Пример конфигурации "ASA/PIX: BGP through ASA"

Содержание

Введение

Этот пример конфигурации демонстрирует, как выполнить Протокол BGP через Устройство безопасности (PIX/ASA) и как достигнуть резервирования в многосетевом BGP и среде PIX. Со схемой сети как пример этот документ объясняет, как автоматически направить трафик к интернет-провайдеру B (ISP-B), когда AS 64496 теряет подключение ISP-A (или реверс), с помощью протоколов динамической маршрутизации, которые работают между всеми маршрутизаторами в AS 64496.

Поскольку BGP использует пакеты TCP индивидуальной рассылки на порту 179 для передачи с его узлами, можно настроить PIX1 и PIX2 для разрешения трафика с конкретным адресом на порте TCP 179. Таким образом, BGP, взаимодействующий, может быть установлен между маршрутизаторами, которые связаны через межсетевой экран. Резервирование и желаемая политика маршрутизации могут быть достигнуты посредством манипулирования атрибутами BGP.

Предварительные условия

Требования

Читатели данной документации должны быть знакомы с BGP Настройки и Основной

Конфигурацией межсетевого экрана.

Используемые компоненты

Примеры сценария в этом документе основываются на этих версиях программного обеспечения:

- Маршрутизаторы Cisco 2600 с Cisco IOS? Выпуск ПО 12.2 (27)
- PIX 515 с Версией 6.3 (3) Межсетевого экрана Cisco PIX и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Эта конфигурация может также использоваться со следующими версиями программного/аппаратного обеспечения:

- Устройство адаптивной защиты Cisco (ASA) серия 5500 с 7.x версия и позже
- Модуль Сервисов межсетевого экрана Cisco (FWSM), который работает под управлением ПО версии 3.2 и позже

