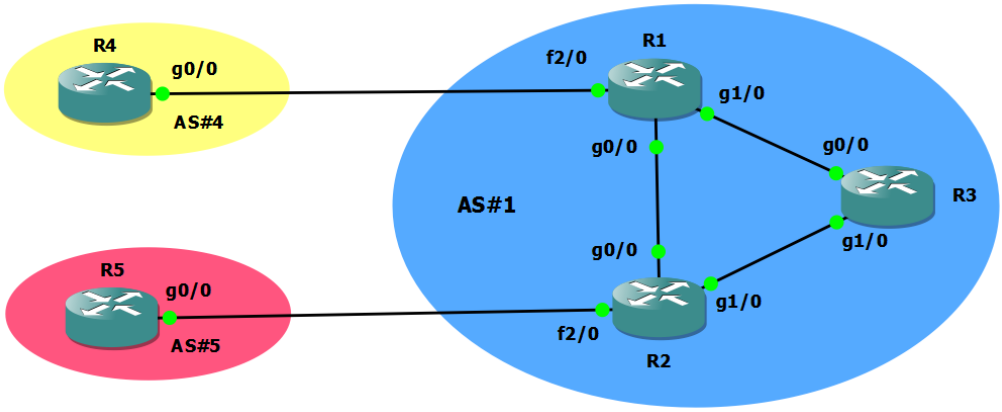
BGP RTBH – Remotely-Triggered Black Hole

Введение

Целью данной работы является знакомство студентов с решением, часто применяемым телекоммуникационными провайдерами для защиты своих клиентов от DoS -атак. Конечно же, защита от DoS и тем более DDoS-атак более сложная и не ограничивается описываемой технологией, однако такое решение весьма интересно само по себе, так как для его применения используются различные опции протокола BGP. При выполнении данной лабораторной работы студенты приобретут практические навыки работы с комьюнити в BGP, а также познакомятся с несколькими другими тонкостями функционирования маршрутизаторов.

При выполнении работы допускается и считается нормальным, если студент будет обращаться к разнообразной литературе и другим источникам информации.

Схема



Описание

На рисунке выше представлена упрощённая схема сети провайдера и двух его небольших клиентов. В сети оператора использовано три маршрутизатора для обеспечения простейшей отказоустойчивости. Сети клиентов представлены одним маршрутизатором для простоты.

Существует две разновидности RTBH: source based и destination based, различающиеся по тому, блокировка отправителя или получателя осуществляется. В данной лабораторной работе рассматривается destination based версия RTBH, например, из-за того, что в DDoS-атаках источников паразитного трафика может быть чрезвычайно много.

Включение RTBH требует предварительной подготовительной работы на сетях провайдера и клиента, проводимой до возникновения атаки. При детектировании паразитного трафика на определённый хост в сети клиента, администраторы компании-клиента могут заблокировать трафик на этот хост в сети оператора без вмешательства специалистов провайдера.

Лабораторная работа выполняется в эмуляторе GNS3 версии 1.1 или более поздней. В качестве маршрутизаторов использована модель 7204VXR с IOS версии 15.2(4)M6 или более поздней с набором опций ADVENTERPRISEK9.

