ASA/PIX:ASA를 통한 BGP 컨피그레이션 예

목차

소개

이 샘플 컨피그레이션에서는 PIX/ASA(Security Appliance)에서 BGP(Border Gateway Protocol)를 실행하는 방법과 멀티홈 BGP 및 PIX 환경에서 이중화를 달성하는 방법을 보여 줍니다.이 문서에서는 AS 64496의 모든 라우터 간에 실행되는 동적 라우팅 프로토콜을 사용하여 AS 64496의 ISP-A 연결이 끊길 때(또는 그 반대) ISP-B(인터넷 서비스 공급자 B)로 트래픽을 자동으로 라우팅하는 방법에 대해 설명합니다.

BGP는 포트 179에서 유니캐스트 TCP 패킷을 사용하여 피어와 통신하므로 TCP 포트 179에서 유니캐스트 트래픽을 허용하도록 PIX1 및 PIX2를 구성할 수 있습니다. 이렇게 하면 방화벽을 통해 연결된 라우터 간에 BGP 피어링을 설정할 수 있습니다.BGP 특성을 조작하여 이중화 및 원하는 라우팅 정책을 구현할 수 있습니다.

사전 요구 사항

요구 사항

이 문서의 독자는 BGP 및 기본 방화벽 컨피그레이션 구성에 익숙해야 합니다.

사용되는 구성 요소

이 문서의 예제 시나리오는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco 2600 라우터와 Cisco IOS?소프트웨어 릴리스 12.2(27)
- PIX 515 with Cisco PIX Firewall Version 6.3(3) 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 컨피그레이션은 다음 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- 7.x 버전 이상의 Cisco ASA(Adaptive Security Appliance) 5500 Series
- 소프트웨어 버전 3.2 이상을 실행하는 Cisco FWSM(Firewall Services Module)

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

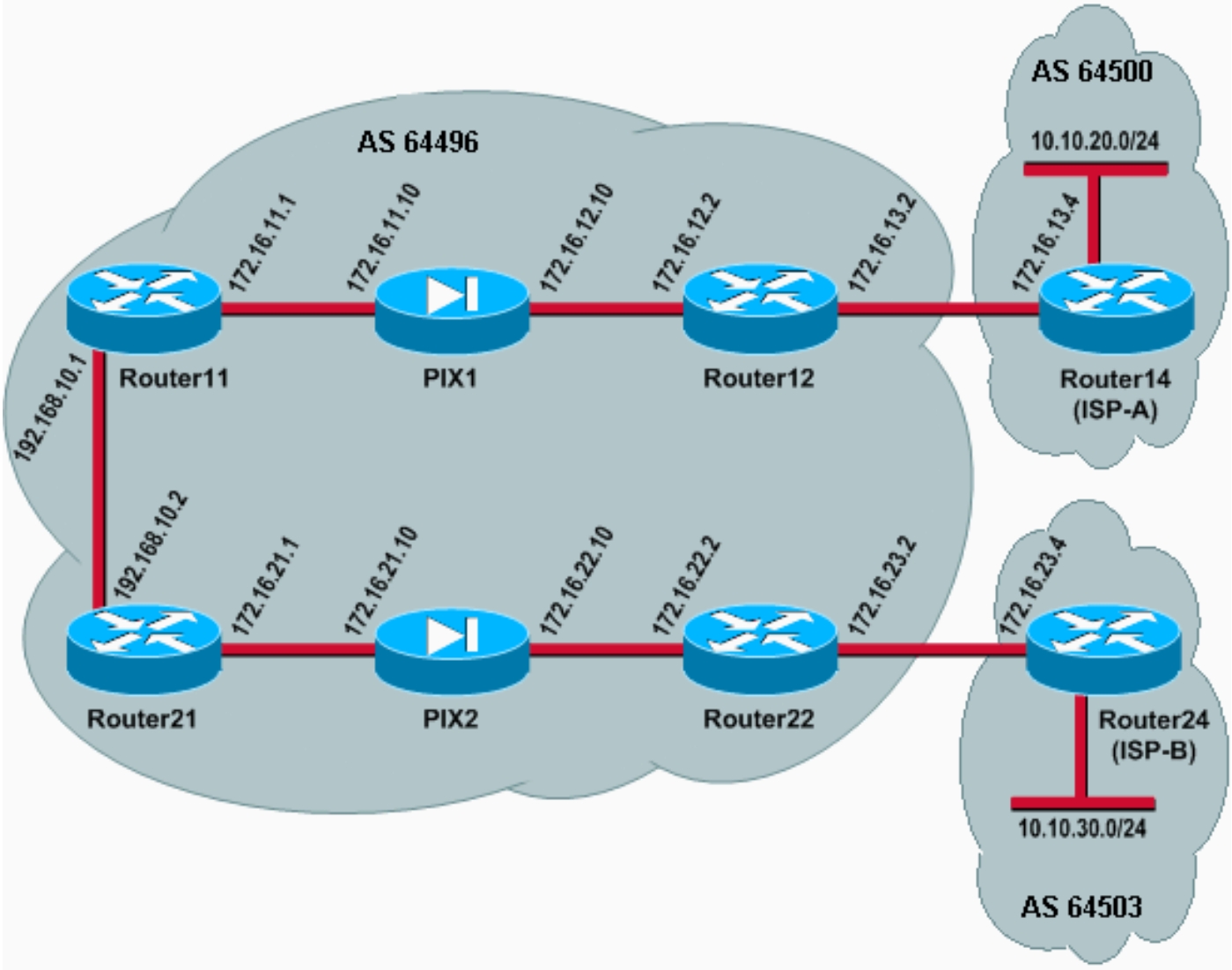
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 방법을 설명합니다.

참고: 이 문서의 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 네트워크 설정에서는 이중화를 위해 Router12 및 Router22(AS 6496에 속함)가 각각 Router14(ISP-A) 및 Router24(ISP-B)에 멀티홈(multihomed)됩니다.내부 네트워크 192.168.10.0/24은 방화벽 내부에 있습니다.Router11 및 Router21은 방화벽을 통해 Router12 및 Router22에 연결됩니다.PIX1 및 PIX2는 NAT(Network Address Translation)를 수행하도록 구성되지 않았습니다.

시나리오 1

이 시나리오에서 AS 64496의 Router12는 AS 64500에서 ISP-A(Router14)를 사용하여 eBGP(외부 BGP) 피어링을 수행합니다. Router12는 Router11에서 PIX1을 통해 내부 BGP(iBGP) 피어링을 수행합니다. eBGP가 ISP-A 라우터에서 학습한 경우 Router1Present1이 표시됩니다. 2는 Router11에 대한 iBGP에서 기본 경로 0.0.0.0/0을 알립니다. ISP-A에 대한 링크가 실패하면 Router12가 기본 경로 공지를 중지합니다.

마찬가지로 AS 64496의 Router22는 AS 64503에서 ISP-B(Router24)를 사용하여 eBGP 피어링을 수행하고 라우팅 테이블에 ISP-B 경로가 있는 것을 조건부로 Router21에 대한 기본 경로를 알립니다.