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

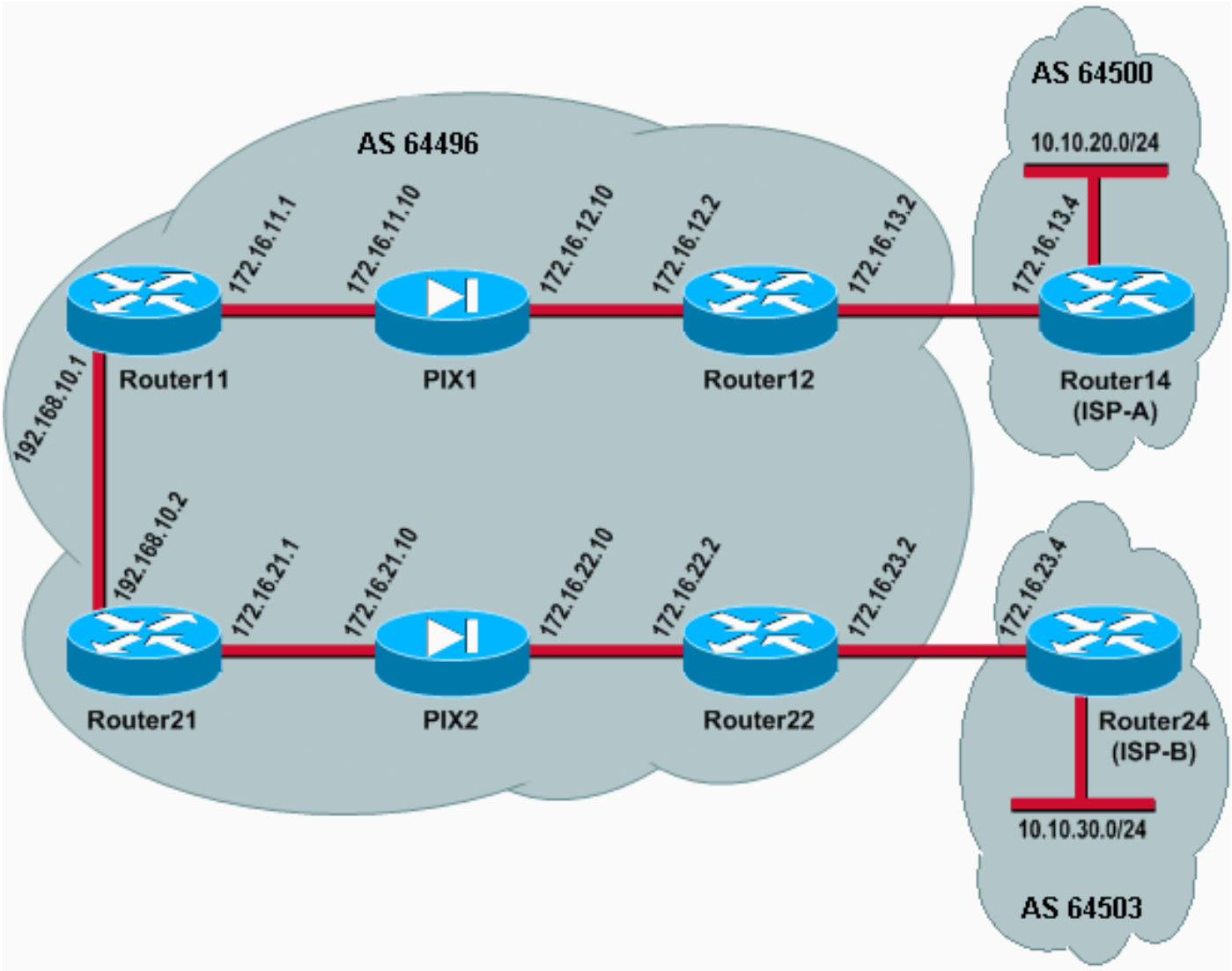
Настройка

Этот раздел предоставляет сведения для настройки функций, описанных в этом документе.

Примечание: Для обнаружения дополнительных сведений о командах в этом документе используйте Средство поиска команд Command Lookup Tool (только зарегистрированные клиенты).

Схема сети

В настоящем документе используется следующая схема сети:



В этой сетевой установке Router12 и Router22 (которые принадлежат AS 64496) являются многосетевыми к Router14 (ISP-A) и Router24 (ISP-B) соответственно для резервирования. Внутренняя сеть 192.168.10.0/24 находится на внутренней части межсетевого экрана. Router11 и Router21 соединяются с Router12 и Router22 через межсетевой экран. PIX1 и PIX2 не настроены для выполнения Технологии NAT.

Сценарий 1

В этом сценарии Router12 в AS 64496 делает внешний информационный обмен (пиринг) (EBGP) с Router14 (ISP-A) в AS 64500. Router12 также делает внутренний BGP (iBGP) пиринг с Router11 через PIX1. Если полученные маршруты eBGP от ISP-A присутствуют, Router12 объявляет о маршруте по умолчанию 0.0.0.0/0 на iBGP к Router11. Если ссылка на сбои ISP-A, Router12 прекращает объявлять о маршруте по умолчанию.

Точно так же Router22 в AS 64496 делает равноправный информационный обмен eBGP с Router24 (ISP-B) в AS 64503 и объявляет о маршруте по умолчанию на iBGP к Router21 условно на основе присутствия маршрутов ISP-B в его таблице маршрутизации.

