ASR9000 قائمة على المصدر يتم تشغيل تصفية BlackHole عن بعد باستخدام مثال تكوين RPL Next-hop discard

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين الثقب الأسود الذي يتم تشغيله عن بعد (RTBH) على موجه خدمات التجميع ((ASR 9000.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند هذه المعلومات الواردة في هذا المستند إلى Cisco® IOS-XR و ASR 9000.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

عندما تعرف أصل الهجوم (على سبيل المثال، من خلال تحليل بيانات NetFlow)، يمكنك تطبيق آليات الاحتواء، مثل قوائم التحكم في الوصول (ACL). عند اكتشاف حركة مرور الهجوم وتصنيفها، يمكنك إنشاء قوائم التحكم في الوصول (ACL) المناسبة ونشرها إلى الموجهات الضرورية. نظرا لأن هذه العملية اليدوية يمكن أن تكون مستهلكة للوقت ومعقدة، يستخدم العديد من الأشخاص بروتوكول العبارة الحدودية (BGP) من أجل نشر معلومات الإسقاط إلى جميع الموجهات بسرعة وكفاءة. يعمل هذا الأسلوب، rtbh، على تعيين الخطوة التالية من عنوان IP للضحية إلى الواجهة الخالية. يتم إسقاط حركة المرور الموجهة إلى الضحية على المدخل إلى الشبكة.

خيار آخر هو أن تسقط حركة المرور من مصدر معين. هذا الأسلوب مماثل للإفلات الموصوف سابقا ولكنه يعتمد على النشر السابق لإعادة توجيه المسار العكسي للبث الأحادي (uRPF)، والذي يسقط حزمة إذا كان مصدرها "غير صالح"، والذي يتضمن المسارات إلى0 فارغ. مع نفس آلية الإسقاط المستند إلى الوجهة، يتم إرسال تحديث BGP، ويعين هذا التحديث الخطوة التالية للمصدر إلى null0. تقوم جميع حركات المرور التي تدخل واجهة مع تمكين uRPF بإسقاط حركة المرور من ذلك المصدر.

تصفية RTBH المستندة إلى المصدر على ASR9000

عند تمكين ميزة uRPF على ASR9000، يتعذر على الموجه إجراء بحث متكرر ل null0. هذا يعني أنه لا يمكن إستخدام تكوين تصفية RTBH المستند إلى المصدر الذي يستخدمه Cisco IOS-XR مباشرة على ASR9000. كبديل، يتم إستخدام **خيار** تجاهل الخطوة التالية **لمجموعة** لغة سياسة التوجيه (RPL) (المقدمة في Cisco IOS XR الإصدار 4.3.0).

التكوين

التكوين على الموجه المشغل

قم بتكوين سياسة إعادة توزيع المسار الثابتة التي تعمل على تعيين مجتمع على المسارات الثابتة التي تحمل علامة خاصة، وطبقها في 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
```

قم بتكوين مسار ثابت باستخدام العلامة الخاصة لبادئة المصدر التي يلزم أن تكون سوداء اللون:

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

التكوين على موجه الحدود

قم بتكوين سياسة مسار تطابق مجموعة المجتمع على الموجه المشغل وتكوين **تعيين تجاهل الخطوة التالية**:

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

تطبيق سياسة المسار على نظائر 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
```

على الواجهات الحدودية، قم بتكوين الوضع غير المحكم uRPF:

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

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

ملاحظة: ينطبق تكوين إعادة توجيه المسار العكسي (uRPF) هذا على جميع حركات المرور على هذه الواجهة.

التحقق من الصحة

على موجه الحدود، يتم تمييز البادئة 32/10.7.7.7 باسم **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
(discarded) from 192.168.102.2 (10.210.0.2) 192.168.102.2
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
```

أنت يستطيع دققت على المدخل خط أن RPF يسقط يقع:

```
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
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- تصفية الثقب الأسود عن بعد - قائمة على الوجهة والمصدر
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).