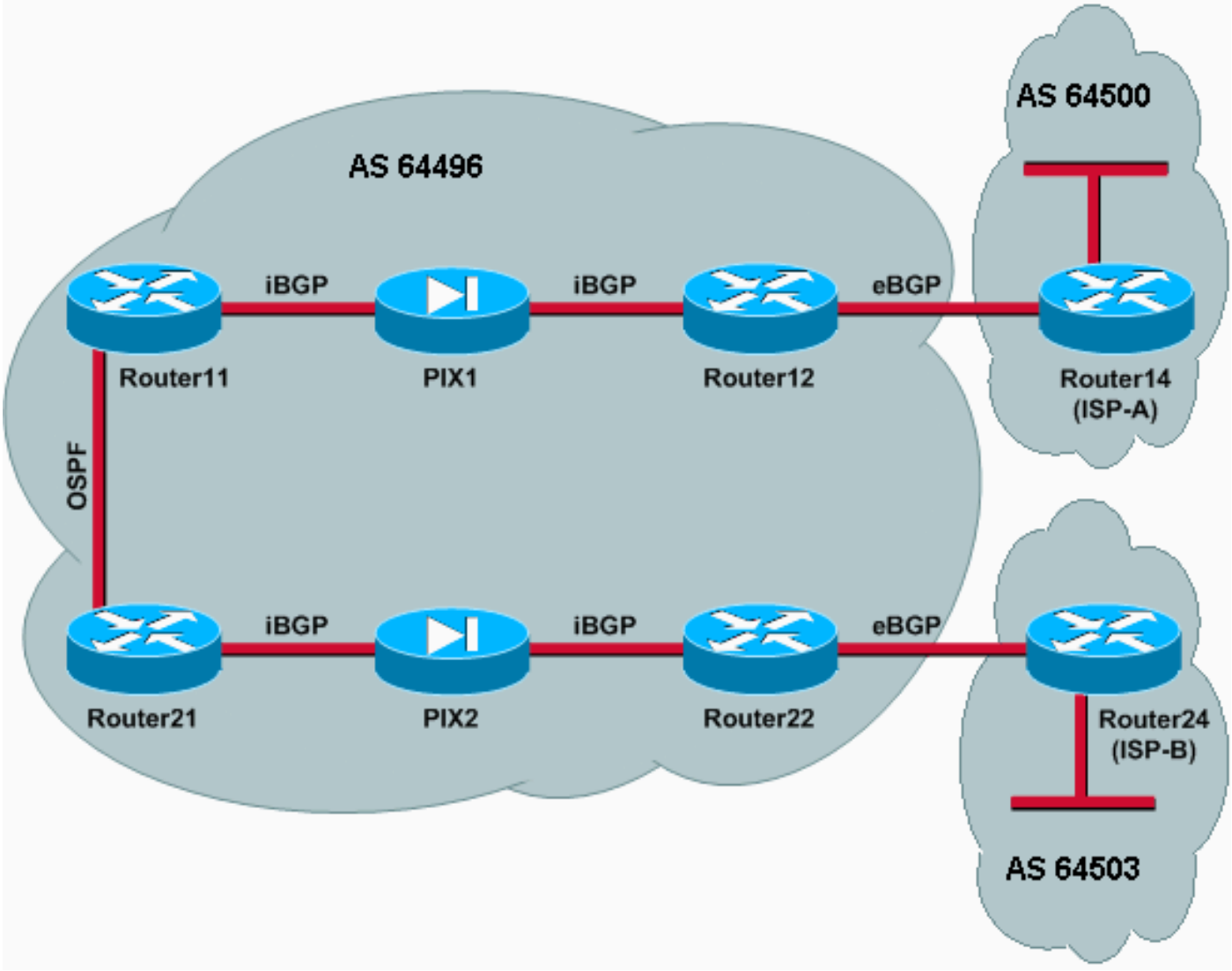
액세스 목록을 사용하여 iBGP 피어 간에 BGP 트래픽(TCP, 포트 179)을 허용하도록 PIX1 및 PIX2가 구성됩니다.이는 PIX 인터페이스에 연결된 보안 수준이 있기 때문입니다.기본적으로 내부 인터페이스(ethernet1)에는 보안 수준이 100이고 외부 인터페이스(ethernet0)에는 보안 수준이 0입니다. 일반적으로 연결 및 트래픽은 상위 인터페이스에서 하위 보안 수준 인터페이스로 허용됩니다.그러나 낮은 보안 수준 인터페이스에서 상위 보안 수준 인터페이스로 가는 트래픽을 허용하려면

PIX에서 액세스 목록을 명시적으로 정의해야 합니다.또한 외부의 라우터가 PIX 내부의 라우터를 사용하여 BGP 세션을 시작할 수 있도록 PIX1 및 PIX2에서 고정 NAT 변환을 구성해야 합니다.

Router11과 Router21은 모두 iBGP 학습 기본 경로를 기반으로 OSPF(Open Shortest Path First) 도메인에 대한 기본 경로를 조건부로 알립니다.Router11은 메트릭이 5인 OSPF 도메인으로 기본 경로를 발표하며, Router21은 메트릭이 30인 기본 경로를 발표하므로 Router11의 기본 경로가 우선합니다.이 컨피그레이션은 기본 경로 0.0.0.0/0만 Router11 및 Router21로 전파하는 데 도움이 됩니다. 이 라우터는 내부 라우터에서 메모리 소비를 유지하며 최적의 성능을 실현합니다.

따라서 이러한 조건을 요약하면, 이는 AS 64496에 대한 라우팅 정책입니다.