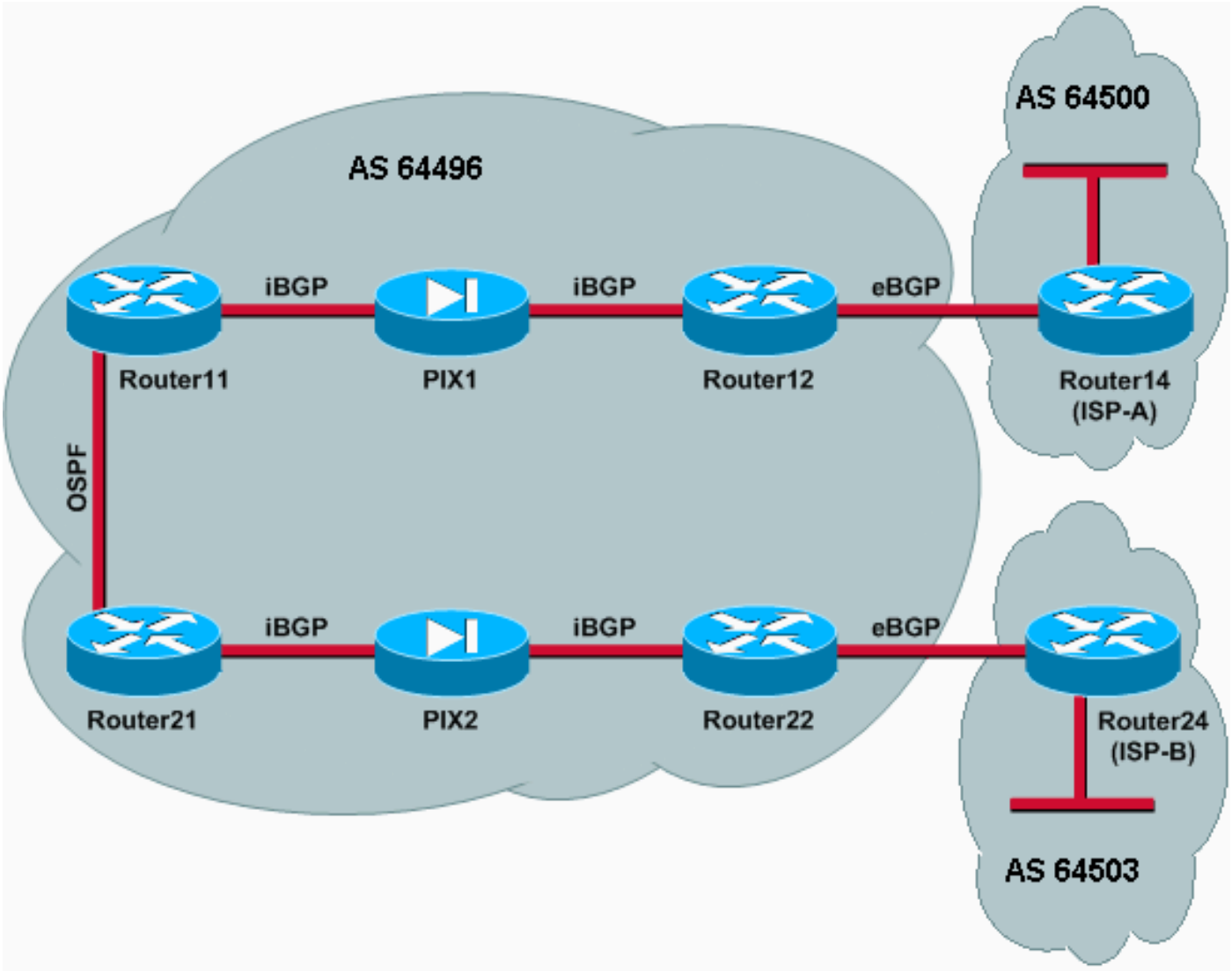
С помощью списка доступа PIX1 и PIX2 настроены для разрешения трафика BGP (TCP, порт 179) между равноправными объектами IBGP. Это вызвано тем, что интерфейсы PIX имеют связанный уровень безопасности. По умолчанию внутренний интерфейс (ethernet1) имеет уровень безопасности 100, и внешний интерфейс (ethernet0) имеет уровень безопасности 0. От соединений и трафика обычно разрешают выше до интерфейсов с более низким

уровнем безопасности. Для разрешения трафика от интерфейса с более низким уровнем безопасности до интерфейса с более высоким уровнем безопасности, однако, необходимо явно определить список доступа на PIX. Кроме того, необходимо настроить статическое преобразование NAT на PIX1 и PIX2, чтобы позволить маршрутизаторам на внешней стороне инициировать сеанс BGP с маршрутизаторами на внутренней части PIX.