1. Соберите схему, представленную выше, в эмуляторе. Включите все устройства. Включите все интерфейсы между маршрутизаторами.
2. На каждом маршрутизаторе настройте интерфейс Loopback1 с IP-адресом X.X.X.X/32, где X – цифра, входящая в название устройства. Так, например, для маршрутизатора R4 назначаемый адрес будет 4.4.4.4.
3. На линках между маршрутизаторами настройте IP-адреса вида 192.168.YZ.Y/24 и 192.168.YZ.Z/24, где Y – номер меньшего устройства в паре, а Z – большего. Так, например, на интерфейсе Gi0/0 R5 должен быть назначен адрес 192.168.25.5, а на интерфейс Fa2/0 R2 – 192.168.25.2.
4. С помощью команды ping с соответствующими аргументами убедитесь в доступности соседнего устройства.
5. На маршрутизаторах R4 и R5 создайте интерфейсы Loopback0, на которых назначьте IP-адреса вида 10.X.0.1/16, где X – номер устройства. Данные префиксы будут эмулировать маршруты для внутренних сетей клиентов.
6. В сети оператора настройте OSPF только между всеми маршрутизаторами провайдера.
7. Передайте все непосредственно подключенные к этим маршрутизаторами сети в OSPF.
8. Убедитесь в корректности маршрутной информации на всех устройствах провайдера.
9. Настройте BGP в сети провайдера между адресами физических интерфейсов для всех маршрутизаторов.
10. Убедитесь в успешном установлении соседства.
11. Настройте BGP между клиентами и провайдером между адресами физических интерфейсов.
12. Отключите автоматическое суммирование маршрутов командой ***no auto-summary***.
13. С помощью команды ***network*** организуйте передачу префиксов 10.X.0.0/16 в BGP от обоих клиентов.

14. Просмотрите таблицы маршрутизации на клиентах. Убедитесь в том, что в них появилась информация о сети другого клиента.
15. Убедитесь, что маршрутная информация о сетях клиентов НЕ появилась в процессе OSPF провайдера. Объясните, почему это важно.
16. С помощью команды ***shutdown*** выключите интерфейс Gi0/0 R1.
17. Убедитесь, что клиенты перестали получать информацию о префиксах друг друга. Объясните, почему так произошло.
18. Только внутри сети оператора перенастройте BGP так, чтобы соседство устанавливалось между интерфейсами Loopback1, а не между физическими интерфейсами.
19. Убедитесь, что BGP-соседство между R1 и R2 восстановилось.
20. Убедитесь, что клиентские маршрутизаторы вновь начали получать информацию о сетях друг друга.
21. Убедитесь, что между сетями клиентов передаётся пользовательский трафик.
22. Так как R3 в данный момент не участвует в передаче обновлений о пользовательских маршрутах, объясните, возможно ли вообще выключить BGP на R3. К чему это приведёт?
23. Включите все интерфейсы, выключенные в предыдущих пунктах.
24. На маршрутизаторе R4 настройте фильтрацию исходящих маршрутов с помощью ***distribute-list*** или ***route-map***. Требуется, чтобы передавались лишь маршруты из сети 10.4.0.0/16 с масками от 16 до 24.
25. Создайте Loopback2 с адресом 10.3.0.1/16 на маршрутизаторе R4. С помощью команды ***network*** осуществите передачу данный префикс в BGP.
26. Убедитесь, что префикс 10.3.0.0/16 попал в таблицу BGP на R4 с помощью команды ***sho ip bgp***.
27. Убедитесь, что префикса 10.3.0.0/16 нет в таблицах BGP других маршрутизаторов.
28. На всех маршрутизаторах включите поддержку нового формата community с помощью команды ***ip bgp-community new-format***.
29. На маршрутизаторе R5 создайте **route-map 666**. Для всех маршрутов с тегом 666 должна выставляться **community 5:666**.
30. На маршрутизаторе R5 осуществите передачу статических маршрутов в BGP с применением **route-map 666** с помощью команды ***redistribute static route-map 666***.
31. Во всей лабораторной сети разрешите передачу **community** вместе с префиксами с помощью опции ***send-community both***, указываемой для каждого BGP-соседа.
32. На всех маршрутизаторах в сети оператора настройте статический маршрут на адрес 192.168.1.1/32 в интерфейс **null 0**.
33. С помощью команды ***clear ip bgp **** на маршрутизаторах R4 и R5 переустановите BGP-соседство с оператором. Не применяйте эту команду в реальной сети! Изучите менее «разрушительные» аналоги данной команды.
34. На маршрутизаторе R5 создайте хостовой статический маршрут для адреса 10.5.1.1/32 в интерфейс **null 0** с тегом 666.
35. Убедитесь, что роутер R5 отдаёт только хостовой маршрут из предыдущего пункта с соответствующим значением **community**, а маршрут на всю сеть 10.5.0.0/16 без данного атрибута.
36. На маршрутизаторе R2 убедитесь в корректности приходящих обновлений от соседа R5.
37. Настройте на маршрутизаторе R2 **route-map** на вход от R5 с двумя записями. Первая должна проверять префикс на наличие атрибута **community** со значением 666. При его наличии заменить атрибут **next-hop** на значение 192.168.1.1. Для проверки наличия определённого значения **community** в обновлении нужно создать соответствующий список сообществ командой ***ip community-list standard 666 permit 5:666***, после чего внутри записи **route-map** осуществлять проверку с помощью команды ***match community 666***. Вторая запись должна проверять, что клиент присылает нам лишь префиксы из разрешённых для него сетей 10.5.0.0/16 с масками от 16 до 24. Логика обработки маршрутизатором объектов route-map похожа на ту, что используется при работе со списками доступа: любое срабатывание условия приводит к окончанию обработки. То есть первая сработавшая запись будет и последней проверяемой. Это означает, что если обновление содержит сообщество 5:666 для какого-либо префикса, то для него проверка на диапазон 10.5.0.0/16 уже выполняться не будет. Чтобы этого не происходило, требуется добавить ключевое слово ***continue*** (новая возможность, добавленная в последние версии IOS) в соответствующую запись внутри **route-map**.
38. Предложите способ написания **route-map** так, чтобы опция ***continue*** не использовалась. Такая конструкция может потребоваться при разворачивании RTBH в сети со старыми маршрутизаторами.
39. Пересоздайте BGP-сессии между устройствами клиентов и провайдера.
40. Изучите BGP-таблицу роутера R2. Что Вы можете сказать о префиксах, получаемых от R5?
41. Убедитесь в отсутствии префикса 10.5.1.1/32 в RIB R2.
42. Наблюдаемое явление связано с тем, что IOS маршрутизатора считает адрес следующего перехода для данного префикса недостижимым, так как сосед и следующий хоп достижимы через разные интерфейсы. Проблема не возникает, если соседство установлено с интерфейса Loopback. Перенастройте маршрутизаторы R2 и R5 так, чтобы BGP-соседство устанавливалось между следующими интерфейсами: R2 Loopback1 и R5 Gi0/0.