- AS 64496은 모든 아웃바운드 트래픽(192.168.10.0/24에서 인터넷으로)에 대해 Router12에서 ISP-A로의 링크를 선호합니다.
- ISP-A 연결이 실패하면 모든 트래픽이 Router22에서 ISP-B로의 링크를 통해 라우팅됩니다.
- 인터넷에서 192.168.10.0/24으로 들어오는 모든 트래픽은 ISP-A에서 Router12로의 링크를 사용합니다.
- ISP-A에서 Router12로의 링크가 실패하면 모든 인바운드 트래픽이 ISP-B에서 Router22로의 링크를 통해 라우팅됩니다.



구성

이 시나리오에서는 다음 컨피그레이션을 사용합니다.

- 라우터11
- 라우터12
- Router14(ISP-A)
- 라우터21
- 라우터22
- PIX1
- PIX2

라우터11

```
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
```

라우터12

```
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. !
```

라우터21

```
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 !
```

라우터22

```
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.
```

라우터24(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.
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

두 BGP 세션이 모두 작동 중일 때 모든 패킷이 ISP-A를 통해 라우팅될 것으로 예상할 수 있습니다 .Router11의 BGP 테이블을 고려합니다. 다음 홉이 172.16.12.2인 Router12에서 기본 경로 0.0.0.0/0을 학습합니다.

```
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
```

BGP를 통해 학습되는 0.0.0.0/0 기본 경로는 Router11의 **show ip route** 출력에 나와 있는 것처럼 라우팅 테이블에 설치됩니다.

```
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
```

이제 Router21에서 BGP 테이블을 고려합니다. 또한 Router22를 통해 기본 경로를 학습합니다.

```
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
```

이제 이 BGP 학습 기본 경로가 Router21의 라우팅 테이블에 설치되었는지 확인합니다.

```
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
```

Router21의 기본 경로는 OSPF를 통해 학습됩니다(0.0.0.0/0 경로의 o 접두사 참고). Router22에서 BGP를 통해 학습된 기본 경로가 있지만 **show ip route** 출력에는 OSPF를 통해 학습된 기본 경로가 표시됩니다.

Router21이 두 소스에서 기본 경로를 인식하므로 OSPF 기본 경로가 Router21에 설치되었습니다 .OSPF를 통한 iBGP 및 Router11을 통한 라우터22.경로 선택 프로세스는 라우팅 테이블에 더 나은 관리 거리를 가진 경로를 설치합니다.OSPF의 관리 영역은 110이고 iBGP의 관리 거리는 200입니다. 따라서 110이 200보다 작으므로 OSPF에서 학습한 기본 경로가 라우팅 테이블에 설치됩니다. 경로 선택에 대한 자세한 내용은 Cisco 라우터의 경로 선택을 참조하십시오.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

Router12와 ISP-A 간의 BGP 세션을 종료합니다.

```
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
```

Router11에는 Router12에서 BGP를 통해 학습된 기본 경로가 없습니다.

```
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
```

Router11의 라우팅 테이블을 확인합니다. 기본 경로는 OSPF(관리 거리 110)를 통해 학습되며 Router21의 다음 홉이 사용됩니다.

```
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
```

이 출력은 미리 정의된 정책에 따라 필요합니다.그러나 이 시점에서는 Router11에서 **distance bgp 20 105 200** 컨피그레이션 명령을 이해하고, Router11에서 경로 선택에 미치는 영향을 이해하는 것이 중요합니다.

이 명령의 기본값은 **distance bgp 200 200 20**입니다. 여기서 eBGP 학습 경로는 관리 거리가 20이고, iBGP 학습 경로는 관리 거리가 200이고, 로컬 BGP 경로는 관리 거리가 200입니다.

Router12와 ISP-A 간의 링크가 다시 시작되면 Router11은 Router12에서 iBGP를 통해 기본 경로를 학습합니다. 그러나 이 iBGP 학습 경로의 기본 관리 거리는 200이므로 OSPF 학습 경로를 대체하지 않습니다(110이 200보다 작기 때문). 이렇게 하면 Router12에서 ISP-A로의 링크가 다시 작동하더라도 Router21에서 Router22로 연결되는 모든 아웃바운드 트래픽이 ISP-B로 연결됩니다.이 문제를 해결하려면 iBGP 학습 경로의 관리 거리를 사용된 IGP(Interior Gateway Protocol)보다 작은 값으로 변경합니다.이 예에서 IGP는 OSPF이므로 105는 110보다 작으므로 105의 거리가 선택됩니다.