И Router11 и Router21 условно объявляют о маршруте по умолчанию в домен Протокола OSPF на основе изученного iBGP маршрута по умолчанию. Router11 объявляет о маршруте по умолчанию в домен OSPF с метрикой 5, Router21 объявляет о маршруте по умолчанию с метрикой 30, и поэтому маршрут по умолчанию от Router11 предпочтен. Эта конфигурация помогает распространяться только маршрут по умолчанию 0.0.0.0/0 к Router11 и Router21, который сохраняет использование памяти на внутренних маршрутизаторах и достигает оптимальной производительности.

Таким образом, для суммирования этих условий это - политика маршрутизации для AS 64496:

- AS 64496 предпочитает ссылку от Router12 до ISP-A для всего исходящего трафика (от 192.168.10.0/24 до Интернета).
- Если подключение к сбоям ISP-A, весь трафик направлен через ссылку от Router22 до ISP-B.
- Весь трафик, который прибывает от Интернета до 192.168.10.0/24, использует ссылку от ISP-A до Router12.
- Если ссылка от ISP-A до сбоев Router12, весь входящий трафик направлен через ссылку от ISP-B до Router22.



Конфигурации

Этот сценарий использует эти конфигурации:

- 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.
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Когда оба сеанса BGP будут подключены, можно ожидать, что все пакеты будут направлены через ISP-A. Рассмотрите таблицу BGP на Router11. Это изучает маршрут по умолчанию 0.0.0.0/0 из Router12 со следующим переходом 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
```

0.0.0.0/0 маршрут по умолчанию, который изучен через BGP, установлен в таблице маршрутизации, как показано в выходных данных **show ip route** на 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
```

Теперь рассмотрите таблицу BGP на Router21. Это также изучает маршрут по умолчанию через 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
```

Теперь посмотрите, установлен ли этот BGP-выученный маршрут по умолчанию в таблице маршрутизации 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
```

Маршрут по умолчанию в Router21 изучен через OSPF (обратите внимание на префикс `O` на маршруте 0.0.0.0/0). Содержательно обратить внимание, что существует маршрут по умолчанию, изученный через BGP из Router22, но **выходные данные show ip route** показывают маршрут по умолчанию, изученный через OSPF.

Маршрут Настроек протокола OSPF по умолчанию был установлен в Router21, потому что Router21 изучает маршрут по умолчанию из двух источников: Router22 через iBGP и Router11 через OSPF. Процесс выбора маршрута устанавливает маршрут с лучшим административным расстоянием в таблицу маршрутизации. В то время как административное расстояние iBGP 200, административное расстояние OSPF равняется 110. Поэтому изученный OSPF маршрут по умолчанию установлен в таблице

маршрутизации, потому что 110 меньше чем 200. Для получения дополнительной информации о выборе маршрута обратитесь к Выбору маршрута в маршрутизаторах Cisco.

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Переведите сеанс BGP в нерабочее состояние между Router12 и ISP-A.

```
Router12(config)# interface fas 0/0

Router12(config-if)# shut

1w0d: %LINK-5-CHANGED: Interface FastEthernet0/0,
      changed state to administratively down
1w0d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
      changed state to down
```

Router11 не изучили маршрут по умолчанию через BGP от 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
```

Проверьте таблицу маршрутизации на Router11. Маршрут по умолчанию изучен через OSPF (административное расстояние 110) со следующим переходом 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
```

Эти выходные данные ожидаются согласно предустановленной политике. На этом этапе, однако, важно понять **distance bgp 20 105 200** команд настройки в Router11 и как это влияет на выбор маршрута на Router11.

Значения по умолчанию этой команды являются **distance bgp 20 200 200**, где полученные маршруты eBGP имеют административное расстояние 20, маршруты с обучением iBGP имеют административное расстояние 200, и локальные маршруты BGP имеют административное расстояние 200.

Когда ссылка между Router12 и ISP-A подходит снова, Router11 изучает маршрут по умолчанию через iBGP от Router12. Однако, потому что административное расстояние по умолчанию этого маршрута с обучением iBGP 200, это не заменит полученный маршрут OSPF (потому что 110 меньше чем 200). Это вызывает весь исходящий трафик к ссылке от Router21 до Router22 к ISP-B, даже при том, что ссылка от Router12 до ISP-A подключена снова. Для решения этой проблемы измените административное расстояние маршрута с обучением iBGP к значению меньше, чем используемый Протокол IGP. В данном примере IGP является OSPF, таким образом, расстояние 105 было выбрано (потому что 105 меньше чем 110).

