ASA/PIX：BGP通过ASA配置示例

目录

简介

此配置示例展示如何通过安全设备 (PIX/ASA) 运行边界网关协议 (BGP)，以及如何在多宿主 BGP 和 PIX 环境中实现冗余。以网络图为例，本文说明如何通过使用在 AS 64496 中所有路由器之间运行的动态路由协议，在 AS 64496 丢失到 ISP-A 的连接（或相反）时自动将流量路由至 Internet 服务提供商 B (ISP-B)。

由于 BGP 使用端口 179 上的单播 TCP 数据包与其对等体联络，因此您可以配置 PIX1 和 PIX2 以允许在 TCP 端口 179 上传送单播流量。这样，可以在通过防火墙连接的路由器之间建立 BGP 对等体。冗余和所需的路由策略可以通过 BGP 属性的处理来实现。

先决条件

要求

本文读者应该熟悉配置 BGP 和基本防火墙配置。

使用的组件

本文中的示例场景基于以下软件版本：

- 有Cisco IOS的Cisco 2600路由器？软件版本12.2(27)

- 带有 Cisco PIX 防火墙版本 6.3(3) 及更高版本的 PIX 515

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可用于以下硬件和软件版本：

- Cisco 自适应安全设备 (ASA) 5500 系列（7.x 版及更高版本）
- Cisco防火墙服务模块(FWSM)该运行软件版本3.2及以后

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

此部分提供本文描述的功能的配置信息。

注意： 要寻找关于本文中指令的其他信息，请使用命令查找工具(注册用户)。

网络图

本文档使用以下网络设置：

在此网络设置中，路由器 12 和路由器 22（属于 AS 64496）宿主分别为路由器 14 (ISP-A) 和路由器 24 (ISP-B)，以提供冗余。内部网络 192.168.10.0/24 在防火墙之内。路由器 11 和路由器 21 通过防火墙连接至路由器 12 和路由器 22。PIX1 和 PIX2 未针对执行网络地址转换 (NAT) 进行配置。

场景 1

在此方案中，AS 64496 中的路由器 12 与 AS 64500 中的路由器 14 (ISP-A) 形成外部 BGP (eBGP) 对等体。路由器 12 还通过 PIX1 与路由器 11 形成内部 BGP (iBGP) 对等体。如果从 ISP-A 获取的 eBGP 路由存在，则路由器 12 宣布路由器 11 的 iBGP 默认路由 0.0.0.0/0。如果到 ISP-A 的链路发生故障，路由器 12 停止宣布该默认路由。

同样地，AS 64496 中的路由器 22 与 AS 64503 中的路由器 24 (ISP-B) 形成 eBGP 对等体，并且根据路由器 21 的路由表中是否存在 ISP-B 路由有条件地宣布路由器 21 的 iBGP 默认路由。

通过使用访问列表，将 PIX1 和 PIX2 配置为允许 iBGP 对等体之间的 BGP 流量（TCP、端口 179）。这是因为 PIX 接口有一个相关的安全等级。默认情况下，内部接口 (ethernet1) 的安全等级为 100，外部接口 (ethernet0) 的安全等级为 0。通常允许从较高安全等级接口到较低安全等级接口的连接和流量。然而，要允许从较低安全等级接口到较高安全等级接口的流量，您必须在 PIX 上明确定义访问列表。并且，您必须在 PIX1 和 PIX2 上配置静态 NAT 转换，以允许外部路由器启动与 PIX 内部路由器的 BGP 会话。

路由器 11 和路由器 21 根据 IBGP 获取的默认路由有条件地将默认路由宣布到开放式最短路径优先 (OSPF) 域。路由器 11 将量度值为 5 的默认路由宣布到 OSPF 域，路由器 21 则宣布量度值为 30 的默认路由，因此首选路由器 11 的默认路由。此配置有助于只将默认路由 0.0.0.0/0 传播到路由器

11 和路由器 21，可节省路由器内部的内存消耗，达到最佳性能。

因此，汇总以上情况，以下为 AS 64496 的路由策略：

- 对于所有出站流量（从 192.168.10.0/24 到 Internet），AS 64496 首选从路由器 12 到 ISP-A 的链路。
- 如果到 ISP-A 的连接发生故障，则通过该链路的所有流量从路由器 22 路由到 ISP-B。
- 从 Internet 到 192.168.10.0/24 的所有流量使用从 ISP-A 到路由器 12 的链路。
- 如果从 ISP-A 到路由器 12 的链路发生故障，则通过该链路的所有入站流量从 ISP-B 路由到路由器 22。

配置

此方案使用以下配置：

- Router11
- Router12
- 路由器 14 (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
```

路由器 14 (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.
```

路由器 24 (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.
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

当两个 BGP 会话均打开时，您可能期望所有数据包都通过 ISP-A 进行路由。考虑路由器 11 上的 BGP 表。它从路由器 12 获取默认路由 0.0.0.0/0，下一跳为 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
```

通过 BGP 获取的 0.0.0.0/0 默认路由会安装在路由表中，如在路由器 11 上的 **show ip route** 的输出所示。

