directamente con el Router24 (ISP-B). El Router12 y el Router22 no participan en el peering BGP, pero sí proporcionan la conectividad IP a los ISP. Debido a que los peers eBGP no son vecinos directamente conectados, el comando **neighbor ebgp-multihop** se utiliza en los routers participantes. El comando **neighbor ebgp-multihop** permite que BGP reemplace el límite predeterminado de eBGP de un salto porque cambia el Tiempo de Vida (TTL) de los paquetes eBGP del valor predeterminado de 1. En este escenario, el vecino eBGP está a 3 saltos, por lo que el **vecino ebgp-multihop 3** se configura en los routers participantes para que el valor TTL se

cambie a 3. Además, las rutas estáticas se configuran en los routers y en el PIX para asegurarse de que el Router11 pueda hacer ping a la dirección del Router14 (ISP-A) 172.16.13.4 y para asegurarse de que el Router21 pueda hacer ping a la dirección 172.16.23.4 del Router24.

De forma predeterminada, el PIX no permite que pasen los paquetes de protocolo de mensajes de control de Internet (ICMP) (enviados cuando se ejecuta el comando **ping**). Para permitir los paquetes ICMP, utilice el comando **access-list** como se muestra en la siguiente configuración PIX. Para obtener más información sobre el comando **access-list**, refiérase a los Comandos PIX Firewall A a B.

La política de ruteo es la misma que en la situación 1: se prefiere el link entre el Router12 y el ISP-A sobre el link entre el Router22 y el ISP-B, y cuando el link ISP-A cae el link 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

```
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
```

Verificación

Comience con la situación en la que los links a ISP-A y ISP-B están activos. El resultado del comando **show ip bgp summary** en el Router11 y el Router21 confirma las sesiones BGP establecidas con ISP-A e 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 predeterminada (0.0.0.0/0) hacia el ISP-A 172.16.13.4 de siguiente salto.

```
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 verifique la tabla BGP en el Router21. Tiene dos rutas 0.0.0.0/0: uno aprendió de ISP-B con un salto siguiente de 172.16.23.4 en eBGP, y el otro aprendió a través de iBGP con una preferencia local de 200. El Router21 prefiere las rutas aprendidas por iBGP debido al atributo de preferencia local más alto, por lo que instala esa ruta en la tabla de ruteo. Para obtener más información sobre la selección de la trayectoria BGP, consulte Algoritmo de Selección de la Mejor Trayectoria de 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
```

Troubleshoot

Apague la sesión BGP Router11 e 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 a ISP-A se desactiva cuando caduca el temporizador de retención (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 hacia abajo a ISP-A, el Router11 instala 0.0.0.0/0 con un salto siguiente de