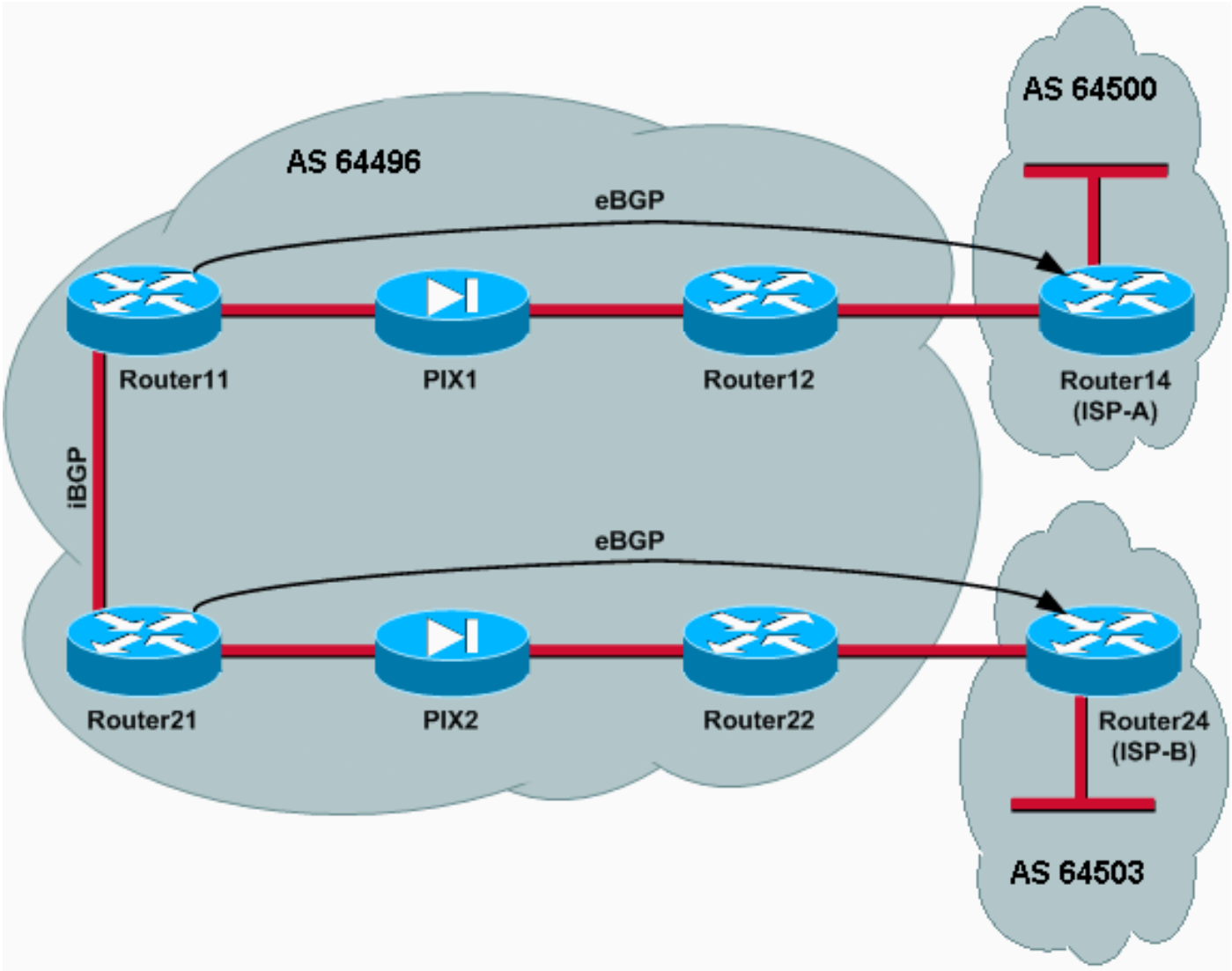
distance bgp 명령에 대한 자세한 내용은 **BGP 명령**을 참조하십시오.BGP를 사용한 멀티홈(multihoming)에 대한 자세한 내용은 단일 및 멀티홈 환경에서 BGP를 통한 로드 공유:샘플 구성.

시나리오 2

이 시나리오에서 Router11은 ISP-A(Router 14)를 통한 직접 eBGP 피어링이고 Router21은 ISP-B(Router24)를 통한 직접 eBGP 피어링입니다. Router12 및 Router22는 BGP 피어링에 참여하지 않지만 ISP에 IP 연결을 제공합니다.eBGP 피어는 직접 연결된 인접 디바이스가 아니므로 neighbor ebgp-**multihop** 명령은 참여 라우터에서 사용됩니다.neighbor ebgp-**multihop** 명령을 사용하면 eBGP 패킷의 TTL(Time to Live)을 기본값 1에서 변경하므로 BGP가 기본 one hop eBGP 제한을 재정의할 수 있습니다. 이 시나리오에서는 eBGP 네이버가 3홉이므로 **네이버-멀티호프 3이 참여자**에 구성되어 TTL 값을 3으로 변경합니다. 또한 고정 라우터와 PIX로 구성된 라우터에 고정 경로를 구성합니다. Router11은 Router14(ISP-A) 주소 172.16.13.4을 ping할 수 있으며 Router21이 ISP-B(Router24) 주소 172.16.23.4에 ping할 수 있도록 할 수 있습니다.

기본적으로 PIX는 **ping** 명령을 실행할 때 전송되는 ICMP(Internet Control Message Protocol) 패킷을 통과하도록 허용하지 않습니다.ICMP 패킷을 허용하려면 다음 PIX 컨피그레이션**에** 표시된 대로 access-list 명령을 사용합니다.**access-list** 명령에 대한 자세한 내용은 PIX **Firewall** A에서 B 명령을 참조하십시오.

라우팅 정책은 시나리오 1과 동일합니다.Router22와 ISP-B 간의 링크보다 Router12와 ISP-A 간의 링크가 우선하며, ISP-A 링크가 다운되면 ISP-B 링크가 모든 인바운드 및 아웃바운드 트래픽에 사용됩니다.



구성

이 시나리오에서는 다음 컨피그레이션을 사용합니다.

- 라우터11
- 라우터12
- Router14(ISP-A)
- 라우터21
- 라우터22
- PIX1
- PIX2

라우터11

```
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 !
```

라우터12

```
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.
```

라우터21

```
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
```

라우터22

```
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
```

라우터24(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
```

다음을 확인합니다.

ISP-A 및 ISP-B에 대한 링크가 가동되는 상황부터 시작합니다.Router11 및 Router21의 **show ip bgp summary** 명령 출력은 ISP-A 및 ISP-B로 설정된 BGP 세션을 확인합니다.

```
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
```

Router11의 BGP 테이블에는 다음 홉의 ISP-A 172.16.13.4에 대한 기본 경로(0.0.0.0/0)이 표시됩니다.

```
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
```

이제 Router21에서 BGP 테이블을 확인합니다. 2개의 0.0.0.0/0 경로가 있습니다.하나는 eBGP에서 다음 홉이 172.16.23.4인 ISP-B에서 학습한 것이고 다른 하나는 로컬 환경 설정이 200인 iBGP를 통해 학습한 것입니다. 라우터21은 높은 로컬 환경 설정 특성으로 인해 iBGP 학습 경로를 선호하므로 라우팅 테이블에 해당 경로를 설치합니다.BGP 경로 선택에 대한 자세한 내용은 BGP Best Path

Selection Algorithm을 참조하십시오.

```
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
```

문제 해결

Router11 및 ISP-A BGP 세션을 종료합니다.

```
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
```

ISP-A에 대한 eBGP 세션은 보류 타이머(180초)가 만료되면 중단됩니다.

```
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
```

ISP-A에 대한 링크를 다운하면 Router11은 라우팅 테이블에서 iBGP를 통해 학습하는 192.168.10.2(Router21)의 다음 홉과 함께 0.0.0.0/0을 설치합니다.이렇게 하면 다음 출력과 같이 Router21을 통해 모든 아웃바운드 트래픽을 ISP-B로 푸시합니다.