```
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
```

现在请考虑路由器 21 上的 BGP 表。它也通过路由器 22 获取默认路由。

```
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
```

现在请检查此 BGP 获取的默认路由是否已安装在路由器 21 的路由表中。

```
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
```

路由器 21 中的默认路由是通过 OSPF 获取的（请注意 0.0.0.0/0 路由的 O 前缀）。有趣的是，您会注意到，有一个默认路由是通过 BGP 从路由器 22 获取的，但 **show ip route** 输出却显示，默认路由是通过 OSPF 获取的。

由于路由器 21 从以下两个源获取 OSPF 默认路由，因此该默认路由已安装在路由器 21 中：路由器 22（通过 iBGP）和路由器 11（通过 OSPF）。路由选择过程将具有更好的管理距离的路由安装

到路由表中。OSPF 的管理距离是 110，而 iBGP 的管理距离是 200。所以，OSPF 获取的默认路由被安装在路由表中，因为 110 小于 200。有关路由选择的详细信息，请参阅 Cisco 路由器的路由选择。

故障排除

使用本部分可排除配置故障。

关闭路由器 12 和 ISP-A 之间的 BGP 会话。

```
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
```

路由器 11 没有通过 BGP 从路由器 12 获取的默认路由。

```
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
```

检查路由器 11 上的路由表。默认路由是通过 OSPF 获取的（管理距离为 110），下一跳为路由器 21。

```
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
```

此输出根据预定义策略的预期输出。不过，此时重要的是了解路由器 11 中的 distance bgp 20 105 200 配置命令及其对路由器 11 上的路由选择的影响。

此命令值默认为distance bgp 20 200 200，在该命令中，eBGP学习的路由的管理距离为20，IBGP学习的路由的管理距离为200，本地BGP路由的管理距离这200。

当路由器 12 与 ISP-A 之间的链路再次接通时，路由器 11 通过 iBGP 从路由器 12 获取默认路由。然而，因为此 IBGP 获取的路由的默认管理距离是 200，所以它不会替换 OSPF 获取的路由（因为 110 小于 200）。这会强制从路由器 21 到路由器 22 的链路的所有出站流量流至 ISP-B，即使从路由器 12 到 ISP-A 的链路重新接通也是如此。要解决此问题，请将 iBGP 获取的路由的管理距离更改为小于内部网关协议 (IGP) 所使用的值。在本例中，IGP 是 OSPF，因此选择距离 105（因为 105 小于 110）。

有关 distance bgp 命令的详细信息，请参阅 BGP 命令。有关 BGP 的多宿主的详细信息，请参阅在单宿主和多宿主环境中使用 BGP 进行负载共享：配置示例）。

场景 2

在此方案中，路由器 11 是与路由器 14 (ISP-A) 的直接 eBGP 对等体，路由器 21 是与路由器 24 (ISP-B) 的直接 eBGP 对等体。路由器 12 和路由器 22 不参与 BGP 对等，但是它们向 ISP 提供 IP 连接。由于 eBGP 对等体不是直接连接的邻居，因此 neighbor ebgp-multihop 命令用于参与的路由器。**neighbor ebgp-multihop 命令**可让 BGP 覆盖默认的一跳 eBGP 限制，因为它将 eBGP 数据包的存活时间 (TTL) 从默认值更改为 1。在此方案中，eBGP 邻居距离 3 跳远，因此在参与的路由器上配置 **neighbor ebgp-multihop 3**，以便将 TTL 值更改为 3。另外，在路由器和 PIX 上配置静态路由，以确保路由器 11 能 Ping 通路由器 14 (ISP-A) 地址 172.16.13.4，以及确保路由器 21 能 Ping 通路由器 24 (ISP-B) 地址 172.16.23.4。

默认情况下，PIX 不允许 Internet 控制信息协议 (ICMP) 数据包（在发出 **ping** 命令时发送）通过。

要允许 ICMP 数据包，请使用 **access-list** 命令，如在下一 PIX 配置中所示。有关 access-list 命令的详细信息，请参阅 PIX 防火墙 A 至 B 命令。

路由策略与方案 1 中的相同：路由器 12 和 ISP-A 之间的链路优先于路由器 22 和 ISP-B 之间的链路，当 ISP-A 链路关闭时，ISP-B 链路用于所有入站和出站流量。

配置

此方案使用以下配置：

- Router11
- Router12
- 路由器 14 (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
```

路由器 14 (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
```

路由器 24 (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
```

验证

首先是到 ISP-A 和 ISP-B 的链路开通的情况。在路由器 11 和路由器 21 上的 **show ip bgp summary** 命令的输出确认已分别建立与 ISP-A 和 ISP-B 的 BGP 会话。

```
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
```

路由器 11 上的 BGP 表显示流往下一跳 ISP-A 172.16.13.4 的默认路由 (0.0.0.0/0)。

```
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
```

现在请检查路由器 21 上的 BGP 表。它有两个 0.0.0.0/0 路由：一个是从 ISP-B 获取的，下一跳为 eBGP 上的 172.16.23.4；另一个是通过 iBGP 获取的，其本地优先级为 200。由于 iBGP 获取的路由具有更高的本地优先级属性，路由器 21 首选 iBGP 获取的路由，因此它会将该路由安装在路由表中。有关 BGP 路径选择的详细信息，请参阅 BGP 最佳路径选择算法。

```
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
```

