Exemple de configuration du filtrage de trou noir déclenché à distance basé sur la source ASR9000 avec suppression du tronçon suivant RPL

Table des matières

Introduction

Ce document décrit comment configurer le RTBH (Remote Triggered Blackhole) sur le routeur ASR (Aggregation Services Router) 9000.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco IOS-XR® et ASR 9000.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Informations générales

Lorsque vous connaissez l'origine d'une attaque (par exemple, par une analyse des données NetFlow), vous pouvez appliquer des mécanismes de confinement, tels que des listes de contrôle d'accès (ACL). Lorsque le trafic d'attaque est détecté et classifié, vous pouvez créer et déployer les listes de contrôle d'accès appropriées sur les routeurs nécessaires. Étant donné que ce processus manuel peut être long et complexe, de nombreuses personnes utilisent le protocole BGP (Border Gateway Protocol) afin de propager rapidement et efficacement les informations d'abandon à tous les routeurs. Cette technique, RTBH, définit le tronçon suivant de l'adresse IP de la victime sur l'interface Null. Le trafic destiné à la victime est abandonné en entrée dans le réseau.

Une autre option consiste à supprimer le trafic d'une source particulière. Cette méthode est similaire à la suppression décrite précédemment, mais s'appuie sur le déploiement précédent de Unicast Reverse Path Forwarding (uRPF), qui supprime un paquet si sa source est « invalide », ce qui inclut les routes vers null0. Avec le même mécanisme de la suppression basée sur la destination, une mise à jour BGP est envoyée, et cette mise à jour définit le saut suivant pour une source sur null0. Maintenant, tout le trafic qui entre dans une interface avec uRPF activé abandonne le trafic de cette source.

Filtrage RTBH basé sur la source sur l'ASR9000

Lorsque la fonctionnalité uRPF est activée sur l'ASR9000, le routeur ne peut pas effectuer de recherche récursive sur null0. Cela signifie que la configuration de filtrage RTBH basée sur la source utilisée par Cisco IOS ne peut pas être utilisée directement par Cisco IOS-XR sur l'ASR9000. L'option RPL (Routing Policy Language) **set next-hop discard** (introduite dans Cisco IOS XR version 4.3.0) est utilisée comme alternative.

Configurer

Configuration sur le routeur déclencheur

Configurez une stratégie de redistribution de route statique qui définit une communauté sur les

routes statiques marquées d'une balise spéciale, et appliquez-la dans 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 route statique avec la balise spéciale pour le préfixe source qui doit être marqué d'un trou noir :

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

Configuration sur le routeur périphérique

Configurez une stratégie de route qui correspond à l'ensemble de communauté sur le routeur déclencheur et configurez **set next-hop discard** :

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

Appliquez la politique de routage sur les homologues 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 périphériques, configurez le mode lâche 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 uRPF s'applique à tout le trafic sur cette interface.

Vérifier

Sur le routeur périphérique, le préfixe **10.7.7.7/32** est marqué comme **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.
```

Vous pouvez vérifier sur les cartes de ligne d'entrée que des abandons 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 :
```

Dépannage

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

Informations connexes

- FILTRAGE DES TROUS NOIRS DÉCLENCHÉ À DISTANCE - BASÉ SUR LA DESTINATION ET SUR LA SOURCE
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.