192.168.10.2 (Router21), que se aprende a través de iBGP en su tabla de ruteo. Esto empuja todo el tráfico saliente a través del Router21 y luego al ISP-B, como se muestra en este resultado:

```
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 MD5 para Vecinos BGP a través de PIX/ASA

Configuración de PIX 6.x

Al igual que cualquier otro protocolo de ruteo, el BGP se puede configurar para la autenticación. Puede configurar la autenticación MD5 entre dos peers BGP, lo que significa que se verifica cada segmento enviado en la conexión TCP entre los peers. La autenticación MD5 debe configurarse con la misma contraseña en ambos peers BGP; de lo contrario, la conexión entre ellos no se realizará. La configuración de la autenticación MD5 hace que el software Cisco IOS genere y verifique el resumen MD5 de cada segmento enviado en la conexión TCP. Si se invoca la autenticación y un segmento falla la autenticación, se genera un mensaje de error.

Cuando configura peers BGP con autenticación MD5 que pasan a través de un firewall PIX, es importante configurar el PIX entre los vecinos BGP para que los números de secuencia para los flujos TCP entre los vecinos BGP no sean aleatorios. Esto se debe a que la función de número de secuencia aleatoria TCP en el firewall PIX está habilitada de forma predeterminada y cambia el número de secuencia TCP de los paquetes entrantes antes de que los reenvíe.

La autenticación MD5 se aplica en el encabezado TCP psuedo-IP, el encabezado TCP y los datos (consulte RFC 2385). TCP utiliza estos datos, que incluyen la secuencia TCP y los números ACK, junto con la contraseña de vecino BGP para crear un número hash de 128 bits. El número hash se incluye en el paquete en un campo de opción de encabezado TCP. De forma predeterminada, el PIX desactiva el número de secuencia por un número aleatorio, por flujo TCP. En el peer BGP de envío, TCP utiliza el número de secuencia original para crear el número hash MD5 de 128 bits e incluye este número hash en el paquete. Cuando el par BGP receptor obtiene el paquete, TCP utiliza el número de secuencia modificado por PIX para crear un número hash MD5 de 128 bits y lo compara con el número hash que se incluye en el paquete.

El número hash es diferente porque el PIX cambió el valor de la secuencia TCP y TCP en el vecino BGP descarta el paquete y registra un mensaje de error MD5 similar a éste:

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

Utilice la palabra clave **norandomseq** con el comando **static (inside, outside) 172.16.11.1 172.16.11.1 netmask 255.255.0 norandomseq** para resolver este problema y para detener el PIX de la desconfiguración del número de secuencia TCP. Este ejemplo ilustra el uso de la palabra clave **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

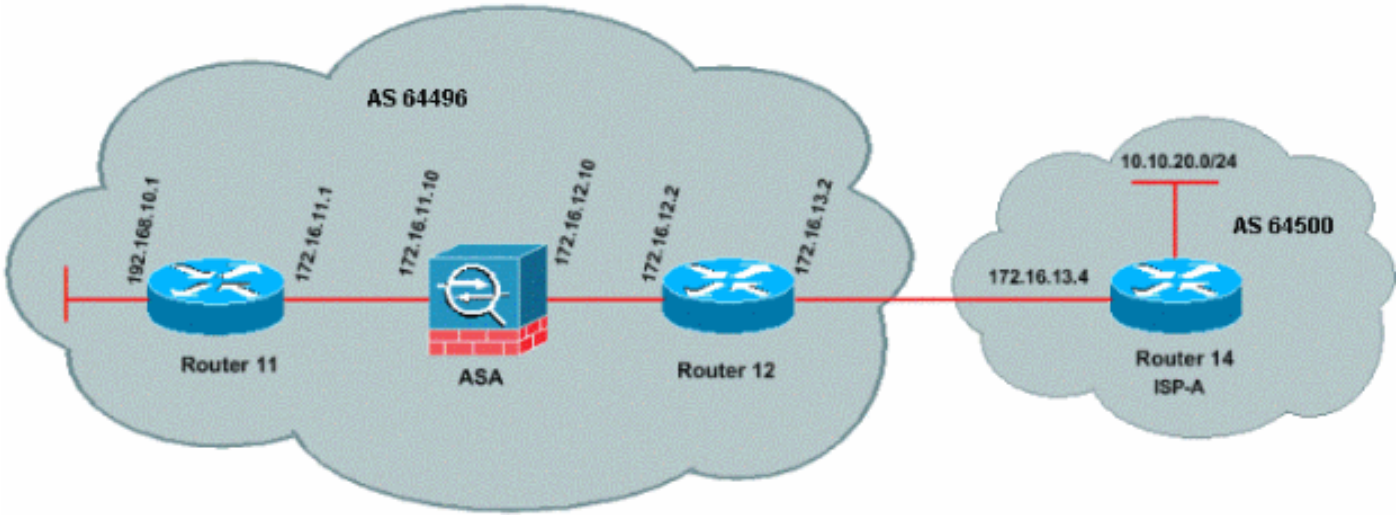
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside.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

Esta sección utiliza esta configuración de red.



PIX/ASA versión 7.x y posteriores presentan un desafío adicional cuando intenta establecer una sesión de peering BGP con autenticación MD5. De forma predeterminada, la versión 7.x y posterior de PIX/ASA reescribe cualquier opción MD5 de TCP incluida en un datagrama TCP que pasa por el dispositivo y reemplaza el tipo de opción, el tamaño y el valor por los bytes de opción NOP. Esto interrumpe de manera efectiva la autenticación MD5 de BGP y da lugar a mensajes de error como este en cada router de peering:

```
000296: 7 de abril de 2010 15:13:22.221 EDT: %TCP-6-BADAUTH: No MD5 digest de 172.16.11.1(28894)
a 172.16.12.2(179)
```

Para que una sesión BGP con autenticación MD5 se establezca correctamente, estos tres problemas deben resolverse:

- Deshabilitar la aleatorización del número de secuencia TCP
- Deshabilitar reescritura de la opción MD5 de TCP
- Deshabilitar NAT entre peers

Un mapa de clase y una lista de acceso se utilizan para seleccionar el tráfico entre los pares que deben estar exentos de la función de aleatorización de número de secuencia TCP y se les permite llevar una opción MD5 sin reescribir. Se utiliza un tcp-map para especificar el tipo de opción que se permitirá, en este caso, la opción type 19 (opción TCP MD5). Tanto el mapa de clase como el mapa de TCP están enlazados a través de un mapa de políticas, que forma parte de la infraestructura de estructura de políticas modular. La configuración se activa luego con el comando **service-policy**.

Nota: La necesidad de inhabilitar la NAT entre los peers es manejada por el comando **no nat-control**.

En la versión 7.0 y posteriores, la naturaleza predeterminada de un ASA **no** es **nat-control**, que indica que cada conexión a través de ASA, de forma predeterminada, no necesita pasar la prueba NAT. Se supone que ASA tiene un valor predeterminado de **no nat-control**. Consulte nat-control para obtener más información. Si se aplica **nat-control**, debe inhabilitar explícitamente la NAT para los peers BGP. Esto se puede hacer con el comando **static** entre interfaces internas y externas.

```
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
```

Verificación

El resultado del comando **show ip bgp summary** indica que la autenticación es exitosa y que la sesión BGP se establece en el Router11.

```
Router11#show ip bgp summary
BGP router identifier 192.168.10.1, local AS number 64496
BGP table version is 8, main routing table version 8
3 network entries using 360 bytes of memory
3 path entries using 156 bytes of memory
2/2 BGP path/bestpath attribute entries using 248 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 764 total bytes of memory
BGP activity 25/22 prefixes, 26/23 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.13.2     4        64496     137     138        8    0    0 02:01:16        1
Router11#
```

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
- Configuración y Prueba de PIX Firewall
- Soporte Técnico y Documentación - Cisco Systems