故障排除

关闭路由器 11 和 ISP-A BGP 会话。

```
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
```

当 hold-down timer（180 秒）到期时，eBGP 到 ISP-A 的会话关闭。

```
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
```

随着到 ISP-A 的链路关闭，路由器 11 安装 0.0.0.0/0，且下一跳为 192.168.10.2（路由器 21），这是通过 iBGP 在其路由表中获取的。这会推送所有出站流量通过路由器 21 然后到 ISP-B，如以下输出所示：

```
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
```

通过 PIX/ASA 对 BGP 邻居的 MD5 身份验证

PIX 6.x 配置

正如任何其他路由协议，可以配置 BGP 进行身份验证。您可以配置两个 BGP 对等体之间的 MD5 身份验证，这意味着将对在对等体之间的 TCP 连接上发送的每一段进行验证。在两个 BGP 对等体上必须使用同一个口令配置 MD5 身份验证；否则，不会在它们之间建立连接。MD5 身份验证的配置造成 Cisco IOS 软件生成和检查在 TCP 连接上发送的每一段的 MD5 摘要。如果身份验证被调用，并且某一段不能通过身份验证，将生成错误消息。

当您使用 MD5 身份验证配置穿过 PIX 防火墙的 BGP 对等体时，在 BGP 邻居之间配置 PIX 非常重要，以便在 BGP 邻居之间流过的 TCP 的序列号不是随机的。这是因为默认情况下在 PIX 防火墙上会启用 TCP 随机序列号功能，并且在转发传入数据包之前会更改它们的 TCP 序列号。

MD5 身份验证应用于 TCP 伪 IP 报头、TCP 报头和数据（请参阅 RFC 2385 ）。 TCP 使用这些数据（包括 TCP 序列号和 ACK 码）及 BGP 邻居口令创建 128 位的哈希码。哈希码包含在 TCP 报头选项字段的数据包中。默认情况下，对于每个 TCP 流，PIX 都用一个随机数字来对序列号进行偏移。在发送的 BGP 对等体中，TCP 使用原始序列号来创建 128 位的 MD5 哈希码并且将此哈希码包括在该数据包中。在接收 BGP 对等体获得该数据包后，TCP 使用 PIX 已修改的序列号来创建 128 位的 MD5 哈希码，并将此编号与该数据包中包含的哈希码相比较。

由于 TCP 序列值已由 PIX 更改，因此哈希码是不同的，并且 BGP 邻居的 TCP 丢弃该数据包并记

录与以下消息类似的 MD5 失败消息：

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

使用 **static (inside,outside) 172.16.11.1 172.16.11.1 netmask 255.255.255.0 norandomseq** 命令的 **norandomseq** 关键字可解决此问题，并阻止 PIX 对 TCP 序列号进行偏移。此示例说明 **norandomseq** 关键字的用法：

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 及更高版本

本部分使用以下网络设置。

当您设法建立带有 MD5 身份验证的 BGP 对等会话时，PIX/ASA 版本 7.x 及更高版本会引入额外的挑战。默认情况下，PIX/ASA 版本 7.x 及更高版本会重写通过设备的 TCP 数据报中包括的所有 TCP MD5 选项，并且用 NOP 选项字节替换选项种类、大小和值。这将有效中断 BGP MD5 身份验证，并且导致在每个对等路由器上出现类似下面的错误消息：

```
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)
```

为了顺利地建立带有 MD5 身份验证的 BGP 会话，必须解决以下三个问题：

- 禁用 TCP 序列号随机化
- 禁用 TCP MD5 选项重写
- 在对等体之间的禁用 NAT

class-map 和 access-list 用于选择必须免除 TCP 序列号随机化功能且允许携带 MD5 选项而无需重写的对等体之间的流量。tcp-map 用于指定要允许的选项类型，在本例中即为选项种类 19（TCP MD5 选项）。class-map 和 tcp-map 均通过作为模块化策略框架基础架构一部分的 policy-map 链接在一起。然后用 **service-policy** 命令激活配置。

注意： 在对等体之间禁用 NAT 的需要由 **no nat-control** 命令处理。

在版本 7.0 及更高版本中，ASA 的默认属性是 **no nat-control**，它声明默认情况下通过 ASA 的每个连接不需要通过 NAT 测试。假设 ASA 的默认设置为 no **nat-control**。有关详细信息，请参阅 nat-control。如果 **nat-control** 被强制执行，您必须明确禁用 BGP 对等体的 NAT。这可以在内部和外部接口之间使用 **static** 命令完成。

```
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
```

路由器 14 (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
```

验证

show ip bgp summary 命令的输出表明身份验证是成功的，并且已在路由器 11 上建立 BGP 会话。

```
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#
```

相关信息

- BGP 支持页

- BGP 最佳路径选择算法
- 在单宿主和多宿主环境中加载 BGP 共享：示例配置
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 配置和测试 PIX 防火墙
- 技术支持和文档 - Cisco Systems