```
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
```

PIX/ASA를 통한 BGP 인접 디바이스에 대한 MD5 인증

PIX 6.x 구성

다른 라우팅 프로토콜과 마찬가지로, 인증을 위해 BGP를 구성할 수 있습니다.두 BGP 피어 간에 MD5 인증을 구성할 수 있습니다. 즉 피어 간 TCP 연결에서 전송된 각 세그먼트가 확인됩니다.MD5 인증은 두 BGP 피어에서 동일한 비밀번호로 구성해야 합니다.그렇지 않으면 두 사람 사이의 연결이 되지 않습니다.MD5 인증을 구성하면 Cisco IOS 소프트웨어가 TCP 연결에서 전송되는 모든 세그먼트의 MD5 다이제스트를 생성하고 확인합니다.인증이 호출되고 세그먼트가 인증에 실패하면 오류 메시지가 생성됩니다.

PIX 방화벽을 통과하는 MD5 인증을 사용하여 BGP 피어를 구성할 때 BGP 네이버 간의 TCP 흐름에 대한 시퀀스 번호가 무작위가 되지 않도록 BGP 네이버 간에 PIX를 구성하는 것이 중요합니다.이는 PIX 방화벽의 TCP 난수 시퀀스 번호 기능이 기본적으로 활성화되어 있으며, 이를 전달하기 전에 수신 패킷의 TCP 시퀀스 번호를 변경하기 때문입니다.

MD5 인증은 TCP psuedo-IP 헤더, TCP 헤더 및 데이터에 적용됩니다(RFC 2385 참조).TCP는 128비트 해시 번호를 생성하기 위해 BGP 인접 디바이스 비밀번호와 함께 TCP 시퀀스 및 ACK 번호를 포함하는 이 데이터를 사용합니다.해시 번호는 TCP 헤더 옵션 필드의 패킷에 포함됩니다.기본적으로 PIX는 시퀀스 번호를 TCP 플로우당 임의의 숫자로 오프셋합니다.보내는 BGP 피어에서 TCP는 원래 시퀀스 번호를 사용하여 128비트 MD5 해시 번호를 만들고 이 해시 번호를 패킷에 포함합니다.수신 BGP 피어가 패킷을 가져올 때 TCP는 PIX 수정 시퀀스 번호를 사용하여 128비트 MD5 해시 번호를 만들고 이를 패킷에 포함된 해시 번호와 비교합니다.

PIX에서 TCP 시퀀스 값을 변경하고 BGP 네이버의 TCP가 패킷을 삭제하고 다음과 유사한 MD5 실패 메시지를 기록하므로 해시 번호가 다릅니다.

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

norandomseq 키워드를 **static(inside,outside)172.16.11.1 netmask 255.255.255.0 norandomseq** 명령을 사용하여 이 문제를 해결하고 PIX가 TCP 시퀀스 번호를 오프셋하지 못하도록 합니다.다음 예에서는 norandomseq 키워드의 사용을 보여 줍니다.

라우터11

```
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
```

라우터12

```
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

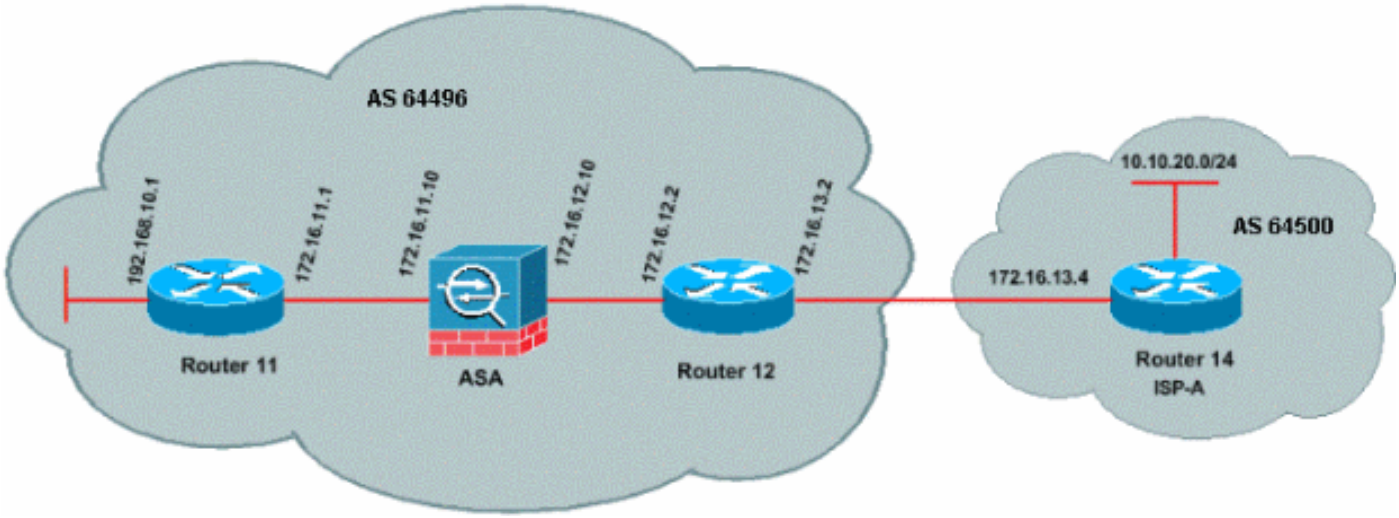
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside.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

이 섹션에서는 이 네트워크 설정을 사용합니다.



PIX/ASA 버전 7.x 이상에서는 MD5 인증을 사용하여 BGP 피어링 세션을 설정하려고 시도할 때 추가적인 문제가 발생합니다.기본적으로 PIX/ASA 버전 7.x 이상에서는 TCP 데이터그램에 포함된 모든 TCP MD5 옵션을 재작성하여 디바이스를 통과하고 옵션 종류, 크기 및 값을 NOP 옵션 바이트로 대체합니다.이렇게 하면 BGP MD5 인증이 효과적으로 중단되고 각 피어링 라우터에서 다음과 같은 오류 메시지가 발생합니다.

```
000296:2010 4 7 15:13:22.221 EDT:%TCP-6-BADMAUTH:172.16.11.1(28894) 172.16.12.2(179) MD5
```

MD5 인증이 있는 BGP 세션을 성공적으로 설정하려면 다음 세 가지 문제를 해결해야 합니다.

- TCP 시퀀스 번호 임의 설정 비활성화
- TCP MD5 옵션 재작성 비활성화
- 피어 간 NAT 비활성화

class-map 및 access-list는 TCP 시퀀스 번호 임의 설정 기능에서 모두 제외되어야 하고 재작성 없이 MD5 옵션을 전달할 수 있는 피어 간의 트래픽을 선택하는 데 사용됩니다.tcp-map은 허용되는 옵션 유형을 지정하는 데 사용됩니다(이 경우 옵션 종류 19(TCP MD5 옵션). class-map과 tcp-map은 모두 Modular Policy Framework 인프라의 일부인 policy-map을 통해 연결됩니다.그런 다음 service-**policy** 명령을 사용하여 컨피그레이션**이** 활성화됩니다.

참고: 피어 간 NAT를 비활성화해야 하는 사항은 no nat-**control** 명령에 의해 처리됩니다.

버전 7.0 이상에서는 ASA의 기본 특성이 **no nat-control**이며, ASA를 통한 모든 연결이 기본적으로 NAT 테스트를 통과하지 않아도 된다고 합니다.ASA에 no nat-**control**의 기본 설정**이 있는 것으로 가정합니다**.자세한 내용은 nat-control을 참조하십시오.nat-**control이** 적용되는 경우 BGP 피어에 대해 NAT를 명시적으로 비활성화해야 합니다.이는 내부 및 외부 인터페이스 간에 **static** 명령을 사용하여 수행할 수 있습니다.

```
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
```

라우터11

```
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
```

라우터12

```
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
```

다음을 확인합니다.

show ip bgp **summary** 명령의 출력은 인증이 성공하고 BGP 세션이 Router11에 설정되었음을 나타냅니다.

```
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#
```

관련 정보

- BGP 지원 페이지
- BGP 최적 경로 선택 알고리즘
- 단일 및 멀티홉 환경에서 BGP와 로드 공유:샘플 구성
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- PIX 방화벽 구성 및 테스트
- 기술 지원 및 문서 – Cisco Systems