ASR9000 Blackhole à distance déclenché basé sur source filtrant avec l'exemple de configuration d'écart de Prochain-saut RPL

Contenu

Introduction

Ce document décrit comment configurer Blackhole à distance déclenché (RTBH) sur le routeur de services d'agrégation (ASR) 9000.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ces informations dans ce document sont basées sur le ® et l'ASR 9000 de Cisco IOS XR.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Quand vous connaissez l'origine d'une attaque (par exemple, par une analyse des données de NetFlow), vous pouvez appliquer des mécanismes de retenue, tels que le Listes de contrôle d'accès (ACL). Quand le trafic d'attaque est détecté et classifié, vous pouvez créer et déployer ACLs approprié vers les Routeurs nécessaires. Puisque ce processus manuel peut être long et complexe, beaucoup de personnes emploient le Protocole BGP (Border Gateway Protocol) afin de propager les informations de baisse à tous les Routeurs rapidement et efficacement. Cette technique, RTBH, place le prochain saut de l'adresse IP de la victime à l'interface null. Le trafic destiné à la victime est abandonné sur le d'entrée dans le réseau.

Une autre option est de relâcher le trafic d'une source particulière. Cette méthode est semblable à la baisse décrite précédemment mais se fonde sur le déploiement précédent du Fonction Unicast Reverse Path Forwarding (uRPF), qui relâche un paquet si sa source est « non valide, » qui inclut des artères à null0. Avec le même mécanisme de la baisse destination destination, une mise à jour BGP est envoyée, et cette mise à jour place le prochain saut pour une source à null0. Maintenant tout le trafic qui écrit une interface avec l'uRPF a activé le trafic de baisses de cette source.

RTBH basé sur source filtrant sur l'ASR9000

Quand l'uRPF de caractéristique est activé sur l'ASR9000, le routeur ne peut pas faire la recherche récursive à null0. Ceci signifie que la configuration de filtrage basée sur source RTBH utilisée par Cisco IOS ne peut pas directement être utilisée par Cisco IOS XR sur l'ASR9000. Comme alternative, l'option d'**écart de set next-hop du** langage de stratégie de routage (RPL) (introduite dans la version 4.3.0 de Cisco IOS XR) est utilisée.

Configurez

Configuration sur le routeur de déclencheur

Configurez une stratégie statique de redistribution de routage qui place une communauté sur les artères statiques identifiées par une balise spéciale, et appliquez-la dans le 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
```

Configurez une artère statique avec la balise spéciale pour le préfixe de source qui doit noir-être troué :

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

Configuration sur le routeur de cadre

Configurez une stratégie d'artère qui apparie le positionnement de la communauté sur le routeur de déclencheur et configurez l'**écart de set next-hop** :

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

Appliquez la stratégie d'artère sur les pairs d'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
```

Sur les interfaces de cadre, configurez le mode lâche d'uRPF :

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

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

> Remarque: Cette configuration d'uRPF s'applique à tout le trafic sur cette interface.

Vérifiez

Sur le routeur de cadre, le préfixe 10.7.7.7/32 est signalé comme Nexthop-écart :

```
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.
```

Vous pouvez vérifier sur les cartes de ligne d'entrée que les baisses RPF se produisent :

```
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 :
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- FILTRAGE À DISTANCE DÉCLENCHÉ DE TROU NOIR - DESTINATION BASÉE ET SOURCE BASÉE
- Support et documentation techniques - Cisco Systems