ФИЛЬТРАЦИЯ МАРШРУТНЫХ ОБЪЯВЛЕНИЙ

Особый вид фильтрации **- фильтрация маршрутных объявлений.** Она помогает защитить IP-маршрутизацию от непреднамеренных ошибок администраторов и атак злоумышленников. Особенно важна такая фильтрация для протокола BGP, который распространяет данные о достижимости той или иной сети через последовательность автономных систем Интернет и тем самым обеспечивает его связность.

Посмотрим, каким образом маршрутизатор может выполнять фильтрацию маршрутных объявлений BGP на примере маршрутизаторов Cisco.

Фильтровать маршрутные объявления BGP можно как на основе префиксов IP адресов, так и на основе номеров автономных систем.

Синтакис списков доступа на основе префиксов весьма прост, например запись

```
ip prefix-list abc1 deny 10.0.0.0/8
```

запрещает объявления о префиксе 10.0.0.0/8, который относится к диапазонам адресов, зарезервированных IANA в качестве частных (это определено в RFC1918), поэтому хорошей практикой является фильтрация их в публичном адресном пространстве Интернет. Для того, чтобы список доступа начал работать, его нужно применить к конфигурации BGP для определенного соседа и указать направление фильтрации, например:

```
switch# configure terminal

switch(config)# ip prefix-list allowprefix 10 permit 192.0.2.0 eq 24

switch(config)# ip prefix-list allowprefix 20 permit 209.165.201.0 eq
27

switch(config) router bgp 65536:20

switch(config-router)# neighbor 192.0.2.1/16 remote-as 65536:20

switch(config-router-neighbor)# address-family ipv4 unicast

switch(config-router-neighbor-af)# prefix-list allowprefix in

switch(config-router-neighbor-af)#
```

В этом примере в списке доступа *allowprefix* созданы две записи, 10 и 20, разрешающие префиксы 192.0.2.0.24 и 209.165.201.0/27, а затем этот список применен к BGP-соседу 192.0.2.1 во входном направлении, то есть от этого соседа разрешено принимать только эти префиксы.

В словаре администраторов Интернет-провайдеров закрепился такой термин как «***богоны***» (***bogons***). Он обозначает префиксы, которые не должны появляться в публичном адресном пространстве Интернет. Богоны включают адреса, зарезервированные в RFC 1918 как частные, но не только – в них входят также адреса, еще не распределенные между региональными Интернет центрами (такими как RIPE NCC, ARIN и т..д) или же зарезервированные для специальных целей. IANA публикует список распределенных адресов на своем сайте[1], этот список периодически обновляется, так что провайдер должен отсеживать изменения и корректировать свой список богонов, использующихся в списках доступа.

Синтаксис списков доступа на основе номеров автономных систем более гибок, так как он позволяет использовать регулярные выражения в стиле Unix. Рассмотрим следующий пример:

```
router bgp 200

 neighbor 193.1.12.10 remote-as 100

 neighbor 193.1.12.10 filter-list 1 out

 neighbor 193.1.12.10 filter-list 2 in

ip as-path access-list 1 permit _109_

ip as-path access-list 1 permit ^117_

ip as-path access-list 2 permit _200$

ip as-path access-list 2 permit ^100$
```

Здесь список доступа 1 разрешает маршрутные объявления, содержащее номер AS109 в любом месте списка номеров объявления (символ «_» определяет это), а также обявления от соседа с номером 117 (символ «^» обозначает начало выражения). Список доступа 2 разрешает объявления, в которых исходной автономной системой является AS200 (символ «$» относится к концу строки), а также объявления от непосредственного соседа AS100, в которых он объявляет себя исходной AS (так как номер 100 должен быть первым и последним в последовательности AS, а значит – единственным).

---

[1] *http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml*