ASR9000 RPL Next-hop Discard 컨피그레이션을 사용한 소스 기반 원격으로 트리거된 블랙홀 필터링 예시

목차

소개

이 문서에서는 ASR(Aggregation Services Router) 9000에서 RTBH(Remotely Triggered Blackhole)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 이 정보는 Cisco IOS-XR® 및 ASR 9000을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

공격의 출처를 알고 있는 경우(예: NetFlow 데이터 분석), ACL(Access Control List)과 같은 억제 메커니즘을 적용할 수 있습니다. 공격 트래픽이 탐지되고 분류되면 적절한 ACL을 생성하여 필요한 라우터에 구축할 수 있습니다. 이 수동 프로세스는 시간이 많이 소요되고 복잡할 수 있으므로 많은 사용자가 BGP(Border Gateway Protocol)를 사용하여 삭제 정보를 모든 라우터에 빠르고 효율적으로 전파합니다. 이 기술인 RTBH는 피해자 IP 주소의 다음 홉을 널 인터페이스로 설정합니다. 피해자로 향하는 트래픽은 네트워크 인그레스(ingress)에서 삭제됩니다.

또 다른 옵션은 특정 소스에서 트래픽을 삭제하는 것입니다. 이 메서드는 이전에 설명한 삭제와 비슷하지만 uRPF(Unicast Reverse Path Forwarding)의 이전 구축에 의존합니다. uRPF의 소스는 null0에 대한 경로를 포함하는 "invalid"인 경우 패킷을 삭제합니다. 대상 기반 삭제와 동일한 메커니즘으로 BGP 업데이트가 전송되며 이 업데이트는 소스에 대한 다음 홉을 null0으로 설정합니다. 이제 uRPF가 활성화된 인터페이스에 들어오는 모든 트래픽은 해당 소스의 트래픽을 삭제합니다.

ASR9000의 소스 기반 RTBH 필터링

ASR9000에서 uRPF 기능이 활성화된 경우 라우터는 null0에 대한 재귀 조회를 수행할 수 없습니다. 즉, Cisco IOS에서 사용하는 소스 기반 RTBH 필터링 컨피그레이션은 Cisco IOS-XR에서 ASR9000에서 직접 사용할 수 없습니다. 대안으로 RPL(Routing Policy Language) **set next-hop discard** 옵션(Cisco IOS XR 버전 4.3.0에 도입됨)이 사용됩니다.

구성

트리거 라우터의 컨피그레이션

특수 태그로 표시된 고정 경로에서 커뮤니티를 설정하고 BGP에 적용하는 고정 경로 재배포 정책을 구성합니다.

```
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
```

블랙홀드해야 하는 소스 접두사에 대한 특수 태그로 고정 경로를 구성합니다.

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

보더 라우터의 컨피그레이션

트리거 라우터의 커뮤니티 집합과 일치하는 경로 정책을 구성하고 **set next-hop discard를 구성합니다**.

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

iBGP 피어에 경로 정책을 적용합니다.

```
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
```

경계 인터페이스에서 uRPF 느슨한 모드를 구성합니다.

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

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

참고: 이 uRPF 컨피그레이션은 이 인터페이스의 모든 트래픽에 적용됩니다.

다음을 확인합니다.

보더 라우터에서 접두사 **10.7.7.7/32**는 **Nexthop-discard**로 **플래그됩니다**.

```
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.
```

인그레스 라인 카드에서 RPF 드롭이 발생하는지 확인할 수 있습니다.

```
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 :
```

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 원격으로 트리거되는 블랙홀 필터링 - 대상 기반 및 소스 기반
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.