ASR9000 на основе источника удаленно инициированная фильтрация черной дыры с примером конфигурации сброса следующего перехода RPL

Содержание

Введение

Этот документ описывает, как настроить Удаленно Инициированную Черную дыру (RTBH) на Маршрутизаторе агрегации (ASR) 9000.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Эти сведения в этом документе основываются на Cisco IOS-XR® и ASR 9000.

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.

Общие сведения

Когда вы знаете происхождение атаки (например, анализом Данных NetFlow), можно применить механизмы включения, такие как Списки контроля доступа (ACL). Когда трафик атаки обнаружен и классифицирован, можно создать и развернуть соответствующие ACL на необходимых маршрутизаторах. Поскольку этот ручной процесс может быть длительным и сложным, много людей используют Протокол BGP для распространения информации об отбрасывании ко всем маршрутизаторам быстро и эффективно. Этот способ, RTBH, устанавливает следующий переход IP-адреса жертвы к интерфейсу NULL. Трафик, предназначенный жертве, отброшен на входе в сеть.

Другая опция должна отбросить трафик от конкретного источника. Этот метод подобен отбрасыванию, описанному ранее, но полагается на предыдущие развертывания Одноадресной пересылки по обратному пути (uRPF), которая отбрасывает пакет, если его источник "недопустим", который включает маршруты в null0. С тем же механизмом основанного на назначении отбрасывания передается Обновление BGP, и это обновление устанавливает следующий переход для источника к null0. Теперь весь трафик, который вводит интерфейс с uRPF, включил трафик отбрасываний из того источника.

На основе источника фильтрация RTBH на ASR9000

Когда uRPF функции включен на ASR9000, маршрутизатор неспособен сделать рекурсивный поиск к null0. Это означает, что На основе источника конфигурация фильтрации RTBH, используемая Cisco IOS, не может непосредственно использоваться Cisco IOS XR на ASR9000. Как альтернатива, используется опция **сброса set next-hop** Языка политики маршрутизации (RPL) (представленный в Версии 4.3.0 Cisco IOS XR).

Настройка

Конфигурация на триггерном маршрутизаторе

Настройте политику перераспределения статического маршрута, которая устанавливает

сообщество на статических маршрутах, отмеченных специальной меткой, и примените его в BGP:

```
route-policy RTBH-trigger
if tag is 777 then
set community (1234:4321, no-export) additive
pass
else
pass
endif
end-policy

router bgp 65001
address-family ipv4 unicast
redistribute static route-policy RTBH-trigger
!
neighbor 192.168.102.1
remote-as 65001
address-family ipv4 unicast
route-policy bgp_all in
route-policy bgp_all out
```

Настройте статический маршрут со специальной меткой для исходного префикса, который должен быть помещен в черный список:

```
router static
address-family ipv4 unicast
10.7.7.7/32 Null0 tag 777
```

Конфигурация на граничном маршрутизаторе

Настройте политику маршрутизации, которая совпадает с сообществом на триггерном маршрутизаторе, и настройте **сброс set next-hop**:

```
route-policy RTBH
if community matches-any (1234:4321) then
set next-hop discard
else
pass
endif
end-policy
```

Примените политику маршрутизации на равноправные объекты IBGP:

```
router bgp 65001
address-family ipv4 unicast
!
neighbor 192.168.102.2
remote-as 65001
address-family ipv4 unicast
route-policy RTBH in
route-policy bgp_all out
```

На интерфейсах границы настройте uRPF свободный режим:

```
interface TenGigE0/0/2/2
cdp

ipv4 address 192.168.101.2 255.255.255.0
ipv4 verify unicast source reachable-via any
```

Примечание: Эта конфигурация uRPF применяется ко всему трафику на этом

интерфейсе.

Проверка

На граничном маршрутизаторе префикс **10.7.7.7/32** отмечен как **Nexthop-сброс**:

```
RP/0/RSP0/CPU0:router#show bgp
BGP router identifier 10.210.0.5, local AS number 65001
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000 RD version: 12
BGP main routing table version 12
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
N>i10.7.7.7/32        192.168.102.2            0    100      0 ?

RP/0/RSP0/CPU0:router#show bgp 10.7.7.7/32
BGP routing table entry for 10.7.7.7/32
Versions:
Process bRIB/RIB SendTblVer
Speaker 12 12
Last Modified: Jul 4 14:37:29.048 for 00:20:52
Paths: (1 available, best #1, not advertised to EBGP peer)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
192.168.102.2 (discarded) from 192.168.102.2 (10.210.0.2)
Origin incomplete, metric 0, localpref 100, valid, internal best, group-best
Received Path ID 0, Local Path ID 1, version 12
Community: 1234:4321 no-export

RP/0/RSP0/CPU0:router#show route 10.7.7.7/32

Routing entry for 10.7.7.7/32
 Known via "bgp 65001", distance 200, metric 0, type internal
 Installed Jul 4 14:37:29.394 for 01:47:02
 Routing Descriptor Blocks
   directly connected, via Null0
     Route metric is 0
 No advertising protos.
```

Можно проверить на входных линейных платах, что происходят отбрасывания RPF:

```
RP/0/RSP0/CPU0:router#show cef drop location 0/0/CPU0
CEF Drop Statistics
Node: 0/0/CPU0
Unresolved drops packets : 0
Unsupported drops packets : 0
Null0 drops packets : 10
No route drops packets : 17
No Adjacency drops packets : 0
Checksum error drops packets : 0
RPF drops            packets :           48505   <=====
RPF suppressed drops packets : 0
RP destined drops packets : 0
```

```
Discard drops packets : 37
GRE lookup drops packets : 0
GRE processing drops packets : 0
LISP punt drops packets : 0
LISP encap err drops packets : 0
LISP decap err drops packets :
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- УДАЛЕННО ИНИЦИИРОВАННАЯ ФИЛЬТРАЦИЯ ЧЕРНОЙ ДЫРЫ - НАЗНАЧЕНИЕ БАЗИРОВАЛОСЬ И ОСНОВАННЫЙ ИСТОЧНИК
- Cisco Systems – техническая поддержка и документация