ASR9000基於源的遠端觸發的使用RPL下一跳丟棄的黑洞過濾配置示例

目錄

簡介

本檔案介紹如何在聚合服務路由器(ASR)9000上設定遠端觸發封鎖線(RTBH)。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco IOS-XR®和ASR 9000。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

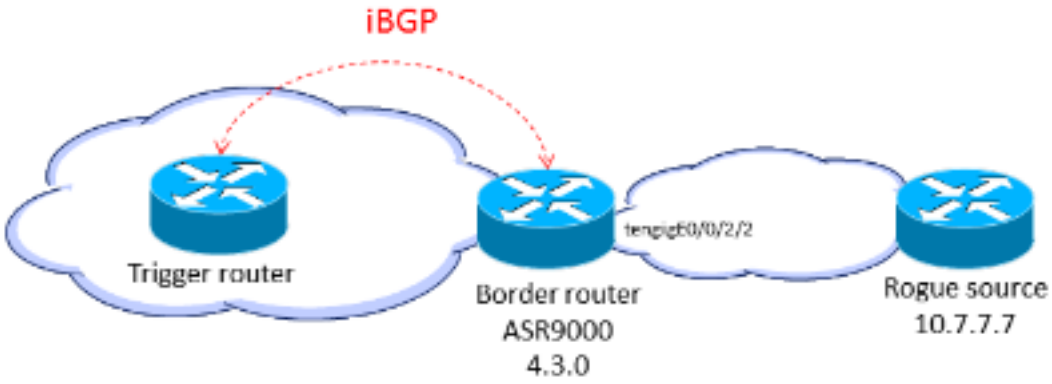
背景資訊

當您知道攻擊的來源（例如，通過分析NetFlow資料）時，可以應用包含機制，例如訪問控制清單(ACL)。當檢測到攻擊流量並將其分類時，您可以建立相應的ACL並將其部署到所需的路由器。由於此手動過程可能既耗時又複雜，因此許多人使用邊界閘道通訊協定(BGP)來迅速和有效地將捨棄資訊傳播到所有路由器。此技術RTBH將受害者IP地址的下一跳設定為空介面。目的地為受害者的流量會在輸入到網路時捨棄。

另一種方法是捨棄來自特定來源的流量。此方法與前面介紹的捨棄類似，但依賴於單播反向路徑轉送(uRPF)的先前部署，如果封包的來源「無效」（包括到null0的路由），此部署將捨棄封包。使用與基於目標的丟棄相同的機制，將傳送BGP更新，並且此更新將源的下一跳設定為null0。現在，所有進入已啟用uRPF的介面的流量都會丟棄來自該源的流量。

ASR9000上基於源的RTBH過濾

在ASR9000上啟用uRPF功能時，路由器無法對null0執行遞迴查詢。這意味著Cisco IOS使用的基於源的RTBH過濾配置不能直接由ASR9000上的Cisco IOS-XR使用。或者，會使用路由原則語言(RPL)**set next-hop discard**選項（在Cisco IOS XR 4.3.0版中介紹）。



設定

觸發路由器上的配置

配置靜態路由重分發策略，該策略在標籤了特殊標籤的靜態路由上設定一個社群，並將其應用到BGP中：

```
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
```
使用需要黑洞的源字首的特殊標籤配置靜態路由：

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

邊界路由器上的配置

配置與觸發路由器上的團體集匹配的路由策略，並配置set next-hop discard:

```
route-policy RTBH
if community matches-any (1234:4321) then
set next-hop discard
else
pass
endif
end-policy
```
在iBGP對等體上應用路由策略：

```
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
```
在邊界介面上配置uRPF鬆動模式：

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

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

注意：此uRPF配置適用於此介面上的所有流量。

驗證

在邊界路由器上，字首10.7.7.7/32標籤為Nexthop-discard:

```
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.
```

您可以在輸入線路卡上驗證是否發生RPF丟棄：

```
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 :
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 遠端觸發的黑洞過濾 — 基於目的地和基於源
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。