Для получения дополнительной информации о **команде distance bgp** обратитесь к Командам BGP. Для получения дополнительной информации о множественной адресации с BGP

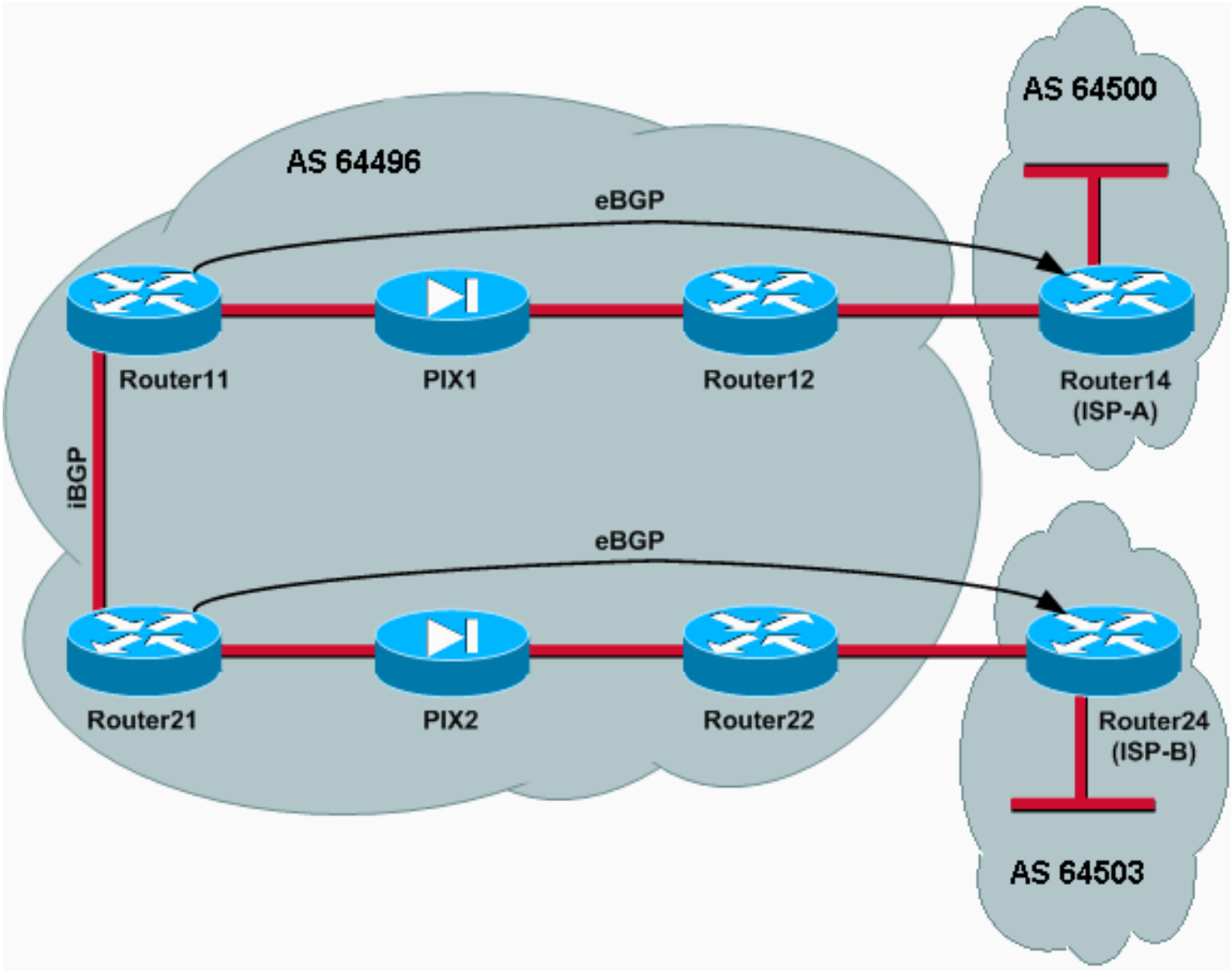
обратитесь к Распределению нагрузки с BGP в Одиночном и Многосетевых средах: Примеры конфигураций.

