ASR9000: Source-basierte, remote ausgelöste Blackhole-Filterung mit RPL Next-Hop Discard - Konfigurationsbeispiel

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration eines remote ausgelösten Blackholes (RTBH) auf dem Aggregation Services Router (ASR) 9000 beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Diese Informationen in diesem Dokument basieren auf Cisco IOS-XR® und ASR 9000.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Wenn Sie den Ursprung eines Angriffs kennen (z. B. durch eine Analyse von NetFlow-Daten), können Sie Eindämmungsmechanismen wie Zugriffskontrolllisten (Access Control Lists, ACLs) anwenden. Wenn Angriffsverkehr erkannt und klassifiziert wird, können Sie entsprechende ACLs erstellen und auf den erforderlichen Routern bereitstellen. Da dieser manuelle Prozess zeitaufwendig und komplex sein kann, verwenden viele Benutzer das Border Gateway Protocol (BGP), um Verwerfungsinformationen schnell und effizient an alle Router weiterzugeben. Diese Technik, RTBH, setzt den nächsten Hop der IP-Adresse des Opfers auf die Null-Schnittstelle. Der an das Opfer gerichtete Datenverkehr wird beim Eintritt in das Netzwerk verworfen.

Eine weitere Option besteht darin, Datenverkehr von einer bestimmten Quelle zu verwerfen. Diese Methode ähnelt der zuvor beschriebenen Verwerfung, basiert jedoch auf der vorherigen Bereitstellung von Unicast Reverse Path Forwarding (uRPF), bei der ein Paket verworfen wird, wenn seine Quelle "ungültig" ist. Dies umfasst Routen zu null0. Mit dem gleichen Mechanismus des zielbasierten Löschens wird ein BGP-Update gesendet, und dieses Update setzt den nächsten Hop für eine Quelle auf null0. Nun verwirft der gesamte Datenverkehr, der an eine Schnittstelle mit aktivierter uRPF gelangt, den Datenverkehr von dieser Quelle.

Quellbasierte RTBH-Filterung auf dem ASR9000

Wenn die Funktion uRPF auf dem ASR9000 aktiviert ist, kann der Router keine rekursive Suche nach null0 durchführen. Das bedeutet, dass die von Cisco IOS verwendete quellenbasierte RTBH-Filterkonfiguration nicht direkt von Cisco IOS-XR auf dem ASR9000 verwendet werden kann. Alternativ wird die Option **Next-Hop Discard (Next-Hop Discard)** der Routing Policy Language (RPL) (eingeführt in Cisco IOS XR Version 4.3.0) verwendet.

Konfigurieren

Konfiguration auf dem Trigger-Router

Konfigurieren Sie eine Richtlinie für die Umverteilung statischer Routen, die eine Community für statische Routen mit einem speziellen Tag festlegt, und wenden Sie diese im BGP an:

```
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
```

Konfigurieren Sie eine statische Route mit dem speziellen Tag für das Quell-Präfix, das schwarz gehalten werden muss:

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

Konfiguration auf dem Border Router

Konfigurieren Sie eine Routenrichtlinie, die mit dem Community-Set auf dem Trigger-Router übereinstimmt, und konfigurieren Sie **set next-hop discard**:

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

Wenden Sie die Routenrichtlinie auf die iBGP-Peers an:

```
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
```

Konfigurieren Sie an den Grenzschnittstellen den losen uRPF-Modus:

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

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

Hinweis: Diese uRPF-Konfiguration gilt für den gesamten Datenverkehr auf dieser Schnittstelle.

Überprüfung

Auf dem Border Router wird das Präfix **10.7.7.7/32** als **Nexthop-discard** markiert:

```
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.
```

Auf den Eingangs-Linecards können Sie überprüfen, ob RPF-Ausfälle auftreten:

```
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 :
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- FERNGESTEUERTE SCHWARZLOCHFILTERUNG - ZIEL- UND QUELLENBASIERT
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.