43. Какие ещё настройки необходимо сделать на R5, чтобы соседство начало устанавливаться?
44. Убедитесь, что BGP-сессия так и не установилась, даже после ввода дополнительных настроек на R2. Указанная проблема связана с тем, что при установлении eBGP сессии требуется, чтобы она устанавливалась только между непосредственно подключёнными физическими интерфейсами (проверка с помощью TTL). При установлении iBGP-сессии такая проверка не производится. Чтобы маршрутизаторы могли установить eBGP-соединение между устройствами, которые не подключены друг к другу напрямую, нужно использовать опцию ***ebgp-multihop 255*** для соответствующего соседа. На R2 и R5 произведите требуемую настройку.
45. Убедитесь в установлении BGP-сессии между R2 и R5.
46. Проверьте, что префикс 10.5.1.1/32 появился в таблице маршрутизации устройств провайдера и указывает на правильный интерфейс.
47. Убедитесь, что информация об этом префиксе также достигла роутера другого клиента.
48. На маршрутизаторе R2 внесите изменение в **route-map *666*** так, чтобы для обновлений с сообществом 5:666 не только заменялся атрибут **next-hop**, но также и добавлялось **community *no-export***.
49. Переустановите BGP-соседство между R2 и R5.
50. На остальных роутерах оператора проверьте, какие сообщества выставлены для префикса 10.5.1.1/32.
51. Убедитесь, что префикс 10.5.1.1/32 теперь отсутствует в RIB второго клиента.
52. Проверьте, как передаётся трафик с роутера R4 на адрес 10.5.1.1. Поясните увиденное.
53. Проанализируйте все выполненные ранее настройки. Убедитесь, что присутствует полное понимание всех действий.