Сценарий 2

В этом сценарии Router11 является непосредственно равноправным информационным обменом eBGP с маршрутизатором 14 (ISP-A), и Router21 является непосредственно равноправным информационным обменом eBGP с Router24 (ISP-B). Router12 и Router22 не участвуют в пиринге BGP, но они действительно предоставляют возможность подключения с помощью IP-адреса интернет-провайдерам. Поскольку узлы eBGP не являются непосредственно подключенными соседями, **команда neighbor ebgp-multihop** используется на рабочих маршрутизаторах. **Команда neighbor ebgp-multihop** позволяет BGP отвергнуть по умолчанию один предел eBGP перехода, потому что это изменяет Время жизни (TTL) пакетов eBGP от значения по умолчанию 1. В этом сценарии сосед по протоколу EBGP является 3 переходами далеко, таким образом**, neighbor ebgp-multihop 3** настроен на рабочих маршрутизаторах так, чтобы значение TTL было изменено на 3. Кроме того, статические маршруты настроены на маршрутизаторах и PIX, чтобы гарантировать, что Router11 может пропинговать Router14 (ISP-A) адрес 172.16.13.4 и гарантировать, что Router21 может пропинговать Router24 (ISP-B) адрес 172.16.23.4.

По умолчанию PIX не позволяет пакеты Протокола ICMP (передаваемый при запуске **команды ping**) проходить. Для разрешения пакетов ICMP используйте **команду access-list** как показано в в следующей конфигурации PIX. Для получения дополнительной информации о **команде access-list** обратитесь к Межсетевому экрану PIX посредством Команд B.

Политика маршрутизации совпадает с в Сценарии 1: ссылка между Router12 и ISP-A предпочтена по ссылке между Router22 и ISP-B, и когда Канал ISP-A выключается, ссылка ISP-B используется для всего входящего и исходящего трафика.



Конфигурации

Этот сценарий использует эти конфигурации:

- 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
```

Проверка

Начните с ситуации, где ссылки на ISP-A и ISP-B подключены. Выходные данные **команды show ip bgp summary** на Router11 и Router21 подтверждают установленные сеансы BGP с ISP-A и ISP-B соответственно.

```
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
```

Таблица BGP на Router11 показывает маршрут по умолчанию (0.0.0.0/0) к ISP-A следующего перехода 172.16.13.4.

```
Router11# show ip bgp

BGP table version is 13, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          172.16.13.4                  200      0 20 i
*> 10.10.20.0/24    172.16.13.4              0   200      0 64500 i
*>i10.10.30.0/24    192.168.10.2             0   100      0 64503 i
* i192.168.10.0     192.168.10.2             0   100      0 i
*>                  0.0.0.0                  0         32768 i
```

Теперь проверьте таблицу BGP на Router21. Это имеет два маршрута 0.0.0.0/0: один

изученный от ISP-B со следующим переходом 172.16.23.4 на eBGP, и другой изученный через iBGP с local-preference 200. Router21 предпочитает маршруты с обучением iBGP из-за более высокого атрибута local-preference, таким образом, это устанавливает тот маршрут в таблице маршрутизации. Для получения дополнительной информации о выборе пути BGP обратитесь к Алгоритму выбора оптимального пути 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
```

Устранение неполадок

Переведите в нерабочее состояние сеанс BGP ISP-A и Router11.

```
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
```

Когда таймер удержания (180 секунд) истекает, сеанс eBGP к ISP-A выключается.

```
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
```

Со ссылкой на ISP-A вниз, Router11 устанавливает 0.0.0.0/0 со следующим переходом 192.168.10.2 (Router21), который изучен через iBGP в его таблице маршрутизации. Это выдвигает весь исходящий трафик через Router21 и затем к ISP-B, как показано в этих выходных данных:

```
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
```

Аутентификация MD5 для Соседних BGP узел через PIX/ASA

Настройка PIX 6.x

Точно так же, как любой другой протокол маршрутизации BGP может быть настроен для аутентификации. Можно настроить Аутентификацию MD5 между двумя Одноранговыми соединениями по протоколу BGP, что означает, что проверен каждый сегмент, передаваемый на TCP - подключении между узлами. Аутентификация MD5 должна быть настроена с тем же паролем на обоих Одноранговых соединениях по протоколу BGP; иначе, соединение между ними не будет сделано. Конфигурация Аутентификации MD5 заставляет программное обеспечение Cisco IOS генерировать и проверять дайджест MD5 каждого сегмента, передаваемого на TCP - подключении. Если аутентификация вызвана, и сегмент отказывает аутентификацию, сообщение об ошибках генерируется.

Когда вы настраиваете Одноранговые соединения по протоколу BGP с Аутентификацией MD5, которые проходят через межсетевой экран PIX, важно настроить PIX между Соседними BGP узел так, чтобы порядковые номера для потоков TCP между Соседними BGP узел не были случайны. Это вызвано тем, что опция номера случайной последовательности TCP на межсетевом экране PIX активирована по умолчанию, и это изменяет порядковый номер TCP входящих пакетов перед ним вперед их.

Аутентификация MD5 применена на PSUEDO-IP-ЗАГОЛОВОК TCP, заголовок TCP и данные (обратитесь к RFC 2385). TCP использует эти данные — который включает последовательность TCP и номера ACK — наряду с паролем Соседнего BGP узел для создания номера хэша на 128 битов. Номер хэша включен в пакет в поле параметров заголовка TCP. По умолчанию PIX смещает порядковый номер случайным числом на поток TCP. На одноранговых узлах BGP - отправителях TCP использует исходный номер последовательности, чтобы создать 128-битный хэш-номер MD5, и включает его в пакет. Когда Одноранговое соединение по протоколу BGP получения получает пакет, TCP использует модифицируемый PIX порядковый номер для создания номера хэша MD5 на 128 битов и сравнивает его с номером хэша, который включен в пакет.

Номер хэша является другим, потому что значение последовательности TCP было изменено PIX, и TCP на Соседнем BGP узел отбрасывает пакет и регистрирует сообщение об ошибках MD5, подобное этому:

```
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
```

Используйте **norandomseq** ключевое слово с **помехами (внутри, снаружи) 172.16.11.1 172.16.11.1 масок подсети 255.255.255.0 norandomseq** команд, чтобы решить эту проблему и мешать PIX сместить порядковый номер TCP. Данный пример иллюстрирует использование **norandomseq** ключевого слова:

