BGP - фильтрация входящих префиксов

Опубликовано muff в Вс, 2014-07-20 12:53

На днях обратился знакомый с просьбой о помощи. Часть ресурсов его сети стала недоступна.

После диагностики обнаружил, что проблема заключается в отсутсвии "защиты от дурака" в настройках **BGP**. В сети знакомого используются сети из блока **192.168.0.0/16** с маской **/24**, а провайдер по **BGP** начал анонсировать эти же сети с маской **/26**. Соответственно, таблица маршрутизации перестроилась и трафик, вместо того, чтобы "бежать" к ресурсам локальной сети, направлялся к провайдеру. Как говорится, "офигел молча", но нужно что-то решать.

Возмущаться и разбираться с сапортом провайдера - дело долгое. Поэтому решаем вопрос на стороне сети знакомого.

Создадим **prefix-list**, в котором запретим все зарезервированные сети, которые не должны маршрутизироваться в сети **Internet** (в табличке колонка **Global** из статьи о зарезервированных IPv4 адресах [1]):

```
bgp(config)# ip prefix-list Deny_Reserved_Net seq 5 deny 0.0.0.0/8 le 24bgp(config)#
 ip prefix-list Deny_Reserved_Net seq 10 deny 10.0.0.0/8 le 24bgp(config)# ip prefix
-list Deny_Reserved_Net seq 15 deny 100.64.0.0/10 le 24bgp(config)# ip prefix-list D
eny_Reserved_Net seq 20 deny 127.0.0.0/8 le 24bgp(config)# ip prefix-list Deny_Reser
ved_Net seq 25 deny 169.254.0.0/16 le 24bgp(config)# ip prefix-list Deny_Reserved_Ne
t seq 30 deny 172.16.0.0/12 le 24bgp(config)# ip prefix-list Deny_Reserved_Net seq 3
5 deny 192.0.0.0/24bgp(config)# ip prefix-list Deny_Reserved_Net seq 40 deny 192.0.2
.0/24bgp(config)# ip prefix-list Deny_Reserved_Net seq 45 deny 192.168.0.0/16 le 24b
gp(config)# ip prefix-list Deny_Reserved_Net seq 50 deny 198.18.0.0/15 le 24bgp(conf
ig)# ip prefix-list Deny_Reserved_Net seq 55 deny 198.51.100.0/24bgp(config)# ip pre
fix-list Deny_Reserved_Net seq 60 deny 203.0.113.0/24bgp(config)# ip prefix-list Den
y_Reserved_Net seq 65 deny 240.0.0.0/4 le 24bgp(config)# ip prefix-list Deny_Reserve
d_Net seq 100 permit 0.0.0.0/0 le 24
```

Также последним правилом "отрезаем" все сети с маской длиннее **/24**, поскольку они не должны маршрутизироваться в сети **Internet**. Теперь можно просто "наложить" этот **prefix-list** на **neighbor**-а провайдера, однако я обычно использую **route-map**, что добавляет гибкости при настройке. Создадим **route-map**, включим в него созданный **prefix-list** и "наложим" на **neighbor**-а провайдера.

```
bgp(config)# route-map UPLINK-in permit 10bgp(config-route-map)# match ip address pr
efix-list Deny_Reserved_Netbgp(config-route-map)# exitbgp(config)# router bgp 65001b
gp(config-router)# neighbor x.x.x.x route-map UPLINK-in in
```

Последний штрих - очистка входящих маршрутов и сохранение конфигурации.

```
bgp# clear ip bgp x.x.x.x soft inbgp# copy running-config startup-config
```

Источник (получено *2025-12-13 11:36*):
http://muff.kiev.ua/content/bgp-filtratsiya-vkhodyashchikh-prefiksov

Ссылки:
[1] http://muff.kiev.ua/content/reserved-ipv4-addresses-zarezervirovannye-ipv4-adresa