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

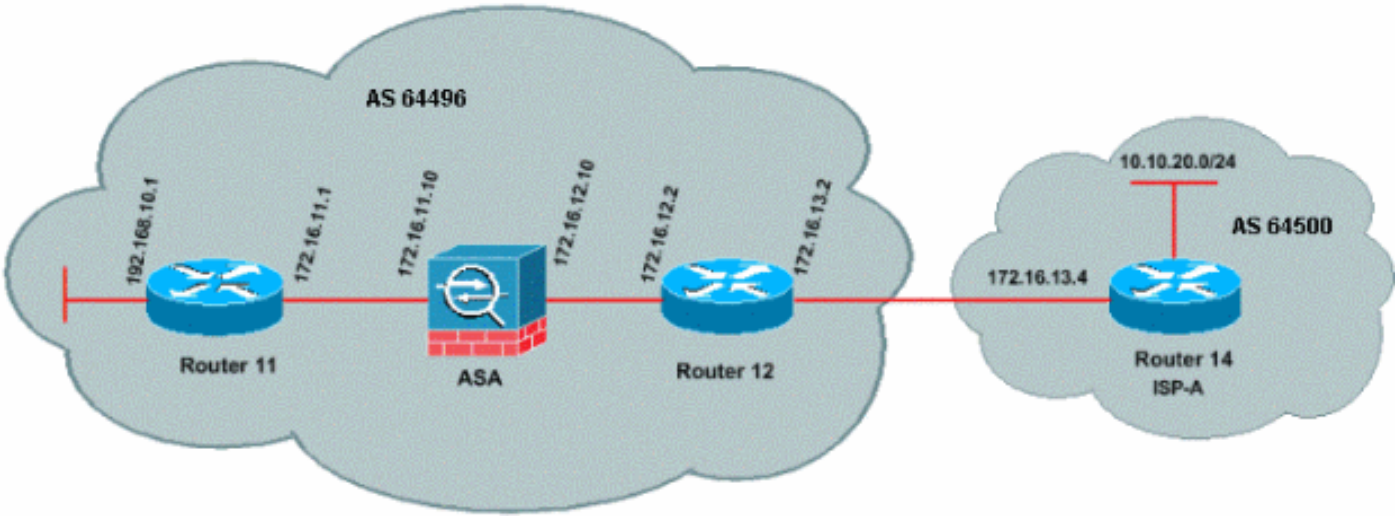
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
ip address outside 172.16.12.10 255.255.255.0
ip address inside 172.16.11.10 255.255.255.0
access-list acl-1 permit tcp host 172.16.13.4 host
172.16.11.1 eq bgp
!--- Access list allows BGP traffic to pass from outside
to inside.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

В данном разделе используются следующие настройки сети.



Когда вы пытаетесь установить сеанс с равноправным участием BGP с Аутентификацией MD5, версия 7.x PIX/ASA и позже представляет дополнительную проблему. По умолчанию, версия 7.x PIX/ASA и более поздние перезаписи, которые любая опция TCP MD5 включала на датаграмме TCP, которая проходит устройство и заменяет вид опции, размер и значение с байтами опции NOP. Это эффективно ломает Аутентификацию MD5 BGP и приводит к сообщениям об ошибках как это на каждом маршрутизаторе равноправного информационного обмена:

```
000296: Apr 7 2010 15:13:22.221 EDT: %TCP-6-BADAUTH: No MD5 digest from 172.16.11.1(28894) to
172.16.12.2(179)
```

Для сеанса BGP с Аутентификацией MD5, которая будет успешно установлена, должны быть решены эти три вопроса:

- Отключите рандомизацию порядкового номера TCP
- Отключите перезапись опции TCP MD5
- Отключите NAT между узлами

Class-map и access-list используются для выбора трафика между узлами, которые должны и быть освобождены от функции рандомизации порядкового номера TCP и позволены нести опцию MD5 без перезаписи. Карта tcp используется для определения типа опции, который будет позволен, в этом случае, вид опции 19 (опция TCP MD5). Class-map и карта tcp оба соединены через policy-map, часть Модульной инфраструктуры Системы политик. Конфигурация тогда активирована с **командой service-policy**.

Примечание: Потребность отключить NAT между узлами обрабатывается **командой no nat-control**.

В версии 7.0 и позже, природа по умолчанию ASA является **никаким nat-control**, который сообщает, что каждое соединение через ASA, по умолчанию, не должно проходить тест NAT. Предполагается, что ASA имеет настройку по умолчанию **никакого nat-control**. См. nat-control для получения дополнительной информации. Если **nat-control** принужден, необходимо явно отключить NAT для Одноранговых соединений по протоколу BGP. Это может быть сделано со **статической** командой между внутренними и внешними интерфейсами.

```
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
```

Проверка

Выходные данные от **команды show ip bgp summary** указывают, что аутентификация успешна и что сеанс BGP установлен на 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
```

Дополнительные сведения

- Страница поддержки BGP
- Алгоритм выбора лучшего пути BGP
- Распределение нагрузки в одно- и многоканальной среде BGP: Примеры конфигураций
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Настройка и межсетевой экран PIX тестирования
- Cisco Systems – техническая поддержка и документация